BLiNQ Networks Inc.

X-100 Intelligent Wireless Backhaul System

User Guide

Release 1.0

Issue 01

February 2013

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.

Revision History

Date	Issue	Reason for Issue
February 2013	01	General Availability (GA) release.

Contact Information:

BLiNQ Networks Inc.
400 March Road, Suite 240
Ottawa, ON K2K 3H4

Web Site:

http://www.blinqnetworks.com

Sales Inquiries:

Email: sales@blinqnetworks.com
Telephone: 1-613-599-3388 x280

Support:

Web: http://www.blinqnetworks.com/support
Email: support@blinqnetworks.com
Telephone: 1-613-599-3388 x270

Table of Contents

List of Figures

List of Tables

1 X-100 System Overview

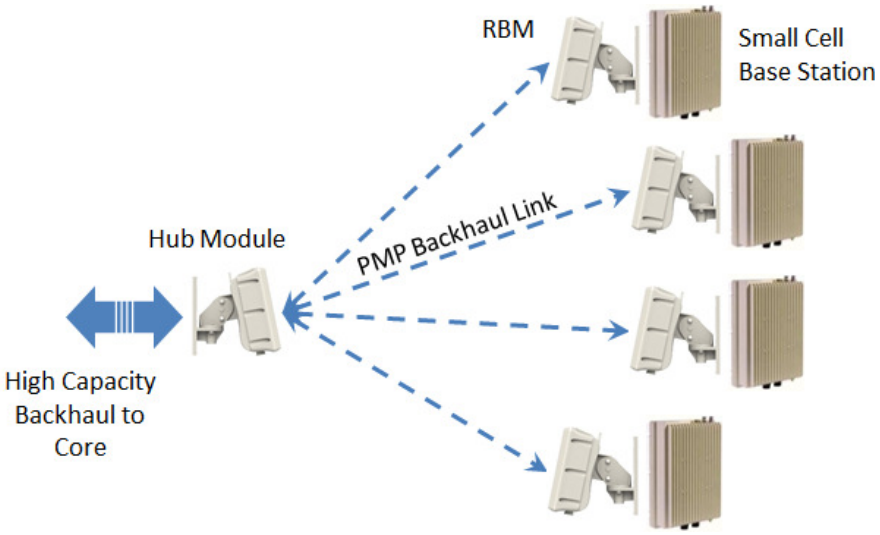


Figure 1 BLiNQ X-100 System in a Wireless Backhaul Application

BLiNQ Networks is a pioneer of next-generation wireless backhaul solutions that feature intelligent systems capable of adapting to the radio frequency environment to maximise capacity and performance.

The BLiNQ X-100 system operates in the sub 6 GHz licensed frequency bands and are designed for Non-Line-of-Sight (NLOS) operation by incorporating advanced physical layer and medium access control layer algorithms and techniques. BLiNQ has developed proprietary interference mitigation algorithms and incorporated self-organizing network techniques into its solutions to increase capacity and reliability beyond that of ordinary backhaul solutions. This is because in a NLOS environment, interference and shadowing are the two main reasons that limit capacity and link reliability. Mitigating interference and enhancing signal reliability maximizes system performance.

The X-100 system delivers 8 b/s/Hz spectral efficiency. The system is designed for use in multiple applications that includes mobile backhaul, optical fibre cable extension and corporate and enterprise data backhaul services by providing over 80 Mbps of throughput in a 10 MHz channel. The interference mitigation technology allows network operators to deploy a greater density of wireless links in a small spectrum allocation (such as 10 or 20 MHz).

The X-100 system operates in non-exclusive licensed Time Division Multiplexing (TDD) band 3.65 – 3.7 GHz in both Point-to-Point (PTP) and Point-to-Multipoint (PMP) configurations. Some of the main product characteristics are shown in Table 1. The X-100 system incorporates Multiple Input Multiple Output (MIMO technology and operates at high Modulation and Coding Scheme (MCS) rates to provide high capacity. In addition, the product incorporates BLiNQ's interference management techniques which include multiple power control algorithms to maximize performance in dense networks.

The X-100 system using a 10 MHz channel employs a large number of sub-carriers (1024) which helps

optimize bandwidth use. A large number of sub-carriers yields a long symbol time because the minimum symbol time is inversely proportional to the sub-carrier bandwidth. Transmitted signals are subject to time delay dispersion because of multiple paths. While the most direct path might involve no reflections, other paths involve one or more thus presenting the signal with longer path lengths and hence longer transit times. To prevent interference between successive symbols due to this dispersion, a gap called the cyclic prefix (or guard time) is added to each symbol. Dispersion dictates a cyclic prefix length of about 3-5 µsec in urban areas where small cells are deployed. For short symbol times on the order of a few µsec the added cyclic prefix would substantially cut into the useful bandwidth. For the longer symbol times used by the X-100 system the cyclic prefix is only a small fraction of the total bandwidth.

Table 1 Overview of Main X-100 System Characteristics

Duplex Mode	Time Division Multiplexing (TDD)
Physical Layer/Antenna System	1024 sub-carrier OFDM – NLOS 2x2 MIMO
Operation Configuration	Point-to-Point Point-to-Multipoint
Throughput	Total 83 Mbps shared between DL and UL depending on user defined TDD DL/UL traffic ratios; e.g. DL 53 Mbps for 65:35 traffic ratio (user selectable in X-100 WebUI through Setup Page).
Frequency of Operation	3.65 – 3.7 GHz (non-exclusive licensed band)
Channel Bandwidth	10 MHz
Network Interface	Ethernet (Fiber optional for Hub)
Quality of Service (QoS)	Two classes: Guaranteed Bit Rate (GBR) and Best Effort (BE)
Form Factor	All-outdoor; zero-footprint

Hub Module (HM)

Remote Backhaul Module (RBM)

(The RBM mechanical enclosure is similar to the Hub Module, except that the RF connectors, the SFP receptacle and the integrated GPS antenna are absent).

Figure 2 BLiNQ X-100 Hub Module (HM) and Remote Backhaul Module (RBM)

The X-100 system consists of the following modules:

- **Hub Modules (HMs)**: These are sector controllers that control several RBMs. Hub Modules feature two RF connectors for an external user-defined sectored antenna.
- **Remote Backhaul Modules (RBMs)**: These are subscriber units that are installed outdoors on customer premises, including public infrastructure assets such as light and utility poles in mobile backhaul applications. The RBMs feature an integrated antenna.
- **Configuration System**: This consists of the X-100 WebUI tool and X-100 CLI for configuration management, as well as fault and performance management.

  Note: Fault and performance management is also made available through a standard Simple Network Management Protocol (SNMPv2C/v3) interface to existing third-party managing applications such as element/network management systems (EMSs/NMSs).

The X-100 system has a small, all-outdoor, zero-footprint form factor that can be easily deployed on towers, poles, building sidewalls, or rooftops unobtrusively.

