



SINGLE BAND **FW-600**

USER GUIDE

FW6-B48-00-NA / FW6-B42-43-EU / FW6-B41-00-WW / FW6-B53-00-NA

April 2023



Revision History

DATE	RELEASE	ISSUE	REASON FOR ISSUE
Jan 2021	1.0		Initial Release
June 2021	2.0		Added Bulk IMSI uploads, removed 6 beams antenna and updates for SW 2.1.9
Aug 2021	2.1	210803	Updates for SW 2.1.12 features – 2CC + 1CC configuration and CSG. Also added note for PCI value changes in 2CC mode.
December 2021	3.0	211209	Updates for features up to 3.0.4 – QCI-QoS mapping, Whitelist, AAA server authentication and Core Connectivity status pages.
January 2022	3.0	220112	Updates for CBSD features in 3.0.5
April 2022	3.1	220420	Updates for SW 3.1.2 features (Secure Gateway, Separate S1 Traffic etc.) and removed information prior to SW 3.0.3.
July 2022	4.0	220714	Updates for SW 4.0.3 features – Mobility configuration/support. Removal of EEPC information.
August 2022	4.1	220805	Added Granted Power Alarm Trigger feature, information on CPI Signed Generator, history and alarm export feature as well as a note on MME pool.
January 2023	4.2	230116	Modified Tx Power/EIRP tables and configuration flowchart, added new features for CBSD registration, removed MCS modulation feature mention, added TR-069 features and updated eNB weights.
February 2023	4.3	230208	Updates done to provide further details about UEs supported, added 3CC and adjacent neighbor (mobility) config, and modified TNC and AISG porta support.
April 2023	4.4	230406	Addition of new model FW6-B53-00-NA.
May 2023	4.5	230529	Modifications to FW6-B53-00-NA Specifications, removal of “Confidential” and addition of ISED Statement.

Contact Us

BLiNQ Networks (CCARI)
 140 Renfrew Drive, Suite 200
 Markham, ON L3R 6B3

www.blinqnetworks.com

Sales

sales@blinqnetworks.com

Support

+1-800-301-4962
support@blinqnetworks.com



Table of Contents

- Revision History 2
- Table of Contents 3
- Tables 5
- 1. About This Guide 6
 - 1.1. Manual Conventions 7
- 2. FW-600 System Overview 8
 - 2.1. Technical Features 9
 - 2.2. Network Management Features 10
 - 2.2.1. Security Protocols 11
- 3. Technical Specifications 13
 - 3.1. System Parameters 13
 - 3.2. System Enclosure & Brackets 16
 - 3.3. FW-600 Brackets 16
 - 3.4. FW-600 Beams 18
- 4. Antenna Model and Specifications 19
 - 4.1. FW6-MBA3F-E3AB 20
 - 4.2. FW6-MBA3F-H3AA 21
- 5. Getting Started with the FW-600 22
 - 5.1. FW-600 Web User Interface (WebUI) 22
 - 5.1.1. Common Tools 24
 - 5.1.2. System Status Messages 25
- 6. WebUI Configuration 27
 - 6.1. System Configuration Process 27
 - 6.2. System 28
 - 6.2.1. Configuring a System Name 28
 - 6.2.2. System Synchronization 28
 - 6.2.3. Network Connectivity Parameters 30
 - 6.2.4. Advanced Options 30
 - 6.3. Carriers 36
 - 6.3.1. Antennas 36
 - 6.3.2. Cell Parameters 38
 - 6.3.3. Carriers Parameters 39
 - 6.3.4. Muting Carriers 42
 - 6.3.5. Advance Options 43
 - 6.4. LTE Baseline 44



- 6.4.1. Configuring LTE Baseline Parameters 45
- 6.4.2. eNB Identifiers 48
- 6.4.3. EPC Settings 49
- 6.4.4. Advanced Options 51
- 6.5. Mobility 55
 - 6.5.1. Neighbors 55
 - 6.5.2. Cell Reselection 59
 - 6.5.3. Handover 62
- 6.6. Embedded EPC 64
- 6.7. CBSD 64
 - 6.7.1. Configure SAS Server Connectivity 64
 - 6.7.2. Device Parameters 67
 - 6.7.3. Advanced Option 69
- 6.8. Management 74
 - 6.8.1. UI & Reporting 74
 - 6.8.2. Syslog 78
 - 6.8.3. KPI Reporting 79
 - 6.8.4. SNMP 80
- 6.9. Verify, Save & Activate Current Running Configuration 83
 - 6.9.1. Verify and Save Running Configuration 83
- 7. Operation and Maintenance 84
 - 7.1. Administration 84
 - 7.1.1. Software Manager 84
 - 7.1.2. SAS Cert Download 89
 - 7.1.3. IPSec Cert Download 90
 - 7.1.4. Configuration Manager 91
 - 7.2. Events 92
 - 7.2.1. Alarms Page 92
 - 7.2.2. History Page 93
 - 7.3. Performance 95
 - 7.3.1. eNB Statistics Page 95
 - 7.3.2. UE Stats Page 95
 - 7.3.3. Core Connectivity 97
 - 7.3.4. Network Status 98
 - 7.3.5. Mobility Status 100
 - 7.3.6. KPI Reports 101



7.4. Troubleshooting.....	103
7.4.1. Band Scan.....	103
7.4.2. iPerf.....	103
7.4.3. Network Diagnostics	105
7.4.4. Troubleshooting Guide.....	106
Appendix A BLiNQ Wireless Devices and RF Safety/Les appareils sans fil BLiNQ et la sécurité RF	108
Equipment Compliance	108
Appendix B PCI Planning Guidelines	111
Appendix C Commonly Used DSCP Values	113
Appendix D UEs Supported for Different Carrier Aggregation Modes.....	114
Appendix E Alarms and Events (Fault Management).....	115
Appendix F List of Acronyms	120

Tables

Table A FW6-B41-00-WW System Parameters	13
Table B FW6-B42-43-EU & FW6-B48-00-NA System Parameters.....	14
Table C FW6-B53-00-NA System Parameters.....	15
Table D FW6-MBA3F-E3AB Antenna Specifications	20
Table E FW6-MBA3F-H3AA Antenna Specifications	21
Table G Power Level Configurations Authorized for FW6-B48-00-NA.....	40
Table H Commonly Used DSCP Values.....	113
Table I Active UEs Supported per Sector/Beam per eNB.....	114
Table J List of Alarms	116
Table K List of Events	118

1. About This Guide

This manual contains informational and overview chapters, and then continues as a guide to the recommended order that you configure and then monitor your FW-600 system. **It covers features from SW Version 3.0.3 onwards.** If a certain feature is specific to a software version, it will be indicated in the respective sections.



NOTE: 2.0 SW Versions are not compatible with the FW-600 units. For information with regards to software versions prior to 3.0.3, please refer to *FW-600 User Guide_210803*.

The FW-600 models that are covered in this manual are:

- FW6-B41-00-WW
- FW6-B48-00-NA
- FW6-B42-43-EU
- FW6-B53-00-NA

As such, whenever “FW-600” is mentioned in the manual, it covers all the above models unless otherwise stated.



NOTE: The Dual Band FW-600 LAA system have a separate user guide. If your FW-600 unit has the model number FW6-B48-46-NA, please refer to the “*FW-600 LAA User Guide*” for configuration details instead.

There are two methods to configure the FW-600:

- FW-600 Web-based User Interface (WebUI) (recommended) or
- Command Line Interface (CLI)

This user manual contains step-by-step instructions for the FW-600 WebUI. For information about CLI configurations, please contact BLiNQ Customer Support.

The WebUI menu structure is the basis for the order of the chapters and the processes contained within those chapters:

- Initial system setup: See Chapter 5, “Getting Started with the FW-600”
- Configuration: See Chapter 6 for configuring the FW-600 system using WebUI.
- Operation and Maintenance: See Chapter 7, “Operation and Maintenance”
 - Software upgrade
 - Performance containing Evolved Node B (eNB) and Customer Premise Equipment (CPE) statistics plus trace log files and measurements
 - Events including alarms and past events (History)
 - Troubleshooting
- Management: See Chapter 6.8, “Management”
 - User operations (Local security)
 - Simple Network Management Protocol (SNMP)
 - Syslog server

1.1. Manual Conventions



This document uses the following conventions:

- **Bold** words indicate actual page names, fields or buttons within the software. It may also be words that need to be emphasized.

Examples:

- In the **LTE** (Long-Term Evolution) **Baseline Parameters** section, enter a value between 0-6 for the **Subframe Assignment** field. As a default, it has the value of 2.

LTE Baseline Parameters			
Subframe Assignment	<input type="text" value="2"/>	Special Subframe	<input type="text" value="7"/>
Baseline eNB ID	<input type="text" value="100"/>	PCI Seed Value	<input type="text" value="10"/>
Tracking Area Code	<input type="text" value="1"/>	Enable Mobility	<input type="radio" value="NO"/>

- **Compact All-Outdoor and Zero-Footprint Form Factor:** The FW-600 meets IP67 requirements for operation in tough environments with the capability to handle temperature variations from extreme cold to extreme heat.
- **Bold and Underlined items** indicate items that need additional attention.
- References to related documentation are shown in *italic* text.
- Commands typed at a console are shown in a **blue monospaced** font.
- The following icons are used to indicate the level of attention that are needed:
 -  This icon indicates crucial information. Failure to observe the information may result in installation failure or error.
 -  This icon indicates important information that needs to be observed.



2. FW-600 System Overview

The FW-600 is an ultra-high capacity, all integrated multicarrier LTE base station system designed as a response to today's broadband connectivity needs in rural and dense suburban markets.

It packs up to three 2x2 Multiple-Input Multiple-Output (MIMO) carrier radios in one compact form factor. The FW-600 is paired to passive beamforming antenna systems to bring spectral efficiency and capacity to new horizons.



FIGURE 2-1 THREE FW-600 UNITS ON A POLE

Key features:

- Stock Keeping Units (SKUs) supporting Band 41, 42, 43, 48 and 53
- Citizens Broadband Radio Service (CBRS) Category B Certified for FW6-B48-00-NA
- Supports multiple Time Division Duplexing (TDD) profiles, including TDD Configs 1-7 & 2-7
- Up to 96 User Equipment (UEs) per beam in 1 Component Carrier (CC) mode
- 32 UEs per beam for 2 CC mode



2.1. Technical Features

Some of the main technical product characteristics are as follows:

- **Compact All-Outdoor and Zero-Footprint Form Factor:** The FW-600 meets IP67 requirements for operation in tough environments with the capability to handle temperature variations from extreme cold to extreme heat. BLINQ's state-of-the-art and unique mounting design allows an unobtrusive deployment of multiple FW-600 systems on towers, poles, building sidewalls or rooftops with ease (See the "FW-600 Installation Guide" for more details).
- **For CBRS Band (for FW6-B48-00-NA):** The FW-600 implements a native Spectrum Access System client that fully enables easy Citizens Broadband Radio Service (CBRS) deployments. As a Category B Citizens Broadband Radio Service Device (CBSD), the FW-600 can operate on a Priority Access or General Authorized Access basis in the CBRS band consistent with Title 47 Crest Factor Reduction (CFR) Part 96.
- **Industry Standard TDD LTE-A Release 13 Radio Interface:** The FW-600 solution utilizes industry standard (TDD) LTE-A Release 13 radio capabilities. This allows for robust wireless performance, with extremely cost-effective deployments of CPEs.
- **Configuration:** The FW-600 supports all LTE TDD frame configurations but focuses on Configuration 1 and Configuration 2.
- **Carrier Aggregation:** The FW-600 supports carrier aggregation (CA) with up to two (2) Component Carriers (2CC), allowing for increased throughput to support high bandwidth deployments in both dense suburban and rural environments.
- **Multiple Input Multiple Output (MIMO):** The FW-600 system features standard 2x2 MIMO configurations in both downlink (DL) and uplink (UL) directions for each active beam.
- **Quality of Service (QoS):** The FW-600 system implements advanced features such Traffic Classification, Admission Control, Rate Shaping plus Active Scheduling and Queue Management in order to deliver the most optimal quality of service.

The FW-600 can be paired with different antenna types as to match coverage and/or capacity needs from the operator. This flexibility allows the FW-600 to support both large coverage models, as well as capacity driven models.

Here is the recommended antenna for the **FW6-B41-00-WW** (Band 41) units:

- **FW6-MBA3F-E3AB (3 Beam antenna) | 21.5 decibels relative to isotropic (dBi) | 12.8° Azimuth (Az) Beamwidth (BW) / Beam**
 This single band, six port multibeam array antenna contains three independent LTE optimized beams covering 1695-2690 MHz frequencies. The LTE Optimized Beams improve LTE data throughput by minimizing beam crossover, providing for an efficient use of valuable radio capacity and frequency spectrum.

Here is the recommended antenna for the **FW6-B48-00-NA** (Band 48) and **FW6-B42-43-EU** (Band 42/43) units:

- **FW6-MBA3F-H3AA (3 Beam antenna) | 22.3 dBi | 17.6° Az BW / Beam**
 This multi-beam antenna contains three independent LTE Optimized Beams with 2x2 MIMO capability. Pairing the FW-600 with the FW6-MBA3F-H3AA allows the operator to easily manage network growth and high through deliverables without compromising coverage.

2.2. Network Management Features

The FW-600 implements complete web-based user interface (WebUI) and Command Line Interface (CLI) functionality, plus strong Element Management System (EMS) implementation that suits any type of customer needs.

- **FW-600 Web Interface (WebUI)** — Accessible via HTTP(S), the WebUI provides an interactive visual toolset that allows you to modify the full configuration of the FW-600 system, as well as view state, fault and performance indicators. The WebUI displays performance data using visual charts and provides applications to visualize the performance data.
- **FW-600 Command Line Interface (CLI)** — Accessible via Secure Shell protocol (SSH), the CLI provides a well-structured command language in an industry standard idiom. The interface allows you (or third-party system) to manipulate the full configuration of the unit and examine state, performance and fault indicators.
- **TR-069** — Accessible via Auto Configuration Server (ACS), the TR-069 protocol allows a safe, remote management and configuration of the eNB.
- **Element Management System (EMS)** — The NetLiNQ EMS system, enables a state-of-the-art Operations, Administration, Maintenance and Provisioning (OAM&P) feature set. The OAM&P possesses a strong set of interfaces to connect to northbound provision systems.

Providing comprehensive Fault, Configuration, Accounting, Performance, and Security (FCAPS) functionality, the FW-600 system uses standard networking protocols and tools that facilitate a full range of element and network management operations—from local craft Internet Protocol (IP) address configuration to complex integration in Simple Network Management Protocol (SNMP) or script-based Element Management System (EMS) and Operations Support System (OSS) infrastructures.

- **Community-Based Simple Network Management Protocol version 2 (SNMPv2c)**— The SNMPv2c interface provide complete access to configuration, state, performance and fault information in the FW-600 system. This allows for high levels of integration in existing EMS/OSS infrastructure for monitoring, Service Level Agreement (SLA) assurance and administrative task automation.
- **Syslog** — The syslog interface allows the FW-600 system to send standard syslog fault management information (that is, syslog alarms, events, and log entries) to external syslog servers.

The FW-600 system provides the following IP addresses for management purposes:

- **Local Craft IP Address** — A fixed, non-routable IP address: *169.254.1.1* which is always accessible without Virtual Local Area Network (VLAN) encapsulation. This address is always present on eNodeB (eNB). You use this address in situations where the Management IP Address (see below) is not configured or is unavailable, including initial commissioning and field troubleshooting scenarios. Typically, a technician accesses the Local Craft IP Address by plugging directly into the RJ45 Ethernet port of the eNB.
- **WAN IPv4/IPv6 IP Address** — A user assigned, static or Dynamic Host Configuration Protocol (DHCP) IPv4/IPv6 address. The device uses this address to exchange traffic and control information with the network. The operator will also use this IPv4/IPv6 address to remotely manage the system. A user-configurable Virtual Local Area Network (VLAN) encapsulates all traffic to and from the Wide Area Network (WAN) interface.

The FW-600 system provides the following network management functions:

- **Configuration Management** — The system configuration covers several functional areas:
 - Radio Link Commissioning
Radio Link Commissioning parameters (for example, radio frequency, synchronization, TDD configuration) needs to be set before system deployment and are particular to the operator Radio Frequency (RF) network.

- **EPC Configuration**
The Evolved Packet Core (EPC) Configuration parameters configure the EPC interface (e.g. Public Land Mobility Network Identifier (PLMN-ID), Mobility Management Entity (MME) interface, Serving Gateway (SGW) interface).
- **Security Configuration**
Security Configuration parameters allow you to secure access or disable specific management interfaces (add local user accounts) and perform various unit administrative operations.
- **EMS Interfaces Configuration**
Element Management Systems (EMS) enables you to configure SNMP, Syslog, plus the automatic upload of Performance Management (PM) files.

All parameters in these areas are accessible via all the network management interfaces previously described.

- **Fault Management** — The FW-600 system provides fault management service via a comprehensive list of alarms and events. Some of the potential faults that the system detects and initiates alarms on include:
 - radio and Ethernet link failures
 - hardware module failures
 - synchronization faults
 - software module faults
- SNMP traps or Syslog relays all alarms and events to higher level managers. The system also allows you to access active alarm and event history information using either the CLI or WebUI.
- **Performance Management** — The FW-600 system maintains a comprehensive set of performance counters and indicators to facilitate:
 - performance monitoring
 - SLA monitoring
 - troubleshooting

The system provides a full set of Ethernet counters at the interface, module and service flow level, as well as radio quality indicators at the module level. The system makes all the counters available as instantaneous values (via SNMP, CLI or WebUI).

- **Administrative Operations** - The FW-600 system provides tools that allow you to perform all standard unit administration operations using the provided remote network management interfaces. The system supports remote software upgrade operations using either a pull paradigm (that is, the system modules retrieve the software package files from external file transfer protocol (FTP) servers or a push scheme using the WebUI (uploading a software package file to the system modules through the WebUI). The FW-600 system also supports remote configuration backups and backup restoration.

2.2.1. Security Protocols

The FW-600 system supports local security access regarding system configuration and maintenance. With this model, you can configure the username, password and access level for the user through the WebUI or CLI. The configuration is stored on the unit.

Other than local security access, user credentials can also be created and stored on external AAA (Authentication, Authorization and Accounting) servers. The FW-600 system supports Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) servers. Please refer to the respective server guides for more details.



2.2.1.1. Local Networking Protocols

Local security protocol is the default protocol for the FW-600 modules. This means that you set each username, password and access level on each module. Each module stores the configuration data in its configuration database.

To configure the local security with the WebUI, please see Section 6.8.1.1 “SSH/Web Users”.

2.2.1.2. External Servers

The eNB is also able to reach out to external AAA server and authenticate username and password. This provides scalability and flexibility for your organization when it comes to AAA implementation. RADIUS and TACACS+ servers are supported by the FW-600 system.

Two external AAA servers can be configured either with WebUI or CLI. Please see Section 6.8.1.1 for WebUI configuration details.

3. Technical Specifications

This chapter covers:

- System Parameters
- System Enclosure and
- FW-600 Single Band System Beams

3.1. System Parameters

Table A lists the FW6-B41-00-WW system parameters, Table B lists the FW6-B42-43-EU and FW6-B48-00-NA system parameters, and Table C lists the FW6-B53-00-NA system parameters.

TABLE A FW6-B41-00-WW SYSTEM PARAMETERS

Radio & MBA Specifications	
Frequency Band	2.49-2.69 GHz (LTE Band 41)
Transmit Power (Max.)	39 dBm/antenna port (+ 3 dBm MIMO)
Channel Bandwidths	10, 15, 20 MHz
RF Propagation	3x MIMO (2Tx x 2Rx)
LTE Compliance	3GPP Release 10 (SW upgrade to Release 13)
Performance & Attributes	
Connected/Active User Equipment (UE)	Up to 288 Provisioned UEs per Base Unit (3 Beams) <ul style="list-style-type: none"> ▪ 96 Provisioned UEs per Beam: <ul style="list-style-type: none"> ▪ 48 Active UEs per 1CC (CA is performed over the air)
Carrier Aggregation	<ul style="list-style-type: none"> ▪ Up to 3 Carriers per Base Unit ▪ Supports Contiguous and Non-Contiguous 2CC, 3CC.
Throughput DL TDD Config 2-7 (default)	<ul style="list-style-type: none"> ▪ 110 Mbps per carrier of 1CC ▪ 330 Mbps per base unit - 3 x 1 CC
Throughput UL TDD Config 2-7 (default)	<ul style="list-style-type: none"> ▪ 11 Mbps per carrier of 1CC ▪ 33 Mbps per base unit - 3 x 1 CC
Operating Mode	TD-LTE
Power Consumption	480 W maximum
Power	48 VDC
Connectivity	<ul style="list-style-type: none"> ▪ 1 x Copper 1000BaseT ▪ 1 x SFP ▪ 1 x PPS TNC Connector* ▪ 1 x AISG/RET Control Port* ▪ 6 x 2.2-5 RF Ports
Synchronization	Integral GPS antenna (GPS, GLONASS, BeiDou)
Embedded EPC	Software Option
Operations, Administration and Maintenance (OAM)	
Configuration	WebUI, CLI, TR-069 and EMS

EMS Integration	RESTCONF
OAM Protocols	RESTCONF, HTTPS, SSH, SNMPv2c and TR-069
MECHANICAL	
Dimensions (L x W x D)	19.4" x 12" x 8.4" (492 x 304 x 160 mm)
Survival Wind Speed	Up to 124 mph (200 km/hour)
Weight	43.2 lbs. (19.6 Kg)
Operational Temperature	-40°F to 140°F (-40°C to 60°C)

*Currently not supported.

TABLE B FW6-B42-43-EU & FW6-B48-00-NA SYSTEM PARAMETERS

Radio & MBA Specifications		
	FW6-B42-43-EU	FW6-B48-00-NA
Frequency Band	3.4 - 3.6 GHz (LTE Band 42/43)	3.55 - 3.7 GHz (LTE Band 48)
Transmit Power (Max.)	39 dBm/antenna port (+ 3 dBm MIMO)	33 dBm/antenna port (+ 3 dBm MIMO)
Channel Bandwidths	10, 20 MHz	
RF Propagation	3x MIMO (2Tx x 2Rx)	
LTE Compliance	3GPP Release 10 (SW upgrade to Release 13)	
Performance & Attributes		
	FW6-B42-43-EU	FW6-B48-00-NA
Connected/Active User Equipment (UE)	Up to 288 Provisioned UEs per Base Unit (3 Beams) <ul style="list-style-type: none"> ▪ 96 Provisioned UEs per Beam: <ul style="list-style-type: none"> ▪ 48 Active UEs for 1CC ▪ 32 Active UEs for 2CC and 3CC 	
Carrier Aggregation	<ul style="list-style-type: none"> ▪ Up to 3 Carriers per Base Unit ▪ Supports Contiguous and Non-Contiguous 2CC, 3CC. ▪ Covers Full CBRS Band (150 MHz) for FW6-B48-00-NA 	
Throughput DL TDD Config 2-7 (default)	<ul style="list-style-type: none"> ▪ 110 Mbps per carrier of 1CC ▪ 330 Mbps per base unit - 3 x 1 CC 	
Throughput UL TDD Config 2-7 (default)	<ul style="list-style-type: none"> ▪ 11 Mbps per carrier - 1CC ▪ 33 Mbps per base unit - 3 x 1 CC 	
Operating Mode	TD-LTE	
Power Consumption	480 W	180 W
Power	48 VDC	
Connectivity	<ul style="list-style-type: none"> ▪ 1 x Copper 1000BaseT ▪ 1 x SFP ▪ 1 x PPS TNC Connector* ▪ 1 x AISG/RET Control Port* ▪ 6 x 2.2-5 RF Ports 	
Synchronization	Integral GPS antenna (GPS, GLONASS, BeiDou)	
Embedded EPC	Software Option	

Operations, Administration and Maintenance (OAM)	
Configuration	WebUI, CLI, TR-069 and EMS
EMS Integration	RESTCONF
OAM Protocols	RESTCONF, HTTPS, SSH, SNMPv2c and TR-069
MECHANICAL	
Dimensions (L x W x D)	19.4" x 12" x 8.4" (492 x 304 x 160 mm)
Survival Wind Speed	Up to 124 mph (200 km/hour)
Weight	43.2 lbs. (19.6 Kg)
Operational Temperature	-40°F to 140°F (-40°C to 60°C)

*Currently not supported.

TABLE C FW6-B53-00-NA SYSTEM PARAMETERS

Radio & MBA Specifications	
Frequency Band	2483.5-2495 MHz (LTE Band 53)
Transmit Power (Max.)	18 dBm/antenna port (+21 dBm MIMO aggregate)
Channel Bandwidths	10 MHz
RF Propagation	3x MIMO (2Tx x 2Rx)
LTE Compliance	3GPP Release 10 (SW upgrade to Release 13)
Performance & Attributes	
Connected/Active User Equipment (UE)	Up to 288 Provisioned UEs per Base Unit (3 Beams) <ul style="list-style-type: none"> ▪ 96 Provisioned UEs per Beam: <ul style="list-style-type: none"> ▪ 48 Active UEs per 1CC
Throughput DL TDD Config 2-7 (default)	<ul style="list-style-type: none"> ▪ 110 Mbps per carrier of 1CC ▪ 330 Mbps per base unit - 3 x 1 CC
Throughput UL TDD Config 2-7 (default)	<ul style="list-style-type: none"> ▪ 11 Mbps per carrier - 1CC ▪ 33 Mbps per base unit - 3 x 1 CC
Operating Mode	TD-LTE
Power Consumption	100 W
Power	48 VDC
Connectivity	<ul style="list-style-type: none"> ▪ 1 x Copper 1000BaseT ▪ 1 x SFP ▪ 1 x PPS TNC Connector* ▪ 1 x AISG/RET Control Port* ▪ 6 x 2.2-5 RF Ports
Synchronization	Integral GPS antenna (GPS, GLONASS, BeiDou)
Embedded EPC	Software Option
Operations, Administration and Maintenance (OAM)	
Configuration	WebUI, CLI, TR-069 and EMS
EMS Integration	RESTCONF

OAM Protocols	RESTCONF, HTTPS, SSH, SNMPv2c and TR-069
MECHANICAL	
Dimensions (L x W x D)	19.4" x 12" x 8.4" (492 x 304 x 160 mm)
Survival Wind Speed	Up to 124 mph (200 km/hour)
Weight	37.0 lbs. (16.8 Kg)
Operational Temperature	-40°F to 140°F (-40°C to 60°C)

**Currently not supported.*

3.2. System Enclosure & Brackets

The mechanical enclosure for the FW-600 has a GPS antenna attached to it. There are eleven ports on the bottom of the FW-600:

- 1 x Power Port
- 1 x Ethernet Port for network connectivity
- 6 x 2.2-5 RF Ports
- 1 x Small Form-Factor Pluggable (SFP) Port
- 1 x Antenna Interface Standards Group/Remote Electrical Tilt (AISG/RET) Control Port*
- 1 x Threaded Neill-Concelman (TNC) Connector Port*

**Currently not supported.*

3.3. FW-600 Brackets

You have the option of using a single unit mount (FW6-BRK1-K) or the three units mount (FW6-BRK-K) to install your FW-600 eNB(s) based on your deployment.

The single unit mount is made with zinc-plated steel for durability and is designed to ensure that installation will be a breeze.



FIGURE 3-1 FW-600 SINGLE UNIT BRACKET MOUNT

If you need to deploy more than one FW-600 eNB on the same tower, you can consider using the 3 units bracket mount (FW6-BRK-K). Due to the unique bracket design, up to three FW-600 units can be installed on one single bracket. This bracket system boosts an ease of installation and simplifies the FW-600 replacement procedure. The figures below show a few examples of possible placements of the FW-600 units on the 3 units mounting bracket.



1 x FW-600 mounted in the middle position

2 x FW-600 mounted on the right side



3 x FW-600 on mounting bracket

FIGURE 3-2 FW-600 ENBs ON THE 3 UNITS BRACKET MOUNT

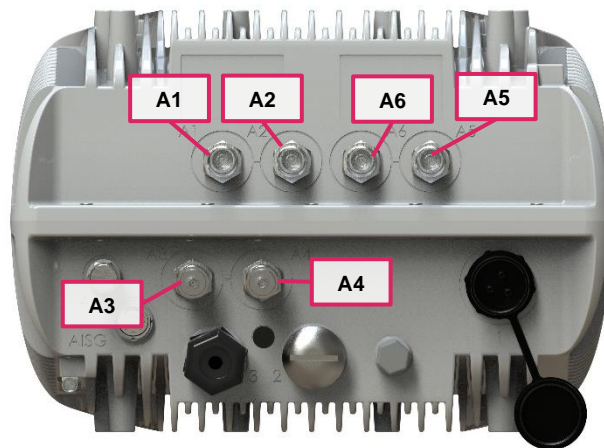
3.4. FW-600 Beams

The FW-600 has three beams – Beam 0, 1 and 2 (a software configuration).

As such, the RF connector ports at the bottom of the FW-600 unit have markings on them to facilitate the correct external antenna connection.

Please refer to the list below for the Connections:

BEAM 0	A1
	A2
BEAM 1	A3
	A4
BEAM 2	A5
	A6



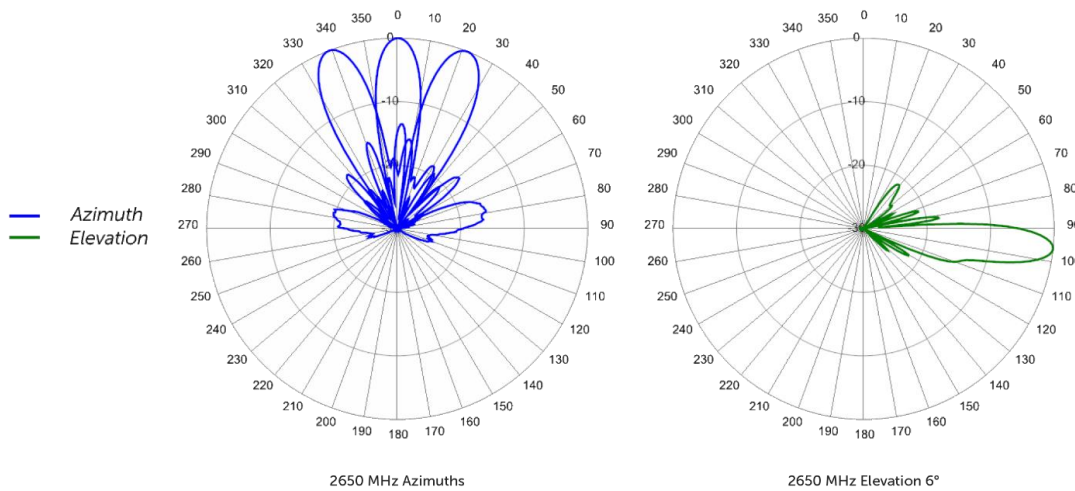
4. Antenna Model and Specifications

The FW-600 is designed to operate with external antennas. There are the 2 in house antennas that BLiNQ is currently recommending for the FW6-B41-00-WW and FW6-B48-00-NA/FW6-B42-43-EU eNBs.

For FW6-B53-00-NA eNBs, please speak with BLiNQ Support if you need a 3rd party recommendation.