2 X-100 System Description

The BLiNQ X-100 system is designed to meet the requirements of network operators for high capacity and reliability in small cell base station backhaul applications, as well as in a number of other applications. The system can function either as Point-to-Point (PTP) or Point-to-Multipoint (PMP) wireless Ethernet bridge equipment. Some of the main product characteristics include:

Orthogonal Frequency-Division Multiple Access (OFDMA) Physical Layer: This includes 1024 sub-carriers (data, pilot and guard-band). The OFDMA physical layer coupled with multiple antenna technology provides robust performance in a non-line-of-sight (NLOS) environment.

Time Division Duplex (TDD): The X-100 system features TDD access mode with variable frame length (user selectable 3.125 and 5 msec). The TDD frame includes the downlink and uplink sub-frames. Each subframe includes a number of OFDM symbols which are assigned to different Remote Backhaul Modules (RBMs). The length of each sub-frame determines the traffic ratio for downlink and uplink traffic and is a user settable parameter.

Note: Frame length of 3.125 msec not supported in current release.

Multiple Input Multiple Output (MIMO): The X-100 system features spatial multiplexing on two antennas (2x2) for high capacity.

Adaptive Modulation with Link Adaptation: The X-100 system supports QPSK, 16QAM, 64QAM and 256QAM on both the downlink and uplink path to achieve high capacity in limited channel bandwidth (83 Mbps Ethernet layer throughput in a 10 MHz channel for combined downlink and uplink traffic).

Note: Total 71.5 Mbps throughput is in effect this release.

Intelligent Interference Management: The X-100 system implements the BLiNQ proprietary Managed Adaptive Resource Allocation (MARA) algorithm to identify the links with highest interference in the backhaul network and to manage the transmission of backhaul nodes to eliminate interference. The MARA algorithm improves capacity and link reliability. It also reduces the operational and capital costs associated with site design, deployment and optimization activities as interference is automatically identified and mitigated, thereby reducing the design and optimization effort required from RF engineers and field technicians.

Backhaul Self-Organizing Networks: The X-100 system periodically characterizes the radio frequency (RF) environment in the backhaul network to account for changes such as deployment of new sites or changes that affect interference (for example, foliage, variation between seasons, new building construction). The measurements, termed RF Environment Characterization (RFEC), are typically scheduled by the operator to run at a certain time of the day and used in MARA/power control algorithms.

Power Control: The X-100 system incorporates power control on both the downlink and uplink streams to minimize interference at physical layer and maximize capacity. Two types of power control are implemented: link level and network level. Link-level power control optimizes the power for a certain link to meet its capacity requirements, whereas network-level power control optimizes link power based on network level constraints to maximize network performance.

Antennas: The X-100 Remote Backhaul Modules (RBMs) integrate a specially designed slant-45 cross-polarized antenna to reduce interference and provide high co-polar isolation between the two branches. For example, the sidelobe level in the azimuthal plane is 8 dB below European Telecommunications Standards Institute (ETSI) Directory Number (DN) 4and 5 mask requirements and 15 dB below ETSI DN 2 mask requirements.

Point-to-Multipoint (PMP) with Dynamic Bandwidth Allocation: The X-100 system can operate in PTP or PMP configurations with up to four RBMs. The capacity allocated to each RBM is variable according to subscriber requirements (for example, compact base station).

Quality of Service (QoS): Two levels of QoS are defined in the X-100 system for traffic classification: Guaranteed Bit Rate and Best Effort. Through service-level agreements (SLAs), customers can subscribe to the service class desired for their application.

Service Class		Description
GBR	Guaranteed Bit Rate	Provides the most stringent scheduling, maintaining guarantees on throughput, latency, and jitter to the levels necessary for synchronization/timing packets such as NTP v4.0 and Time Division Multiplexed (TDM) services.
BE	Best Effort	No guaranteed minimum throughput. For data streams for which no minimum service level is required and therefore may be handled on a space-available basis.

Traffic Classification: Ethernet traffic is classified by the Layer 2 (L2) Media Access Control (MAC) source and destination address, 802.1p/Q settings, differentiated services code point (DSCP) and type of service (ToS) bits, L3 IP source and destination address, and protocol.

Form Factor: The all-outdoor, zero-footprint Hub Module (HM) and RBMs are built to IP67 requirements for operation in tough environments with the capability to handle large variations in temperature from extreme cold to extreme heat.

High-level of Integration: The X-100 systems are highly integrated and include:

- The RBM which integrates a high-gain 17 dBi antenna. The RBM derives its synchronization from the Hub Module.
- The HM which integrates a complete Global Positioning System (GPS) antenna and receiver with high holdover (10 minutes). Therefore, no additional synchronization module is required for the X-100 system, which reduces the total cost of ownership of the solution while simplifying and accelerating installation.

The X-100 system is small in size (31x21x8 cm) and low in weight (3.5 kg) so it can be easily mounted on the network operator's existing tower assets. The small size and weight allows quick deployment of the RBMs at customer premises in different enterprise/corporate data backhaul applications or other types of industrial and commercial applications.

All modules offer a standard RJ45 Ethernet port, while the Hub Module offers optional optical connectivity through a field-installable SFP optical transceiver module.

The BLiNQ X-100 system also provides the following network management features:

- **Fault and Performance Management:** The X-100 system incorporates fault and performance management through a standard Simple Network Management Protocol (SNMP)v2c interface. For this BLiNQ provides its Management Information Base (MIB) to network operators for integration into existing third-party managing applications such as element/network management systems (EMSs/NMSs), thereby providing access to key information on X-100 service availability and performance.
- **Configuration Management:** BLiNQ products are designed to minimize the configuration effort by the network operator. For example, when deployed in the field, the X-100 system can obtain its IP address through DHCP rather than have it statically assigned by the user. Further, the X-100 system provides a web-based configuration tool called the X-100 WebUI and a standard Command Line Interface (CLI) that run directly on the X-100 equipment.
- **Software Upgrade:** BLiNQ products are field upgradeable through remote download and activation of software release upgrades.

3 Technical Specifications

3.1 System Parameters

Table 2 shows general X-100 system parameters.

Table 2 General X-100 System Parameters

Access Technology	Orthogonal Frequency-Division Multiplexing (OFDM) Non-Line-of-Sight (NLOS)
RF Bands	3.65 – 3.7 GHz
Channel Size (Bandwidth)	10 MHz
Data Rate	Up to 83 Mbps (Layer 2/Ethernet)
Tx Power	23 dBm / 0.2 W (per antenna port, two ports)
Duplex Mode	Time Domain Duplex (TDD)
Modulation & Coding	Quadrature Phase Shit Keying (QPSK), 16/64/256 QAM; Bidirectional Dynamic Adaptive Convolutional Turbo Codes
Advanced Antenna Systems	2x2 Multiple Input Multiple Output (MIMO) / Spatial Multiplexing
Antenna	Remote Backhaul Module (RBM): Integrated 17 dBi gain Hub Module (HM): External antenna
Synchronization	Global Positioning System (GPS); IEEE 1588v2
Encryption	AES-128
Network Interface[1]	Copper: RJ45 100BaseT Ethernet Fiber (Optional on HM): Optical Gigabit Ethernet
Network Attributes	Ethernet bridge, 802.1Q, 802.1ad, DSCP/ToS/802.1p (IPv4/IPv6) and QinQ Tagging
Power Requirement	-48 VDC
Power Consumption	35 W (typical); 65 W (max)
Operating Temperature	-40°C to 55°C
Weight	<3.8 kg / 7.7 lbs
Dimensions	31 x 21.8 x 8.3 cm
Humidity	Up to 95% non-condensing
Compliance	EMC: FCC Part 15, EN 301 489-1 RF: ETSI EN 302 326, EN 302 544, ECC/REC/(04)05, FCC Part 27, FCC Part 90 Safety: IEC, EN and UL/CSA 60950 Environmental: IP 67
System Configuration	X-100 WebUI/X-100 CLI
Fault and Performance Management	Simple Network Management Protocol (SNMP)v2C/v3

[1]The copper Ethernet interface on the HM has priority over the fiber optical Gigabit Ethernet interface. If, for example, an on-site technician connects to the HM locally by the copper interface while the HM is providing network services to its users through the fiber interface, the fiber interface is then disabled and taken out of service. Network service through the fiber interface is restored when the copper interface is disconnected.

3.2 OFDMA and Frame Parameters

Orthogonal Frequency-Division Multiple Access (OFDMA) and Frame Parameters for 10 MHz channel bandwidth option are shown in Table 3. The frame duration or size is a user settable feature in the X-100 WebUI (through the Setup Page for the Radio Interface) and is part of system configuration.

Table 3 OFDMA and Frame Parameters for a 10 MHz Channel Bandwidth

Number of Subcarriers	1024			
Data Carriers	720			
Pilot Subcarriers	120			
Subcarrier Spacing	10.9375 KHz			
Frame Duration or Size	5 msec		3.125 msec	
Frames per Second	200		320	
Cyclic Prefix	1/8	1/16	1/8[1]	1/16
Number of Symbols	48	51	30[1]	32

3.3 Integrated RBM Antenna

The Remote Backhaul Module (RBM) features a high-quality antenna that has very low side lobes (-30 dBc) to minimize interference. This allows greater scalability of deployment of BLiNQ X-100 system modules in a market and allows smaller frequency reuse factor for higher spectrum utilization. Figure 3 shows the antenna patterns and compares them to standard off-the-shelf antennas typically available in commercial systems such as WiMAX Customer Premise Equipment (CPE) and other backhaul devices in the 3.5 GHz band.

High gain (17 dBi) and directivity (narrow horizontal beamwidth of 22 degrees) work to increase system gain and reduce the interference transmitted and received at angles away from the boresight of the antenna. This is critical for small cell mobile backhaul applications as the backhaul network is interference limited. It also works to increase the range in other types of applications where distance is the overriding factor.

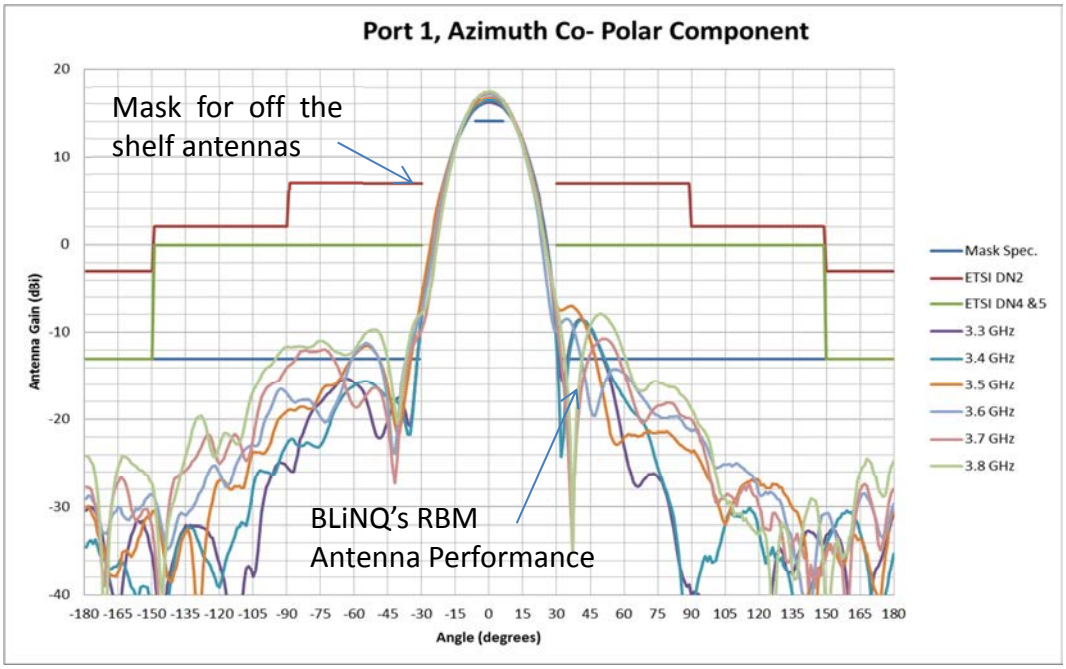


Figure 3 Horizontal antenna pattern (Port 1) for 3.5 GHz band

Table 4 Integrated Antenna Specifications in the 3.65 GHz Band

Gain	17.0 ± 1 dBi
Voltage Standing Wave Ratio (VSWR)	1.8:1 (max) 1.5:1 (typ)
-3 dB Azimuth Beam Width	22.5° ± 2°
-3 dB Elevation Beam Width	27° ± 3°
AZ and EL Beam Squint	± 2 °
Polarization	Dual Slant ± 45°
Port To Port Isolation	22 dB (min), 28 dB (typ)
Front to Back (F/B) Ratio	-45 dB (typ)

3.4 System Enclosure

The enclosure for both the Hub and RBM is a rugged IP67 casing supplied with an optional mounting bracket with both horizontal and vertical tilt capabilities to mount the unit on towers, poles, and building side walls while allowing full flexibility in the range of orientation to establish best connectivity between the Hub and RBMs.

In Figure 2, the mechanical enclosure for the HM has two RF port connectors for an external user-defined sectored antenna. Two connectors are also provided on the back of the HM: a -48 VDC power connector, and an RJ45 connector for 1000 BaseT copper Ethernet network connectivity. An optional small form-factor pluggable (SFP) fiber connector for optical Gigabit Ethernet network connectivity can also be installed in the field. An integrated Global Positioning System (GPS) antenna is shown on the top (flat square patch). Therefore, no additional synchronization equipment is required to reduce total cost of ownership.

Note: The copper Ethernet interface on the HM has priority over the fiber optical Gigabit Ethernet interface. If, for example, an on-site technician connects to the HM locally by the copper interface while the HM is providing network services to its users through the fiber interface, the fiber interface is then disabled and taken out of service. Network service through the fiber interface is restored when the copper interface is disconnected.

The RBM is the exact same size and dimension as the HM. It differs in that the antenna is integrated, hence there are no external RF connectors. Also, the RBM does not include an integrated GPS antenna as synchronization is available from the HM. There is also no provision for an SFP fiber connector.

4 Link Budget and System Gain

Table 6 lists the link budget for the BLiNQ X-100 system at 3.65 GHz in a 2x2 Multiple Input Multiple Output-Spatial Multiplexing (MIMO-SM) operation.