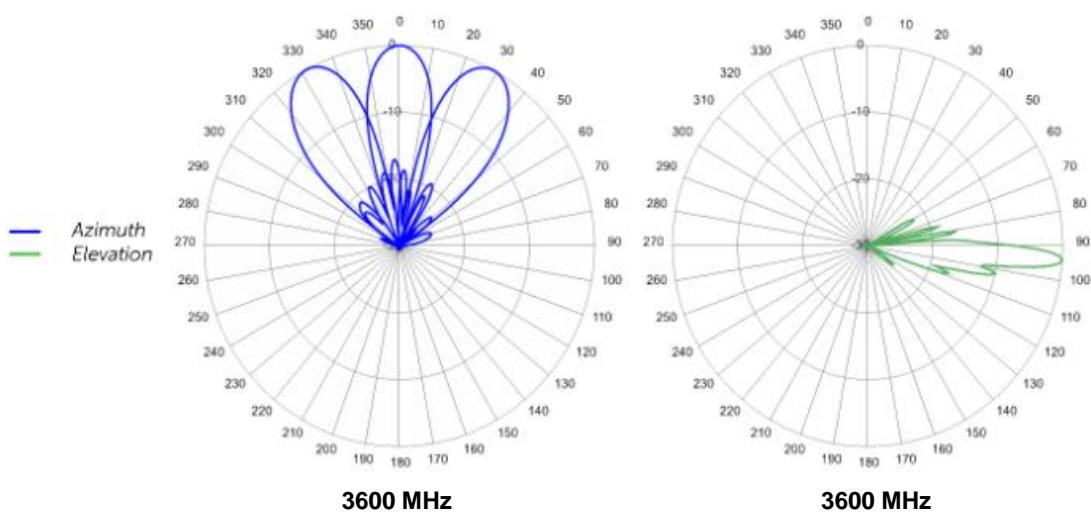
- **FW6-MBA3F-E3AB** - 3 Beam Antenna recommended for **FW6-B41-00-WW**

- 21.5 dBi
- 12 deg. Azimuth BW/Beam



- **FW6-MBA3F-H3AA** - 3 Beam Antenna recommended for **FW6-B42-43-EU** and **FW6-B48-00-NA**.

- 22.3 dBi
- 17.6 deg. Azimuth BW/Beam



4.1. FW6-MBA3F-E3AB

Table D shows the specifications for the FW6-MBA3F-E3AB 3 beam antenna.

TABLE D FW6-MBA3F-E3AB ANTENNA SPECIFICATIONS

Electrical	
Frequency Range	2.49 – 2.69 GHz
Gain	21.5 dBi
Azimuth Beamwidth (-3 dB)	12.8°
Azimuth Beam Crossover	11.0 dB
Elevation Beamwidth (-3 dB)	9.7°
Electrical Downtilt	6°
Elevation Sidelobes (1 st Upper) (Typ.)	< -16 dB
Front-to-back Ratio @180° (Typ.)	> 35 dB
Cross-Polar Discrimination (at Peak)	> 19 dB
Cross-Polar Port-to-Port Isolation	> 24 dB
Interbeam Co-Pol Isolation	> 15 dB
Interbeam Co-Pol Isolation (Non-Adjacent Beams) (Worse Case)	> 12 dB
Voltage Standing Wave Ratio (VSWR)	< 1.5:1
Passive Intermodulation (2x20W)	≤ -153 dBc
Input Power Continuous Wave (CW)	200 Watts
Polarization	Dual Pol 45°
Input Impedance	50 ohms
Lightning Protection	DC Ground
Mechanical	
Dimensions (L x W x D)	30.5" x 24.9" x 6.6" (776 x 633 x 167 mm)
Survival Wind Speed	Up to 150 mph (up to 241 km/hr)
Weight (not including mount)	41.6 lbs. (18.9 Kg)
Front Wind Load	162 lbs (722 N) @ 100 mph (161 kph)
Side Wind Load	46 lbs (206 N) @ 100 mph (161 kph)
Equivalent Flat Plate Area	6.3 ft ² (0.6 m ²)
Connector	6 x 7-16 DIN female long neck or 4.3-10 female
Mounting Pole	2"-5" (5 – 12 cm)

4.2. FW6-MBA3F-H3AA

Table E shows the specifications for the FW6-MBA3F-H3AA 3 beam antenna.

TABLE E FW6-MBA3F-H3AA ANTENNA SPECIFICATIONS

Electrical	
Frequency Range	3.40 - 3.80 GHz
Gain	22.3 dBi
Azimuth Beamwidth (-3 dB)	17.6°
Azimuth Beam Crossover	11.1°
Elevation Beamwidth (-3 dB)	5.4°
Electrical Downtilt	4°
Elevation Sidelobes (1st Upper)	< -22 dB
Front-to-back Ratio @180° (Typ.)	> 35 dB
Cross-Polar Discrimination	> 18 dB
Cross-Polar Port-to-Port Isolation	> 25 dB
Interbeam Co-Pol Isolation (Adjacent Beams)	> 25 dB
Interbeam Co-Pol Isolation (Non-Adjacent Beams) (Worse Case)	> 15 dB
Voltage Standing Wave Ratio (VSWR)	< 1.5:1
Passive Intermodulation (2x20W)	≤ -140 dBc
Input Power Continuous Wave (CW)	200 Watts
Polarization	Dual Pol 45°
Input Impedance	50 ohms
Lightning Protection	DC Ground
Mechanical	
Dimensions (L x W x D)	35.6" x 12.9" x 6.3" (904 x 328 x 160 mm)
Survival Wind Speed	> 150 mph (241 km/hr)
Weight (not including mount)	22.5 lbs. (10.2 Kg)
Front Wind Load	99 lbs (440 N) @ 100 mph (161 kph)
Side Wind Load	53 lbs (237 N) @ 100 mph (161 kph)
Equivalent Flat Plate Area	3.9 ft ² (0.4 m ²)
Connector	6 x 4.3-10 female
Mounting Pole	2"-5" (5 – 12 cm)

5. Getting Started with the FW-600

To initially log in to the FW-600:

- Connect your computer directly to the FW-600 through an Ethernet cable, and then check your connectivity by pinging the FW-600 using **169.254.1.1** (the Craft IP address that is always accessible).



NOTE: You need to statically set the IP address on the computer to **169.254.1.x** subnet before pinging.

After successfully pinging the Craft IP address, open a web browser and navigate to the pinged **169.254.1.1** to bring up the FW-600 WebUI.

To complete the initial system setup with the WebUI, follow the procedures under the desired chapter.



NOTE: If required, consult the “FW-600 Installation Guide” for instructions on powering or installing the unit.

5.1. FW-600 Web User Interface (WebUI)

LOGIN CREDENTIALS

When prompted for login credentials, enter the default username and password: **admin / admin**.

The screenshot shows the FW-600 WebUI dashboard for 'FW-600 B41'. Key features are annotated with red boxes and arrows:

- Dashboard Navigation Bar:** A vertical sidebar on the left containing menu items: Dashboard, Setup, Events, Performance, Troubleshoot, and Administration.
- Title Bar: Tool Area:** A horizontal bar at the top right containing the user greeting 'Welcome, admin', a power icon, a refresh icon, and a hamburger menu icon.
- Increase Width Button:** A small circular button with a plus sign located at the bottom of the navigation bar.
- System Information Bar:** A dark horizontal bar at the very bottom of the page containing copyright and model information.

The main content area displays a 'System Overview' table with the following data:

System Name	Joe 2 Cool eNB	Local Time	Jan 11, 2021 2:13:36 AM (UTC-05:00)
Device Model	FW-600 B48	Uptime	2 days 4 hr 14 min 50 sec
Device Code	FW06004141WWEA0000	WAN If IP Address	10.100.0.103
Serial Number	FE06-20080032	WAN If IPv6 Address	fe80::ea1:38ff:fe00:448
Software Version	2.1.4_1	WAN If MAC Address	0ca1:38:00:04:48
GPS	Local (Free Run)	S1-MME	Connected
Operational Status	Operational, 1 minor alarm active		
Licenses			

Below the system overview is an 'LTE Cells Status' table:

LTE Cell	Attached UEs	S1-MME	CBSD	eNBID	PCI	Carrier Frequency [MHz]	Carrier TX Power [dBm]	Active Secondary Cells
0	0	Connected	Authorized	14080	492	3625	-10	None
1 (Discovered)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Increase Width	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

The footer of the page contains the following text:

BLINQ Networks © 2021 Model: FW-300 B48 Serial Number: JOECO01000002 Board Identifier: BORED-00002 Version: 2.1.4_1 EEPC Version: 3.2.39

On initial log in to the FW-600 Web User Interface (WebUI), you see an overview of the FW-600 details; BLiNQ refers to this page as the **Dashboard**. The figure below identifies the various elements of the FW-600 WebUI.

The dashboard gives you the summary of your system. It shows you the **System Overview**, which includes the **System Name**, **Device Code**, **Serial Number**, **Software Version**, **Operational Status** just to name a few.

FW-600 B41 > Overview Dashboard

System Overview			
System Name	Joe 2 Cool eNB	Local Time	Jan 11, 2021 2:13:36 AM (UTC-05:00)
Device Model	FW-600 B48	Uptime	2 days 4 hr 14 min 50 sec
Device Code	FW06004141WWEA0000	WAN If IP Address	10.100.0.103
Serial Number	FE06-20080032	WAN If IPv6 Address	fe80::ea1:38ff:fe00:448
Software Version	2.1.4_1	WAN If MAC Address	0ca1:38:00:04:48
GPS	Local (Free Run)	S1-MME	Connected
Operational Status	Operational, 1 minor alarm active		
Licenses			

Please note that the serial number shown represents the serial number of your FW-600 Unit. It will come with the prefix of “F60X-YYWWNNNN”, where “YY” is the year, “WW” is the week and “NNNN” is the unit number produced in that particular year and week. “X” indicates the model of the FW-600:

- **F60A** – FW6-B48-00-NA
- **F60B** – FW6-B42-43-EU
- **F60C** – FW6-B41-00-WW
- **F60E** – FW6-B53-00-NA

There are two tabs at the bottom: **Alarms** and **LTE Cells Status**

- **Alarms:** Errors on your system will appear in this section, giving you the **Alarm ID**, **Alarm Time**, **Component**, **Severity**, **Type**, **Probable Cause** and **Description** of the error.

ID	Alarm ID	Module ID	Alarm Time	Component	Severity	Type	Probable Cause	Description
1	12001	0ca1:38:00:fb:47	Oct 29, 2021 11:09:31 AM (UTC-04:00)	CELL 3	Critical	Operational-status	Operating-mode	Sector 3 S1 State disabled
2	12001	0ca1:38:00:fb:47	Oct 29, 2021 11:09:31 AM (UTC-04:00)	CELL 4	Critical	Operational-status	Operating-mode	Sector 4 S1 State disabled

Showing 1 to 2 of 2 entries

First 1 Last

- **LTE Cells Status:** This is where you can monitor the LTE Cells’ operational parameters.

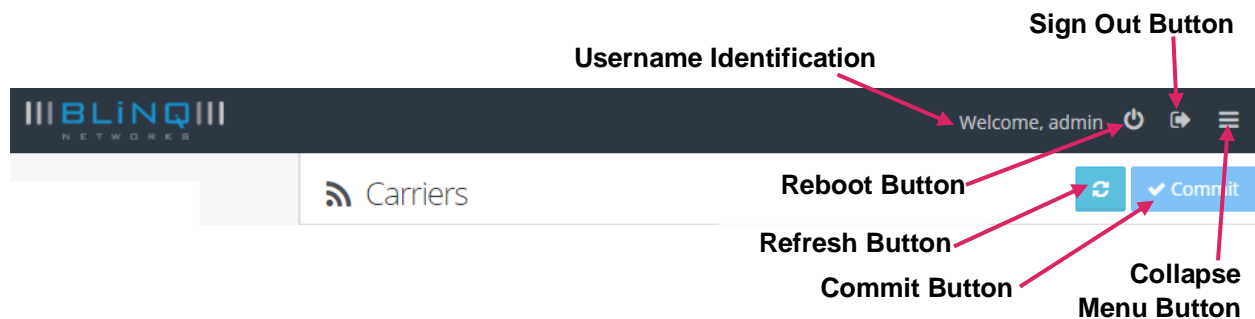
LTE Cell	Attached UEs	S1-MME	CBSID	eNBID	PCI	Carrier Frequency [MHz]	Carrier TX Power [dBm]	Active Secondary Cells
0	29	Connected	Not Configured	6912	82	3610	23	1
1	0	Connected	Not Configured	6913	81	3630	23	None
2	10	Connected	Not Configured	6914	83	3650	23	None

5.1.1. Common Tools

Following are some common features of the FW-600 WebUI.

5.1.1.1. Title Bar: Tool Area

Most WebUI pages have either a **Commit** button or a **Refresh** button or both in the top right-hand corner.



- **Commit** button: If you change any settings on a page, select **Commit** *before* navigating to another page to save your changes.
- **Refresh** button: Updates any read-only data on a page or returns any altered settings to their original values.
- **Reboot** button (🔄): Reboot the FW-600, at any time. It is available at the top of every page.

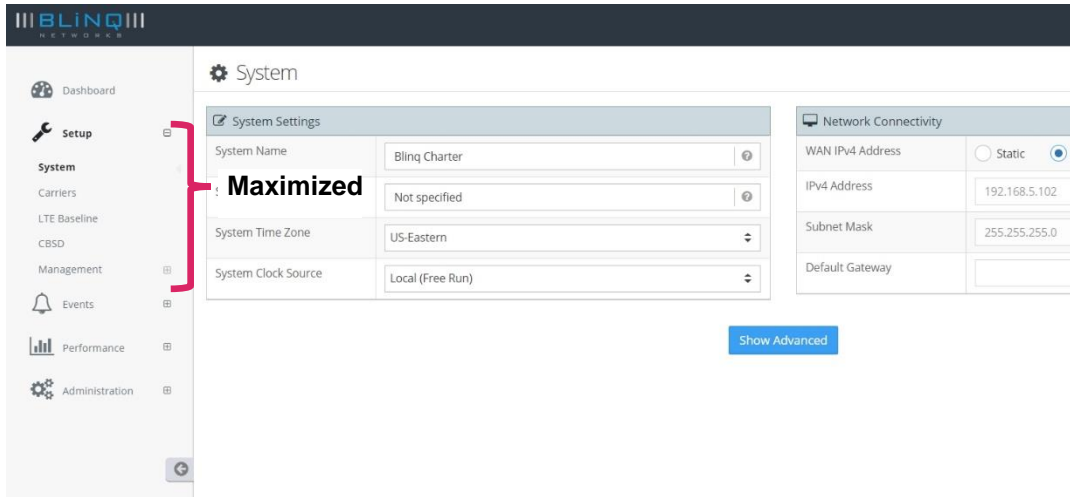


Note: Before a reboot, the FW-600 system performs a verification check between the running configuration and the start-up configuration to determine if there are any changes. This is to prevent the loss of any changes. If there is a change, the system prompts you to save your changes.

- **Sign Out** button: Ends each session.
- **Collapse Menu** button (☰): Minimizes the **Dashboard Navigation Bar** on the left side. You can still access the menu by positioning your cursor over the thin visible portion of the **Dashboard Navigation Bar**. Select the **Collapse Menu** button again to make the menu visible again.

5.1.1.2. Minimized and Maximized Menus

When a plus sign (+) is present beside a menu title, this indicates that you can minimize/maximize this area to reduce or see more options. To maximize an area, select the plus sign (+); the area expands so that all options are visible. To minimize, select the minus sign (-); the menu closes.



5.1.1.3. System Information Bar

The FW-600 system displays the model number, serial number, software version, EEPC version and current license (if applicable) status/number along the bottom of each main page. For example:



5.1.2. System Status Messages

The FW-600 WebUI outputs the following types of real-time messages to report on the interaction and/or change results between you and the FW-600 system:

Success Message (Green):

- A Success message in green advises, for example, of a successful data or configuration change.
- Success messages automatically disappear after about 4 seconds. You can dismiss them earlier by clicking on the message.



Warning Message (Yellow):

- A Warning message in yellow usually cautions of a validation error. For example, if there are problems with entered data, then a Warning message in yellow appears to explain the issue.
- You must click on a Warning message to dismiss it. They do not disappear automatically.





Error Message (Red):

- An Error message in red usually advises, for example, when the server is returning an error.
- Error messages signify syntactical issues (or a required field being left empty) with the settings you are trying to commit.
- You must click on an Error message to dismiss it. They do not disappear automatically.



6. WebUI Configuration

This chapter describes the tasks associated with preparing a FW-600 system to provide network services to its users using the WebUI.

The recommended FW-600 system commissioning process includes the following steps:

- Pre-Configuration in the Warehouse
- Field Installation (See the “FW-600 Installation Guide”)

The FW-600 system allows efficient installation processes by supporting full pre-configuration of equipment in the warehouse and a field installation process that does not require other installation tools other than the ones needed for the physical installation.

6.1. System Configuration Process

The FW-600 WebUI menu structure is the basis for the configuration process. This means that the configuration steps are set up so that you logically input all the related parameters on a page before you move to the next page/step in the configuration process. Please perform these steps in the order presented.

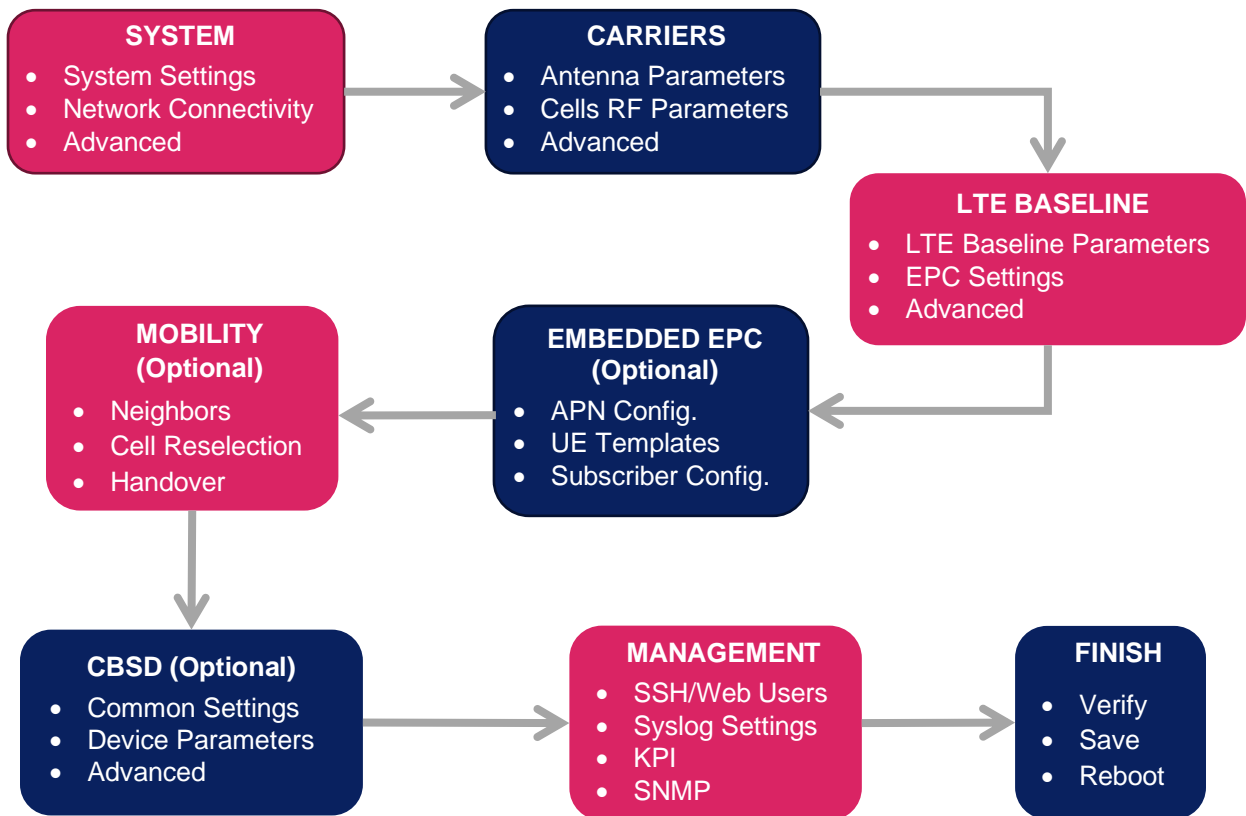


FIGURE 6-1 FW-600 CONFIGURATION PROCESS

6.2. System

On the WebUI (under “**Setup**”) **System** page you set a few parameters:

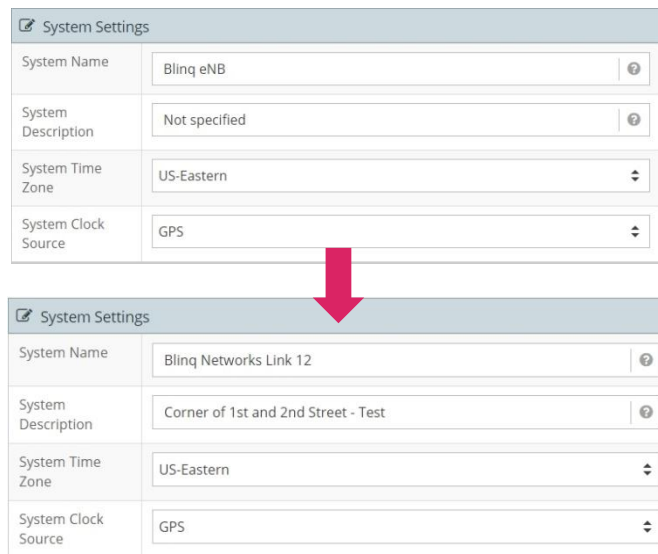
- System Name and Description
- System Time Zone and Clock Source
- Network Connectivity parameters
- Advanced (IPv6, Domain Name System (DNS), Network Time Protocol (NTP), VLAN)

6.2.1. Configuring a System Name

When pre-configuring the FW-600, it is highly recommended that you set a unique hostname to differentiate it from other devices.

- Navigate to the **Setup > System** page of the FW-600 WebUI.
- Under the **System Settings** area, assign a descriptive name to the module in the **System Name** field.

If desired, assign more identifying information via the **System Description** field. Use **System Time Zone** and **System Clock Source** to set your time zone and clock source.



System Settings	
System Name	Blinq eNB
System Description	Not specified
System Time Zone	US-Eastern
System Clock Source	GPS

System Settings	
System Name	Blinq Networks Link 12
System Description	Corner of 1st and 2nd Street - Test
System Time Zone	US-Eastern
System Clock Source	GPS

Select **Commit** in the top right corner to save the changes or select the **Refresh** (↺) button to cancel and return to the previous settings.

Repeat as needed for each device in your system.

Please note that most configuration changes are only applied after system reboot. To ensure that all your pre-configuration changes are saved to the start-up configuration file and to activate all your current configuration settings, see Section 6.9, “Verify, Save & Activate Current Running Configuration”.

6.2.2. System Synchronization

The FW-600 system is a Time Division Multiplexed (TDM) radio system. Therefore, FW-600 networks require proper synchronization of the air interface to provide optimal service. The FW-600 system provides flexible synchronization options as well as providing a high-performance extension to existing synchronization networks which delivers quality clock services to downstream devices such as small cells.

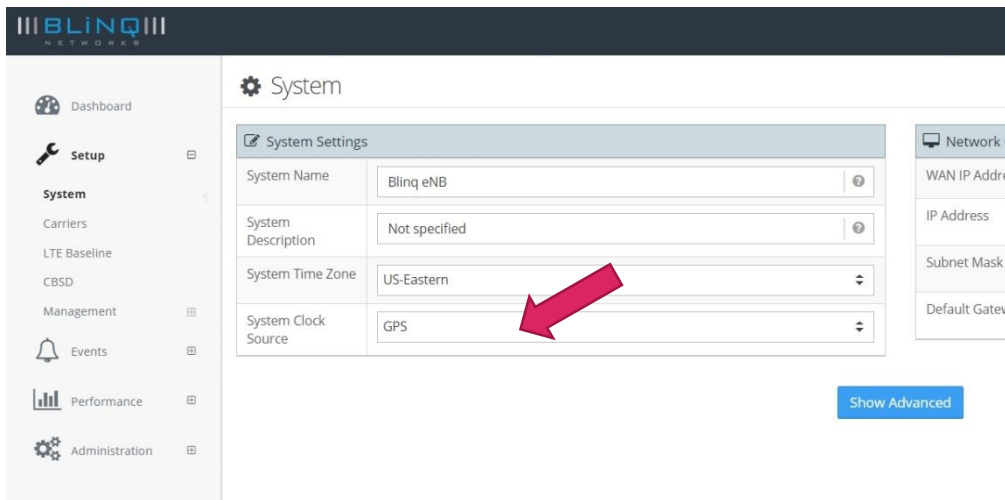
The eNodeB synchronizes using the Global Positioning System (GPS).

When configured to synchronize via GPS, the FW-600 system uses its internal GPS antenna and receiver module to synchronize to the GPS network. This allows all network deployed FW-600 eNodeBs to accurately synchronize their transmit and receive operations on the air interface. The GPS system also allows the FW-600 system to determine accurate time of day and date information. This time information, together with a user configured time zone setting, tells time across the system and is essential in functions such as fault management (for example, event and alarm time stamping) and historical performance (for example, performance indicator processing and performance file creation). If needed, there is also an optional external GPS source available.

The FW-600 system includes a high-performance crystal oscillator that allows it to maintain its clock properties (Holdover) even if the primary clock reference (that is, GPS) is no longer available. The system provides a Holdover period of 5 minutes. During this time the radio is operational, and the system attempts to recover its primary clock source. If the system does not reacquire the clock source after the Holdover period expires, the system is deemed **“Not synchronized”** and therefore ceases radio operation in order to not interfere with other deployed FW-600 systems.

On the WebUI, to set the system synchronization:


- Navigate the **Setup>System** page on the FW-600 WebUI.
- In the **System Settings** area, you set the system synchronization via the **System Clock Source** option. Select system clock course to **GPS**.



NOTES:

- Networks of FW-600 systems depend on proper synchronization through GPS clock references to operate in an optimal manner and may experience significant performance degradation or even outage if not deployed accordingly.
- The system allows you to use local clock as a clock source. This parameter is meant for lab testing only.
- A change in clock source requires a reboot!
When you change the system time, you need to commit to save the changes and then perform a FW-600 reboot in order for the change to take effect.

Before moving to a new page, select **Commit** in the top right corner to save your changes or select the **Refresh** button to cancel and return to the previous settings.

Reboot the system to activate all your saved changes, by selecting the **Reboot System** button  in the top right corner.

6.2.3. Network Connectivity Parameters

Once logged on to the FW-600, you can change the IP address of the WAN interface under **Network Connectivity**. There are two possible methods of assigning IP address to the system. You can choose either:

- **Static:** statically assign the IP address for the WAN interface. If set to **Static:** you must configure the IP address, subnet mask and default gateway, or
- **DHCP:** use the Dynamic Host Configuration Protocol (DHCP) to configure this IP address.



NOTE: To have DHCP properly assign an address to your FW-600 system, the system must have network access to a DHCP server on your local network. This DHCP server must have available addresses in its address pool, which are in the desired subnet you wish to assign to the system.

By default, the FW-600 WAN IPv4 address is assigned via DHCP.

To set the IPv4 address, please follow these steps:



- Navigate to the **Setup>System** page of the FW-600 WebUI.
- Under **Network Connectivity**, you find all the configurable options.

Network Connectivity	
WAN IPv4 Address	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv4 Address	<input type="text" value="192.168.5.102"/> ?
Subnet Mask	<input type="text" value="255.255.255.0"/> ?
Default Gateway	<input type="text" value="192.168.5.1"/> ?

- Ensure the **WAN IPv4 Address** option is set to **Static**.
- Enter an **IPv4 address**, **Subnet Mask** and optionally an address for the **Default Gateway** (local router) using the applicable fields.
- Select **Commit** in the top right corner to save your changes.



NOTES:

- At any time during configuration changes and before clicking the **Commit** button, use the **Refresh**  button to return to the previous settings and/or to update the information on the screen.
- The changes do not take effect until you reboot the system. Reboot the system by selecting the **Reboot System** button  in the top right corner.

6.2.4. Advanced Options

When you click on the **Show Advanced** button, more configurable fields (**IPv6, Advanced Network Connectivity and QCI-QoS Mapping**) will appear.

The screenshot displays the configuration interface for the FW-600. It is divided into several sections:

- System Settings:** Includes fields for System Name (Blinq eNB), System Description (eNB ID 777), System Time Zone (US-Eastern), and System Clock Source (Local (Free Run)).
- Network Connectivity:** Shows WAN IPv4 Address set to Static, with fields for IPv4 Address (10.100.0.47), Subnet Mask (255.255.255.0), and Default Gateway (10.100.0.250).
- IPv6:** Features a toggle for 'Enable IPv6' (set to YES), a 'WAN IPv6 Address' section with 'Static' selected, and fields for IPv6 Address (fc00:192:168:32::1), IPv6 Prefix Length (64), and Default Gateway (fc00:192:168:32::241).
- Advanced Network Connectivity:** Contains fields for DNS1 (192.168.37.42), DNS2 (8.8.8.8), NTP1 (192.168.5.1), and NTP2. The 'VLAN' section is currently set to OFF.
- QCI-QoS Mapping:** Includes a toggle for 'Enable QoS mapping' (set to NO).

A red circle highlights the 'Show Advanced' button, and a red arrow points from it to the 'Advanced Network Connectivity' section. A 'Reset Advanced' button is located at the bottom of the interface.

6.2.4.1. Setting up IPv6

- Toggle (**Yes** or **No**) to enable or disable IPv6 option.
- Ensure the **WAN IPv6 Address** option is set to **Static**. (**WAN IPv4 Address** needs to be set to **Static** for this section to be fillable.)
- Enter an **IPv6 address**, **IPv6 Prefix Length** and optionally an address for the **Default Gateway** (local router) using the applicable fields.
- Select **Commit** in the top right corner to save your changes.

IPv6	
Enable IPv6	<input checked="" type="radio"/> YES
WAN IPv6 Address	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv6 Address	<input type="text" value="fc00::a"/>
IPv6 Prefix Length	<input type="text" value="64"/>
Default Gateway	<input type="text"/>

IPv6	
Enable IPv6	<input checked="" type="radio"/> YES
WAN IPv6 Address	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IPv6 Address	<input type="text" value="2600:6ce6:4400:35::e"/>
IPv6 Prefix Length	<input type="text" value="64"/>
Default Gateway	<input type="text" value="2600:6ce6:4400:35::1"/>



NOTES: At any time during configuration changes in advanced mode and before clicking the **Commit** button, use the **Reset Advanced** button (at the bottom) to return to the previous/default settings.

6.2.4.2. Advanced Network Connectivity

This is where you can configure the **DNS1**, **DNS2**, **NTP1**, **NTP2** and **VLAN** settings.

- Enter your desired **DNS1**, **DNS2**, **NTP1**, **NTP2** and **VLAN** values into each of the applicable fields.
- Select **Commit** in the top right corner to save your changes.