The X-100 system provides very high system gain (134 dB for 256 Quadrature Amplitude Modulation [QAM] 5/8 Modulation and Coding Scheme [MCS]). This is due to a relatively high transmit power for both the Hub and Remote Backhaul Modules (RBMs) (27 dBm per antenna port; a total of 30 dBm).

The X-100 system gain allows network design to incorporate a high fade margin to combat shadow and fast fading and enable high link availability in urban areas which is important in small cell mobile backhaul applications. Alternatively, high system gain translates into longer range in applications where this is required.

Table 5 Link Budget for X-100 System at 3.65 GHz in a 2x2 MIMO-SM Operation

Transmitter	**256-QAM 7/8**	**256-QAM 6/8**	**256-QAM 5/8**	**64-QAM 5/6**	**64-QAM 3/4**	**64-QAM 2/3**	**64-QAM 1/2**	**Units**
Power per Stream	23	23	23	23	23	23	23	dBm
Hub Antenna Gain	17	17	17	17	17	17	17	dBi
Tx Losses	0.25	0.25	0.25	0.25	0.25	0.25	0.25	dB
EIRP (per Stream)	39.8	39.8	39.8	39.8	39.8	39.8	39.8	dBm
Receiver	**256-QAM 7/8**	**256-QAM 6/8**	**256-QAM 5/8**	**64-QAM 5/6**	**64-QAM 3/4**	**64-QAM 2/3**	**64-QAM 1/2**	**Units**
Thermal Noise	-174	-174	-174	-174	-174	-174	-174	dBm/Hz
Noise Figure	4	4	4	4	4	4	4	dB
Noise BW (per Tone)	10.9375	10.9375	10.9375	10.9375	10.9375	10.9375	10.9375	kHz
Receive Noise Floor (per Tone)	-129.6	-129.6	-129.6	-129.6	-129.6	-129.6	-129.6	dBm
RBM Antenna Gain	17	17	17	17	17	17	17	dBi
Required RX Power per Branch	-65.5	-74.4	-75.5	-76.8	-78.7	-79.7	-83.6	dBm
System Gain (dB)	122.3	131.2	132.3	133.6	135.5	136.5	140.4	dB

Table 7 shows the system gain at 3.65 GHz for different modulation rates and the associated capacity and Non-Line-of-Sight (NLOS) distance for 99.9% availability in urban and rural environments.

Table 6 NLOS Range at 3.65 GHz for 2x2 MIMO-SM Mode

Modulation	System Gain (dB)	Capacity (Mbps)	NLOS (m) (99.9% Link Availability)	
			Urban (SUI 5/6)	Rural (SUI 1/2)
256QAM7/8	122.25	83	243	425
256QAM6/8	131.15	71	373	700
256QAM5/8	132.25	61	454	880
64QAM5/6	133.55	59	483	946
64QAM3/4	135.45	53	529	1,052
64QAM2/3	136.45	47	555	1,113
64QAM1/2	140.35	35	669	1,384

The system gain for maximum distance calculations for the lower modulation schemes is shown in Table 8 for a single antenna operation (that is, Single Input Single Output [SISO]) with receive diversity gain of 3 dB included to account for 2-branch maximal ratio combining.

Table 7 System Gain for Lower Modulation and Coding Schemes; Includes Maximal Ratio Combining (MRC) Gain

Modulation	Required Rx Power (dBm)	System Gain (dB)
16QAM3/4	-85	144.75
16QAM2/3	-88.7	148.45
QPSK3/4	-91.3	151.05

4.1 System Trade-offs

Range, capacity and reliability are three factors that can be traded off against each other. The higher the fade margin, the lower the reach of the X-100 is to achieve a certain capacity target. For example, Figure shows a system gain of 136 dB for 256-QAM 5/8 MCS which results in a throughput of 61 Mbps. Budgeting 25 dB of fade margin for 99.9% availability results in a maximum allowable path loss of 136-25 = 111 dB, or a corresponding range of just over 400 m. Higher reliability is possible by using a larger fade margin which reduces the distance. Alternatively, higher reliability can be achieved at this range with a lower MCS such as 64-QAM 3/4.

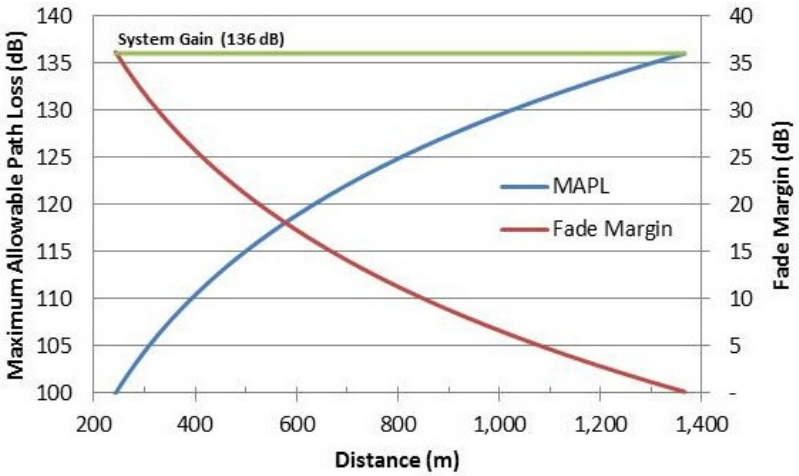


Figure 4 Performance Versus Distance for 256 QAM 5/6 MCS

The BLiNQ proprietary Managed Adaptive Resource Allocation (MARA) interference management technology built into the X-100 system contributes to increasing the link availability while also providing higher capacity.

5 System Synchronization

The X-100 system is a Time Division Multiplexed (TDD) radio system. Therefore, X-100 networks require proper synchronization of the air interface to provide optimal service. The X-100 system is designed to provide flexible synchronization options as well as provide a high-performance extension to existing synchronization networks to provide quality clock services to downstream devices such as small-cells.

The X-100 system is synchronized at the Hub Module (HM) using one of two standard synchronization mechanisms: Global Positioning System (GPS) or IEEE 1588v2.

When configured to synchronize on GPS, the X-100 system uses its internal GPS antenna and receiver module to synchronize to the GPS network. This allows all X-100 HMs deployed in the network to accurately synchronize their transmit and receive operations on the air interface. The GPS system also allows the X-100 system to determine accurate time of day and date information. This time information together with a user configured timezone setting is used to inform time across the system and is essential in functions such as fault management (for example, event and alarm timestamping) and historical performance (for example, performance indicator processing and performance file creation). Time information is automatically transmitted from the HM to any Remote Backhaul Module (RBM) associated to that HM.

When configured to synchronize on IEEE 1588v2, the X-100 system synchronizes to IEEE 1588v2 master clocks deployed on the operator network. The HM can either be configured to use a specific master clock (by providing the master clock identity) or can perform the standard Best Master Clock (BMC) Algorithm to select the best available master clock on the network. Just like GPS, the IEEE 1588v2 infrastructure allows the HM to precisely synchronize its air interface. It also provides accurate time of day information.

The X-100 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 or IEEE 1588v2) is no longer available. The system is designed to provide a Holdover period of 10 minutes. During this time the radio is operational and the system attempts to recover its primary clock source. If the clock source has not be reacquired after the Holdover period expires, the system is deemed “Not synchronized” and therefore ceases radio operation so as to not interfere with other deployed X-100 systems.

5.1 Synchronization Services

Based on its high-performance internal synchronization mechanisms, the X-100 system is designed to provide in-band synchronization services to downstream devices using the IEEE 1588v2 protocol. The HM and RBMs include IEEE 1588 capable Ethernet PHY modules that provide accurate hardware based timestamping, necessary for high-performance synchronization applications.

The X-100 system supports two operating modes for synchronization services, depending on the primary clock reference used at the HM: GPS or IEEE 1588v2..

In the first mode, the HM uses the GPS as its primary clock reference. Based on the intrinsic synchronized nature of the HM to RBM protocol, the clock reference is accurately transported at the RBM and therefore the entire cluster implements the behavioral requirements of an IEEE 1588v2 master clock. The X-100 system allows the configuration of the main IEEE 1588v2 master clock parameters such as transport protocol and messaging intervals.

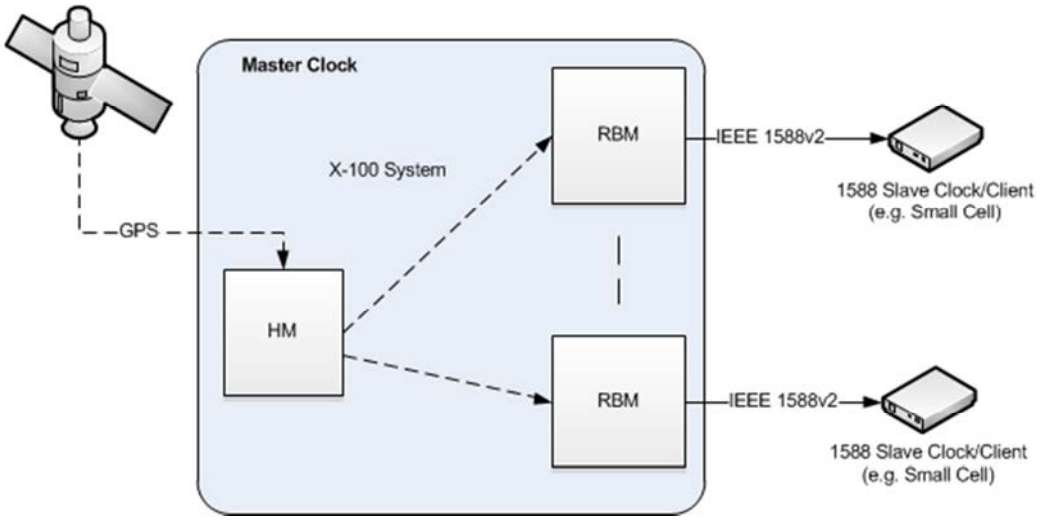


Figure 5 System Synchronization Using GPS

In the second mode, the HM is configured to synchronize using the IEEE 1588v2 network, making the X-100 cluster effectively behave as an IEEE 1588v2 boundary clock. The system provides master clock services at the RBM Ethernet port, and advertises itself as a boundary clock that uses the same grandmaster clock as the HM parent clock. In this mode, all upstream IEEE 1588 messaging is dropped at the HM.

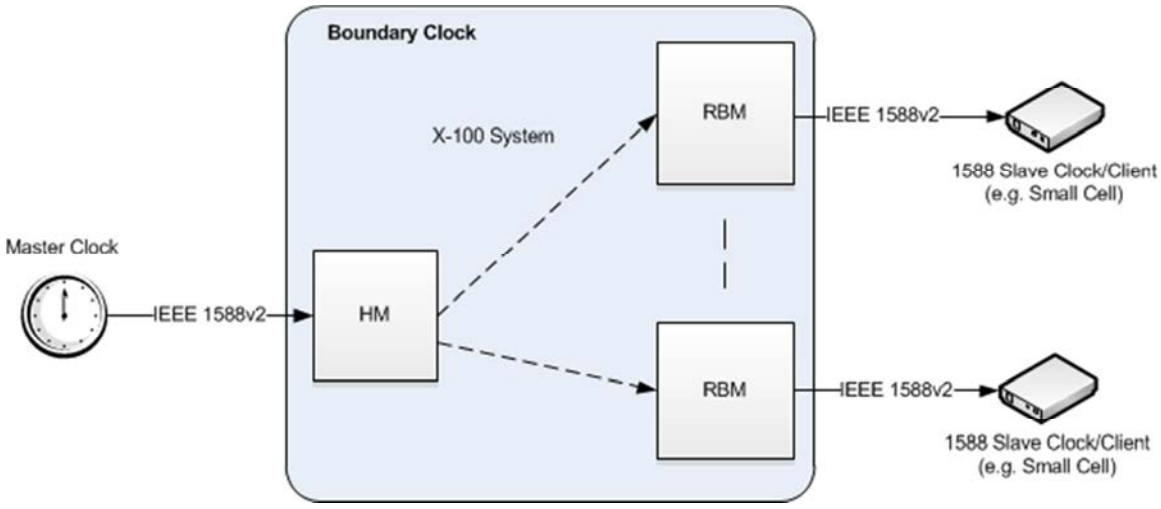


Figure 6 System Synchronization Using IEEE 1588v2

6 System Throughput

The X-100 system uses time division duplexing (TDD) access mode, employing a single frequency for both transmit and receive paths. The throughput for the downlink and uplink depends on several user-settable parameters such as frame duration or size (3.125 or 5 ms), downlink-to-uplink frame bandwidth ratio (option of 50:50 or 65:35), and the number of Remote Backhaul Modules (RBMs) connected to a Hub Module (HM). Furthermore, the system throughput depends on the Modulation and Coding Rate (MCS) and whether the Multiple Input Multiple Output-Spatial Multiplexing (MIMO-SM) mode is active, both of which vary according to link and signal conditions.

Note: Frame length of 3.125 msec not supported in current release.

Tables 9 and 10 show the maximum link throughput for the X-100 system assuming 10 MHz channel MIMO operation which doubles the channel throughput by transmitting two independent codewords on each antenna.

Note: System throughput is set using the X-100 WebUI Setup Page for the Radio Interface. See 10.3.4 for details.