Advanced Network Connectivity	
DNS1	<input type="text"/>
DNS2	<input type="text"/>
NTP1	192.168.5.1
NTP2	<input type="text"/>
VLAN	<input type="checkbox"/> OFF



Advanced Network Connectivity	
DNS1	8.8.8.8
DNS2	8.8.4.4
NTP1	192.168.6.15
NTP2	192.168.6.16
VLAN	<input checked="" type="checkbox"/> ON



NOTES:

- At any time during configuration changes and before clicking the **Commit** button, use the **Reset Advance** button to return to the previous settings and/or to update the information on the screen.
- All of these advanced parameters (DNS, NTP and VLAN) are optional settings and are not critical for the system to be working.

6.2.4.3. IPv4 and IPv6 Static Routes

IPv4 and IPv6 static routes can be added, edited or deleted in this section. This is a feature that is available for SW 3.1.2 onwards.

Please note that static routes are needed for the eNB to sent management and S1 traffic over different interfaces. For more information about separating S1 and management interfaces, please see Section 6.4.3.1.

IPv4 Static Routes			
Destination	Next Hop	Interface	Metric
<input type="button" value="+ Add Route"/> <input type="button" value="Delete Route"/>			

IPv6 Static Routes			
Destination	Next Hop	Interface	Metric
<input type="button" value="+ Add Route"/> <input type="button" value="Delete Route"/>			

To add a static route:

- Click on the blue “+ Add Route” button.
- A pop-up window will appear as follows:

Adding an IPv4 Static Route

Adding an IPv6 Static Route

- **Destination:** Specify the route’s destination address. This is a required parameter.
- **Next Hop:** Specify the next hop IP address. “**Next Hop**” is a routing term that refers to the next closest router a packet can go through. This is a required parameter.
- **Interface:** Select the desired interface (**S1** or **mgmt**) for this route.
- **Metric:** The weighted cost assigned to the route. Lower metrics take precedence over higher costs.
- When the parameters are entered in, click on “**+ Add Route**” to add the static route.
- The route should appear on the respective table

IPv4 Static Routes				
	Destination	Next Hop	Interface	Metric
<input type="checkbox"/>	10.110.0.0/24	10.113.0.250	s1	1
<input type="checkbox"/>	179.19.0.0/16	10.113.0.250	s1	1
<input type="checkbox"/>	182.11.1.0/24	10.113.0.250	s1	1
<input type="checkbox"/>	193.1.1.1/32	10.113.0.250	s1	1

IPv4 Static Routes Added

IPv6 Static Routes				
	Destination	Next Hop	Interface	Metric
<input type="checkbox"/>	fc00:110:1::/64	FD00:172::250	s1	1024
<input type="checkbox"/>	fc00:110:2::/64	FD00:172::250	s1	1024
<input type="checkbox"/>	fc00:110:3::/64	FD00:172::250	s1	1024
<input type="checkbox"/>	fc00:110:4::/64	FD00:172::250	s1	1024

IPv6 Static Routes Added

- Click on “**Commit**” to save the changes.



NOTE: “**Separate interface for S1 Traffic**” option needs to be selected and configured in **LTE Baseline > EPC Settings** for the “**S1**” option to be available in the drop-down menu on the **Interface** field. If not, **mgmt** will be the only option.

To delete a static route:

- Check the box beside the desired route and click on the red “**Delete Route**” button.

	Destination	Next Hop	Interface	Metric
<input checked="" type="checkbox"/>	10.110.0.0/24	10.113.0.250	s1	1
<input type="checkbox"/>	179.19.0.0/16	10.113.0.250	s1	1
<input type="checkbox"/>	182.11.1.0/24	10.113.0.250	s1	1
<input type="checkbox"/>	193.1.1.1/32	10.113.0.250	s1	1

6.2.4.4. QCI-QoS Mapping

Data sent from eNB to EPC is transported over backhaul network. The backhaul network may have limited capacity and be used for transport of other types of data. As a result, the data sent by the eNB may be dropped during congestion. This is a problem both for user plane traffic - as the wireless traffic already has higher probability of error than wireline traffic, and for control plane traffic - as losing these may affect all the connected users (e.g. S1 failure or CBSD Heartbeat drop).

With the **QCI-QoS Mapping** feature, DSCP (Differentiated Services Field Codepoints) values can be configured to be used for specific QCIs (QoS Class Identifier). This will help in prioritizing more important traffic.

The default mapping for all QCI values is DSCP 0 and the changes will be applied when the **Commit** button is clicked. An eNB reboot is not required for this change.

To Enable QoS Mapping:

- Toggle the button to **“YES”** and a list of **Traffic Type** and its corresponding **DSCP** value will appear.

Traffic Type	DSCP	Traffic Type	DSCP
QCI-1	CS0	QCI-9	CS0
QCI-2	CS0	QCI-10	CS0
QCI-3	CS0	QCI-11	CS0
QCI-4	CS0	QCI-12	CS0
QCI-5	CS0	QCI-13	CS0
QCI-6	CS0	QCI-14	CS0
QCI-7	CS0	QCI-15	CS0
QCI-8	CS0	GTP Management	CS0
S1-C Traffic	CS0	Device Management	CS0

- Configure the **DSCP** values by using the drop-down menu.
- Click on **“Commit”** to apply the changes.



NOTE: Please refer to Appendix D for the list of DSCP values.

6.3. Carriers

On the WebUI **Carriers** page you set the following parameters:

- Antenna Settings
- Carriers Baseline Parameter (such as Channel Bandwidth and Frequency Setting Mode)
- Cell 0-5 RF Parameters

6.3.1. Antennas

By default, navigating to **Setup > Carriers** will open the **Carriers** tab first. To set up the antenna for the FW-600, go to **Setup > Carriers** and click on the **Antennas** tab when the **Carriers** page opens up.

	Antenna Type	Antenna Name	Number of Beams	Beams	Beamwidth [°]		Antenna Gain [dBi]	Central Azimuth [°]	Downtilt [°]		FW-600 Ports			
					Horizontal	Vertical			Mechanical	Electrical	A1&2	A3&4	A5&6	
<input type="checkbox"/>	BLiNQ 3Beam	integrated	3	BL	18	5	22	0	0	0	x			
				B0	18	5	22			0	0		x	
				BR	18	5	22			0	0			x
<input type="checkbox"/>	3rd Party		3	B0	20	10	18	0	0	0				
				B1	20	10	18			0	0			
				B2	20	10	18			0	0			

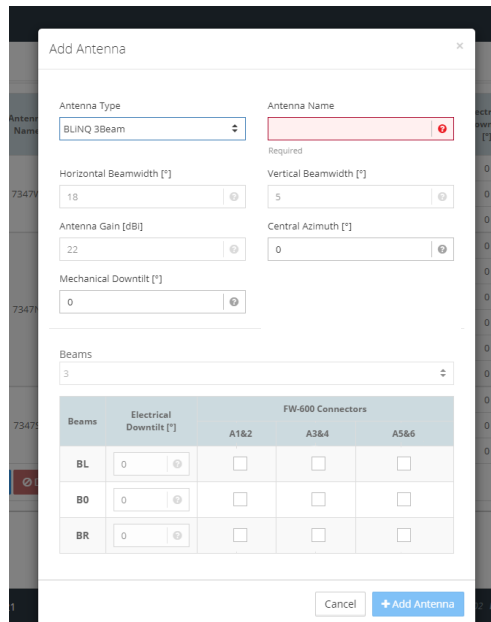
On the **Antennas** page, it will show the list of antennas that have been added with their settings defined.

6.3.1.1. Add an Antenna

To add a new antenna:

- Click on **+ Add Antenna**. A pop-up window will appear.

- Click on “**Antenna Type**” to reveal the drop-down menu. Select one of three antenna types: “**BLiNQ 3Beam**”, “**BLiNQ 6Beam**”, or “**3rd party**”.
 - For “**BLiNQ 3 Beam**” and “**BLiNQ 6 Beams**”, the system will automatically fill in the **Horizontal Beamwidth**, **Vertical Beamwidth** and the **Antenna Gain**. These three fields are greyed out and are not fillable.
 - If a “**3rd Party**” Antenna is selected, all the fields will need to be filled in with the appropriate information, including the number of beams.
- Enter a name for the Antenna.
- **Central Azimuth**: Central azimuth corresponds to overall antenna azimuth. Based on this parameter, the system will calculate azimuth for each beam. The assumption made here is that there is no spacing between beams. By default, azimuth is set at 0.
- **Mechanical Downtilt** applies to entire antenna. All the beams inherit this value. This value should match the physical antenna bracket’s downtilt, if any. The default is 0.
- **Beams Settings**:



- The system will then automatically open three sub-rows if a 3-beam antenna is selected or six sub-rows if a 6-beam antenna is selected. In the case of a 3rd party antenna, select the appropriate number of beams from the drop-down menu and the corresponding number of sub-rows will appear for configuration.
- Each beam corresponds to two RF **Connectors** on FW-600. Refer to Section 3.3 to see the FW-600 beams and connectors.
- Check off the appropriate boxes as per the connections done at installation (see the *FW-600 Installation Guide* for more information)
- While some ports can be left unconnected, checking the same **Connectors** for a different beam would not be allowed
- When all the parameters are entered, click on “**+ Add Antenna**”. The new antenna will be added on the Antennas page.



NOTES:

- It is the user’s responsibility to keep the FW-600 operating within the certified limits. See Table F for the maximum Effective Isotropic Radiated Power (EIRP) and Power allowed.
- The WebUI only allows up to three antennas on the list.** When the list has three antennas, a new antenna cannot be added. **One of the antennas will have to be deleted before adding a new antenna.** Please see Section 6.3.1.2 for information on deletion of antennas.

6.3.1.2. Deleting an Antenna

- To delete an antenna, navigate to **Setup > Carriers > Antennas**
- Click on the box beside the antenna that you wish to delete:

<input type="checkbox"/>	BLiNQ 6Beam	7347N	6	B26L	9	5	24	0	0
				B8L	9	5	24		
				B8R	9	5	24		
				B26R	9	5	24		
				B46R	9	5	24		
<input checked="" type="checkbox"/>	3rd Party	7347S	3	B0	60	12	17	0	0
				B1	60	12	17		
				B2	60	12	17		

+ Add Antenna Delete Antenna

- Click on “Delete Antenna” and the Antenna will be removed from the list.



Deletion of all antennas is not allowed. At least ONE antenna needs to remain on the list.

6.3.2. Cell Parameters

Navigate to **Setup > Carriers** to set up parameters that are common for all the cells:

- Channel Size:** Select the desired bandwidth via the **Channel Size (MHz)** drop-down menu.
 - 20 Megahertz (MHz) (default) and 10 MHz:** The system supports 10MHz and 20MHz bandwidth configuration for all single band, except the FW6-B53-00-NA units which only support 10MHz.
 - 15 MHz:** This option is only available for FW6-B41-00-WW units. However, please note that there is a limit of 32 CPEs per sector (for 1CC) for this bandwidth.
- Frequency Setting Mode** (EARFCN or Frequency)
 - Set the frequency mode for your carrier from the **Frequency Setting Mode** drop-down list. The options are: **EARFCN** (E-UTRA Absolute Radio Frequency Channel Number) or **Frequency**. The default is set to **Frequency**.

Antennas **Carriers**

Cell Parameters

Channel Size: 20 MHz

Frequency Setting Mode: Frequency



NOTE: If you select **EARFCN**, configure each **Cell x Carrier EARFCN** (where x is the desired cell number) to the EARFCN licensed for your operation.

- Click **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.

6.3.3. Carriers Parameters

This is where you can set the parameters that are unique for each cell:

Cell	Enable Cell	Sector Antenna	Carrier Frequency [MHz]	Carrier TX Power [dBm]	Mute Carrier
Cell 0	<input checked="" type="checkbox"/>	Blinq Antenna-BL	3610	23	<input type="checkbox"/>
Cell 1	<input checked="" type="checkbox"/>	Blinq Antenna-B0	3630	23	<input type="checkbox"/>
Cell 2	<input checked="" type="checkbox"/>	Blinq Antenna-BR	3650	23	<input type="checkbox"/>

Carrier Aggregation: Disabled

- Make sure that the box under “**Enable Cell**” is checked for each of the cell that you are configuring.
- Assign the **Sector Antenna** to each cell using the drop-down list. The list will be populated based on the information on the **Antennas** tab.
- Carrier Frequency:** Enter the desired frequency for each cell
- The EARFCN or RF Frequency parameter **must match between the FW-600 and the CPE(s)** to create a link.
- Mute Carrier:** Check the box to mute a single cell. Muting a cell takes effect immediately without having to reboot the eNB.
- Click **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.

6.3.3.1. Tx Power

The software recognizes different product codes and will adjust the TX Power (Transmit Power) limit accordingly. Please note that **FW6-B53-00-NA (Band 53)** units have a **max. TX Power of 18 dBm**.



Do NOT set the transmit power to above 23 dBm with RF connectors open or unterminated. It will cause a critical damage the hardware and would require an RMA/repair of the FW-600 unit.

You can transmit power per cell. Table F shows the power level configurations authorized by FCC for the **FW6-B48-00-NA**. Please refer to this table when configuring the Cell Parameters. It is the user’s responsibility to keep the power levels within the authorized range

TABLE F POWER LEVEL CONFIGURATIONS AUTHORIZED FOR FW6-B48-00-NA

FCC ID ROR00000008 – FW-600 FW6-B48-00-NA (CBRS) external antennas authorized for use																	
Ant. Ref#	Vendor	Antenna Model #	Ant. Gain (dBi)	Antenna Azimuth BW (deg)	Int / Ext Loss (dB)	Carrier BW (MHz)	FW-600 Cell No.	Maximum Configured Power / Antenna Port (dBm)			EIRP / Antenna Port* (dBm/10MHz)			EIRP / Antenna Port* (dBm/Bandwidth)			
Operation Mode								1CC	2CC	3CC	1CC	2CC	3CC	1CC	2CC	3CC	
1	CCI	MBA12F-HJ5A	24.5	10	1.5	10	0	24	NA	NA	47	NA	NA	47	NA	NA	
							1	24	24	24	47	47	47	47	47	47	
							2	24	NA	NA	47	NA	NA	47	NA	NA	
							20	0	27	NA	NA	47	NA	NA	50	NA	NA
								1	27	27	27	47	47	47	50	50	50
								2	27	NA	NA	47	NA	NA	50	NA	NA
2	CCI	MBA3F-H3A	22.4	18		10	0	26	NA	NA	46.9	NA	NA	46.9	NA	NA	
							1	26	26	26	46.9	46.9	46.9	46.9	46.9	46.9	
							2	26	NA	NA	46.9	NA	NA	46.9	NA	NA	
							20	0	29	NA	NA	46.9	NA	NA	49.9	NA	NA
								1	29	29	29	46.9	46.9	46.9	49.9	49.9	49.9
								2	29	NA	NA	46.9	NA	NA	49.9	NA	NA
3	MTI	MT036S18DS	18	45	10	0	30	NA	NA	46.5	NA	NA	46.5	NA	NA		
						1	30	30	29	46.5	46.5	45.5	46.5	46.5	45.5		
						2	30	NA	NA	46.5	NA	NA	46.5	NA	NA		
						20	0	30	NA	NA	43.5	NA	NA	46.5	NA	NA	
							1	33	30	29	46.5	43.5	42.5	49.5	46.5	45.5	
							2	30	NA	NA	43.5	NA	NA	46.5	NA	NA	
4	MTI	MT-404083/ND	17	90	10	0	30	NA	NA	45.5	NA	NA	45.5	NA	NA		
						1	30	30	29	45.5	45.5	44.5	45.5	45.5	44.5		
						2	30	NA	NA	45.5	NA	NA	45.5	NA	NA		
						20	0	30	NA	NA	42.5	NA	NA	45.5	NA	NA	
							1	33	30	29	45.5	42.5	41.5	48.5	45.5	44.5	
							2	30	NA	NA	42.5	NA	NA	45.5	NA	NA	

*Power per antenna connector for each CCI

6.3.3.2. Carrier Aggregation

FW-600 supports DL Carrier Aggregation of up to 3CC starting from SW 4.2.1. This means that for example, the FW-600 can use two 20 MHz channels to transmit towards a single CPE that also support carrier aggregation plus one other independent 20 MHz channel for a 2CC + 1CC configuration.



NOTE: FW6-B53-00-NA does not support carrier aggregation.

FW-600 supports the following DL Carrier Aggregation modes:

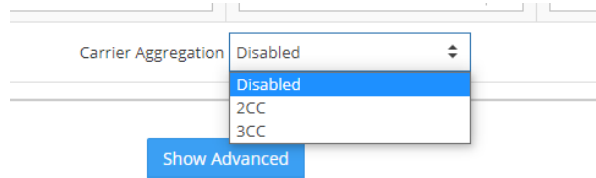
- 1CC
- 2CC
- 2CC + 1 CC
- 3CC



NOTES:

- Please note that 2CC and 3CC carrier aggregation can support up to 32 active UEs per beam. For more information about the number of active UEs supported, please refer to Appendix E.
- The FW6-B41-00-WW only supports carrier aggregation over the air. Please keep that in mind during network planning.

The drop-down list for **Carrier Aggregation** gives the options of “Disabled”, “2 CC” or “3 CC”.



To enable this function:

- Select option “2CC” or “3 CC” from **Carrier Aggregation** drop-down list.
- For **2CC** option:

Cell	Enable Cell	Sector Antenna	Carrier Frequency [MHz]	Carrier TX Power [dBm]	Mute Carrier
Cell 0 (2CC - Primary carrier)	<input checked="" type="checkbox"/>	integrated-B0	3610	23	<input type="checkbox"/>
Cell 1 (2CC - Secondary carrier)	<input checked="" type="checkbox"/>	integrated-B0	3630	23	<input type="checkbox"/>
Cell 2 (Independent carrier)	<input checked="" type="checkbox"/>	integrated-BR	3650	23	<input type="checkbox"/>
Carrier Aggregation			2CC		

- With this option selected, the system automatically selects **Cell 0** as **Primary Carrier** and **Cell 1** as **Secondary Carrier**. **Cell 2** will become the independent carrier.
- Configure the respective **Sector Antenna** and **Carrier Frequency**, keeping in mind that **Cell 0** and **Cell 1** **must use the same antenna**. Cell 2 on the other hand can use any of the remaining 2 antennas.

- In addition, **Cell 2** can be disabled by unchecking the box in the **Enable Cell** column if the independent carrier is not needed.

Cell	Enable Cell
Cell 0 (2CC - Primary carrier)	<input checked="" type="checkbox"/>
Cell 1 (2CC - Secondary carrier)	<input checked="" type="checkbox"/>
Cell 2	<input type="checkbox"/>

- For **3CC** Option:
 - Cell 0** will be set as **Primary Carrier**, **Cell 1** and **Cell 2** will be the **Secondary Carriers**.
 - Configure the respective **Sector Antenna** and **Carrier Frequency**, keeping in mind that all three cells must use the same antenna.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.



NOTES:

- For **FW6-B48-00-NA** and **FW6-B42-43-EU**, only antenna ports A3 and A4 supports 2CC/3CC operations. Therefore, please use the antenna connected to A3 and A4 ports for 2CC and 3CC configurations.
- FW6-B41-00-WW** supports over the air carrier aggregation. Thus, any of the sector antennas can be used for carrier aggregation operations as long as the Primary and Secondary cells are using the same antenna.
- An error message will appear if the Primary and Secondary cells are configured with different Sector Antennas when in 2CC or 3CC Carrier Aggregation modes.

6.3.4. Muting Carriers

Carriers/Cells can be muted individually as well as collectively at the same time.

To mute carriers/cells individually:

- Check the box for the desired cell(s) to be muted.

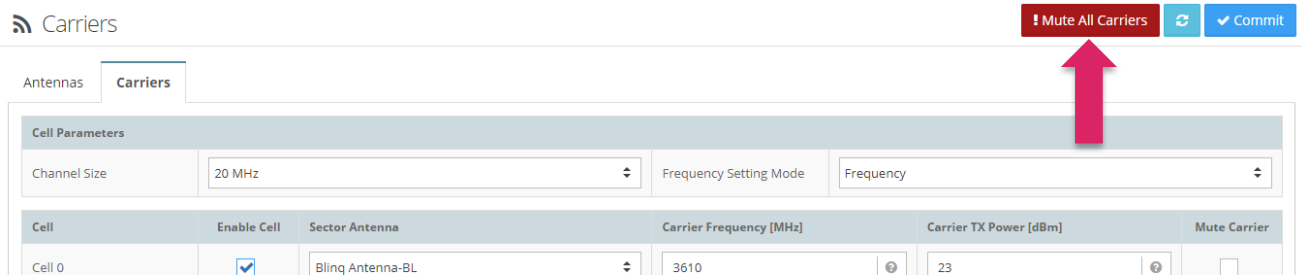
Cell	Enable Cell	Sector Antenna	Carrier Frequency [MHz]	Carrier TX Power [dBm]	Mute Carrier
Cell 0	<input checked="" type="checkbox"/>	Blinq Antenna-BL	3610	23	<input type="checkbox"/>
Cell 1	<input checked="" type="checkbox"/>	Blinq Antenna-B0	3630	23	<input type="checkbox"/>
Cell 2	<input checked="" type="checkbox"/>	Blinq Antenna-BR	3650	23	<input type="checkbox"/>

Carrier Aggregation Disabled

- The cell(s) will be muted immediately, without a reboot of the eNB. Please note that the carriers can still enabled.

To mute all the carriers/cells at the same time:

- Click on the red “!Mute All Carriers” button at the top right corner of the page.



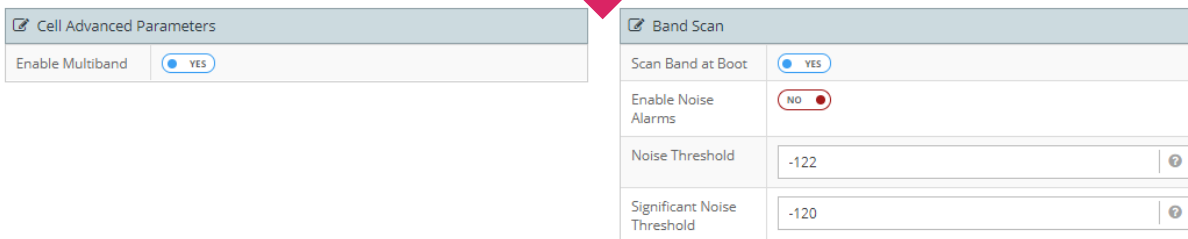
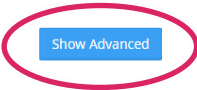
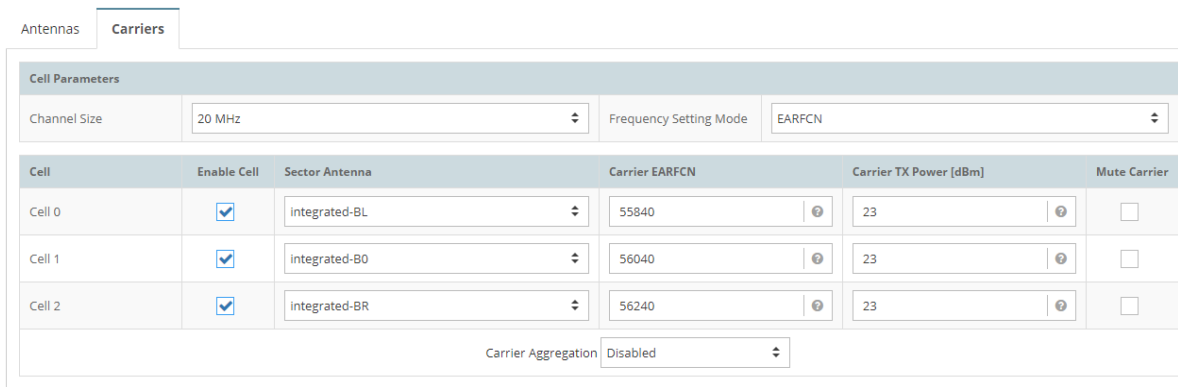
- All the carriers will be muted immediately, without rebooting the eNB. Please note that the carriers are still enabled.



NOTE: A simple analogy to help understand the difference between enabling a cell versus muting a cell is this: When you are listening to music and you mute it, the music is still running in the background, but you would not hear anything. On another hand, when you turn the music off (disable), it stops completely.

6.3.5. Advance Options

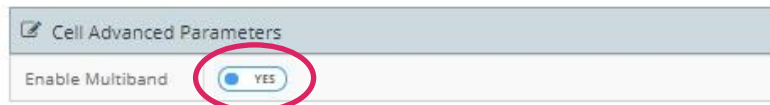
When you click “Show Advanced” button at the bottom of the page, you will reveal more configurable parameters – **Cell Advanced Parameters** (where the Multiband feature is revealed) and **Band Scan**.



6.3.5.1. Cell Advance Parameters

Band 48 overlaps with Band 42 and 43 (3550-3700MHz). The Multiband feature allows CPE that do not support Band 48 to connect to the FW-600 operating on Band 48. (ie. Backwards compatibility) To enable this feature, make sure that the “**Enable Multiband**” is turned to “**YES**”.

(Not applicable for Band 41, Band 46 or Band 53 products)

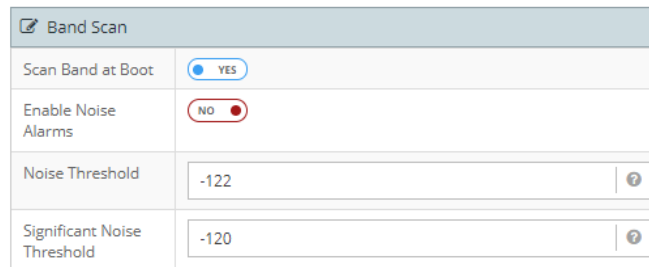


NOTE: CPE’s support for multiband feature (MFBI) is also required. Please consult your CPE manual to verify this. All BLiNQ CPEs support the multiband feature.

6.3.5.2. Band Scan

You can set the FW-600 to scan the frequency band automatically when it is booting up.

When this feature is on, the FW-600 will scan and register noise levels across the entire span of the band (150 MHz) in 5 MHz steps for all cells.



- Under **Carriers > Show Advanced > Band Scan**, click on the button to toggle between “**YES**” and “**NO**”. Select the option you desire.
- **Enable Noise Alarms** will raise alarms when the noise levels surpass the set thresholds.
- If you have selected “**YES**”, please set up the **Noise Threshold** and **Significant Noise Threshold** levels for the scan. The eNB will register anything from -130 dBm to 90 dBm.



NOTE: The noise thresholds can be set without rebooting the eNB. Simply click on “**Commit**” to apply the changes.

6.4. LTE Baseline

On the **LTE Baseline** page, you configure the following parameters for all modes of operation:

- The baseline parameters (such as eNB ID and Cell Range)
- EPC settings

LTE Baseline ↻ Commit

LTE Baseline Parameters				eNB Identifiers		
Subframe Assignment	<input type="text" value="2"/>	Special Subframe	<input type="text" value="7"/>	Cell	eNB ID	PCI
Baseline eNB ID	<input type="text" value="100"/>	PCI Seed Value	<input type="text" value="10"/>	Cell 0	25600	30
Tracking Area Code	<input type="text" value="1"/>	Enable Mobility	<input checked="" type="radio"/> NO	Cell 1	25601	31
				Cell 2	25602	32

EPC Settings			
PLMN Id	<input type="text" value="99999"/>		
EPC	<input checked="" type="radio"/> External <input type="radio"/> Embedded		
MME Name	MME0	MME Host	10.110.0.78
	MME1		10.110.0.76
<input type="checkbox"/> Separate interface for S1 traffic			
<input type="checkbox"/> Connect to EPC via Secure Gateway			

[Show Advanced](#)

6.4.1. Configuring LTE Baseline Parameters

In this section, you can assign values to **Subframe Assignment**, **Special Subframe**, **eNB ID**, **PCI Seed Value**, **Cell Range** and **Tracking Area Code**.

Based on **Baseline eNB ID** and **PCI Seed Value**, the system will calculate **eNB Identifiers** and **PCIs** for each of the cells and display these values in the **eNB Identifiers** table.

eNB Identifiers		
LTE Cell	eNB ID	PCI
LTE Cell 0	25600	30
LTE Cell 1	25601	31
LTE Cell 2	25602	32

6.4.1.1. Subframe Assignment and Special Subframe

The advantage of using TDD is that it is possible to change the up and downlink balance and characteristics to meet the load conditions. Please refer to [ETSI TS 136 211 Chapter 4.2](#) to properly configure your subframes.

- Navigate to the **Setup > LTE Baseline** page of the FW-600 WebUI.
- In the **LTE Baseline Parameters** section, enter a value between 0-6 for the **Subframe Assignment** field. As a default, it has the value of 2.
- Under the **Special Subframe** field, set a value between 0-8. It is set at 7 by default.

LTE Baseline Parameters			
Subframe Assignment	<input type="text" value="2"/>	Special Subframe	<input type="text" value="7"/>
Baseline eNB ID	<input type="text" value="100"/>	PCI Seed Value	<input type="text" value="10"/>
Tracking Area Code	<input type="text" value="1"/>	Enable Mobility	<input checked="" type="radio" value="NO"/>

- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.

6.4.1.2. Assign a Baseline eNodeB ID

You use the eNodeB ID to identify each cell when establishing a connection with the Evolved Packet Core (EPC). The system automatically generates three IDs from the baseline value of this parameter for each cell respectively, using the following logic:

- $\{[eNB\ Id]*256\}$,
- $\{[eNB\ Id]*256+1\}$,
- $\{[eNB\ Id]*256+2\}$.

This setting **must** match with the configured value in the EPC.

To setup the Baseline eNodeB ID:

- Navigate to the **Setup > LTE Baseline** page of the FW-600 WebUI.
- Under the **LTE Baseline Parameters** section, assign the eNodeB identification in the **Baseline eNB ID** field. The default value for this parameter is 100.

LTE Baseline Parameters			
Subframe Assignment	<input type="text" value="2"/>	Special Subframe	<input type="text" value="7"/>
Baseline eNB ID	<input type="text" value="100"/>	PCI Seed Value	<input type="text" value="10"/>
Tracking Area Code	<input type="text" value="1"/>	Enable Mobility	<input checked="" type="radio" value="NO"/>

Before going to another section, select **Commit** in the top right corner to save your changes or select the **Refresh** button to cancel and return to the previous settings.

6.4.1.3. Entering PCI Seed Value

The **Cell ID** and **PCI Seed Value** define each cell's Physical Cell ID (PCI) which the system uses to decode data transmission.

- PCI calculation: $3*[PCI\ Seed\ Value] + [Cell\ Id]$
- Cell IDs are fixed at 0, 1 and 2 respectively.

- BLiNQ recommends to pre-draft a PCI assignment strategy carefully to avoid interference due to PCI reuse; you can use preconfigured default values.
- Refer to Appendix B for more information on creating a PCI assignment strategy.

To enter PCI Seed Value:

- Navigate to the **Setup > LTE Baseline Parameters** page of the FW-600 WebUI.
- Under the **LTE Baseline Parameters** area, assign the PCI Seed Value in the **PCI Seed Value** field (You can enter any value between 0-167). It is set to 10 by default.

LTE Baseline Parameters			
Subframe Assignment	<input type="text" value="2"/>	Special Subframe	<input type="text" value="7"/>
Baseline eNB ID	<input type="text" value="100"/>	PCI Seed Value	<input type="text" value="10"/>
Tracking Area Code	<input type="text" value="1"/>	Enable Mobility	<input checked="" type="radio" value="NO"/>

- Before going to another section, select **Commit** in the top right corner to save your changes or select the **Refresh** (🔄) button to cancel and return to the previous settings.



NOTE: When using 2CC configuration, the system automatically assigns the primary carrier the PCI value of Cell 1 and the secondary carrier will have the PCI value of Cell 0. If the CPE was previously locked onto the PCI of Cell 0 in 1CC mode, please log into the CPE, release/delete the PCI lock and relock it with the PCI of cell 1. This way, the CPE will be locked onto the primary carrier when it is in 2CC mode.

6.4.1.4. Setting Tracking Area Code

The Tracking Area Code identifies the tracking area within a particular network. You need to set the same code that matches the settings on your EPC.

- Navigate to **Setup > LTE Baseline** page to set the tracking area code under LTE Baseline Parameters section.
- Set the Tracking Area code via the **Tracking Area Code** field. By default, the value is set at 1.

LTE Baseline Parameters			
Subframe Assignment	<input type="text" value="2"/>	Special Subframe	<input type="text" value="7"/>
Baseline eNB ID	<input type="text" value="100"/>	PCI Seed Value	<input type="text" value="10"/>
Tracking Area Code	<input type="text" value="1"/>	Enable Mobility	<input checked="" type="radio" value="NO"/>

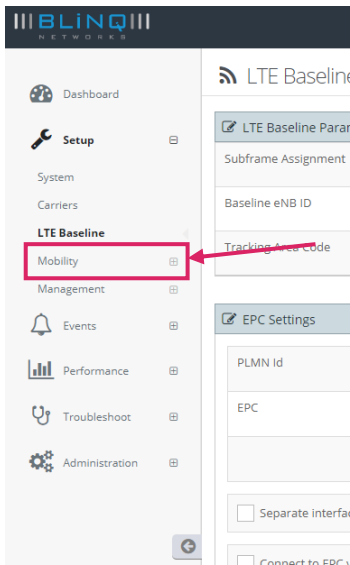
- Before going to another section on the page, select **Commit** in the top right corner to save your changes or select the **Refresh** (🔄) button to cancel and return to the previous settings

6.4.1.5. Enable Mobility

The eNB does not turn on mobility functionality by default. This has to be done manually.

To enable mobility support:

- Go to **Setup > LTE Baseline > LTE Baseline Parameters**
- Toggle the **Enable Mobility** button to YES
- Click on **Commit** in the top right corner to commit the change.
- An additional option (**Mobility**) will appear on the Navigation Bar/Menu



6.4.2. eNB Identifiers

The values in this section are read-only and will change based on the values inserted in the **LTE Baseline Parameters** section.

To manipulate the values in this section, change the **Baseline eNB ID** and **PCI Seed Value** (see Section 6.4.1.2 and Section 6.4.1.3) in **LTE Baseline Parameters**.

eNB Identifiers		
LTE Cell	eNB ID	PCI
LTE Cell 0	25600	30
LTE Cell 1	25601	31
LTE Cell 2	25602	32

Varies with
Baseline eNB ID



Varies with PCI
Seed Value



6.4.3. EPC Settings

The Evolved Packet Core (EPC) sets up the optional integrated (embedded) Evolved Packet Core on the FW-600 system. In the EPC Settings section, you will configure the system to use External EPC.

This is also the section where you configure the PLMN ID.

The Public Land Mobile Network Identifier or PLMN ID defines the network. The PLMN ID consists of a 3-digit mobile country code (MCC) and a 2 (or 3)-digit mobile network code (MNC), thus PLMN-ID = MCC + MNC. You **must** enter the value that matches the one in the EPC.

To configure the Evolved Packet Core (EPC) for the FW-600:

- Navigate to the **Setup > LTE Baseline** page of the FW-600 WebUI.
- Under the **PLMN Id** area of the **EPC Settings** section, assign the Public Land Mobile Network identification in the **PLMN Id** field. The default value is 00101 (test network).

- Select either **“External”** or **“Embedded”** under EPC
 - If **“Embedded”** is selected, please refer to *Embedded EPC Install and Config Guide* for more information.
 - If **“External”** is selected, enter the **“MME Name”** and **“MME Host”** (IPv4 or IPv6 address). If more than one MME Name/Host is entered, MME pooling will automatically be enabled.

Enter more than one MME Name/Host to enable MME Pooling

- Select **Commit** in the top right corner to save your changes or select the **Refresh** (🔄) button to cancel and return to the previous settings.



NOTES:

- Mobile Management Entity (MME) plays an import role in LTE EPC architecture. MME is the main signalling node in the EPC. Multiple MMEs can be grouped together in a pool to meet increasing signalling load in the network.
- MME 0 and MME 1 cannot have the same Name and Host.

6.4.3.1. Separate Interface for S1 Traffic

To set up a separate interface for S1 traffic (instead of sending both mgmt. and S1 traffic over a single interface):

- Check off the box for **“Separate Interface for S1 Traffic”**. This will reveal a set of editable configuration parameters.

<input checked="" type="checkbox"/> Separate interface for S1 traffic			
Enable VLAN	<input type="radio"/> YES	VLAN ID	<input type="text" value="0"/>
IPv4 Address	<input type="text" value="192.168.26.100"/>	Subnet Mask	<input type="text" value="255.255.255.0"/>
IPv6 Address	<input type="text" value="fc00::a"/>	IPv6 Prefix Length	<input type="text" value="64"/>
<input type="checkbox"/> Connect to EPC via Secure Gateway			

- Please fill in the following items:
 - Enable VLAN:** This option is set on **“YES”** and is not editable.
 - VLAN ID:** VLAN ID has a value range from 0 to 4094. It specifies which VLAN ID tag to add to a packet.
 - IPv4/IPv6 Address:** Enter the IP addresses for the S1 traffic interface.
 - Subnet Mask:** Enter the subnet mask for this interface.
 - IPv6 Prefix Length:** Enter the IPv6 prefix length, a value between 1 to 127.
- Click on **“Commit”** to save the changes.



NOTE: This option is not available when the external EPC is connected via secure gateway.

6.4.3.2. Secure Gateway

The FW-600 system can connect to an external EPC via secure gateway for added security. Up to 2 separate secure gateways can be set at the same time for redundancy purposes. SecGW 1 is optional.

To set up secure gateway:

- Select **“Connect to EPC via Secure Gateway”** option by checking the box. This will open a section with various configuration parameters.

<input checked="" type="checkbox"/> Connect to EPC via Secure Gateway			
Use SecGW	SecGW	IKEv2	IPSec
<input checked="" type="checkbox"/> SecGW 0	Name: <input type="text"/> Host: <input type="text"/> <small>Required</small>	Encryption Algorithm: 256 bit AES-CBC Auth Algorithm: SHA2_256_128 HMAC Auth Method: Pre-shared Key Pre-shared Key: <input type="text"/> <small>Required</small> DH Group: 14 Rekey Time: 4h	Encryption Algorithm: 256 bit AES-CBC Auth Algorithm: SHA2_256_128 HMAC DH Group: 14 Rekey Time: 1h
<input type="checkbox"/> SecGW 1			

- Enter the secure gateway **Name** and **Host** address.



- **IKEv2:** Internet Key Exchange Version 2 (IKEv2) is the second-generation standard for a secure key exchange between connected devices. IKEv2 works by using an IPSec-based tunneling protocol to establish a secure connection. Configure the parameters below.
 - **Encryption Algorithm:** Select **168 bit 3DES-EDE-CBC**, **128 bit AES-CBC**, **192 bit AES-CBC** or **256 bit AES-CBC** (default) from the drop-down menu.
 - **Auth Algorithm:** Select one of the algorithms from the drop-down menu. **SHA2_256_128 HMAC** is the default selection.
 - **Auth Method:** Select either a Pre-shared Key or a Public Key. Pre-shared Key is the default selection.
 - **Pre-shared Key:** This option is only available if a “Pre-shared Key” is selected under the Auth Method. Enter the key that was given.
 - **DH Group:** Select one of the DH Group from the drop-down menu. By default, it is set at DH Group 14. DH Groups 1, 2 and 5 is not recommended as they do not provide adequate security against modern threats and should not be used to protect sensitive information.
 - **Rekey Time:** The default time is set at 4 hours.
- **IPSec:** IPSec, or Internet Protocol Security, is a set of protocols used to secure internet protocol (IP) data transmissions and communications, or more simply, internet traffic. To establish a secure connection, IPSec works by authenticating and encrypting each packet of data during the time you are connected.
 - **Encryption Algorithm:** Select **168 bit 3DES-EDE-CBC**, **128 bit AES-CBC**, **192 bit AES-CBC** or **256 bit AES-CBC** (default) from the drop-down menu.
 - **Auth Algorithm:** Select one of the algorithms from the drop-down menu. **SHA2_256_128 HMAC** is the default selection.
 - **DH Group:** Select one of the **DH Group** from the drop-down menu. By default, it is set at **DH Group 14**. DH Groups 1, 2 and 5 is not recommended as they do not provide adequate security against modern threats and should not be used to protect sensitive information.
 - **Rekey Time:** The default time is set at 4 hours.
- Click on “**Commit**” to save the changes.

6.4.4. Advanced Options

The **Show Advanced** Option in the **LTE Baseline** page opens three more sections where you can set different values for each cell. The sections are **LTE Advanced – General**, **PDSCH/PDDCH**, **Closed Subscriber Group**, **UE Reporting** and **Random-access channel / Physical Random-access channel (RACH/PRACH)**.

LTE Advanced - General

Cell	Max Number of UEs	P-max value [dBm]	Q Rx Rev Min [dBm]
Cell 0	32	23	-65
Cell 1	32	23	-65
Cell 2	32	23	-65

Closed Subscriber Group

CSG Indication: NO

CSG Identity:

UE Reporting

Enable DL Measurements: YES

PDSCH / PDCCH

PDCCH CFI:

RACH / PRACH

Use RACH/PRACH to configure Cell Range

Cell range [km]:

Cell	RACH Powerramping Step	RACH Powerramping Preamble Initial RTP	RACH Preamble Trans Max	PRACH Config Idx	PRACH Zero Corr Zone
Cell 0	4 dB	90 dBm	3		
Cell 1	4 dB	90 dBm	3		
Cell 2	4 dB	90 dBm	3		

Reset Advanced

6.4.4.1. LTE Advanced – General Settings

- Set the **max. number of UEs** (between 0-96) of the respective cells. It is set to 32 by default.
- Enter the **P-max Value**. This is the maximum power the CPE can transmit. The maximum value for this parameter is 23dBm.
- Lastly, configure the **Q Rx Lev Min** value, which is the minimum signal strength that the CPE needs to see in order to connect. Care must be taken when modifying this parameter. Please note that a value of -65 dBm configured on the FW-600 translates to a min. threshold of -130 dBm (i.e., Multiplied by 2). If the CPE measures the signal strength lower than -130 dBm, then it will not attempt to connect. Increasing the value of this parameter will severely impact the cell range.

LTE Advanced - General

Cell	Max Number of UEs	P-max value [dBm]	Q Rx Rev Min [dBm]
Cell 0	32	23	-65
Cell 1	32	23	-65
Cell 2	32	23	-65

- Select **Commit** in the top right corner to save your changes or select the **Reset Advanced** button to cancel and return to the previous advanced settings.

6.4.4.2. Setting up RACH/PRACH Values

Setting up the right values for RACH is critical to achieve up link synchronization between UE and eNB. The default parameters are carefully selected by BLiNQ. Please do not modify unless instructed by BLiNQ Customer Support.

- **Cell Range:** Configuring the cell range parameter automatically sets the parameters that the CPE requires to establish the link
 - There is an option to **Use RACH/PRACH to configure Cell Range** or enter the **Cell Range** manually. If the former option is chosen, cell range will be calculated automatically. For the latter option, enter the desired **Cell Range**. The default is set at 20 km.
- Choose a value from the drop-down list in the **RACH Powerramping Step** field. This is the amount of power that will be added onto the Initial RTP (which you will be configuring next) after each connection attempt.

✎ RACH / PRACH

Use RACH/PRACH to configure Cell Range

Cell range [km]

20

?

Cell	RACH Powerramping Step	RACH Powerramping Preamble Initial RTP	RACH Preamble Trans Max	PRACH Config Idx	PRACH Zero Corr Zone
Cell 0	4 dB	90 dBm	3		
Cell 1	4 dB	90 dBm	3		
Cell 2	4 dB	90 dBm	3		

- The next column is **RACH Powerramping Preamble Initial RTP**. Similarly, select a value from the drop-down list to set the initial power to use for connection to the CPE.
- Select the maximum number of connection attempts from the drop-down list under **RACH Preamble Trans Max** field.
- The next two columns (**PRACH Config Idx** and **PRACH Zero Corr Zone**) are used only if you wish to use RACH/PRACH to configure your cell range instead of setting it.
 - Check off the box at the top left corner of this section.
 - Set your **PRACH Config Idx** and the **PRACH Zero Corr Zone** to establish your cell range.

RACH / PRACH

Use RACH/PRACH to configure Cell Range

Cell	RACH Powerramping Step	RACH Powerramping Preamble Initial RTP	RACH Preamble Trans Max	PRACH Config Idx	PRACH Zero Corr Zone
Cell 0	4 dB	90 dBm	3	3	5
Cell 1	4 dB	90 dBm	3	3	5
Cell 2	4 dB	90 dBm	3	3	5

- Once you are satisfied with your values, select **Commit** in the top right corner to save your changes or select the **Reset Advanced** button to cancel and return to the previous advanced settings

6.4.4.3. Closed Subscriber Group

The closed subscriber group (CSG) feature is used when it is needed to further limit UE PLMN selection. This allows the UE to connect to the desired eNB when neighboring radios are using the CBRS shared PLMN.

Enable the feature by toggling **CSG Indication** to **Yes**.

Closed Subscriber Group

CSG Indication YES

CSG Identity

Configure the same “**CSG Identity**” for both the eNB as well as the UE.

All UEs with matching CSG identity will then be able to attach to the eNB.

6.4.4.4. UE Reporting

The FW-600 can obtain DL measurements from CPEs using periodic measurement reports. This way the eNB can add DL measurements to the performance measurements for each UE.

To enable this feature, simply click the slider to “**YES**”.

UE Reporting

Enable DL Measurements YES

The default reporting interval is **1024ms**. As of SW 3.1.2, this value can only be changed by using CLI. Please contact BLiNQ Customer Support for more information.

6.4.4.5. PDSCH/PDCCH

This section sets up the PDCCH (Physical Downlink Control Channel) CFI (Control Format Indicator) value. It defines the number of symbols in each subframe allocated to PDCCH. The default is set at 1.

BLiNQ Networks recommends keeping this value at 1.

PDSCH / PDCCH

PDCCH CFI	<input style="width: 90%;" type="text" value="1"/>
-----------	--

6.5. Mobility

This is a feature that is only available for SW 4.0 onwards. Please see Section 6.4.1.5 to enable this feature.

There are three sections under Mobility:

- Neighbors
- Cell Reselection
- Handover

6.5.1. Neighbors

Under the section of Neighbors, you can configure the following items:

- Cells
- Frequencies
- X2 Neighbors

The following sections will detail the configurations of each item.

6.5.1.1. Cells

The cells configured in this section are advertised in SIB4 (to help with intra-frequency cell reselection), SIB5 (to help with inter-frequency cell reselection), or RRC Connection Reconfiguration (to help with handover). It is not mandatory to advertise them, but they do narrow down the candidates to look for.

The system currently supports up to 16 neighbor cells (SW 4.0.2 onwards).

Neighbor Cells ↻

Neighbor Cells										
		Parameters								
No.		PLMN ID	Cell ID	PCell 0	PCell 1	PCell 2	Initial EARFCN			
<input type="checkbox"/>	0	99999	18944	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	43790			▼
<input type="checkbox"/>	1	00101	7680	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	43790			▼

+ Add Neighbor Cell
Delete Neighbor Cell

To add a neighbor cell:

- Click on the blue “+ Add Neighbor Cell” button. A pop-up window will appear.
- Enter the following parameters to add the neighbor cell:
 - **PCell 0 / PCell 1 / PCell 2:** These 3 Boolean values determine to which PCell of this eNB the neighbor cell should be applied to. Check off the respective boxes as needed.
 - **PLMN ID:** The default PLMN ID is set at 00101. This can be changed to your desired value. However, if it is left blank, it will just return to its default value.

- **Cell ID:** Cell ID is a required parameter. Together with the PLMN ID and Tracking Area Code, the Cell ID helps to uniquely identify cell.
- **Initial EARFCN:** This is an optional parameter that represents the initial frequency associated with this cell. Once the operator adds this cell to PCell’s neighbor list or blacklist, this frequency will be advertised in relevant SIBs and RRC Connection Reconfiguration messages.
- Next, click on the **Advanced** tab and enter the following parameters.

- **TAC:** This is the Tracking Area Code and it plays a part in uniquely identifying the cell.
- **PCI:** Similar to EARFCN (see above), this is the initial PCI value to be used. If neighbor advertises different value, the advertised value will be used.
- **Q Offset Cell:** This parameter is used if cell is in neighbor cell list. The offset can be positive (decreases the chances of cell to be considered, as it is subtracted from the measured value) or negative (increases the chances of cell to be considered). The range is from -24dB to 24dB.
- **HO Allowed:** Check this box to allow Handover. If it is not checked, the cell will be added to blacklist in ALL advertisements. By default, it is set to allow handover.
- Once the required values are entered, click on the blue + Add Neighbor Cell to add this new cell.

6.5.1.2. Frequencies

This section is used for cell reselection to other frequencies (and then information is advertised in SIB5) and for creating measurement reports (and then it is advertised in RRC Connection Reconfiguration message).

The system supports entering up to 30 neighboring frequency relations, however up to 8 can be assigned to PCell. There is a separate row for each frequency.

Frequency Relations

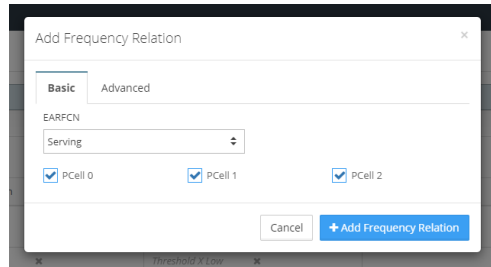


Frequency Relations										
No.	Parameters									
<input type="checkbox"/>	0	EARFCN	All	PCell 0 ✓	PCell 1 ✓	PCell 2 ✓	Cell Reselection Priority	4	T Reselection E-UTRA	▼
		Threshold X High	0	Threshold X Low	0					
<input type="checkbox"/>	1	EARFCN	Serving	PCell 0 ✓	PCell 1 ✓	PCell 2 ✓	Cell Reselection Priority	✖	T Reselection E-UTRA	✖
		Threshold X High	✖	Threshold X Low	✖					

[+ Add Frequency Relation](#) [Delete Frequency Relation](#)

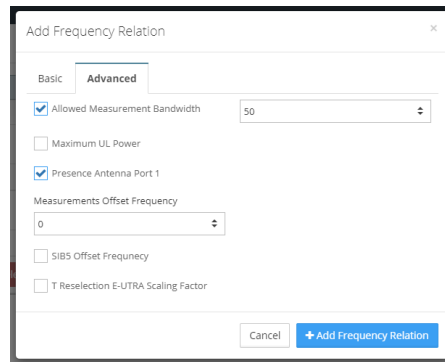
To add a new frequency:

- Click on the blue + Add Frequency Relation. A popup window will appear



- Under the **Basic** tab,
 - EARFCN:** There are 3 different options for this – All, Serving and Specific
The “All” frequency is placeholder for the neighboring frequencies the system learns in dynamic fashion. When “Serving” frequency is selected, the eNB will apply all the parameters defined in this section and use the frequency that eNB cell is using at the moment.
 - PCell 0 / PCell 1 / PCell 2:** You can select the cell out of which this frequency will be advertised. By default all PCells are selected.

- Under the **Advanced** Tab,



- Allowed Measurement Bandwidth:** This parameter represents the channel bandwidth the UE should assume when scanning for a neighbor frequency. The drop-down menu gives the options for the number of PRBs (Physical Resource Blocks). For example, if the neighboring frequency is 20 MHz wide, the number of PRBs will be 100.
- Maximum UL Power:** This is the TX power. The maximum is 23 dBm.
- Presence Antenna Port 1:** This field is used to indicate whether all the neighbouring cells use Antenna Port 1.
- Measurements offset Frequency:** This value represents the offset that should be added by the UE when comparing measurement of neighbor frequency against relevant threshold (the actual rules depends on the event type).
- SIB5 Offset Frequency:** When this option is checked off, a dropdown menu will appear for selection. This is the value used by the UE when calculating neighbor’s suitability for cell-reselection. In this case the value is SUBTRACTED from the neighboring frequency measurement.
- T Reselection E-UTRA Scaling Factor:** This parameter is used in cell reselection and tells UE for how long required condition to consider neighboring frequency needs to be satisfied for the UE to move to the target frequency.

When this option is checked, more fields will appear.

- When all the parameters have been set, click on the “+ Add Frequency Relation” to add the new frequency.

6.5.1.3. X2 Neighbors

The purpose of this configuration section is to allow X2 communication with the neighboring cells. X2 neighbor information will be learnt via X2 procedures - X2 setup/X2 response or X2 eNB configuration update.

The operation data will be updated based on latest information received. On reboot, configured and learnt data will be used again until it learns new information from peers.

For each X2 neighbor, the operator will be able to define the address (ext-enb-host). The address can be IPv4, IPv6, or hostname. It is also possible to specify the SCTP port number (ext-enb-sctp-port) – default is 36422. The ENB keeps track about the entity that created the entry (read only variable created-by).

Up to 5 X2 neighbors can be configured on the system currently (SW 4.0.2 onwards).



NOTE: Please note that only primary cell information will be included in X2 messages as we don't support mobility features on secondary cell.

X2 Neighbors

X2 Neighbors					
	No.	Host	SCTP Port	Adjacent Neighbor	Creator
<input type="checkbox"/>	0	192.168.34.22	36422	x	operator

+ Add X2 Neighbor Delete X2 Neighbor

To add an X2 neighbor:

- Click on the blue “+ Add X2 Neighbor” button. A pop-up window will appear.

- Enter the **Host** details. This can be the IPv4, IPv6 or hostname (domain name) of the X2 neighbor.
- Enter the **SCTP** Port number. The default is set at 36422.

- **Adjacent Neighbour** box can be ignored as this does not apply to the FW-600 eNB.
- Click on the blue **+Add X2 Neighbor** to add the new X2 neighbor. The newly added neighbor should be listed on the X2 Neighbors' page without needing a reboot.

To delete an existing neighbor, simply click on the checkbox beside the desired item on the table and hit the red **Delete X2 Neighbor** button.

X2 Neighbors					
	No.	Host	SCTP Port	Adjacent Neighbor	Creator
<input type="checkbox"/>	0	192.168.34.22	36422	x	operator
<input type="checkbox"/>	1	192.168.32.33	36422	x	operator
<input checked="" type="checkbox"/>	2	192.168.32.32	36422	x	operator
<input type="checkbox"/>	3	192.168.32.3	36422	x	operator

+ Add X2 Neighbor
Delete X2 Neighbor

6.5.2. Cell Reselection

Cell Reselection page handles parameters that instruct UEs how to handle cell reselection while in IDLE mode. Most of these parameters are advertised in SIB3, SIB4, and SIB5.

These parameters are configured per enabled PCell.

Cell Reselection Settings

PCell	Parameters						Blacklisted Cells PLMNID-CellID			
	SIB3 Q Hysteresis		SIB3 SNonIntra Search		SIB3 Threshold Serving Low				SIB3 Cell Reselection Priority	
0	SIB3 Q Hysteresis	4	SIB3 SNonIntra Search	0	SIB3 Threshold Serving Low	0	SIB3 Cell Reselection Priority	7	99999-18945	▼
	SIB3 Sintra Search	8	SIB3 T Reselection E-UTRA	2						
1	SIB3 Q Hysteresis	4	SIB3 SNonIntra Search	0	SIB3 Threshold Serving Low	0	SIB3 Cell Reselection Priority	7		▼
	SIB3 Sintra Search	8	SIB3 T Reselection E-UTRA	2						
2	SIB3 Q Hysteresis	4	SIB3 SNonIntra Search	0	SIB3 Threshold Serving Low	0	SIB3 Cell Reselection Priority	7		▼
	SIB3 Sintra Search	8	SIB3 T Reselection E-UTRA	2						

To modify the parameters of a PCell, click on the blue PCell number on the left column. A popup window will appear where configurations in 3 different tabs can be modified.



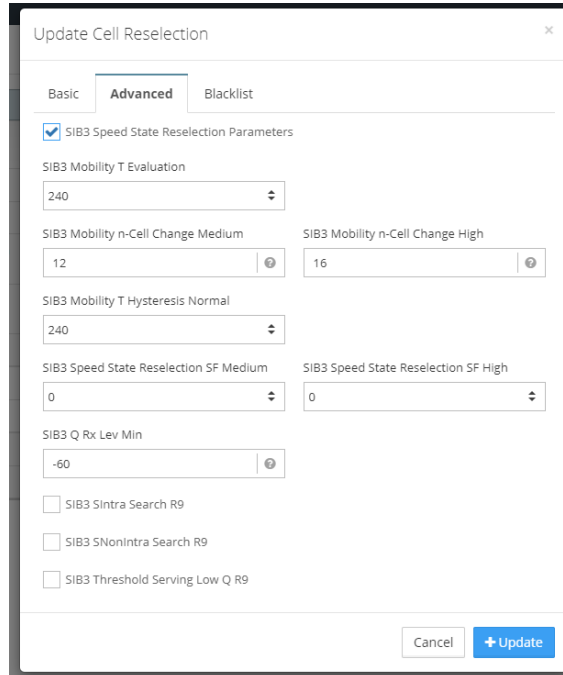
- Under **Basic** tab:

The screenshot shows the 'Update Cell Reselection' dialog box with the 'Basic' tab selected. The fields and their values are as follows:

Parameter	Value
SIB3 Q Hysteresis	4
SIB3 SNonIntra Search	<input checked="" type="checkbox"/> 0
SIB3 Threshold Serving Low	0
SIB3 Cell Reselection Priority	7
SIB3 Sintra Search	<input checked="" type="checkbox"/> 8
SIB3 T Reselection E-UTRA	2

- **SIB3 Q Hysteresis:** This value defines how much the serving cell signal should be preferred compared to a neighbor cell.
- **SIB3 SNonIntra Search:** This parameter represents the minimum acceptable value of the serving cell Srxlev for the UE NOT to start considering inter-frequency cell reselection to cells of lower or equal priority as the serving cell.
- **SIB3 Threshold Serving Low:** This parameter represents the minimum acceptable value for serving cell Srxlev (which is roughly difference between serving cell Reference Signal Received Power (RSRP) and minimum acceptable RSRP for the serving cell) for the UE NOT to start considering inter-frequency cell reselection to cells of lower or equal priority as the serving cell.
- **SIB3 Cell Reselection Priority:** This is serving cell reselection priority. The UE uses this value to decide if other frequencies defined in SIB5 are of higher priority or not. The default value is set at 7.
- **SIB3 Sintra Search:** It specifies the serving cell Srxlev threshold (in dB) for intra-frequency measurements. (Srxlev represents the difference between measured RSRP and minimum acceptable RSRP). By default, this is set at 8.
- **SIB3 T Reselection E-UTRA:** This parameter determines for how long the reselection criteria needs to be satisfied for UE to move to another cell on the same frequency. The default value is set at 2.

- Under the **Advanced** tab:

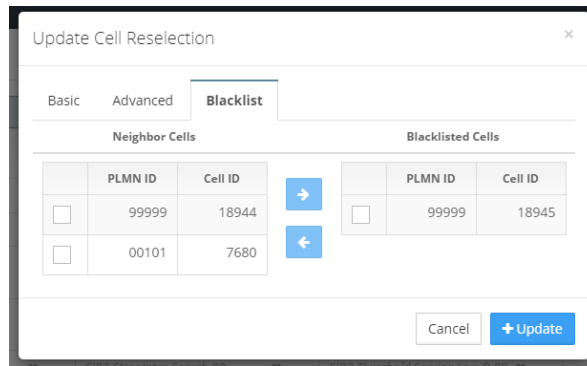


- SIB3 Speed State Reselection Parameters:** This parameter determines if speed state reselection parameters are advertised or not. By default it is set to Yes.
- SIB3 Mobility T Evaluation:** This parameter determines how long the UE needs to satisfy the criteria for moving to Medium or High Mobility state in order to actually move to those states. By default it is set to 240 seconds. You can select any value from the dropdown menu.
- SIB3 Mobility n-Cell Change Medium:** This specifies the maximum number of cell reselections to enter Medium-mobility state. Its default is set to 12, and the range is from 1 to 16.
- SIB3 Mobility n-Cell Change High:** This specifies the maximum number of cell reselections to enter High-mobility state. Its default is set to 16, and the range is from 1 to 16.
- SIB3 Mobility T Hysteresis Normal:** This parameter determines how long the criteria for UE being in Medium or High Mobility need to be NOT satisfied before UE moves to Normal state. Default setting is 240 seconds. Valid values are 60, 120, 180 and 240.
- SIB3 Speed State Reselection SF Medium:** When the UE compares neighbor cell with the serving cell, it adds SIB3 Q Hysteresis to the measurement of the serving cell, effectively ensuring that neighboring cell needs to be at least SIB3 Q Hysteresis or better for the UE to move to it.
- SIB3 Speed State Reselection SF High:** This parameter is added to the measurement of the serving cell when UE is in state of High Mobility. This makes it easier to UE to move to a neighboring cell. In general it makes sense to have this parameter lower than similar parameter for Medium Mobility (for example if it is -2 for Medium Mobility, it can be -4 for High Mobility)
- SIB3 Q Rx Lev Min:** This value represents the minimum acceptable RSRP for neighboring cells on the same frequency. The default value for this parameter is -60 (the same as for the serving cell) with the range of -70 to -13.
- SIB3 Sintra Search R9:** This parameter define the threshold of the minimum acceptable quality that serving cell has to drop to for the UE to start looking for the alternative cell on the same frequency. This

has the same functionality as **SIB3 Sintra Search** (Basic Tab), but it has a higher priority than that. If both values are present/configured, the UE will use **SIB3 Sintra Search R9** first.

- **SIB3 SNonIntra Search R9:** This parameter represents the threshold – if the serving cell signal level (either RSRP or RSRQ) drops below the threshold, the UE should start looking for other cells. The difference is that this is **NonIntra**, so UE will start looking at different frequencies. The default values are 8 (RSRP) and 9 (RSRQ).
- **SIB2 Threshold Serving Low Q R9:** This parameter determines the condition under which the UE would move to a frequency with a lower priority than the serving cell. It is not turned on by default. If it is selected, the default value will be set to 0.

▪ Under **Blacklist** tab:



- You can select the cells listed under **Neighbor Cells** and place them onto the **Blacklisted Cells** with the arrow keys. Cells need to be added on as a Neighbor cell before they can be put on the Blacklist.
- **A maximum of 16 cells** can be blacklisted.
- Once all the configurations are modified, click on the **+ Update** button.

6.5.3. Handover

Handover is triggered by UE reporting that an event that ENB told UE to look for took place. Hence, this section is primarily about measurement configuration (i.e., what should ENB tell UE to look for and what to do once the event is detected).