Table 8 Throughput Performance for Cyclic Prefix of 1/8

TDD Frame Length, DL/UL	5 ms, 20/20				3.125 ms, 12/10			
MCS	1 RBM	2 RBMs	3 RBMs	4 RBMs	1 RBM	2 RBMs	3 RBMs	4 RBMs
256-QAM 7/8[1]	76.0	73.1	70.0	67.0	64.5	60.6	54.9	49.9
256-QAM 6/8	65.0	62.6	60.1	57.6	55.3	52.1	47.1	42.5
64-QAM 5/6	54.2	51.9	49.8	47.7	45.9	43.2	39.0	35.1
64-QAM 3/4	48.7	46.8	44.6	42.7	41.1	38.7	34.9	31.4
64-QAM 2/3	43.3	41.5	39.9	37.8	36.7	34.5	30.9	27.7
16-QAM 3/4	32.3	31.0	29.6	28.4	27.5	25.8	23.1	20.3
16-QAM 1/2	21.5	20.5	19.6	18.5	18.3	17.0	15.0	13.0
QPSK 3/4	16.1	15.2	14.5	13.5	13.5	12.6	10.9	9.3

Table 9 Throughput Performance for Cyclic Prefix of 1/16

TDD Frame Length, DL/UL	5 ms, 22/22				3.125 ms, 12/12			
MCS	**1 RBM**	**2 RBMs**	**3 RBMs**	**4 RBMs**	**1 RBM**	**2 RBMs**	**3 RBMs**	**4 RBMs**
256-QAM 7/8[1]	83.5	80.4	77.1	73.7	70.4	67.4	64.4	54.5
256-QAM 6/8	71.5	68.9	66.2	63.4	60.3	57.9	55.5	46.4
64-QAM 5/6	59.6	57.2	54.8	52.5	50.2	48.0	45.9	38.4
64-QAM 3/4	53.6	51.5	49.2	47.1	44.8	43.0	41.2	34.3
64-QAM 2/3	47.6	45.6	43.9	41.6	40.1	38.5	36.4	30.3
16-QAM 3/4	35.7	34.1	32.6	31.3	30.0	28.6	27.4	22.3
16-QAM 1/2	23.7	22.6	21.7	20.4	20.0	19.0	17.9	14.2
QPSK 3/4	17.7	16.7	16.0	14.9	14.8	14.1	13.1	10.2

7 Element and Network Management

Designed to provide comprehensive Fault, Configuration, Accounting, Performance, and Security (FCAPS) functionality, the X-100 system uses standard networking protocols and tools that facilitate a full range of element and network management operations—from local craft configuration, to complex integration in Simple Network Management Protocol (SNMP) or script-based Network Management System (NMS) and Operations Support System (OSS) infrastructures.

The X-100 system supports the following network management Interfaces:

- **X-100 Command Line Interface (CLI)**. Accessible via Secure Shell protocol (SSH), the X-100 CLI provides a well-structured command language in an industry standard idiom. The interface allows an operator (or third-party system) to manipulate the full configuration of the unit and examine state, performance and fault indicators.
- **X-100 Web Interface (WebUI).** Accessible via HTTP(S), the X-100 WebUI provides an interactive visual toolset that allows an operator to modify the full configuration of the X-100 system as well as view state, fault, and performance indicators. The performance data is displayed using visual charts, and applications are provided to visualize up to 24 hours of historical performance data stored on the system.
- **Community-Based Simple Network Management Protocol version 2 (SNMPv2C) and SNMP version 3 (SNMPv3).** The SNMPv2C and SNMPv3 interfaces provides complete access to configuration, state, performance and fault information in the X-100 system to allow for high levels of integration in existing NMS/OSS infrastructure for monitoring, Service Level Agreement (SLA) assurance, and administrative task automation.
- **Syslog.** The syslog interface allows the X-100 system to send standard syslog fault management information (that is, syslog alarms, events, and log entries) from itself to external syslog servers.

All network management interfaces on the X-100 system are accessible via Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/IP (UDP/IP). The X-100 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 VLAN encapsulation. This address is always present on both the Hub Modules and Remote Backhaul Modules (RBMs) and should be used in situations where the Management IP Address (see below) is not configured or is unavailable, including initial commissioning and field troubleshooting scenarios. Typically, the Local Craft IP Address is accessed by an operator by plugging in directly in the RJ-45 Ethernet port of the module.

  Note: The RJ-45 port has priority over the optional optical connector on the HM. If the latter is installed and the operator plugs into the RJ-45 port, the fiber connection is disabled as long as the RJ-45 port is active.

- **Management IP Address -** An operator assigned, static or Dynamic Host Configuration Protocol (DHCP) IP address used for remote management of the units. Both HMs and RBMs need a management IP address. For the HM the management IP Address is accessible from the Ethernet side of the network, while for the RBM the management IP Address is accessible from the wireless side (that is, from behind the HM). All traffic to and from the management IP address can be encapsulated in an operator-configurable Virtual Local Area Network (VLAN).

The X-100 system provides the following network management functions:

- **Configuration Management**. The system configuration covers several functional areas:
    - radio link commissioning
    - service flow provisioning
    - bridge configuration
    - security configuration

  All parameters in these areas are accessible via all the network management interfaces described previously.
    - The radio link commissioning parameters (for example, radio frequency, synchronization, radio frame size, TDD downlink/uplink ratio, preamble indexes) need to be set *before* system deployment and are particular to the RF network of the operator.
    - Service Flow Provisioning parameters are set on the HM to configure the quality parameters for the over-the-air service flows provided to RBMs. The system supports both a simple provisioning model based on a default service flow configuration, or an advanced provisioning model where service flow parameters can be configured individually for each RBM.
    - The bridge configuration parameters control the Ethernet bridge and core network data behavior of the X-100 cluster.
    - The security configuration parameters allow the operator to secure access or disable specific management interfaces and perform various unit administrative operations.
- **Fault Management**. The X-100 system provides fault management service via a comprehensive list of alarms and events. Some of the potential faults that the system is able to detect and alarm upon include:
    - radio and Ethernet link failures
    - hardware module failures
    - synchronization faults
    - software module faults

  All alarms and events are relayed to higher level managers via SNMP traps or Syslog. The system also allows operators to access active alarm and event history information using either the X-100 CLI or X-100 WebUI.
- **Performance Management.** The X-100 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 either instantaneous values (via SNMP, CLI or WebUI), or historical performance files. The system maintains 24 hours of performance data at a 15 minute granularity. Performance files are stored only on the HM and can be extracted from the system on-demand.

  Alternatively, the system can be configured to automatically push these files to an operator-

provided File Transfer Protocol (FTP) server.

- **Administrative Operations.** The X-100 system provides tools that allow operators 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 FTP servers), or a push scheme using the X-100 WebUI (that is, the operator uploads a software package file to the system modules using the X-100 WebUI). The X-100 system also supports remote configuration backups and backup restoration.

8 Ethernet Bridge Support

Designed to seamlessly integrate into existing Ethernet backhaul or general purpose networks, the X-100 system is built for Ethernet services and provides network functionality as a standard Layer 2 (L2) Transparent Bridge (IEEE 802.1d), whereby the X-100 cluster (a cluster being one Hub Module [HM] with its group of up to four Remove Backhaul Modules [RBMs]) is the bridge, and the Ethernet ports on the HM and associated RBMs are the ports of the bridge.

The embedded bridge functionality performs Media Access Control (MAC) address learning (up to 4096 MAC addresses). This function allows the HM to perform an optimal allocation of radio resources by sending traffic to the RBM behind which the destination of that traffic is actually located. In addition, the X-100 system provides support for advanced traffic classification and prioritization as part of its service provisioning model. Service flow definitions can be used to engineer traffic so that specific packets are either dropped or forwarded under a specific Quality of Service (QoS) provision.