Handover Rules

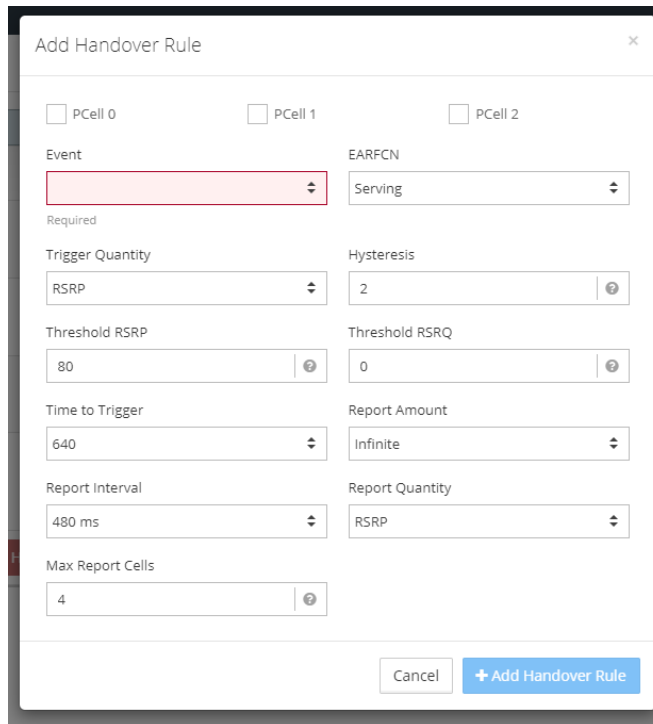


Handover Rules												
No.	PCells	Event	EARFCN	Trigger Quantity	Hysteresis	Threshold / Offset	Time to Trigger	Report Amount	Report Interval	Report Quantity	Max Report Cells	
<input type="checkbox"/>	0	0 ✓ 1 ✓ 2 ✓	A1	Serving	RSRP	2	RSRP 80 RSRQ 0	640	Infinite	480 ms	RSRP	4
<input type="checkbox"/>	1	0 ✓ 1 ✓ 2 ✓	A2	Serving	RSRP	2	RSRP 80 RSRQ 0	640	Infinite	480 ms	RSRP	4
<input type="checkbox"/>	2	0 ✓ 1 ✓ 2 ✓	A3	Serving	RSRP	2	Offset 4	640	Infinite	480 ms	RSRP	4
<input type="checkbox"/>	3	0 ✓ 1 ✓ 2 ✓	A5	All	RSRP	2	RSRP 1 62 RSRQ 1 0 RSRP 2 35 RSRQ 2 0	640	Infinite	480 ms	RSRP	4

+ Add Handover Rule Delete Handover Rule

To add a Handover Rule:

- Click on the blue **+ Add Handover Rule** button. A popup window will appear.



- Enter the following parameters:
 - PCell 0 / PCell 1 / PCell 2:** This determines to what PCell the handover rule will be applied to. (Only enabled PCells can be selected).
 - Event:** Choose A1, A2, A3, A4 or A5 from the dropdown menu. Single PCell supports up to one A1 event type, up to one A2 event type, up to one event for intra-frequency handover, and up to one event for inter-frequency handover.
 - For A5:** A few additional fields will appear as it will need a second Threshold RSRP/RSRQ.
 - EARFCN:** Choose either **All** or **Serving** from the dropdown menu.
 - If event type **A1** or **A2** is chosen from before, the only valid option here will be **Serving** and it will automatically be selected as such.
 - If the event type **A3**, **A4** or **A5** is selected, both **Serving** and **All** will be available.
 - Trigger Quantity:** This parameter tells the UE which RF parameter (RSRP or RSRQ) to evaluate. (This is independent from **Report Quantity**). If RSRP is chosen, then only Threshold RSRP will need to be filled in and the value entered in Threshold Reference Signal Received Quality (RSRQ) will be ignored (and vice versa).
 - Hysteresis:** This parameter is used to reduce “bouncing” effect when the measured signal is close to the threshold. When the signal needs to go above certain threshold for condition to trigger, the hysteresis is added to the threshold; when the signal needs to go below certain threshold for condition to trigger, the hysteresis is subtracted from the threshold. Default value is set at 2.
 - Threshold RSRP:** The default value is set at 80. This will be the threshold value used for measurement depending on the type of event selected.



- **Threshold RSRQ:** The default value is set at 0. This will be the threshold value used for measurement depending on the type of event selected.
- **Time to Trigger:** This parameter specifies for how long the event condition has to be satisfied in order for the UE to send measurement report. The default time is set at 640 ms.
- **Report Amount:** This parameter specifies how many times the measurement report should be sent. The default is set as infinity – as long as the event condition is satisfied, the event will be sent.
- **Report Interval:** If the report-amount is greater than 1, this parameter tells the UE how often to send measurement reports (when the event condition is satisfied).
- **Report Quantity:** This parameter specifies what measured RF value the UE should provide in measurement report.
- **Max. Report Cells:** This parameter specifies how many non-serving cells (that satisfy event condition) to include in measurement report. The default is 4.
- Once the parameters are set, click on “+ **Add Handover Rule**” to add the rule.

6.6. Embedded EPC

Please refer to the *Embedded EPC Install and Config Guide* for Embedded EPC configurations on the WebUI.

6.7. CBSD

CBSD option is only available for frequency band 48 (B48).

When the WebUI loads, it will recognize the eNodeB is operating in B48 and make **CBSD** option available for configuration.

On the WebUI, you use the Citizens Broadband (radio) Service Device (CBSD) page for the Spectrum Access System (SAS) server connectivity. When using the LTE Band 48, eNodeB requires Spectrum Access System (SAS) server connectivity for operation. The eNodeB will automatically configure the operating frequency and transmit power per beam based on the grants received by the SAS server.

Perform these steps in the order presented below.



NOTE: Select the **Commit** button *before* moving to a new page to save the configuration changes.

6.7.1. Configure SAS Server Connectivity

- On the WebUI, navigate to **Setup > CBSD**.

CBSD Settings ↻ Commit

Common Settings

Enable CBSD YES

User ID

SAS URL

Registration Type Single Step (upload data) Single Step (input data) Multi Step

Installation Parameters

Uploaded parameters: Signed at 2022-10-11T17:15:02Z Delete

Upload new parameters file

Device Parameters

FCC ID: ROR00000008

Device Category: B

Cell	Antenna	Initial CBSDSN	Standby Grant	Standby Grant Alarm
0	Internal-B0	OCA1380009BA0	<input type="button" value="Promote"/>	<input type="button" value="Clear"/>
1	Internal-B0	OCA1380009BA1	<input type="button" value="Promote"/>	<input type="button" value="Clear"/>
2	Internal-B0	OCA1380009BA2	<input type="button" value="Promote"/>	<input type="button" value="Clear"/>

- Under the **Common Settings** area, use the following options to set up SAS server connectivity:

Common Settings

Enable CBSD YES

User ID

SAS URL

Registration Type Single Step (upload data) Single Step (input data) Multi Step

Installation Parameters

Uploaded parameters: Signed at 2022-10-11T17:15:02Z Delete

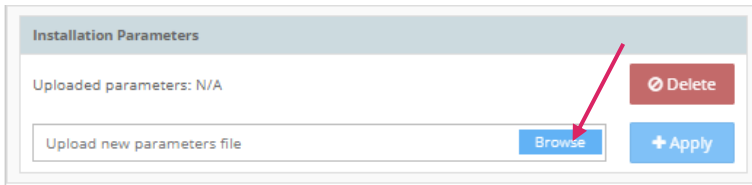
Upload new parameters file

- Enable CBSD:** Toggle the button to Enable (**YES**) or Disable (**NO**) CBSD feature.
- User ID:** Input the CBSD User identification
- SAS Server URL:** Input the Spectrum Access System (SAS) database server Universal Resource Locator (URL), for example: <https://developer-sc-02.federatedwireless.com/v1.2>
- Registration Type:** There are 3 ways to register using the WebUI - **Single Step (Upload data)**, **Single Step (Input data)** or **Multi Step**.
 - Single Step (Upload data):** For this option, a pre-generated the CPI signed CBSD configuration data file needs to be uploaded onto the eNB to enable the registration.
 - To generate the data file, open the program provided by BLiNQ – the CPI Signed Data Generator.

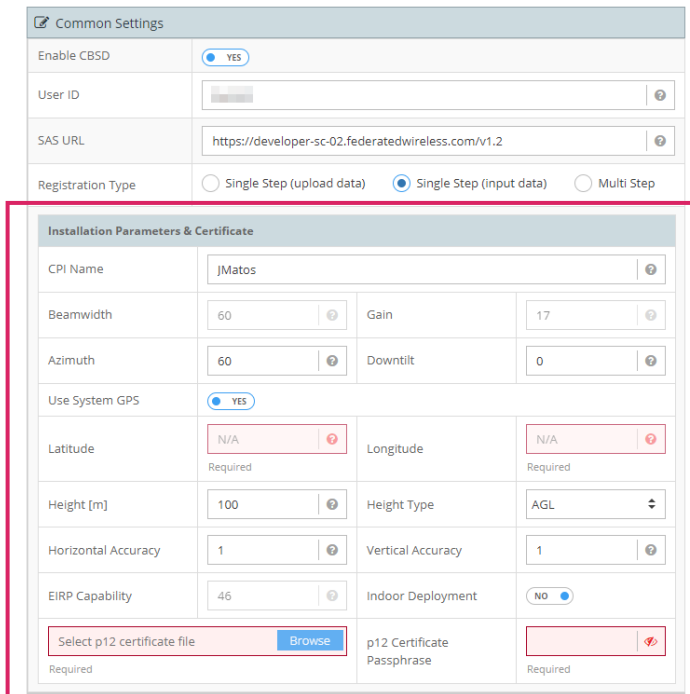
- Click on the top field and select the appropriate unit from the drop-down menu.

- Enter the rest of the installation parameters.
- Upload the CPI certificate and enter the password required to read CPI certificate.

- Click on “**Generate**”. This will create the CPI signed data file ([MXF-WLTGG12248H_<CPE CBSID> .txt](#)) in the same folder where the program is located.
- On the WebUI, click on “**Browse**” to locate the CPI signed data file.



- Select the desired file and click on “+ Apply”.
- **Single Step (Input Data):** When this option is selected, a new section will appear, allowing users to input the eNB’s data that is needed for CBSD SAS registration.



- Fill in or update the fields in this section (**Installation Parameters & Certificate**). Take note that the **Latitude**, **Longitude**, **p12 certificate file** and the **p12 Certificate Passphrase** are required.
- The p12 certificate will be used for certification purposes and will not be stored in the eNB.
- **Multi Step:** For Multi Step registration, installation parameters need to be configured in the SAS portal before configuring on the WebUI.
- Select **Commit** in the top right corner to save the changes on this page or select the **Refresh** (🔄) button to cancel and return to the previous settings.



NOTE: Please ensure that the **Registration Type** is consistent on both the WebUI here as well as on the SAS Portal. For example, if multi step registration is already done on the SAS portal, select **Multi Step** on the WebUI instead of **Single Step**.

6.7.2. Device Parameters

This section shows the **FCC ID** of the eNB as well as its CBSD **Device Category**.

The CBSD status of each cell can also be seen in this section, showing the **CBSDDID** for each cell along with its configured **Antenna** (See Section 6.3.3).

Device Parameters				
FCC ID	ROR00000008			
Device Category	B			
Cell	Antenna	Initial CBSDSN	Standby Grant	Standby Grant Alarm
0	Internal-B0	OCA1380009BA0	Promote	Clear
1	Internal-B0	OCA1380009BA1	Promote	Clear
2	Internal-B0	OCA1380009BA2	Promote	Clear

6.7.2.1. Standby Grant and Standby Grant Alarm

With SW 4.0 onwards, the eNB will notify the operator if the standby grant is better than currently used active grant. This feature will only be activated when “**Multi-Grant**” option is turned on under CBSD Advanced Option (Section 6.7.3.3)

Given that promoting standby grant to active grant requires re-registering of the eNB, it needs to be approved by the operator. Therefore, an alarm (Major) will be raised, specifying the cell that is affected.

Cell	Antenna	Initial CBSDSN	Standby Grant	Standby Grant Alarm
0	Internal-B0	OCA1380009BA0	Promote	Clear
1	Internal-B0	OCA1380009BA1	Promote	Clear
2	Internal-B0	OCA1380009BA2	Promote	Clear

“**Promote**” buttons on the Standby Grant column will be enabled when the **standby grant is better than the active grant for the specific cell.**

- To promote the standby grant to active grant, simply click on the “**Promote**” button.
- The “**Promote**” button will then be greyed out when the standby grant has been promoted.

Cell	Antenna	Initial CBSDSN	Standby Grant	Standby Grant Alarm
0	Internal-B0	OCA1380009BA0	Promote	Clear
1	Internal-B0	OCA1380009BA1	Promote	Clear
2	Internal-B0	OCA1380009BA2	Promote	Clear

“Clear” buttons will be enabled when the Standby Grant Alarm is raised.

- Click on the “Clear” button to clear the alarm. If the standby grant is not promoted, the “Promote” button will remain enabled.
- When the standby grant is no longer better than the active grant, the alarm will automatically be cleared.

6.7.3. Advanced Option

Clicking on the “Show Advanced” button will reveal the following parameters:

- Full Spectrum Request
- Measurement Capability
- Persistent Grant and Multi-grant options
- Heartbeat Intervals, TX Expire Buffer Time and TCP Keepalive
- Granted Power Alarm Trigger

CBSD Settings ↻ Commit

Common Settings

Enable CBSD NO

User ID

SAS URL

Registration Type Single Step (upload data) Single Step (input data) Multi Step

Device Parameters

FCC ID: ROR00000008

Device Category: B

Cell	Antenna	Initial CBSDSN	Standby Grant	Standby Grant Alarm
0	Internal-B0	OCA1380009BA0	Promote	Clear
1	Internal-B0	OCA1380009BA1	Promote	Clear
2	Internal-B0	OCA1380009BA2	Promote	Clear

Show Advanced

CBSD Advanced Parameters

Full Spectrum Request YES

Measurement Capability 0 Measurement Capability 1

Persistent Grant YES Multi-grant YES

Heartbeat Interval [s] TX Expire Buffer Time [s]

TCP Keepalive YES

TCP Keepalive Idle Time [s] TCP Keepalive Interval [s]

Granted Power Alarm Trigger

Reset Advanced

6.7.3.1. Full Spectrum Request

Use the toggle button to turn **Full Spectrum Request** on (YES) or off (NO).



CBSD Advanced Parameters	
Full Spectrum Request	<input checked="" type="radio"/> YES
Measurement Capability 0	Select Meas Cap
Persistent Grant	<input checked="" type="radio"/> YES

When full spectrum request is **ON** (TRUE) the CBSD asks SAS for all the available channels. The eNB considers the channel with maximum allowed power to be the best one; if there are multiple channels available with the maximum allowed power, the eNB will use the channel where it detected the least amount of interference. This feature is set on **ON** by default.

CBSD Advanced Parameters	
Full Spectrum Request	<input type="radio"/> NO
Measurement Capability 0	Select Meas Cap
Persistent Grant	<input checked="" type="radio"/> YES

When full spectrum request is OFF (toggle button to **NO**) the CBSD requests for the carrier frequency that is configured under **Carriers** section (See Section 6.3.3). CBSD will only start to transmit when it receives an authorized grant.

6.7.3.2. Measurement Capability

The SAS may ask the CBSD (the FW-600 in this case) to measure the power it is receiving from other devices in the field, so that SAS can input that in its algorithm when figuring out what frequency to give to CBSDs in that area. The options in this field are:

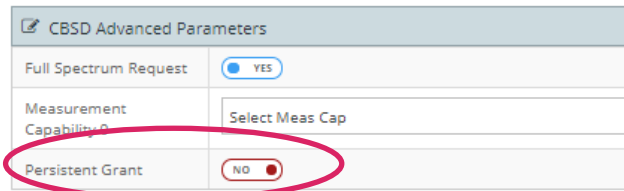
- **Power with Grant:** The eNB will measure power while transmitting.
- **Power without Grant:** The eNB will measure power when it is not authorized to transmit.

At the time of the release of this document, SAS vendors do not support this feature on their end. Therefore, please do not configure **Measurement Capability 0** and **Measurement Capability 1**.

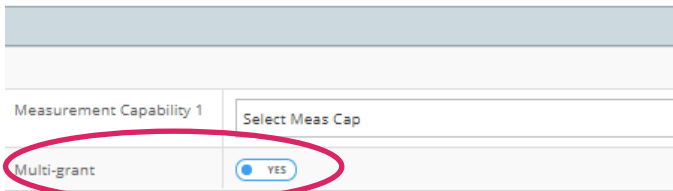
6.7.3.3. Persistent Grant and Multi-Grant

CBSD Advanced Parameters	
Full Spectrum Request	<input type="radio"/> NO
Measurement Capability 0	Select Meas Cap
Persistent Grant	<input checked="" type="radio"/> YES

When **Persistent Grant** is turned **ON** (toggle button to **YES**), the eNB will retain its grant and does not deregister during a reboot. In other words, if the eNB is registered prior to a reboot (be it power failure or a reboot request), it will remain registered after the reboot. If the eNB was authorized before reboot, after reboot the eNB will verify if the authorization is still valid, and if it is, the eNB will continue to transmit.



When the **Persistent Grant** feature is turned OFF (toggle button to **NO**), the eNB will require a re-registration after a reboot.

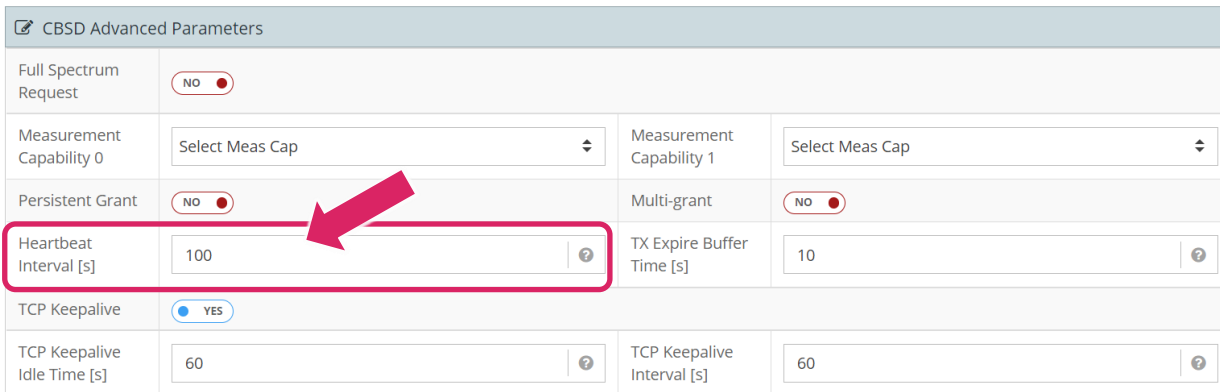


The **Multi-Grant** feature ensures that the eNB will have at least two grants configured before start-up, and request for different frequency ranges that are not overlapped. Therefore, in the event of a grant suspension, the suspension time will be reduced as the eNB will switch to the frequency of the secondary grant for transmission. In the meantime, it will also continue to pursue the primary grant for authorization.

6.7.3.4. Heartbeat Interval

The **Heartbeat Interval** feature allows users to define the preferred interval value which may be adopted by eNB depending on the reference interval value from SAS. After received the first heartbeat response, the eNB compares the interval from SAS response with the configured interval and selects the shorter interval as the final heartbeat interval.

The default interval is set at 100s.



6.7.3.5. TX Expire Buffer Time

The **Tx Expire Buffer Time** is the amount of time guaranteed between next heartbeat request sending time and RF Tx expire time. The buffer time is to counter the system time drift.

The buffer time interacts with heartbeat interval and takes precedence if it is configured longer. For example, given RF Tx expire time is 220s, the final heartbeat interval is 200s, then the time difference between next heartbeat and Tx timer timeout is 20s. If buffer time is set to 40s, the heartbeat interval will be shortened to 180s.

By default, the buffer time on the software is set to 10s.

CBSD Advanced Parameters			
Full Spectrum Request	<input type="radio"/> NO		
Measurement Capability 0	Select Meas Cap	Measurement Capability 1	Select Meas Cap
Persistent Grant	<input type="radio"/> NO		
Heartbeat Interval [s]	100	TX Expire Buffer Time [s]	10
TCP Keepalive	<input checked="" type="radio"/> YES		
TCP Keepalive Idle Time [s]	60	TCP Keepalive Interval [s]	60

6.7.3.6. TCP Keepalive

The **TCP Keepalive** is the message sent from one device to another to prevent the TCP session being broken. In most cases, after TCP session being established, it stays in connected state forever. However, if there is any NAT gateway or firewall in between, due to the limited resources on those intermediate devices, the session may be disconnected after certain amount of time if there is no traffic detected.

The TCP keepalive has two timers, idle and interval. The idle timer is to tell TCP state machine after how long time no traffic the session can be deemed as inactive. The interval timer is to tell TCP state machine how often the keepalive message shall be sent out if session is in an idle state.

To turn this feature on, simply toggle the **TCP Keepalive** button to “YES” and configure the desired **TCP Keepalive Idle Time** and the **TCP Keepalive Interval time**.

CBSD Advanced Parameters			
Full Spectrum Request	<input type="radio"/> NO		
Measurement Capability 0	Select Meas Cap	Measurement Capability 1	Select Meas Cap
Persistent Grant	<input type="radio"/> NO		
Heartbeat Interval [s]	100	TX Expire Buffer Time [s]	10
TCP Keepalive	<input checked="" type="radio"/> YES		
TCP Keepalive Idle Time [s]	60	TCP Keepalive Interval [s]	60

6.7.3.7. Granted Power Alarm Trigger

This feature generates an alarm and SNMP trap whenever a CBSD agent receives a grant with EIRP lower than the maximum EIRP it supports and decides to use it. This is available from SW 4.0.2 onwards.

By default, an alarm will be triggered if the granted power is lower than the maximum power supported.

TCP Keepalive Idle Time [s]	60	TCP Keepalive Interval [s]	60
Granted Power Alarm Trigger	Granted power < maximum power eNB supports Granted power < maximum power eNB supports Granted power < configured alarm threshold		
<input type="button" value="Reset Advanced"/>			

In addition, if the EIRP is needed to be lower than the maximum power, the alarm can be set with a configured threshold.

- Select **“Granted power < configured alarm threshold”**
- Set the **Grant Power Alarm Threshold**

TCP Keepalive	<input checked="" type="radio"/> YES		
TCP Keepalive Idle Time [s]	60	TCP Keepalive Interval [s]	60
Granted Power Alarm Trigger	Granted power < configured alarm threshold	Granted Power Alarm Threshold	0

6.8. Management

Under Management, configure the following items:

- SSH/Web Users
- IP Connectivity Whitelist
- Syslog
- KPI Reporting
- SNMP

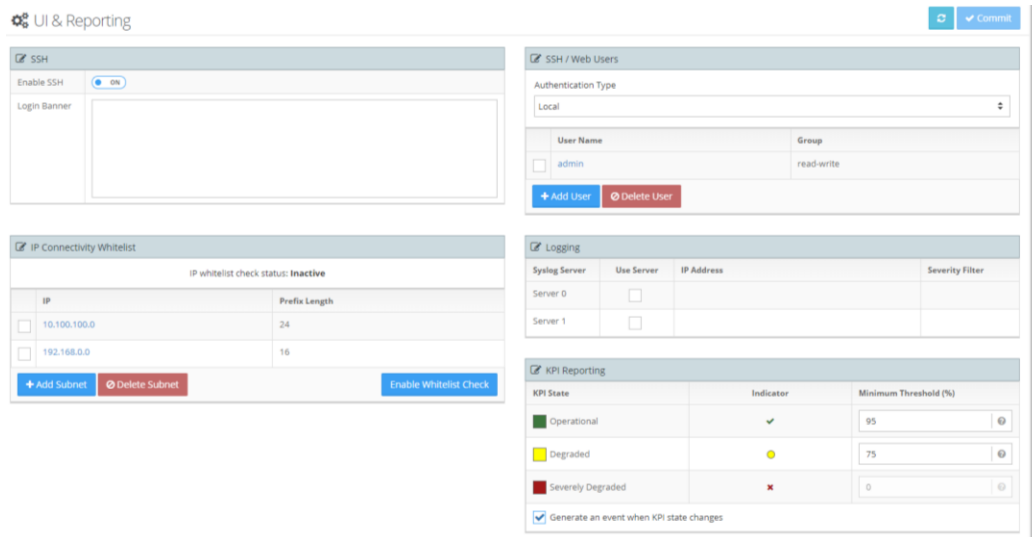
6.8.1. UI & Reporting

Configure Usernames and syslog servers in this section of the WebUI.

6.8.1.1. SSH/Web Users

Configure the Username, password, and access level for the local security of each unit in this section. The **SSH/Web Users** feature allows you to add, modify (update password and read/write privileges level) or delete system users from the FW-600 WebUI. Each unit’s configuration database stores the user configuration data locally.

In addition, the FW-600 is also able to reach out to external AAA server and authenticate username and password. RADIUS and TACACS+ servers are supported.



To add users to (or modify an existing user on) the system using the FW-600 WebUI:

- Navigate to the **Setup > Management > UI & Reporting** page of the FW-600 WebUI.
- Select the **Add User** button to add a user in the **SSH / Web Users** section. An **Add User** dialog box appears.

- From the **Add User** dialog box, you can enter a username, password and choose the access level of that user (**Group**) -- either **Read Only** or **Read Write**.
- When all the fields have been entered, click on “+ Add User” to add the new credentials.

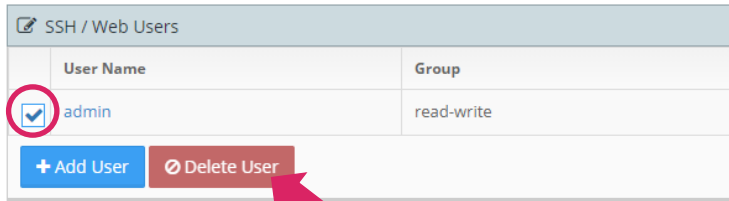


NOTES:

- Usernames must start with a letter and may be composed of alphanumeric characters only.
- Passwords are case sensitive, may be composed of alphanumeric characters including special characters and must contain at least one (1) letter and one (1) digit.
- At least **one user with read/write privileges** needs to exist in the FW-600 system.
- The system will lock out specific user after 6 unsuccessful login attempts.
- You can edit existing FW-600 users by selecting the hyperlinked name of the user you want to modify. The **Update User** dialog box appears.

- To reset a password, type in the new password and select the **Update User** button to confirm the new password. Inform the user of the new password.
- You can also adjust the user’s access level – either **Read Only** or **Read Write**.
- To change a username, **you must delete this user and create the user under a new name.**

- To delete a user: select the check box beside the user that you want to delete. Select the **Delete User** button. The selected user's **Username** disappears from the list.



NOTE: If you cannot login due to a forgotten username or password, contact another user with read/write access privileges to have them reset your login credentials. You can also refer to the *eNB Password Recovery Guide* for more information.

- For any of the actions, select **Commit** for the changes to save your changes or **Cancel** to abandon this action.

Using AAA Server(s):

User credentials have to be created on the RADIUS or TACACS+ server prior to using it on the eNB. Please refer to your RADIUS or TACACS+ server guides for more details.

To use an external RADIUS or TACACS+ server on the eNB:

- Navigate to the **Setup > Management > UI & Reporting** page of the FW-600 WebUI.
- In the **SSH / Web Users** section, click on the drop-down menu for Authentication Type to select one of the options – **Local**, **RADIUS with fallback to Local** or **TACACS+ with fallback to Local**
- Once the **Authentication Type** is selected, click on “**Commit**” to apply the changes. A new section will appear on the page for further configuration based on the selection made.



RADIUS Server Configuration

TACACS+ Configuration

Timeout:

Retries:

TACACS+ Server	Use Server	IP Address	Port	Key
Server 0	<input type="checkbox"/>			
Server 1	<input type="checkbox"/>			

TACACS+ Server Configuration

- Enter the **Timeout** value (in seconds) as well as the number of **Retries** before the system falls back to the Local server for authentication.
- You can configure up to 2 external servers. Check the box under **Use Server** to enable the server.
- Enter the server’s **IP Address**, **Port** and the encryption **Key**.
- Select **Commit** to save the changes or **Cancel** to abandon the change.



NOTE: Please note that Server 0 will always be the primary server and Server 1 will be the secondary. This means that the eNB will always try to reach Server 0 first before trying Server 1.

6.8.1.2. IP Connectivity Whitelist

IP Connectivity Whitelist

IP whitelist check status: **Inactive**

	IP	Prefix Length
<input type="checkbox"/>	10.100.100.0	24
<input type="checkbox"/>	192.168.0.0	16

[+ Add Subnet](#)
[Delete Subnet](#)
[Enable Whitelist Check](#)

This feature would allow the operator to limit the IP addresses that can access the eNB for management purposes. If the IP address is not in the Whitelist, access to HTTPS and SSH will not be allowed.

In this section, it will state if the IP Whitelist check is currently enabled or disabled.

- **IP Whitelist check status: Inactive** → Whitelist is not enabled
- **IP Whitelist check status: Active** → Whitelist is enabled

All the subnets listed will be used in the Whitelist check when it is enabled.

To add new subnet:

- Click on the **“Add Subnet”** button. A new window will pop up.

- Enter the **IP** for the subnet along with the **Prefix Length**.
- Click on **“Add Subnet”** to add the new IP onto the list.
- This list only applies to WAN management IP addresses.
- Reboot is not required for the Whitelist to be enabled. However, once the changes are done, please remember to click on **“Commit”** for all the changes to be applied.

To delete a subnet from the list:

- Click on the check box(es) of the IP(s) to be deleted.

IP	Prefix Length
<input checked="" type="checkbox"/> 10.100.100.0	24
<input type="checkbox"/> 192.168.0.0	16

- Click on the **“Delete Subnet”** once the IP(s) have been selected.
- This will remove the selected IP subnet(s).



NOTE: An empty Whitelist is not allowed by system configuration. To enable Whitelist functionality, **at least one subnet must be provided.**

6.8.2. Syslog

The syslog interface allows the FW-600 system to send standard syslog fault management information (that is, syslog alarms, events and log entries) to external syslog servers.

On the **Setup > Management > UI & Reporting** page, you can set or change their operational status.

6.8.2.1. Using/Editing Syslog Server

- Navigate to the **Management > UI & Reporting** page.
- Select the server you wish to use in the **Logging** section.

Logging			
Syslog Server	Use Server	IP Address	Severity Filter
Server 0	<input checked="" type="checkbox"/>	<input type="text" value=""/>	Info
Server 1	<input type="checkbox"/>		

- Enter either an IPv4 or an IPv6 address in the **IP Address** field.
- Select a **Severity Filter** by using the drop-down list to set the type of information collected.

Logging			
Syslog Server	Use Server	IP Address	Severity Filter
Server 0	<input checked="" type="checkbox"/>	<input type="text" value="192.168.5.102"/>	Info
Server 1	<input type="checkbox"/>		

- Select the **Commit** button at the top of the screen to save your changes.

6.8.2.2. Delete a Syslog Server

- Navigate to the **Management > UI & Reporting** page.
- From the **Logging** section, uncheck the box next to the syslog server that you want to delete.

Logging			
Syslog Server	Use Server	IP Address	Severity Filter
Server 0	<input checked="" type="checkbox"/>	<input type="text" value="192.168.5.102"/>	Debug
Server 1	<input type="checkbox"/>		

- Select the **Commit** button at the top of the screen to save your changes.
- The syslog server would then be deleted

6.8.3. KPI Reporting

This section allows you to set up custom thresholds for your reporting/analysis/monitoring purposes.

- Go to **Management > UI Reporting > KPI Reporting**

KPI State	Indicator	Minimum Threshold (%)
Operational	✓	95
Degraded	●	75
Severely Degraded	✗	0

Generate an event when KPI state changes

- Set up the **Minimum Threshold** (in percentage) for each of the three **KPI State** – **Operational**, **Degraded** and **Severely Degraded**.
- Check the box at the bottom if you wish to generate an event when the **KPI State** changes. For example, an event will then be generated if the unit’s performance changed from **Degraded** to **Operational**.

6.8.4. SNMP

The Simple Network Management Protocol (SNMP) feature allows you to add, delete or edit SNMPv2c users and hosts. These interfaces provide complete access to configuration, state, performance and fault information in the FW-600 system.

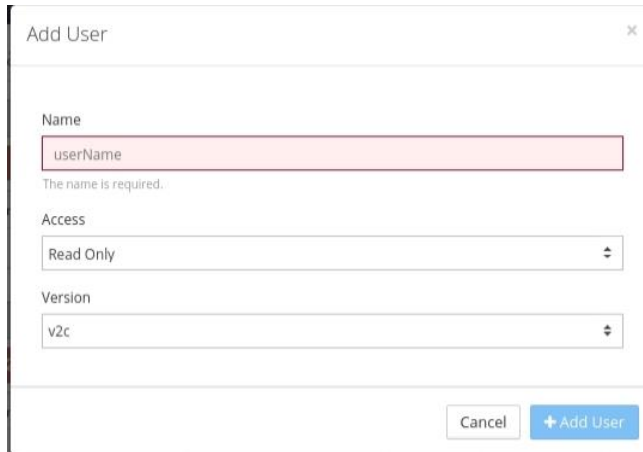
The WebUI SNMP page allows you to set up Simple Network Management Protocol (SNMP) users and host servers, plus add, edit and remove SNMP users and host servers.

6.8.4.1. Add or Remove SNMP User

To add or remove an SNMP user:

- Access the **Management > SNMP** page.

- To add an SNMP user: select the **Add User** button under the **SNMP Users** section. An **Add User** dialog appears. Input the name of the user in the **Name** field. Use the **Access** option to designate the user access level by selecting either the **Read Only** or **Read Write** option.



- **Version** refers to the security protocol level for that user: **v2c** (default). Please use only **v2c** as BLiNQ does not support **v3** as of now.
- Select the **Add User** button to add your user or the **Cancel** button to abandon the addition.
- If you need to edit an existing user, select the hyperlinked name of the desired user, an **Update User** dialog appears. When you finish your edits, select the **Update User** button to save your changes or **Cancel** to abandon these changes.



NOTE: You cannot change the name field. If you do need to change the username, delete that user and repeat the above steps with a new name.

- To remove an SNMP user: select the check box beside the user you want to delete. Select the **Delete User** button. The user disappears from the list.
- Select the **Commit** button at the top of the screen to save your changes.
- If this is your last change/update, reboot the system to activate all of your saved changes, by selecting the **Reboot System** button (🔄) in the top right corner.

6.8.4.2. Add or Remove SNMP Host

To add or remove an SNMP host:

- Access the **Management > SNMP > SNMP Hosts** area.
- To add an SNMP host: select the **Add Server** button. An **Add Server** dialog appears. You need to know the **Name**, **IP Address** and **Port** for your SNMP host.



- **Version** refers to the security protocol level for that host. Select either **v1** (default) or **v2**. BLiNQ does not support **v3** protocol as of now.
- Select the **Add Server** button to add your server or the **Cancel** button to abandon this addition.

- If you need to edit an existing SNMP host, select the hyperlinked name of the desired host, an Update Server dialog will appear. When you finish your edits, select the **Update Server** button to save your changes or **Cancel** to abandon these changes.



NOTE: If you need to change the **Host Name**, delete that host and repeat the above steps with a new name.

- To remove an SNMP host: select the check box beside the host you want to delete. Select the **Delete Server** button. The host disappears from the list.
- Select the **Commit** button at the top of the screen to save your changes.
- If this is your last change/update, reboot the system to activate all of your saved changes, by selecting the **Reboot System** button (🔄) in the top right corner.



6.9. Verify, Save & Activate Current Running Configuration

Before exiting from the pre-configuration setup:


- Verify that the currently running configuration meets all the configuration system setup requirements. If the configuration matches the expected configuration, you **must** save the currently running configuration to the start-up configuration. This ensures that any changes are saved after a reboot. To activate and see your configuration changes, reboot the system.

6.9.1. Verify and Save Running Configuration

To verify and save the currently running configuration:

- Verify the currently running configuration to ensure that it matches the expected configuration. For instance, check that the EARFCN or radio frequencies match on the FW-600 and CPE.

Select the **Commit** button at the top of the screen to save your changes.

Reboot the system to activate all your saved changes, by selecting the **Reboot System** button  in the top right corner.

7. Operation and Maintenance

This section contains the following additional FW-600 operation and maintenance features:

- Software Upgrade
- Performance monitoring statistics for:
 - eNB
 - CPE
 - Trace Log Files
 - Measurements (per Beam)
- Fault management via the Events:
 - Alarms page
 - Events history

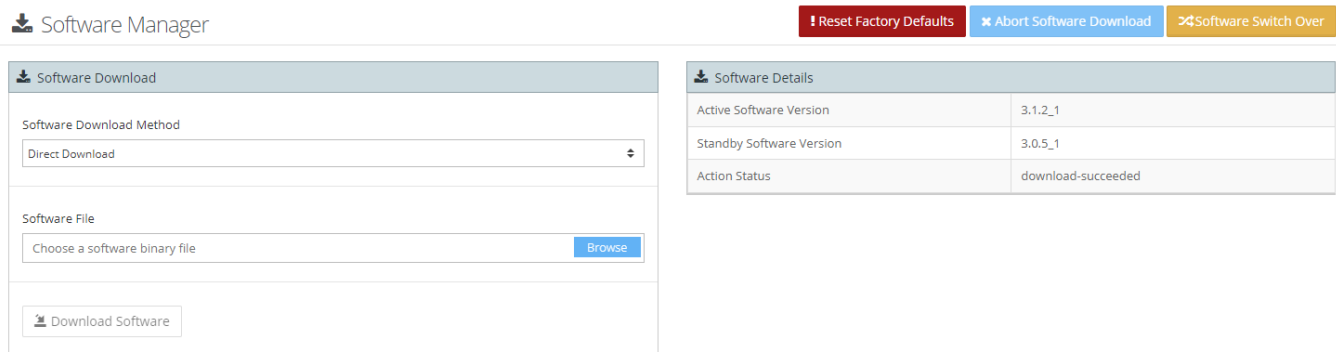
7.1. Administration

Under “**Administration**”, you can manage the following:

- Software Version
- Download SAS Certificate
- Download IPSec Certificate
- Generate/Restore from Configuration backup files

7.1.1. Software Manager

To perform system software upgrade activities, you must have read-write privileges to access this functionality.



The screenshot shows the 'Software Manager' interface. At the top right, there are three buttons: 'Reset Factory Defaults' (red), 'Abort Software Download' (blue), and 'Software Switch Over' (orange). Below these are two main panels:

- Software Download:** Contains a 'Software Download Method' dropdown menu set to 'Direct Download', a 'Software File' section with a 'Choose a software binary file' input and a 'Browse' button, and a 'Download Software' button at the bottom.
- Software Details:** A table showing the current software status.

Software Details	
Active Software Version	3.1.2_1
Standby Software Version	3.0.5_1
Action Status	download-succeeded

The read-only **Software Details** area informs you of the device’s currently running software (active), the available standby software and the current upgrade status.

Software Details	
Active Software Version	3.1.2_1
Standby Software Version	3.0.5_1
Action Status	download-succeeded



NOTE: The running software version can also be seen from the Dashboard when you first log into the WebUI.

7.1.1.1. Reset Factory Defaults

There is a red **!Reset Factory Defaults** button at the top of the page.



ONLY USE the **!Reset Factory Defaults** button, when you want to return all of the configuration settings to the factory defaults. You must have read-write privileges to access this button.

When you select the **!Reset Factory Defaults** button, the Login screen appears.

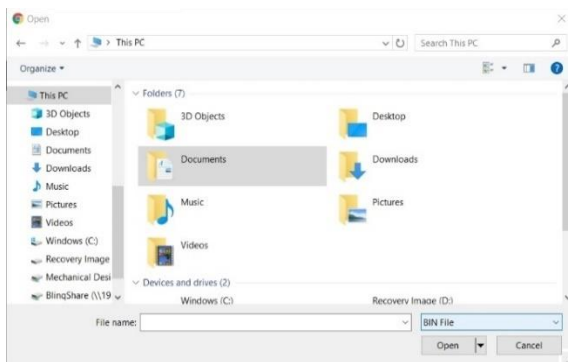
All configurations will return to their factory default values.

7.1.1.2. System Software Upgrade

Software upgrades occur either from an FTP server, SFTP server or from your hard disk. To upgrade the software, do the following:

- Navigate to the **Administration > Software Manager** in the FW-600 WebUI.
- Within the **Software Download** area, from the **Software Download Method**, select **Direct Download, FTP or sFTP**
 - **Direct Download** (for software files located on your hard drive or available network drive)
 - Select the **Browse** button under **Software File**.

- Browse for the binary file to be used for the upgrade from the **File Manager** window that appears. Click **“Open”**.



- The file name should appear in the **Software File**. Click on **Download Software** to download the software.

▪ **FTP or sFTP:**

- Enter the details (**Host Address (IPv4 or IPv6), Username, Password and File Path**) to locate the file.

- After choosing your upgrade file, select the **Download Software** button bottom of the **Software Download** area. A progress bar will appear.

Software Download in Progress

Do not refresh or close the browsers while software download is in progress.

Status: Downloading software binary...

Abort Download

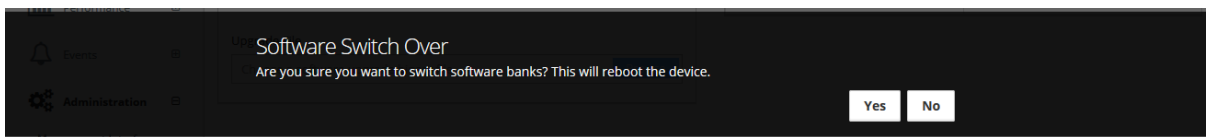
- A green status message at the top of the page will indicate if the software download succeeds.
- The **Standby Software Version** field then shows the new software load version.

Software Details	
Active Software Version	3.0.5_1
Standby Software Version	3.1.2_1
Action Status	download-succeeded

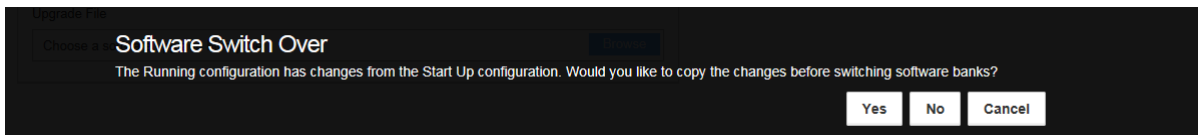
To load the standby software:

- Select the **Software Switch Over** button at the top of the page.

- A **Software Switch Over** query window appears. Select the **Yes** button at the prompt. The system restarts using the new software image. If the banner at the top indicates that this was successful, you have finished this software upgrade procedure. Select the **No** button if you want to abandon this update.



- If there is a difference between the currently running configuration and the saved configuration, a different query window appears. Select **Yes** to save your configuration changes and continue with the switch over or **No** to continue with the software switch over and lose your configuration changes. You can select **Cancel** to stop the switch over completely, for instance to verify the configuration changes.

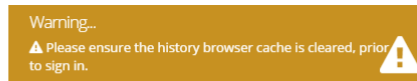


- If the software upgrade fails (for example, due to a corrupt load), the banner at the top of the page indicates the upgrade was unsuccessful. The system tries three (3) times to restart with the new software version; if the software upgrade attempts fail, the system reverts to the previous software version. In this case, select a different version of the new software and repeat this procedure from the beginning.



NOTES:

- **You can only upgrade the FW-600 system software from one active browser session.** This means you cannot open another browser session and start another upgrade process in parallel with the first. If you try this, you get a warning message, and the system does not let you continue. Furthermore, do not close the browser once you start the upgrade; if you do or if your computer crashes, you must reset the FW-600 system that was being upgraded and start the upgrade process over.
- To ensure a fresh installation, after switching over to new software, please clear your browser history cache before launching a new WebUI session.



WebUI Sign In

Username

Password

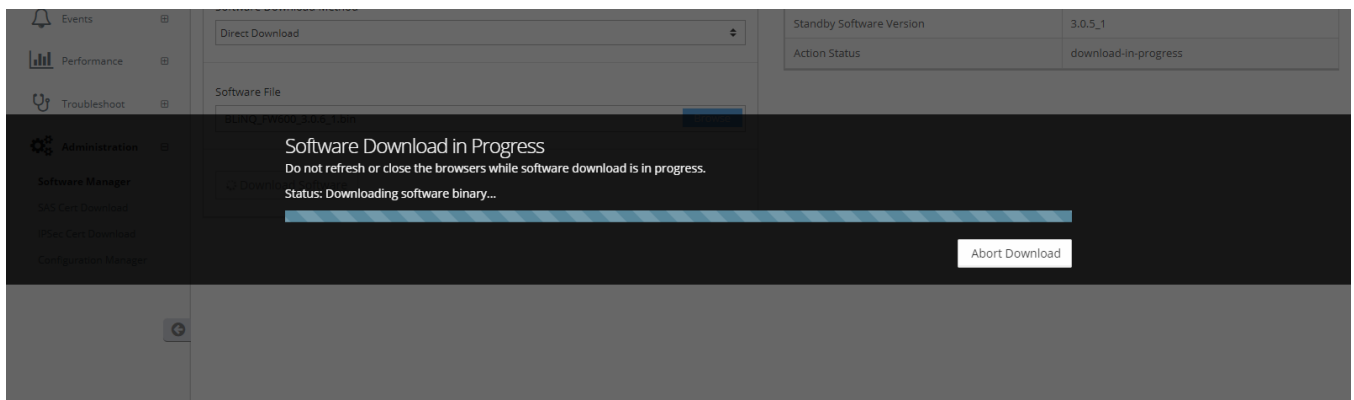
[Sign In](#)

7.1.1.3. Aborting Software Download

Software download can be aborted while the system is downloading the file.

To abort SW download:

- When a SW download has been triggered, a “**Software Download in Progress**” bar will appear.



- Click on the “**Abort Download**” button that is on the bar to abort the download process.
- A red error status message will appear at the top right corner of the page, stating that the download has been aborted.



NOTE: Another way to abort the software download is to open another tab on the browser, login to the eNB and navigate to **Administration > Software Manager**. Under **“Software Details”**, Action Status should display **“Download in Progress”**. Click on the blue **“x Abort Software Download”** button on the top of the page. Download will then be terminated.

7.1.2. SAS Cert Download

To successfully authenticate and establish a TLS connection with the SAS server – CBSD SAS certificate must be installed on the unit. CBSD SAS certificates are generated using the MAC address of the CBSD device and the file format would look like *CBSD-0CA1380004E2-insta_rsa.certs.tgz*



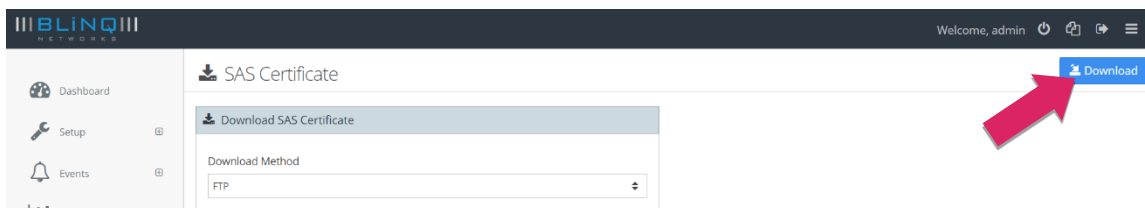
NOTE: Certificate package is installed at factory and no operator action is required by default. The operator would need to upload new certificate only in rare scenario (e.g. certificate becomes corrupted).

You can download SAS Certificate from either from an FTP server or SFTP server.

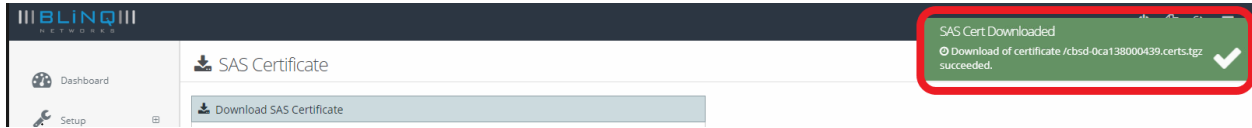
To download the SAS Certificate, do the following:

- Navigate to the **Administration > SAS Cert Download**.
- Within the **Download SAS Certificate** area, select **Download Method: FTP** or **sFTP**
- Enter the details (**Host Address (IPv4 or IPv6)**, **Username**, **Password** and **File Path**)

- Once you have selected the file that you need, click on the **Download** button at the top right of the page.



- A green status window will appear at the top right corner of the WebUI if download is successful.



NOTE: A system reboot is required after the SAS Certificate had been downloaded.

7.1.3. IPSec Cert Download

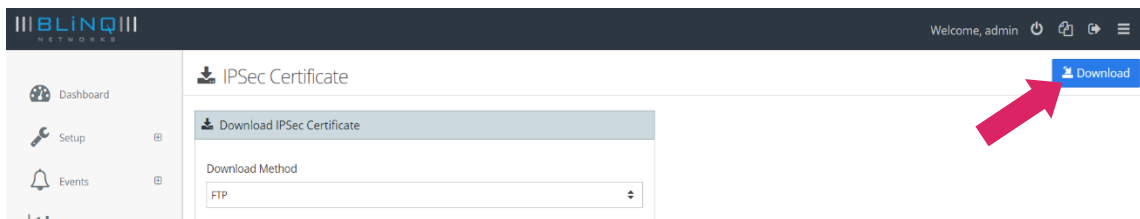


NOTE: IPSec Certificate is needed for communication with Secure Gateway (See Section 6.4.3.2),

You can download IPSec Certificate from either from an FTP server or SFTP server. To download the IPSec Certificate, do the following:

- Navigate to **Administration > SAS Cert Download** in the WebUI.
- Within the **Download IPSec Certificate** area, select **Download Method: FTP** or **sFTP**
- Enter the details (**Host Address (IPv4 or IPv6), Username, Password and File Path**)

- Once you have selected the correct file, click on the **Download** button at the top right of the page.



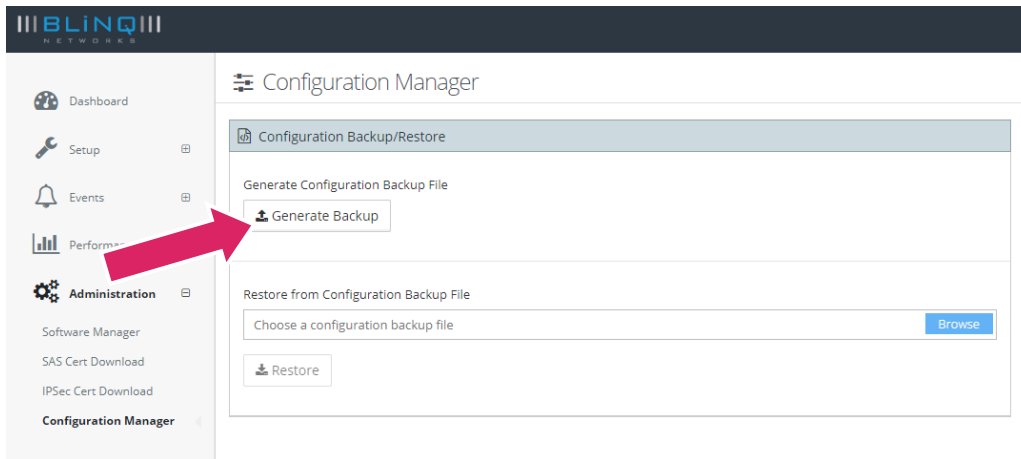
- If download is successful, you will see a green status bar appearing at the top right corner of the WebUI.

7.1.4. Configuration Manager

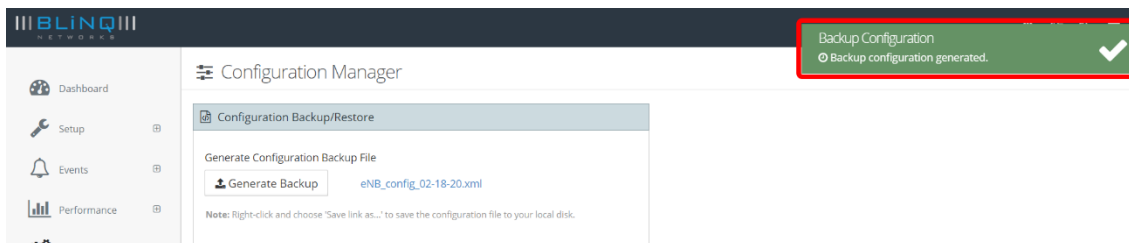
This is the page you can go to **Generate** a **Configuration Backup File** or to **Restore** from a previous **Configuration Backup File**.

To generate a configuration backup file:

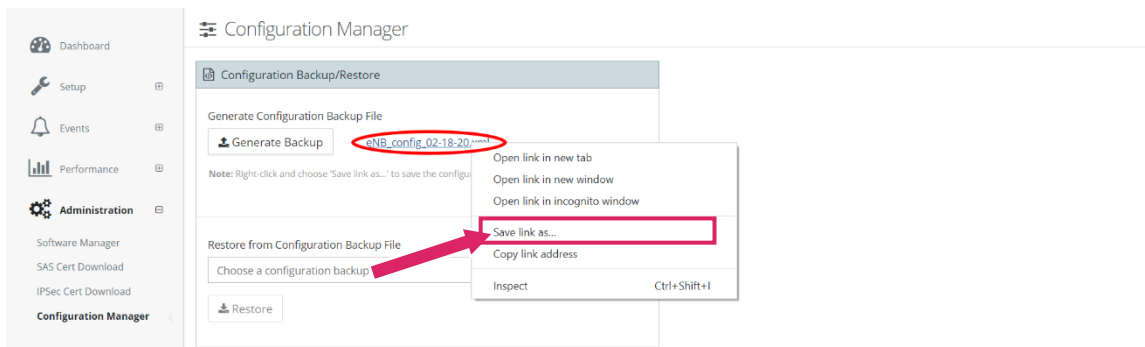
- Navigate to **Administration > Configuration Manager** in the WebUI.
- Within the **Configuration Backup/Restore** section, click on the “**Generate Backup**” button.



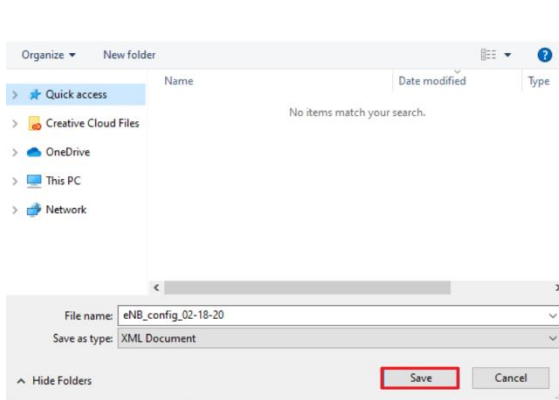
- A green status bar will appear at the top right corner of the WebUI, informing you that the backup file has been successfully generated.



- Right click on the **blue .xml** file link to reveal a popup window. Select “**Save link as...**” to save the configuration file to your local disk.

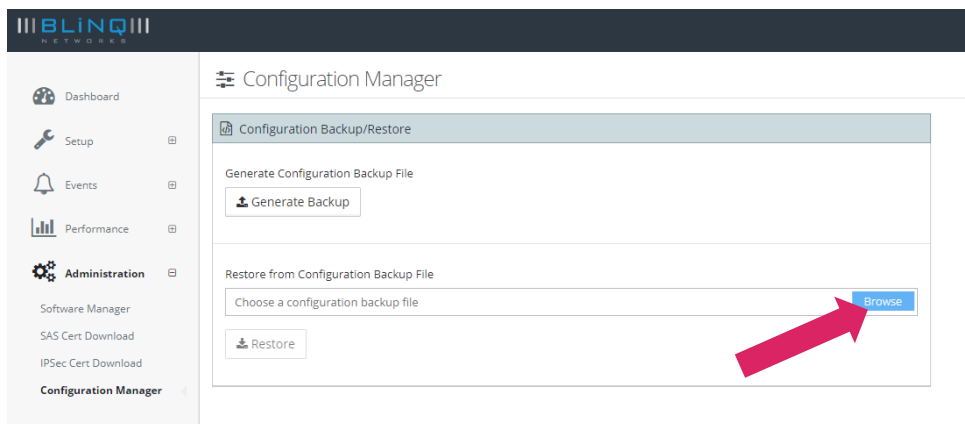


- A **File Manager** window will appear. Choose the location where you want to save the backup file in and click “**Save**”.



To restore from a Configuration Backup file:

- Navigate to **Administration > Configuration Manager** on the WebUI
- Within the **Configuration Backup/Restore** section, click on the “**Browse**” button in the **Restore from Configuration Backup File** field.



- A **File Manager** window will popup. Please select the configuration backup file that you desire and hit the **Restore** button.
- A **green status** message will appear at the top right corner of the page if the restoration has been successful.

7.2. Events

The system events are broken down into two sections:

- Alarms and
- History

7.2.1. Alarms Page

This page lists active alarms (set alarms). Once you clear the Alarm, it appears on the History page along with its details. For a list of alarms, see Appendix E.

Alarms

ID	Alarm ID	Module ID	Alarm Time	Component	Severity	Type	Probable Cause	Description
159	11002	0ca1:38:00:04:46	Sep 24, 2020 2:10:20 AM (UTC-04:00)	Cell#2	Major	Operational-status	Operating-mode	cell#2 has noise (-119.9) above normal level (-120)

Showing 1 to 10 of 1 entries

First 1 Last

Export Refresh

- Use the **Refresh** button to update the information on the screen.
- Use the **Export** button to export the csv file: **active_alarms.csv**

Export Alarms

Alarms exported. Please download from following file:
[active_alarms.csv](#)

OK

- Click on the blue link to download the file.
- The file can be viewed on Excel or other spreadsheet programs.

7.2.2. History Page

The **History** page lists a chronological history of alarms and events along with their details. The most recent events appear first, to view older events use the page buttons or to quickly access the oldest events, use the **Last** button.

There are three different tabs on the page: System, UE and Noise. Click on the desired tab to view the alarms/events categorized under it.



NOTE: For a list of alarms and events see Appendix E.

Event History

System UE Noise

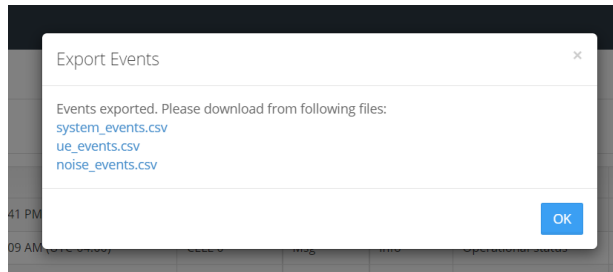
ID	Event ID	Module ID	Event Time	Component	Category	Severity	Type	Probable Cause	Description
16515	8001	0ca1:38:00:04:46	Jul 14, 2022 12:42:41 PM (UTC-04:00)	Security	Msg	Warning	Security-violation	Unauthorized access attempt	Authentication failed for user root
16514	9006	0ca1:38:00:04:46	Jul 14, 2022 12:56:09 AM (UTC-04:00)	CELL 0	Msg	info	Operational-status	Operating-mode	Cell 0 Accessibility state change to Operat
16513	9006	0ca1:38:00:04:46	Jul 14, 2022 12:56:03 AM (UTC-04:00)	CELL 0	Msg	info	Operational-status	Operating-mode	Cell 0 Accessibility state change to Degraded
16512	12009	0ca1:38:00:04:46	Jul 13, 2022 5:07:37 PM (UTC-04:00)	SYSTEM	Msg	info	Operational-status	Operating-mode	Cell 1 add neighbor PCI 98 CELLID 8194 from X2
16511	12009	0ca1:38:00:04:46	Jul 13, 2022 5:07:37 PM (UTC-04:00)	SYSTEM	Msg	info	Operational-status	Operating-mode	Cell 0 add neighbor PCI 98 CELLID 8194 from X2
16510	12009	0ca1:38:00:04:46	Jul 13, 2022 5:07:37 PM (UTC-04:00)	SYSTEM	Msg	info	Operational-status	Operating-mode	Cell 1 add neighbor PCI 97 CELLID 8193 from X2
16509	12009	0ca1:38:00:04:46	Jul 13, 2022 5:07:37 PM (UTC-04:00)	SYSTEM	Msg	info	Operational-status	Operating-mode	Cell 0 add neighbor PCI 97 CELLID 8193 from X2
16508	12009	0ca1:38:00:04:46	Jul 13, 2022 5:07:37 PM (UTC-04:00)	SYSTEM	Msg	info	Operational-status	Operating-mode	Cell 1 add neighbor PCI 96 CELLID 8192 from X2
16507	12009	0ca1:38:00:04:46	Jul 13, 2022 5:07:37 PM (UTC-04:00)	SYSTEM	Msg	info	Operational-status	Operating-mode	Cell 0 add neighbor PCI 96 CELLID 8192 from X2
16506	12010	0ca1:38:00:04:46	Jul 13, 2022 5:07:37 PM (UTC-04:00)	SYSTEM	Msg	info	Operational-status	Operating-mode	Cell 1 remove neighbor PCI 98 CELLID 8194 from X2

Showing 1 to 10 of 1001 entries

First 1 2 3 4 5 Last

Export Clear History Refresh

- Use the **Refresh** button to update the information on the screen.
- **Clear History** completely clears the current alarms and events history from the FW-300i event logging infrastructure.
- Use the **Export** button to export the 3 .csv files: **system_events.csv**, **ue_events.csv**, and **noise_events.csv**.



- Once the events have been exported, click the files to download them onto the computer.
- The file(s) can now be viewed on Excel or other spreadsheet programs.