The X-100 scheduler supports two Classes of Service (CoS): Guaranteed Bit Rate (GBR) and Best Effort (BE). The GBR CoS is designed for latency sensitive traffic (such as voice) and provides an “always on” channel that is able to transport designated packets as soon as they arrive in the system. The BE CoS provides a balanced resource allocation between multiple RBMs in a cluster and ensures radio resource fairness between them. The X-100 scheduler contains proprietary optimizations such as CoS overflow/underflow that allow for an optimal utilization of radio resources in situations where certain service flows are either under or over loaded beyond their designed capacity.

The X-100 classification engine allows the operator to define complex classification rules using basic boolean constructs and packet field matching criteria. The following fields are supported:

- Layer 2 Ethernet frame fields: source/destination MAC Address with masking options, EtherType, VLAN (802.1q), S-VLAN, C-VLAN (as per 802.1ad QinQ)
- Layer 3 IP packet fields: source/destination IP address with masking option, Type of Service (ToS).

The X-100 system can also provide specialized processing of data traffic at the HM Ethernet port (towards the core network). The operator can choose to either pass traffic transparently or, alternatively, encapsulate the data traffic in an L2 tunnel through a Virtual Local Area Network (VLAN) by using the stacking VLAN processing scheme. The system also allows network management traffic to be encapsulated in a dedicated management VLAN.

The X-100 system can transport standard Ethernet frames (up to 1518 bytes) as well as mini Jumbo frames of up to 2048 bytes.

9 Installation Planning

For full installation instructions see the X-100 System Installation Guide.

 **WARNING!**	**Adhere to all safety warnings in the Installation Guide. Failure to do so could result in personal injury or death, or damage to the equipment.**

When planning the installation of X-100 systems, consider the following:

- Delegate installation and repairs to an experienced installer
- Determine if lightning protection is needed and install if required

Be sure to do the following upon unpacking the X-100 system modules. For each Hub and RBM module in your system:

- Locate the label on the module casing that lists the Serial Number (SN) and Media Access Control (MAC) address for the module
- Record the SN on your registration card for future reference
- Record the MAC address for future reference when provisioning the system

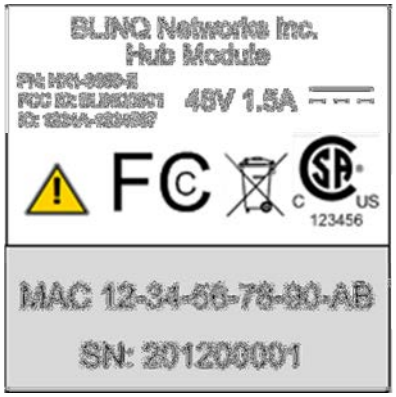


Figure 7 Module Casing Label Example

After installation of the X-100 system modules, perform the tasks described in Chapter 13 “System Provisioning”, and Chapter 14 “Preambles, Flows, and Network Provisioning”, as applicable for your network.

10 Using the X-100 WebUI

10.1 Requirements

The X-100 WebUI is the configuration tool for use with X-100 Hub Modules (HMs) and Remote Backhaul Modules (RBMs). It is a standard web application that runs directly on the X-100 equipment through the default port for HTTP (80), and is accessible at URL http://<*ip of the node*>.

Browser support for X-100 WebUI:

- Mozilla Firefox (Fx)
- Internet Explorer (IE9)
- Safari

Operating System (OS) support for X-100 WebUI:

- Windows
- Mac OS X
- Unix
- Linux

Note: With the exception of IE9, both web browser and OS support for the X-100 WebUI always refer to the most recent versions (for example: Fx17 running on Windows 7).

All required X-100 system configuration tasks can be performed using the X-100 WebUI.

As an alternative, you can use the X-100 Command Line Interface (CLI) for system monitoring and configuration tasks. See Chapter 12 for details.

10.2 Common X-100 WebUI Page Items

Most X-100 WebUI pages have either an **Apply** button or a **Refresh** button or both at the bottom right hand corner.

If you change the settings on a page, ensure to click on **Apply** before navigating to another page. Read-only data on a page can be updated to their current values at any time by clicking on the **Refresh** button.

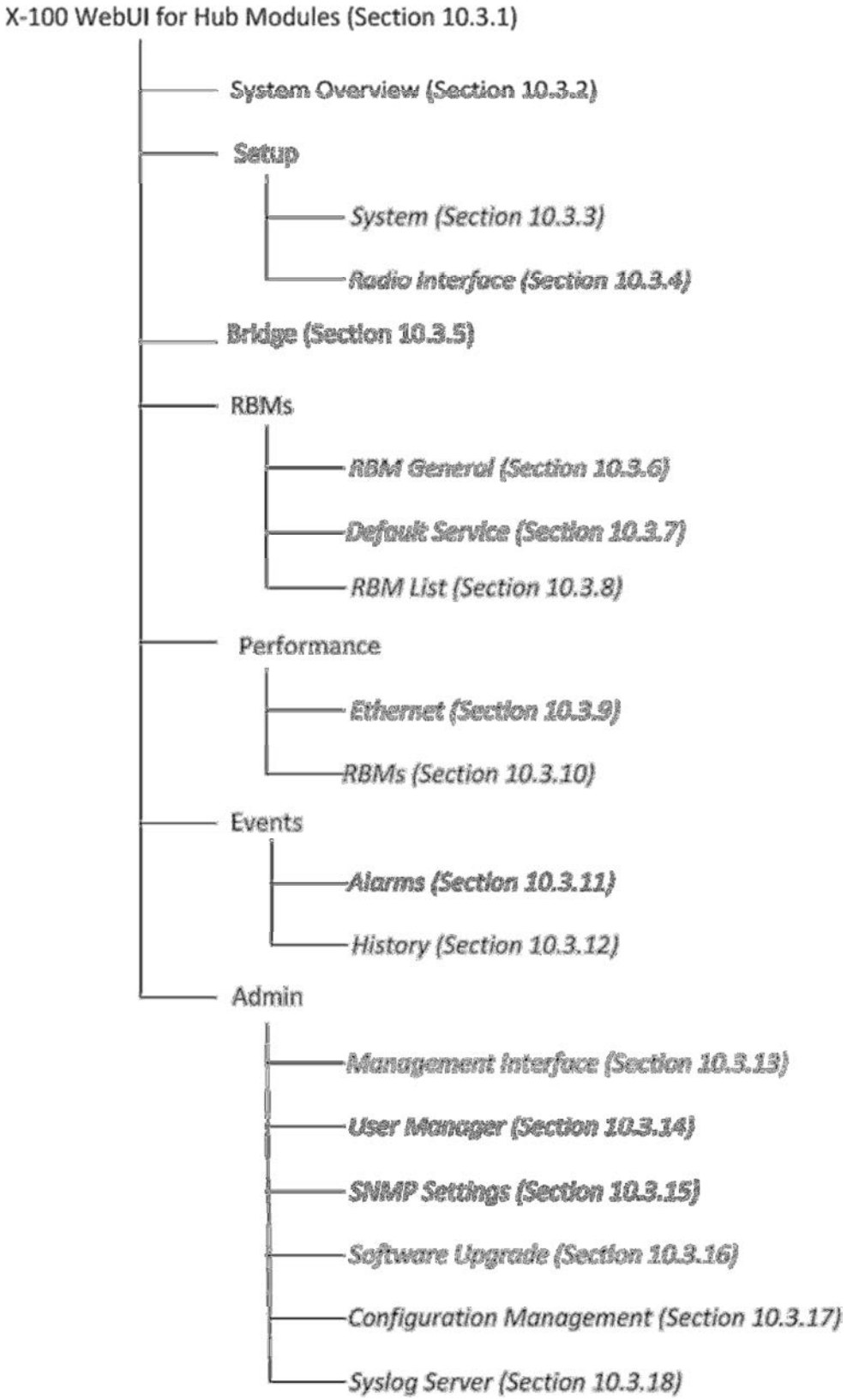
The Hub Module or RBM can be rebooted at any time by clicking on the **Reboot** button at the top of every page.