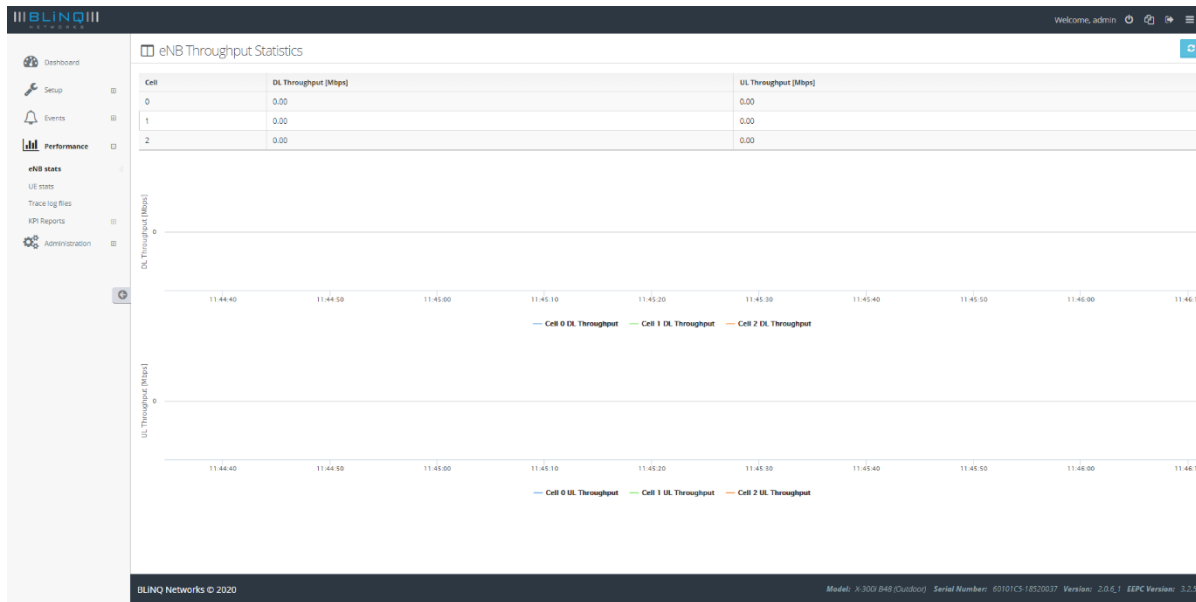
INDEX	MODULE	COMPONENT	EVENT ID	CATEGORY	TYPE	PROBABLE SEVERITY	TIMESTAMP	NOTIFICATION	COMMENT	DATA
1	15515	0c:a1:38:0 CELL 2	9006	msg	operations	operating-info	2022-06-2	466050	Cell 2 Accessibility state change to Operational	
2	15516	0c:a1:38:0 CELL 2	9006	msg	operations	operating-info	2022-06-2	466051	Cell 2 Retainability state change to Operational	
3	15517	0c:a1:38:0 CELL 2	9006	msg	operations	operating-info	2022-06-2	466052	Cell 2 HO Success Rate state change to Operational	
4	15518	0c:a1:38:0 CELL 0	12001	clr	operations	operating-critical	2022-06-2	466053	Sector 0 S1 State enabled	
5	15519	0c:a1:38:0 CELL 1	12001	clr	operations	operating-critical	2022-06-2	466054	Sector 1 S1 State enabled	
6	15520	0c:a1:38:0 CELL 2	12001	clr	operations	operating-critical	2022-06-2	466055	Sector 2 S1 State enabled	
7	15521	0c:a1:38:0 CELL 1	9006	msg	operations	operating-info	2022-06-2	466058	Cell 1 Accessibility state change to Severely Degraded	
8	15522	0c:a1:38:0 CELL 1	9006	msg	operations	operating-info	2022-06-2	466059	Cell 1 Retainability state change to Severely Degraded	
9	15523	0c:a1:38:0 CELL 2	9006	msg	operations	operating-info	2022-06-2	466120	Cell 2 Accessibility state change to Severely Degraded	
10	15524	0c:a1:38:0 CELL 2	9006	msg	operations	operating-info	2022-06-2	466121	Cell 2 Retainability state change to Severely Degraded	
11	15525	0c:a1:38:0 SYSTEM	7021	msg	operations	operating-info	1969-12-3	466297	System startup - reboot by operator	
12	15526	0c:a1:38:0 CELL 0	12001	set	operations	operating-critical	1969-12-3	466298	Sector 0 S1 State disabled	
13	15527	0c:a1:38:0 CELL 1	12001	set	operations	operating-critical	1969-12-3	466299	Sector 1 S1 State disabled	
14	15528	0c:a1:38:0 CELL 2	12001	set	operations	operating-critical	1969-12-3	466300	Sector 2 S1 State disabled	
15	15529	0c:a1:38:0 SYSTEM	12015	msg	operations	operating-info	1969-12-3	466301	Cell 0 add frequency relation EARFCN 55540 source OPER	
16	15530	0c:a1:38:0 SYSTEM	12009	msg	operations	operating-info	1969-12-3	466302	Cell 0 add neighbor PCI 0 CELLID 8192 from OPER	
17	15531	0c:a1:38:0 SYSTEM	12009	msg	operations	operating-info	1969-12-3	466303	Cell 0 add neighbor PCI 94 CELLID 7937 from ANR	
18	15532	0c:a1:38:0 SYSTEM	12009	msg	operations	operating-info	1969-12-3	466304	Cell 0 add neighbor PCI 95 CELLID 7938 from ANR	
19	15533	0c:a1:38:0 SYSTEM	12009	msg	operations	operating-info	1969-12-3	466305	Cell 1 add neighbor PCI 93 CELLID 7936 from ANR	
20	15534	0c:a1:38:0 SYSTEM	12009	msg	operations	operating-info	1969-12-3	466306	Cell 1 add neighbor PCI 95 CELLID 7938 from ANR	
21	15535	0c:a1:38:0 SYSTEM	12009	msg	operations	operating-info	1969-12-3	466307	Cell 2 add neighbor PCI 93 CELLID 7936 from ANR	
22	15536	0c:a1:38:0 SYSTEM	12009	msg	operations	operating-info	1969-12-3	466308	Cell 2 add neighbor PCI 94 CELLID 7937 from ANR	
23	15537	0c:a1:38:0 CELL 0	9006	msg	operations	operating-info	2022-06-2	466309	Cell 0 Accessibility state change to Operational	
24	15538	0c:a1:38:0 CELL 0	9006	msg	operations	operating-info	2022-06-2	466310	Cell 0 Retainability state change to Operational	
25	15539	0c:a1:38:0 CELL 0	9006	msg	operations	operating-info	2022-06-2	466311	Cell 0 HO Success Rate state change to Operational	
26	15540	0c:a1:38:0 CELL 1	9006	msg	operations	operating-info	2022-06-2	466312	Cell 1 Accessibility state change to Operational	
27	15541	0c:a1:38:0 CELL 1	9006	msg	operations	operating-info	2022-06-2	466313	Cell 1 Retainability state change to Operational	
28	15542	0c:a1:38:0 CELL 1	9006	msg	operations	operating-info	2022-06-2	466314	Cell 1 HO Success Rate state change to Operational	
29	system_events									

7.3. Performance

The FW-600 monitors the performance statistics for the eNB and the linked CPE(s).

7.3.1. eNB Statistics Page

The eNodeB Statistics or **eNB stats** page is a read-only page that displays real-time eNB throughput statistics for how the FW-600 and the associated beams have been performing. The system will capture 15 samples in the last 90 seconds and display the information here.



7.3.2. UE Stats Page

The Customer Premise Equipment Statistics or **UE stats** page is a performance read-only page that visualizes the incoming and outgoing traffic for the interface connections between the CPE and the FW-600. This allows you to see traffic and bandwidth usage for the interfaces in real-time and monitor the current download/upload throughput speeds. It also lists the current throughput performance statistics for the interfaces.



NOTE: The screen refresh interval is every 5 seconds

If needed, the **Refresh** button allows you to refresh the data immediately.



UE Statistics

Attach count reset performed 5 days 6 hr 1 min 26 sec ago.

LTE Cell	IMSI	RNTI	Carrier Frequency [MHz]	CC	UL-SINR [dB]	DL-RSRQ [dB]	UL-RSRP [dBm]	DL-RSRP [dBm]	UL-MCS	DL-MCS	UL-BLER [%]	DL-BLER [%]	DL/UL Throughput [Mbps]	Attach Count
1	999995432105000	284	3680	0	28	-8	-92.02	-91	21	27	0.00(0.04)	0.00(0.00)	0.0 / 0.0	4
2	999995432100458	211	3565	0	22	-5.5	-96.7	-95	19	27	0.00(87.65)	0.00(0.26)	0.0 / 0.0	5

Showing 1 to 2 of 2 entries

First 1 Last

Show Advanced

The **UE Statistics** covers:

- **IMSI:** IMSI is used as a unique attribute to identify each SIM card within a CPE
- **RNTI:** Denotes the Radio Network Temporary Identifier (RNTI) of a connected UE
- **Carrier Frequency:** The frequency that the LTE cell is transmitting on
- **CC:** Component Carrier
- **UL-SINR:** Uplink Signal to Interference and Noise Ratio
- **DL-RSRQ:** Downlink Reference Signal Received Quality
- **UL-RSRP:** Uplink Reference Signal Received Power
- **DL-RSRP:** Downlink Reference Signal Received Power
- **UL MCS:** indicates the uplink Modulation and Coding Scheme (MCS)
- **DL MCS:** indicates the downlink Modulation and Coding Scheme (MCS)
- **UL-BLER:** Uplink Block Error Rate – the ratio of the number of erroneous blocks to the total number of blocks transmitted on a digital circuit.
- **DL-BLER:** Downlink Block Error Rate
- **DL/UL Throughput:** Shows the downlink (DL) and uplink (UL) throughput (Tput)
- **Attach Count:** Number of times the CPE connected to the eNB since the eNB started up. From SW 3.0.3 onwards, there is a new “Reset Attach Count” feature that will reset the attach count of the CPE manually without restarting the eNB. Click on the red “Reset Attach Count” button and attach count for all the CPEs will start back at 1.

7.3.2.1. Advanced Option

The **Show Advanced** Option in the **UE Statistics** page show more UE statistics.

LTE Cell	IMSI	UE Tx Power [dBm]	eNB Rx Gain [dB]	CC	PUSCH-SINR [dB]	PUCCH-SINR [dB]	Timing Advance	Erasure	Abnormal Release Count	Failed Attach Count	Connection State
1	999995432105000	23	57	0	27	11	31	0	0	0	IDLE_COMMON_WT
2	999995432100458	23	57	0	31	12	31	0	0	0	IDLE_COMMON_WT

Showing 1 to 2 of 2 entries

First 1 Last



This advanced page covers:

- **IMSI:** IMSI is used as a unique attribute to identify each SIM card within a CPE
- **UE Tx Power:** The strength of the signal that the CPE is producing during transmission.
- **eNB Rx Gain:** Power gain that is received by the eNB.
- **CC:** Carrier Component
- **PUSCH-SINR:** The Signal to Interference plus Noise Ratio reported through Physical Uplink Shared Channel
- **PUCCH-SINR:** The Signal to Interference plus Noise reported through the Physical Uplink Control Channel
- **Timing Advance:** Timing advance is a negative offset, at the UE, between the start of a received downlink subframe and a transmitted uplink subframe. This is the value that the eNB will send to the UE to ensure that downlink and uplink subframes are synchronized at the eNB.
- **Erasure:** Erasure is a flag raised during SRS processing indicating that sounding signal level was below the noise floor. A number of consecutive SRS reports with erasure flag set is the cause of radio link failure (UE disconnection)
- **Abnormal Release Count:** The number of times when the CPE detaches unexpectedly.
- **Failed Attach Count:** The number of times when the CPE fail to attach.
- **Connection State:** UE state of connection to the eNB.

7.3.3. Core Connectivity

The Core Connectivity page shows the status and parameters that the eNB had negotiated with the EPC and other upstream network components.

It contains information relating to **EPC Connectivity**, providing details about the MMEs and SGWs that the eNB is connected to as well as information for **CBRS Connectivity** (if applicable).

Core Connectivity Status



EPC Connectivity			
MME Connectivity			
Cell	Source	Destination	Status
0	10.120.0.15:36412	10.110.0.213:36412	Up
1	10.120.0.15:36413	10.110.0.213:36412	Up
2	10.120.0.15:36414	10.110.0.213:36412	Up
SGW Connectivity			
Cell	Source	Destination	Tunnels
0	10.120.0.15:3386	10.110.0.213:3386	4
1	10.120.0.15:3386	10.110.0.213:3386	17
2	10.120.0.15:3386	10.110.0.213:3386	4

CBRS Connectivity				
SAS Info				
Cell	FCCID-CBSDID	CBSD State	Certificate Status	Valid Until
0	ROR00000005-0CA1380004070	N/A	N/A	N/A
1	ROR00000005-0CA1380004071	N/A	N/A	N/A
2	ROR00000005-0CA1380004072	N/A	N/A	N/A

7.3.4. Network Status

The Network Status page displays the IPv4 and IPv6 **Routing Information**.

It also displays the eNB Ethernet Port statistics and thus allowing the operator/user to perform cable diagnostics easily. The page refreshes every 3 seconds.

Network Status



Routing Information	
IPv4	IPv6
<pre>default via 10.100.0.250 dev eth0.1000 10.100.0.0/24 dev eth0.1000 proto kernel scope link src 10.100.0.27 169.254.1.0/24 dev eth0 proto kernel scope link src 169.254.1.1 169.254.254.0/24 dev eth1 proto kernel scope link src 169.254.254.1</pre>	
Show Route	

Ethernet Statistics																					
! Clear eth0 Counters ! Clear eth1 Counters 🔍 Check eth1 Cable Health ⌵ More Counters																					
Eth	General	Auto-negotiation		Counters	Other																
eth0	State up MAC 0ca:1:38:00:09:ba Media 1000BaseTx Speed 1000Mbps Duplex full	Partner offer N/A Our offer N/A		Last clearing of counters: 0 days, 13 hours, 28 minutes, 44 seconds Total Bytes Receive 13461462 Transmit 270537187 Total Packets 63000 239401																	
eth1	State up MAC 0ca:1:38:00:09:ba Media 1000BaseTx Speed 1000Mbps Duplex full	Partner offer 1000FD, 100FD, 100HD, 10FD, 10HD Our offer 1000FD, 100FD, 100HD, 10FD, 10HD		Last clearing of counters: 0 days, 13 hours, 28 minutes, 44 seconds Total Bytes Receive 635235274 Transmit 3820851328 Total Packets 1741690507 181448034	<table border="1"> <thead> <tr> <th>Pair</th> <th>Cable Length [m]</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td>B</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td>C</td> <td>N/A</td> <td>N/A</td> </tr> <tr> <td>D</td> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Pair	Cable Length [m]	Status	A	N/A	N/A	B	N/A	N/A	C	N/A	N/A	D	N/A	N/A	
Pair	Cable Length [m]	Status																			
A	N/A	N/A																			
B	N/A	N/A																			
C	N/A	N/A																			
D	N/A	N/A																			

7.3.4.1. Routing Information

This section displays the IPv4 and IPv6 routes tables. By default, IPv4 routes will be visible. Click on the tabs to switch between IPv4 and IPv6.

Network Status 🔄

Routing Information

IPv4 | IPv6

```
default via 192.168.32.241 dev eth0
169.254.1.0/24 dev eth0 proto kernel scope link src 169.254.1.1
169.254.254.0/24 dev eth1 proto kernel scope link src 169.254.254.1
192.168.32.0/24 dev eth0 proto kernel scope link src 192.168.32.1
```

[Show Route](#)

To view a specific route or to view all routes:

- Click on **“Show Route”** and a pop-up window will appear.

Show Route ✕

IP Version: Subnet Address:

Required

All Routes: Prefix Length:

Required

[Get Info](#)

[Close](#)

- Select the **IP Version**. Then enter the **Subnet Address** and the **prefix length** of the desired route or toggle the **All Routes** button to **“YES”** to display all routes.
- Click on **“Get Info”** to view the route(s).

7.3.4.2. Ethernet Statistics

! Clear eth0 Counters
! Clear eth1 Counters
🔍 Check eth1 Cable Health
⌵ More Counters

Eth	General	Auto-negotiation	Counters	Other																					
eth0	State: up MAC: 0c:a1:38:00:09:ba Media: 1000BaseTx Speed: 1000Mbps Duplex: full	Partner offer: N/A Our offer: N/A	Last clearing of counters: 0 days, 13 hours, 28 minutes, 44 seconds Total Bytes: <table style="display: inline-table; vertical-align: middle;"><tr><td>Receive</td><td>13461462</td></tr><tr><td>Transmit</td><td>270537187</td></tr></table> Total Packets: <table style="display: inline-table; vertical-align: middle;"><tr><td>63000</td><td>239401</td></tr></table>	Receive	13461462	Transmit	270537187	63000	239401																
Receive	13461462																								
Transmit	270537187																								
63000	239401																								
eth1	State: up MAC: 0c:a1:38:00:09:ba Media: 1000BaseTx Speed: 1000Mbps Duplex: full	Partner offer: 1000FD, 100FD, 100HD, 10FD, 10HD Our offer: 1000FD, 100FD, 100HD, 10FD, 10HD	Last clearing of counters: 0 days, 13 hours, 28 minutes, 44 seconds Total Bytes: <table style="display: inline-table; vertical-align: middle;"><tr><td>Receive</td><td>635235274</td></tr><tr><td>Transmit</td><td>3820851328</td></tr></table> Total Packets: <table style="display: inline-table; vertical-align: middle;"><tr><td>1741690507</td><td>181448034</td></tr></table>	Receive	635235274	Transmit	3820851328	1741690507	181448034	<table border="1" style="font-size: small;"> <thead> <tr> <th>Pair</th> <th>Cable Length [m]</th> <th>Status</th> </tr> </thead> <tbody> <tr><td>A</td><td>N/A</td><td>N/A</td></tr> <tr><td>B</td><td>N/A</td><td>N/A</td></tr> <tr><td>C</td><td>N/A</td><td>N/A</td></tr> <tr><td>D</td><td>N/A</td><td>N/A</td></tr> </tbody> </table>	Pair	Cable Length [m]	Status	A	N/A	N/A	B	N/A	N/A	C	N/A	N/A	D	N/A	N/A
Receive	635235274																								
Transmit	3820851328																								
1741690507	181448034																								
Pair	Cable Length [m]	Status																							
A	N/A	N/A																							
B	N/A	N/A																							
C	N/A	N/A																							
D	N/A	N/A																							

- Click on the **red “! Clear eth0/eth1 Counter”** to reset the counters.

- Use the **yellow** “Check eth1 Cable Health” to check the current state of **eth1**
- To see more counters, click on the **blue** “More Counters” button. This will expand the Counters column, revealing more counters:

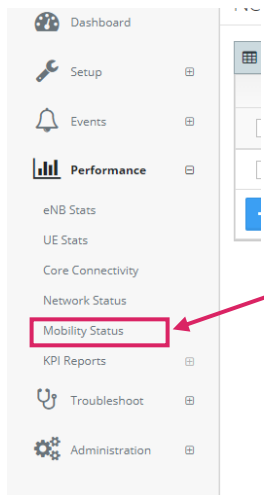
Eth	General	Auto-negotiation	Counters	Other																																																																																										
eth0	State up MAC 0c:a1:38:00:04:07 Media 1000BaseTX Speed 1000Mbps Duplexfull	Partner offer N/A Our offer N/A	<div style="border: 2px solid red; border-radius: 15px; padding: 5px;"> Last clearing of counters: 0 days, 1 hours, 36 minutes, 41 seconds <table border="1"> <thead> <tr> <th></th> <th>Receive</th> <th>Transmit</th> </tr> </thead> <tbody> <tr> <td>Total Bytes</td> <td>478068420</td> <td>120816313</td> </tr> <tr> <td>Total Packets</td> <td>77093521</td> <td>450128</td> </tr> <tr> <td>Unicast Packets</td> <td>77083667</td> <td>436068</td> </tr> <tr> <td>Broadcasts</td> <td>5085</td> <td>2</td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> Multicast</td> <td>4743</td> <td>5</td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> 64-Byte Packets</td> <td>18454</td> <td>4401</td> </tr> <tr> <td> 65-127 Byte</td> <td>28593</td> <td>18938</td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> 128-255 Byte</td> <td>7497</td> <td>302015</td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> 256-511 Byte</td> <td>3995</td> <td>89087</td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> 512-1023 Byte</td> <td>3556</td> <td>3250</td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> 1024-1526 Byte</td> <td>77031426</td> <td>18384</td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> Drop Events</td> <td>66774686</td> <td>0</td> </tr> <tr> <td> Collisions</td> <td></td> <td>0</td> </tr> <tr> <td>Packets with</td> <td></td> <td></td> </tr> <tr> <td> CRC Errors</td> <td>0</td> <td></td> </tr> <tr> <td> Undersized</td> <td>0</td> <td></td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> Oversized</td> <td>0</td> <td></td> </tr> <tr> <td>Packets</td> <td></td> <td></td> </tr> <tr> <td> Packet</td> <td>0</td> <td></td> </tr> <tr> <td> Fragments</td> <td></td> <td></td> </tr> <tr> <td> labbers</td> <td>0</td> <td></td> </tr> </tbody> </table> </div>		Receive	Transmit	Total Bytes	478068420	120816313	Total Packets	77093521	450128	Unicast Packets	77083667	436068	Broadcasts	5085	2	Packets			Multicast	4743	5	Packets			64-Byte Packets	18454	4401	65-127 Byte	28593	18938	Packets			128-255 Byte	7497	302015	Packets			256-511 Byte	3995	89087	Packets			512-1023 Byte	3556	3250	Packets			1024-1526 Byte	77031426	18384	Packets			Drop Events	66774686	0	Collisions		0	Packets with			CRC Errors	0		Undersized	0		Packets			Oversized	0		Packets			Packet	0		Fragments			labbers	0		
	Receive	Transmit																																																																																												
Total Bytes	478068420	120816313																																																																																												
Total Packets	77093521	450128																																																																																												
Unicast Packets	77083667	436068																																																																																												
Broadcasts	5085	2																																																																																												
Packets																																																																																														
Multicast	4743	5																																																																																												
Packets																																																																																														
64-Byte Packets	18454	4401																																																																																												
65-127 Byte	28593	18938																																																																																												
Packets																																																																																														
128-255 Byte	7497	302015																																																																																												
Packets																																																																																														
256-511 Byte	3995	89087																																																																																												
Packets																																																																																														
512-1023 Byte	3556	3250																																																																																												
Packets																																																																																														
1024-1526 Byte	77031426	18384																																																																																												
Packets																																																																																														
Drop Events	66774686	0																																																																																												
Collisions		0																																																																																												
Packets with																																																																																														
CRC Errors	0																																																																																													
Undersized	0																																																																																													
Packets																																																																																														
Oversized	0																																																																																													
Packets																																																																																														
Packet	0																																																																																													
Fragments																																																																																														
labbers	0																																																																																													



NOTE: **eth0** denotes the SFP Port while **eth1** is the RJ45 port.

7.3.5. Mobility Status

For the Mobility status page to appear, Mobility mode needs to be enabled and committed (See Section 6.4.1.5). Reboot the eNB and then the status page will appear under **Performance** on the navigation menu.



This is a read only page that allows users to view the mobility status/overview of the eNB:

Mobility Status



Cell	EARFCN	PCI	PLMN ID	Cell ID	Source	X2 Peer IP	HO Allowed	X2 HO	Blacklisted
0	56440	94	999f99	7937	ANR	-	true	false	false
1	55640	93	999f99	7936	ANR	-	true	false	false

Cell	EARFCN	Source	Neighbor Cells				Blacklisted Cells				
			PLMNID-CellID	PCI	Source	X2 Peer IP	PLMNID-CellID	PCI	Source	X2 Peer IP	
0	55640 (serving cell 0)	OPER									
0	56440	OPER	999f99-7937	94	ANR	-					
1	55640	OPER	999f99-7936	93	ANR	-					
1	56440 (serving cell 1)	OPER									

IP	Port	State	Neighbor Cells		
			PLMNID-CellID	PCI	EARFCN

7.3.6. KPI Reports

Cell x Measurements page, where x represents the cell number, covers Key Performance Indicators (KPI) subcategories: accessibility, retainability, availability and mobility measurements for that cell.

Welcome, admin
⏻ ⌂ ☰

Cell 0 measurements
! Clear Counters
🔄

Accessibility
over 1 days 19 hours 14 min
100%

Retainability
over 1 days 19 hours 14 min
93%

HO Success
over 1 days 19 hours 14 min
N/A

RRC Success Rate	100% ✓
S1 Success Rate	100% ✓
RAB Success Rate	100% ✓

Drop Rate	7% ●
-----------	------

S1 HO Success Rate	N/A
X2 HO Success Rate	N/A

Accessibility

RRC Establishments per Cause	emergency	highPriorityAccess	mt-Access	mo-Signalling	mo-Data	delayTolerantAccess-v10x0	spare2	spare1
RRC.ConnEstabAtt.Cause	0	0	0	33	0	0	0	0
RRC.ConnEstabSucc.Cause	0	0	0	33	0	0	0	0

RRC Reestablishments per Cause	reconfigurationFailure	handoverFailure	otherFailure	spare 1
RRC.ConnReEstabAtt.Cause	0	0	0	0
RRC.ConnReEstabSucc.Cause	0	0	0	0

S1S1G Establishments	S1S1G.ConnEstabAtt
S1S1G.ConnEstabAtt	33

BLINQ Networks © 2021
Model: FW-300 B48 Serial Number: JOE000L000002 Board Identifier: BORED-00002 Version: 2.1.10_45381 EEPIC Version: 3.2.39

7.3.6.1. Accessibility

- **RRC Establishments per Cause:** details Radio Resource Control (RRC) established connections per cause
 - **RRC.ConnEstabAtt.Cause:** shows established RRC connections attempts per cause

- **RRC.ConnEstabSucc.Cause:** demonstrates successful RRC connections established per cause
- **RRC Reestablishments per Cause:** details Radio Resource Control (RRC) re-established connections per cause
 - **RRC.ConnReEstabAtt.Cause:** shows re-established RRC connections attempts per cause
 - **RRC.ConnReEstabSucc.Cause:** demonstrates successful RRC connections re-established per cause
- **S1SIG Establishments:** details established S1 signalling
 - **S1SIG.ConnEstabAtt:** shows S1 signalling established connections attempts per cause
 - **S1SIG.ConnEstabSucc:** demonstrates successful S1 signalling connections established per cause
- **ERAB Establishments per QCI:** details the number of established E-UTRAN Radio Access Bearers (E-RAB) per Quality of Service (QoS) Class Identifier (QCI)
 - **ERAB.EstabInitAttNbr.QCI:** shows the number of established initial attempts E-RAB per QCI
 - **ERAB.EstabInitSuccNbr.QCI:** shows the number of successfully established initial attempts E-RAB per QCI
 - **ERAB.EstabAddAttNbr.QCI:** shows the number of additional established attempts E-RAB per QCI
 - **ERAB.EstabAddSuccNbr.QCI:** shows the number of additional successfully established attempts E-RAB per QCI

7.3.6.2. Retainability

- **ERAB Releases per QCI:** details the number of E-UTRAN Radio Access Bearer (E-RAB) releases per Quality of Service (QoS) Class Identifier (QCI)
 - **ERAB.RelActNbr.QCI:** shows the actual release number of E-RAB per QCI
 - **ERAB.RelEnbNbr.QCI:** shows the eNB release number of E-RAB per QCI
- **ERAB Session time:** details the E-RAB active session time
 - **ERAB.SessionTimeUE:** shows the active session time between the UE and the E-RAB

7.3.6.3. Availability

- **RRU Unavailable time per Cause:** provides percentage of time that the remote radio unit (RRU) is unavailable per cause (0 and 1)
 - **RRU.CellUnavailableTime.Cause**

7.3.6.4. Mobility

- **HO Preparations per QCI:** provides handover(HO) preparations per standardized Quality of Service (QoS) Class Identifier (QCI) characteristics (release 12)
 - **HO.PrepAtt.QCI:** specifies the attempted handover preparations per standardized QCI
 - **HO.PrepSucc.QCI:** states the successful handover preparations per standardized QCI
- **HO Executions:**
 - **HO.ExeAtt:** identifies the number of handover execution attempts
 - **HO.ExeSucc:** details the number of handover execution successes

7.4. Troubleshooting

7.4.1. Band Scan

As mentioned in Section 6.3.5.2., the FW-600 can be set to scan the frequency band automatically when it is booting up. When this feature is turned on from the **Carriers > Advance > Band Scan** page, the FW-600 will scan and register noise levels across the entire span of the band (150 MHz) in 5 MHz steps for all 3 cells.

The results of the scan will be shown here, the read-only **Troubleshooting > Band Scan** page.



7.4.2. iPerf

This feature allows users to verify backhaul connectivity.

Throughput can be checked between two co-located ENBs, between eNB and EPC (requires iPerf on EPC), and between eNB and BLiNQ AWS iPerf servers. This allows not only the detection of potential issue(s) in the backhaul, but also help identify which hop is the likely source of the problem.

⚡ Iperf

Configuration		Report
Iperf is not running Start Stop		Iperf has not been run since system startup
Iperf Version	2	
Device Role	Client	
Server	<input type="text" value=""/> <small>Required</small>	
Server Port	5001	
Local Port	5001	
Test Duration [s]	10	
Report Interval [s]	<input type="text" value=""/>	
Protocol	TCP	
Number of Streams	1	
Test Direction	Client -> Server then Server -> Client	
Summary Reports	<input checked="" type="radio"/> YES	
Include Time Stats	<input type="radio"/> NO	

To set up the iPerf testing:

- Navigate to **Troubleshoot > iPerf**
- Enter the required/desired values in the parameters set out in **Configuration**
 - **Iperf Version:** Select between iPerf2 or iPerf3
 - **Device Role:** Choose between “Client” or “Server”
 - **Server:** Enter the server’s IP address
 - **Server Port:** Enter the server port for the server to listen on and the client to connect to
 - **Local Port:** Enter the local port number to be used
 - **Test Duration:** Enter the duration of the test in seconds
 - **Report Interval:** Enter the interval time in seconds between periodic reports
 - **Protocol:** Select between TCP or UDP
 - **Number of Streams:** Enter the number of streams to be tested
 - **Test Direction:** Select the test direction from the drop-down menu.
 - **Summary Reports:** Toggle the button to choose “YES” for summary reports to be generated or “NO” for no reports.
 - **Include Time Stats:** Toggle the button to “YES” if time stats is to be included or “NO” for the time stats to be excluded.
- When the test parameters are entered, click on “**Start**” to start the iPerf testing.
- The test results will appear in the **Report** section.



NOTE: Parameters available will be changed according to the testing needs. For example, if “**Server**” is chosen for **Device Role**, then the WebUI will display only these parameters: **Server Port**, **Report Interval** and **Protocol**.

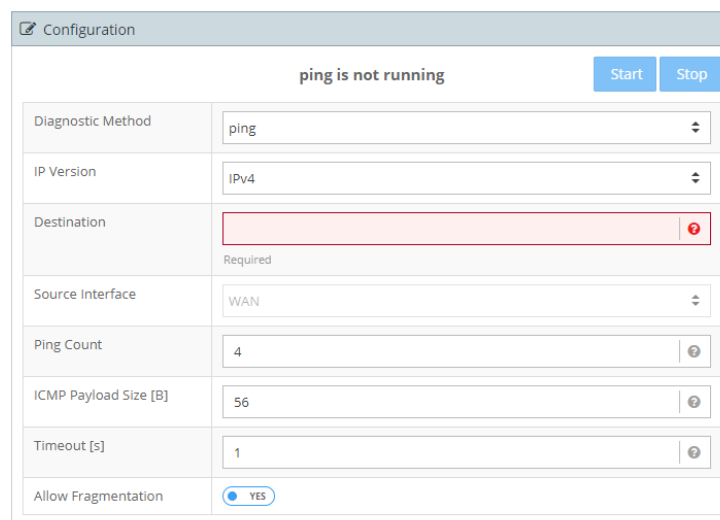
7.4.3. Network Diagnostics

Under this section, users can run a traceroute test or a ping test for diagnostic purposes.

7.4.3.1. Running a Ping Test

To run a ping test:

- Navigate to **Troubleshoot > Network Diagnostics**.
- Under **Configuration > Diagnostic Method**, select “ping” from the drop-down menu.
- Enter the following parameters:



Configuration	
ping is not running Start Stop	
Diagnostic Method	ping
IP Version	IPv4
Destination	<input type="text"/> ?
	Required
Source Interface	WAN
Ping Count	4 ?
ICMP Payload Size [B]	56 ?
Timeout [s]	1 ?
Allow Fragmentation	<input checked="" type="radio"/> YES

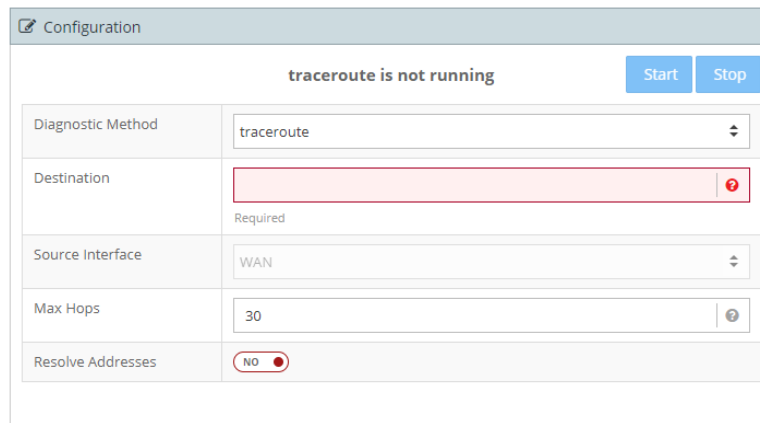
- **IP Version:** Select either “**IPv4**” or “**IPv6**”
- **Destination:** Enter a valid destination IPv4/IPv6 address or domain name.
- **Source Interface:** If separate S1 interface has not been set up (See Section 6.4.3.1), the only option here will be **WAN** and it cannot be changed. If a separate S1 interface has been configured, then select between **Mgmt** (default) or **S1**.
- **Ping Count:** Enter the number of times to repeat ping.
- **ICMP Payload Size:** This is the size of the ping payload. Default is set at 56.
- **Timeout:** Timeout in seconds to wait for the reply.
- **Allow Fragmentation:** Toggle “**YES**” or “**NO**” to break up the packet size.
- When the parameters for the ping test have been entered in, click on “**Start**” to start the test. Click on “**Stop**” to stop the test.
- The results of the test will be shown in the **Report** section.

7.4.3.2. Running Traceroute

A traceroute works by sending Internet Control Message Protocol (ICMP) packets, and every router involved in transferring the data gets these packets. The ICMP packets provide information about whether the routers used in the transmission are able to effectively transfer the data.

To run a traceroute test:

- Navigate to **Troubleshoot > Network Diagnostics**.
- Under **Configuration > Diagnostic Method**, select “**traceroute**” from the drop-down menu.
- Enter the following parameters:



- **Destination:** Enter a valid destination IPv4/IPv6 address or domain name.
- **Source Interface:** If separate S1 interface has not been set up (See Section 6.4.3.1), the only option here will be **WAN** and it cannot be changed. If a separate S1 interface has been configured, then select between **Mgmt** (default) or **S1**.
- **Max Hops:** A “hop” refers to the move data makes as it goes from one router to the next. Enter the maximum number of allowed hops here.
- **Resolve Addresses:** Toggle “**YES**” or “**NO**” for the eNB to resolve addresses.
- When the parameters for the ping test have been entered in, click on “**Start**” to start the test. Click on “**Stop**” to stop the test.
- The results of the test will be shown in the **Report** section.

7.4.4. Troubleshooting Guide

The following is a quick troubleshooting guide:

SYMPTOM	POSSIBLE CAUSE	SOLUTION
State LED stuck continuously on red or amber	OS or configuration mismatch preventing the unit from entering functional state	Reboot unit. If problem persists over multiple reboots, contact BLiNQ Networks Support.
FW-600 cannot be accessed	VLAN mismatch	Connect computer to the FW-600 Ethernet port, open https://169.254.1.1 and verify configured VLAN (exchange with the craft IP is always untagged)

SYMPTOM	POSSIBLE CAUSE	SOLUTION
	Wrong IP is set	Connect computer to the FW-600 Ethernet port, open https://169.254.1.1 and verify that configured IP address, subnet mask and default gateway are set properly
	No dynamic IP address on FW-600	If the FW-600 is configured for DHCP, verify your network and DHCP Server configuration
	Browser uses HTTP instead of HTTPS	Connect to the FW-600 using https://<FW-600_IP_Address>
	Forgotten username/password	Refer to the <i>eNB Password Recovery Guide</i> to log in or contact BLiNQ Customer Support.
FW-600 unable to form S1 link with EPC	GPS is not synchronized	Make sure that the system clock source has been selected to GPS under Setup > Systems > System settings. If the unit is being set up for the first time, please ensure that it has outside visibility and the top of the unit is not heavily obstructed. Please keep in mind that after power disruption that is longer than 10 minutes, GPS synchronization may take up to 45 minutes.
	Wrong MME IP address set	Verify the MME IP address on FW-600
	MME unreachable	Verify that there is network connectivity between FW-600 and MME
	SCTP/GTP filtering	Verify that firewall along the path does not filter SCTP or GTP traffic
	eNB related misconfiguration on EPC	Verify on EPC that eNB is allowed to connect to it (typically EPC will either work in unrestricted mode that allows any eNB to connect, or each eNB has to be allowed explicitly)
	MME inquiry and reply are not going through the same SecGW.	Reboot eNB. (This scenario might occur after both SecGW gets disconnected and gets reconnected)
CPE unable to form link with FW-600	Link is down due to loss of GPS sync	Reboot the FW-600.
	Wrong RF channel number	Verify the RF channel number configured on CPE to confirm that it matches to FW-600
	APN misconfiguration	Verify the APN configured on CPE is the same as in the CPE profile on EPC
	Cell range misconfiguration	Verify FW-600 cell range parameter is larger or equal to the distance of the furthest CPE
CPE unable to pass data traffic	Link is down	Confirm that the RF channel number is correctly configured on CPE. Restart CPE to trigger network entry again
	Link quality is poor	Analyze the link performance metrics (RSRP, CINR, Tx Pwr) on the CPE to determine if it's being served by the best available beam. Antenna orientation optimization may be required.
	APN misconfiguration	If CPE is operating in bridge mode, ensure that on EPC there is an APN defined for user traffic.



Appendix A

BLiNQ Wireless Devices and RF Safety/Les appareils sans fil BLiNQ et la sécurité RF

REMARQUE: La traduction française suit le texte anglais.

BLiNQ Networks evaluates all of its products to ensure that they conform to the Radio Frequency (RF) energy emission safety limits adopted by the Federal Communications Commission (FCC). BLiNQ Networks conducts these evaluations using the compliance rules and guidelines adopted by both the FCC and Industry Canada. They are based on the results of the Maximum Permissible Exposure (MPE) studies by the FCC for mobile or fixed devices, which dictate MPE limits for human exposure to RF energy.

Before selling any wireless networking device to the public, BLiNQ Networks submits its devices to the FCC and Industry Canada for MPE (that is, RF emissions) studies and evaluation. These studies must demonstrate that the device meets the accepted regulatory limits for safe RF emissions, or it is not approved for sale by the FCC and thus cannot be sold to the public. This means that when wireless networking devices, purchased from BLiNQ Networks, are installed and operated as instructed, the RF emissions from the devices is equal to or less than the levels accepted as safe by the FCC and Industry Canada.

When used as intended, BLiNQ wireless networking devices do not pose health risks. Like other devices that emit RF energy (such as computers and microwave ovens), the level of RF emissions from BLiNQ devices is too low to cause harm. Further, BLiNQ wireless networking devices emit far lower levels of RF energy than cellular and cordless telephones, and are almost always used further away from the human body.

To prevent unnecessary exposure to RF energy:

- Always install the FW-600 system so as to provide and maintain a minimum separation distance of at least 1.1 metres (43.3 inches) for Band 48, Band 53 and at least 2 metres (78.5 inches) for Band 41, Band 42/43 from all persons.
- When the FW-600 system is operational, avoid standing directly in front of the FW-600 antennas. RF energy fields may be present when the transmitter is on.
- When the FW-600 system is operational, maintain a distance of at least 1.1 metres (43.3 inches) for Band 48, Band 53 and at least 2 metres (78.5 inches) for Band 41, Band 42/43 from the FW-600 antennas.
- Do not install the FW-600 system in a location where it is possible for people to stand or walk inadvertently in front of an antenna.

Antenna Statement:

The antenna used for this transmitter must be installed to provide a separation distance of at least 1.1 metres (43.3 inches) for Band 48, Band 53 and at least 2 metres (78.5 inches) for Band 41, Band 42/43 from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. Users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.



BLiNQ Networks évalue l'ensemble de ses produits afin de s'assurer qu'ils sont conformes à la limite d'émission énergétique sécuritaire de radiofréquence (RF) adoptée par la «Federal Communications Commission» (FCC). BLiNQ Networks effectue ces évaluations en utilisant les règles et lignes directrices adoptées à la fois par le FCC et Industrie Canada. Elles sont basées sur les résultats de l'exposition maximale admissible, études menées par le FCC sur les appareils mobiles ou fixes, qui dictent les limites de l'exposition maximale admissible pour l'exposition humaine aux énergies RF.

Avant de vendre tout appareil de réseau sans fil au public, BLiNQ Networks présente ses appareils au FCC et à Industrie Canada pour l'évaluation de l'exposition maximale admissible. Ces études doivent démontrer que l'appareil est conforme aux limites réglementaires acceptées pour les émissions RF, sinon les appareils ne sont pas approuvés pour la vente par la FCC et ne peuvent donc pas être vendus au public. Cela signifie que lorsque des équipements sans fil, achetés auprès de BLiNQ Networks, sont installés et utilisés conformément aux instructions, les émissions RF provenant des dispositifs sont inférieures ou égales aux niveaux acceptés comme étant sécuritaire par la FCC et Industrie Canada.

Lorsqu'utilisés comme prévu, les périphériques sans fil BLiNQ ne posent pas de risques pour la santé. De la même façon que les autres appareils qui émettent de l'énergie RF (comme les ordinateurs et les fours à micro-ondes), le niveau des émissions RF des dispositifs BLiNQ est trop faible pour causer des dommages. En outre, les dispositifs de réseau sans fil BLiNQ émettent des niveaux beaucoup plus faibles d'énergie RF que les téléphones cellulaires et sans fil, et sont presque toujours utilisés loin du corps humain.

Pour éviter toute exposition inutile à l'énergie RF :

- Installez toujours le système FW-600 afin de fournir et de maintenir une distance de séparation minimale d'au moins 1.1 mètres (43,3 pouces) pour la bande 48 et la bande 53 et d'au moins 2 mètres (78,5 pouces) pour la bande 41 et la bande 42/43 pour les personnes.
- Lorsque le système FW-600 est opérationnel, éviter de se tenir directement devant les antennes du FW-600 et leurs antennes internes. Les champs d'énergie RF peuvent être présents lorsque l'émetteur est en marche.
- Lorsque le système FW-600 est opérationnel, maintenir une distance d'au moins 1.1 mètre (43,3 pouces) pour la bande 48 et la bande 53 et d'au moins 2 mètres (78,5 pouces) pour la bande 41, bande 42/43 à partir des antennes du FW-600.
- Ne pas installer le système FW-600 dans un endroit où il est possible pour les gens de se tenir debout ou de marcher en face d'une antenne.

Déclaration d'antenne:

L'antenne utilisée pour cet émetteur doit être installé de façon à créer une distance de séparation d'au moins 1.1 mètre (43,3 pouces) pour la bande 48 et la bande 53 et d'au moins 2 mètres (78,5 pouces) pour la bande 41, bande 42/43 de toute personne et ne doit pas être co-localisées ou opérant en conjonction avec une autre antenne ou émetteur. Les utilisateurs et les installateurs doivent avoir reçus des instructions d'installation de l'antenne et des conditions de fonctionnement de l'émetteur pour satisfaire la conformité aux expositions RF.



Equipment Compliance

Federal Communications Commission (FCC) Notices

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

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

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

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



CAUTION: Any changes or modifications not expressly approved by BLINQ Networks could void the user's authority to operate this equipment.



Appendix B ISED Non-Interference Disclaimer

The FW-600 contains licensed transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licensed RSS(s). Operation is subject to the following two conditions:

- (1) The FW-600 may not cause interference.
- (2) The FW-600 must accept any interference, including interference that may cause undesired operation of the device.

The FW-600 complies with the Canadian ICES-003 Class B specifications. CAN ICES-003(B) / NMB-003 (B).

L'émetteur/récepteur autorisée contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio autorisée. L'exploitation est autorisée aux deux conditions suivantes :

- (1) le système FW-600 ne doit pas produire de brouillage;
- (2) le système FW-600 doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet appareil numérique de la Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.



Appendix C PCI Planning Guidelines

When setting up your system, you must abide by the rules outlined below, to minimize Physical Cell ID (PCI) collision and enforce an effective PCI assignment strategy:

Rule 1: Same PCI Utilization

- Multiple cells within a FW-600 on the same frequency should not have the same PCI
- Immediate neighbour cells on the same frequency should not have the same PCI

Rule 2: PCI MOD3

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD3 (i.e., $PCI_{cellA} \neq PCI_{cellB}$)
- Occurs due to the fact that when PCI X is changed by a factor of $X+3n$ (where n is an integer) there is a collision on the reference signals between the two antenna ports, i.e., between the PCI[X]-antenna port0 and PCI[X+3n]-antenna port1
- Applicable for MIMO transmission only

Rule 3: PCI MOD6

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD6
- Applicable for SISO transmission only

Rule 4: PCI MOD30+

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD30
- Occurs due to the collision of the uplink (UL) reference signals (RS) which leads to a higher bit error rate (BER) in the UL

Rule 5: PCI MOD50 (20MHz Bandwidth (BW)) or PCI MOD25 (10MHz BW)

- Cells on the same frequency within a similar coverage area must not have the same PCI MOD50/MOD25
- Occurs due to the collision on the Physical Control Format Indicator Channel (PCFICH) which leads to failure in decoding on the Physical Downlink Control Channel (PDCCH)

Rule 6: Cell Group ID Correlation

- Cell Group ID is derived from two length-31 binary m-sequences (m0, m1)
- Each time m0/m1 repeats, the overall correlation between the two Cell Group ID values is higher
- No impact to the performance of Key Performance Indicators (KPI) due to this type of interference
- Only causes network entry delay (by 5-10ms)



Appendix D Commonly Used DSCP Values

The table below lists the commonly used DSCP values that can be configured with the QCLs in Section 6.2.4.3.

TABLE G COMMONLY USED DSCP VALUES

DSCP Name	Binary Value	Decimal Value	Reference
CS0	000000	0	RFC 2474
CS1	001000	8	RFC 2474
CS2	010000	16	RFC 2474
CS3	011000	24	RFC 2474
CS4	100000	32	RFC 2474
CS5	101000	40	RFC 2474
CS6	110000	48	RFC 2474
CS7	111000	56	RFC 2474
AF11	001010	10	RFC 2597
AF12	001100	12	RFC 2597
AF13	001110	14	RFC 2597
AF21	010010	18	RFC 2597
AF22	010100	20	RFC 2597
AF23	010110	22	RFC 2597
AF31	011010	26	RFC 2597
AF32	011100	28	RFC 2597
AF33	011110	30	RFC 2597
AF41	100010	34	RFC 2597
AF42	100100	36	RFC 2597
AF43	100110	38	RFC 2597
EF	101110	46	RFC 3246
VOICE-ADMIT	101100	44	RFC 5865

Appendix E UEs Supported for Different Carrier Aggregation Modes

TABLE H ACTIVE UES SUPPORTED PER SECTOR/BEAM PER ENB

eNB Model #	Total UEs* (Per Base Unit)	Active UEs per Sector or Beam			Active UEs
		1 CC	2CC	3CC	2CC + 1CC
FW3-B48-00-NA	288	48	32	32	32 + 48
FW3-B48-00-HP-NA	288	48	32	32	32 + 48
FW3-B42-43-HP-EU	288	48	32	32	32 + 48
FW3-B48-46-HP-NA	96	48	32	32	-
FW6-B48-00-NA	288	48	32	32	32 + 48
FW6-B42-43-EU	288	48	32	32	32 + 48
FW6-B41-00-WW	288	48	-	-	-
FW6-B48-46-NA	192**	48	32	32	-
FW6-B53-00-NA	288	48	-	-	-
X3I-35-00-WW-OD	288	48	32	-	32 + 48
X3I-35-00-WW-POE	288	48	32	-	32 + 48
X3I-35-50-WW-POE	288	48	32	-	-

*Up to 3 carriers per base unit unless otherwise stated.

**Up to 6 carriers per base unit.



Appendix F Alarms and Events (Fault Management)

This appendix lists the alarms and events for the BLiNQ FW-600 system.



NOTE: There is no need to open the FW-600 module casing. If there is an unsolvable problem or a module malfunction, please contact BLiNQ Customer Support for help or a return merchandise authorization (RMA) number/procedure.

The FW-600 system issues an alarm notification when a fault condition occurs. You view alarms through the:

- FW-600 WebUI **Events > Alarms** page (See Section 7.2.1) or
- on the CLI via the “**show event-history**” command

These alarms require operation and maintenance actions to restore functionality and/or to prevent a more serious situation from developing.

Table I List of Alarms shows each alarm (whose name also represents the particular problem), the alarm ID, type and explanation on the likely cause of the alarm and possible solution (as applicable).

The FW-600 system issues an event notification when something of importance happens that does not trigger an alarm, but is considered significant enough to take note. You view these events through the:

- FW-600 WebUI **Events > History** page (See Section 7.2.2) or
- On the CLI via the “**show event-history**” command.

Table J List of Events shows each event (whose name also represents the particular problem), the event ID, type and explanation on the likely cause of the event.

Severity is also defined for each listed alarm and event, to indicate the relative level of urgency for operator action:

- **CRITICAL** — the alarm or event requires immediate corrective action, regardless of the time.
- **Major** — the alarm or event requires immediate corrective action, within working hours.
- **Minor** — the alarm or event requires corrective action at a suitable time or, at least, continuous close observation.
- **Warning** — the alarm or event requires corrective action on a scheduled maintenance basis.
- **Information** — the alarm or event requires no corrective action; it is for informational purposes only.

TABLE I LIST OF ALARMS

ID	Name	Description/Comments	Type	Severity
1002	PHY Queue Full	PHY has stopped processing because the queue is full	Comms ¹ .	CRITICAL
3004	Software Boot Failure	This may indicate a physical or logical corruption of the system non-volatile storage.	Equip.	CRITICAL
4001	Ethernet Port Down	Ethernet link is down, can be caused by Eth cable unplugged or connected port defective, administratively disabled, equipment down, etc. System recovers when Ethernet link is re-established.	Comms ² .	Major
5004	Radio Disabled	An operator has administratively disabled the radio in the unit. Identified per beam.	Equip. ³	Major
5006	Radio Module Down	Configuration issue e.g. radio enabled but not used by any beam. Identified per RF instance.	Equip.	Major
5008	Radio Temperature Warning	The radio operating temperature has exceeded the normal operating range. Identified per beam.	Equip.	Major
5009	Radio RF Calibration	This alarm usually indicates a hardware failure. The unit should be replaced. Identified per RF instance.	Equip.	CRITICAL
5014	Radio DCA No Frequency Available	The system is using all the available frequency channels and pauses the jump sequence to prevent flip-flopping.	Comms.	Minor
5015	Radio Board Information Error	Board information is wrong or invalid.	Comms.	CRITICAL
5016	Board Detection Error	Board 1611 not detected / Board 1611 detected but not expected / Board 1610 not detected	Equip.	CRITICAL
5017	Radio Beam Down	PRACH configuration index does not match beam.	Comms.	CRITICAL
5018	RF Mute	All carriers are muted by user operation.	Equip.	Notification
5020	Radio Carrier Down	All active RF carriers are down	Equip.	Major
5021	PAM Warning	Power Amplifier Module (PAM) is in abnormal state.	Equip.	Major

¹ Comms = Communications

² Comms = Communications

³ Equip. = Equipment

ID	Name	Description/Comments	Type	Severity
6002	GPS Antenna Failure	This indicates a hardware fault with the GPS antenna of the FW-600.	Equip.	CRITICAL
6003	Hardware Temperature	The alarm triggers with 2 severity levels: - Major - this warns that temperature is above normal range (85C) and - Critical - when the temperature exceeds safety limits and the radio is stopped (90C).	Equip.	Major/ CRITICAL
6004	Phy Start Issue	Failure to load or start the PHY code.	Comms.	CRITICAL
6005	RF Power Amp Issue	1611 could not start, power failure or other issue	Equip.	CRITICAL
6006	CA Chain Issue	RF card not Carrier Aggregation (CA) capable. Badly configured CA chain.	Comms.	CRITICAL
6007	Core Crash	Crash will be identified in the description on dashboard	Equip.	CRITICAL
6008	TX Rx Issue	FPGA stopped generating Tx and Rx signal	Comms.	CRITICAL
6009	DSP Startup Error	PHY initialization stuck when DSPs cannot be started.	Equip.	CRITICAL
7001	System GPS Synchronization Lost	When operating in GPS mode, the GPS receiver has lost synchronization. When operating in 1588 mode, the 1588 client has lost communication with the 1588 master clock. Upon FW-600 reset, this alarm is not raised until 60 s after reset and if synchronization still is not achieved. After holdover time expires (5 minutes), system transitions to unsynchronized state.	Comms.	Major
7002	System Synchronization Failed	When operating in GPS mode, the GPS receiver has lost synchronization. When operating in 1588 mode, the 1588 client has lost communication with the 1588 master clock. This alarm is raised when the module fails to achieve system timing synchronization. Probably caused by a loss of signal.	Equip.	CRITICAL
7010	DHCP Server Unavailable	The system has not been able to obtain a DHCP address.	Comms.	Major
9003	PM Automatic File Upload Failure	The unit could not perform the FTP transfer of the performance data. The FTP system is inaccessible. (Module cannot upload PM files to the specified server. Indicates a server connectivity or access error. System recovers when	Comms.	Minor

ID	Name	Description/Comments	Type	Severity
		connectivity/access to the PM server is restored.)		
9005	Invalid UE ID	Un-recoverable Dataplane error	Comms.	Minor
11001	SAS Server Registration Failure (CBSD)	Registration with SAS server failed.	Comms.	CRITICAL
11002	Grant Suspended or Terminated (CBSD)	Grant was suspended or terminated by SAS server.	Comms.	CRITICAL
11002	Noise Alarm	Noise level surpassed threshold levels set in Carriers > Advanced > Band Scan	Comms.	Major
12001	S1 State Enabled	S1 disabled/enabled	Equip.	Major
12011	EEPC Lost	EPC Connection Lost	Comms.	CRITICAL

TABLE J LIST OF EVENTS

ID	Name	Description/Comments	Type	Severity
2001	Configuration Changed	A configuration change has been committed to the running configuration.	System	Information
3001	Software Download	Downloading software image.	System	Information
3002	Software Download Successful	Successful download of software image.	System	Information
3003	Software Download Error	Software error: A software download is already in progress.	System	Minor
3004	Software Boot Failure	This may indicate a physical or logical corruption of the system non-volatile storage.	Equip.	CRITICAL
5004	Radio Module Disabled	Radio Module is initialized and has received an administrative disable configuration.	Equip.	Information
7003	System Synchronized	GPS entered synchronized state.	Equip.	Information
7004	GPS State Change	The GPS state machine gained or lost GPS synchronization (specific state indicated by the comment text).	Equip.	Information
8001	Authentication Failed	Attempts to authenticate on one of the management interfaces of the equipment failed.	Security	Warning
10001	License successfully applied	A license was successfully applied to module.	System	Major
10002	Invalid license	Invalid license: Digital signature does not match license content.	System	Major



ID	Name	Description/Comments	Type	Severity
10003	License not applicable	License not applicable to module: MAC address does not match filter or license capabilities do not match the hardware.	System	Major
12001	S1 State Enabled Event (ENB)	S1 State Enabled	System	Information
12002	UE Attached Event (ENB)	User Equipment (UE) Attached	System	Information
12003	UE Detached Event (ENB)	UE Detached	System	Information
12005	PCI Changed	Cell (x) PCI changed by eSON	System	Information
12006	NRT Conflict	Beam (X) has a PCI conflict	System	Information
12007	NRT Confusion	Beam (X) has a PCI confusion	System	Information
12008	UE Connection Event	UE disconnected. IMSI number as identified.	System	Information
12009	NRT Added	Cell (X) added neighbor PCI	System	Information
12010	NRT Remove	Cell (X) removed neighbor PCI	System	Information



Appendix G List of Acronyms

Acronyms	Meaning
3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting (centralized networking protocol)
AES	Advanced Encryption Standard
AF	Assured Forwarding behavior, DSCP
AISG	Antenna Interface Standards Group
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
APN	Access Point Name
Az	Azimuth
BER	Bit Error Rate
BLER	Block Error Rate
BW	Beamwidth
CBRS	Citizens Broadband Radio Service
CBSD	Citizens Broadband Radio Service Device
CA	Carrier Aggregation
CC	Component Carrier
CFI	Control Format Indicator
CFR	Crest Factor Reduction
CINR	Carrier to Interference plus Noise Ratio
CLI	Command Line Interface
CPE	Customer Premise Equipment
CPI	Certified Professional Installer
CQI	Channel Quality Indicator
Craft IP	IP address typically used by technical personnel to test the equipment
CS	Class Selector, DSCP
CSG	Closed Subscriber Group
CW	Continuous Wave (carrier)
dB	Decibels
dB _i	Decibel isotropic
dB _m	Decibels per Milliwatt



Acronyms	Meaning
DC	Direct Current
DCA	Dynamic Channel Assignment
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DSCP	Differentiated Services Code Point
DNS	Domain Name System
EARFCN	Evolved Absolute Radio Frequency Channel Number (LTE)
EF	Expedited Forwarding behavior, DSCP
EIRP	Equivalent/Effective Isotropic Radiated Power
EMS	Element Management System
eNB	See eNodeB
eNodeB	E-UTRAN Node B, also identified as Evolved Node B (abbreviated as eNodeB or eNB) is an element of an LTE Radio Access Network (RAN)
EPC	Evolved Packet Core
ERAB	E-UTRAN Radio Access Bearer
EUTRAN	Evolved Universal Terrestrial Radio Access Network
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
FTP	File Transfer Protocol
GHz	Gigahertz
GPS	Global Positioning System
GTP	GPRS Tunneling Protocol
HARQ	Hybrid Automatic Repeat Request
HO	Handover
HP	High Power
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
Kbps	Kilobits per second
KM	Kilometres
KPI	Key Performance Indicators



Acronyms	Meaning
LOS	Line-of-Sight
LTE	Long Term Evolution refers to a mobile device, high-speed, wireless communications standard.
MAC	Media Access Control
Mbps	Megabits per second
MCC	Mobile Country Code
MCS	Modulation and Coding Scheme
MFBI	Multi-Frequency Band Indicator
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MIMO-SM	Multiple Output-Spatial Multiplexing
MME	Mobility Management Entity; the key control-node for the LTE access-network
MNC	Mobile Network Code
MPE	Maximum Permissible Exposure
MS or Msec	Millisecond
MSR	Multi-Standard Radio
NA	North America
NAT	Network Address Translation
NTP	Network Time Protocol
OAM	Operations, Administration and Maintenance
OPc	Operator Code
PAM	Power Amplifier Module
PBCH	Physical Broadcast Channel
PCCH	Paging Control Channel (PCCH)
PCFICH	Physical Control Format Indicator Channel
PCI	Physical Cell ID
PDCCH	Physical Downlink Control Channel
PDN	Packet Data Network
PDSCH	Physical Downlink Shared Channel
PHICH	Physical Hybrid-Automatic Repeat Request (ARQ) (HARQ) Indicator Channel
PHR	Power Headroom Report
PHY	Physical Layer
PLMN-ID	Public Land Mobile Network Identifier (PLMN-ID = MCC + MNC)
PM	Performance Measurement



Acronyms	Meaning
PPS	Pulse Per Second
PRACH	Physical Random Access Channel
PSS	Primary Synchronization Signal
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel
QAM	Quadrature Amplitude Modulation
QCI	QoS Class Identifier
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RACH	Random Access Channel
RAN	Radio Access Network
RET	Remote Electrical Tilt
RF	Radio Frequency
RI	Rank Indication
RNTI	Radio Network Temporary Identifier
RRC	Radio Resource Control
RRU	Remote Radio Unit
RS	Reference Signal
RSSI	Received Signal Strength Indicator
RSCP	Received Signal Code Power
RSRQ	Reference Signal Received Quality
RSRP	Reference Signal Received Power
RTP	Received Target Power
RX	Received
s	Second
S1	Interface between an eNB and the Core Network (CN)
SAS	Spectrum Access System
SCH	Shared Channel
SCTP	Stream Control Transmission Protocol
SecGW	Security Gateway
SFP	Small form-factor pluggable
SFTP	Secure File Transfer Protocol



Acronyms	Meaning
SGW	Serving Gateway; routes and forwards user data packets, also acts as mobility anchor
SIM	Subscriber Identity Module
SINR	Signal to Interference plus Noise Ratio
SISO	Single Input Single Output
SKU	Stock Keeping Unit
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SR	Scheduling Request
SRS	Sounding Reference Signal
SSH	Secure Shell protocol
SW	Software
TACACS	Terminal Access Controller Access Control System
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time Division Duplexing
TDM	Time Division Multiplexed
TX	Transmit
UDP/IP	User Datagram/Internet Protocol
UE	User Equipment
UI	User Interface
UL	Uplink
UMTS	Universal Mobile Telecommunications System
U-NII	Unlicensed National Information Infrastructure
URL	Universal Resource Locator
UTRAN	UMTS Terrestrial Radio Access Network
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VSWR	Voltage Standing Wave Ratio
WAN	Wide Area Network
XML	Extensible Markup Language



© Copyright 2014-2023 BLiNQ Networks Inc.

CONFIDENTIAL INFORMATION

RESTRICTED USE AND DUPLICATION

All rights reserved. The information contained in this document is proprietary to BLiNQ Networks Inc. This document may not in whole or in part be copied, reproduced, or reduced to any medium without prior consent, in writing, from BLiNQ Networks Inc.

Disclaimer

The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable but are presented without express or implied warranty. Additionally, BLiNQ Networks makes no representations or warranties, either expressed or implied, regarding the contents of this product. BLiNQ Networks shall not be liable for any misuse regarding this product. The information in this document is subject to change without notice.