Any change in configuration can be saved by clicking on the **Save Config** button. This new configuration change will then be loaded upon a system reset. The **Save Config** button remains grayed out until changes are applied via the **Apply** button.

End each session by clicking on **Logout** on the right.

Several pages present graphs of various parameters. By default these have a two minute rolling x-axis. To zoom in on part of this time, hold the **Left Mouse Button** down and move the mouse to enclose the amount of time desired. To reset the default x-axis, click on the **Reset Zoom** button.

10.3 Configuring Hub Modules



10.3.1 Logging In

To log in and access the X-100 WebUI interface for configuring Hub Modules (HMs), do the following:

1. Launch your web browser and set it to allow pop ups (as some screen functions in the X-100 WebUI require pop ups).

   For Firefox: Click on **Tools > Options > Content** and uncheck **Block pop-up windows**. Alternatively, click on the **Exceptions** button and enter a list of Hub IP addresses you will be configuring.

2. If there is a direct connection to the HM (that is, not over a network), use your browser to go to http://169.254.1.1.
3. If connecting over a network to the HM (that is, not locally), use your browser to connect to the management IP address of the Hub.
4. Log on to the system. The default username and password are **admin**:

   User Name: admin
   Password: admin

Note:

- User names and passwords are administered through the X-100 WebUI Admin Page using the User Manager sub-page and can be changed anytime (see section 10.3.14 for details).
- User names must start with a letter and may be composed of alphanumeric characters only.
- Passwords are case sensitive, may be composed of alphanumeric characters and special characters, and must contain at least one letter and one digit.
- At least one user with read/write privileges needs to exist in the X-100 system.
- If you cannot login due to a forgotten user name or password, contact another user with read/write access privileges to have them reset your login credentials. If you have lost all read/write login credentials, contact your supplier.

10.3.2 System Overview Page

This read-only page gives general system information on the particular Hub you are logged in to. The RBMs associated with this Hub are also listed along with their information.

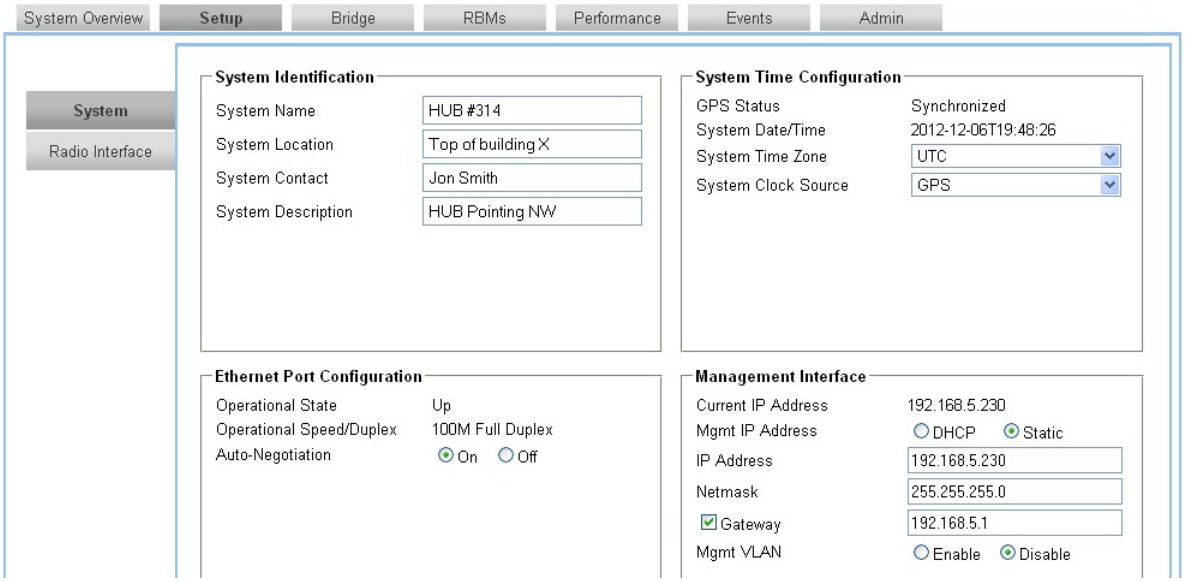
Further, it visualizes the incoming and outgoing traffic for the RBM and Ethernet connections using two graph lines. This allows the user to see traffic and bandwidth usage for the system RBMs and Ethernet interfaces in a real-time, graphical format, and monitor the current download/upload throughput speeds.

The System Overview page also lists the current alarm information at the bottom.

Note: The blue graph line represents the downlink throughput rate, while the red graph line represents the uplink throughput rate. Screen refresh interval is every 5 seconds. For system statistics based on these graphs, see section 10.3.9 for Performance Page (Ethernet) and section 10.3.10 for Performance Page (RBMS).

10.3.3 Setup Page (System)

This sub-page handles configuration of system parameters that govern basic Hub Module operation.



System Identification: Enter information here as desired to aid system identification.

System Name: Name of the module, composed of alphanumeric characters, underscores, and dashes.

System Location: Physical location of the module, composed of alphanumeric characters, underscores, and dashes.

System Contact: Contact information for the module owner, composed of alphanumeric characters, underscores, and dashes. Can also include @ for an email address.

System Description: Description of the module, composed of alphanumeric characters, underscores, and dashes.

Ethernet Port Configuration:
Operational State: (Up/Down) (Read only)
Operational Speed/Duplex: e.g. 100M Full Duplex (Read only)
Auto-Negotiation: (On/Off)
If auto-negotiation "Off", set the following (as applicable):
Configured Speed: 10M/100M/1000M
Configured Duplex: Auto/Full/Half

System Time Configuration:
GPS Status: Synchronized/Not-Synchronized (Read only)
System Date/Time: e.g. 2013-01-01T00:12:24 (Read only)
System Time Zone: Set relative to UTC
System Clock Source: Always set to GPS (not FreeRun)

Note: The "FreeRun" mode is intended for isolated trial or laboratory testing of the X-100 system only. Networks of X-100 systems depend on proper synchronization through either GPS or IEEE 1588v2[1] clock references to operate optimally, and may experience significant performance degradation or even outage if not deployed accordingly. The following system services are also affected in "FreeRun" mode: system time; reporting of time as part of the fault management function; historical performance functions.

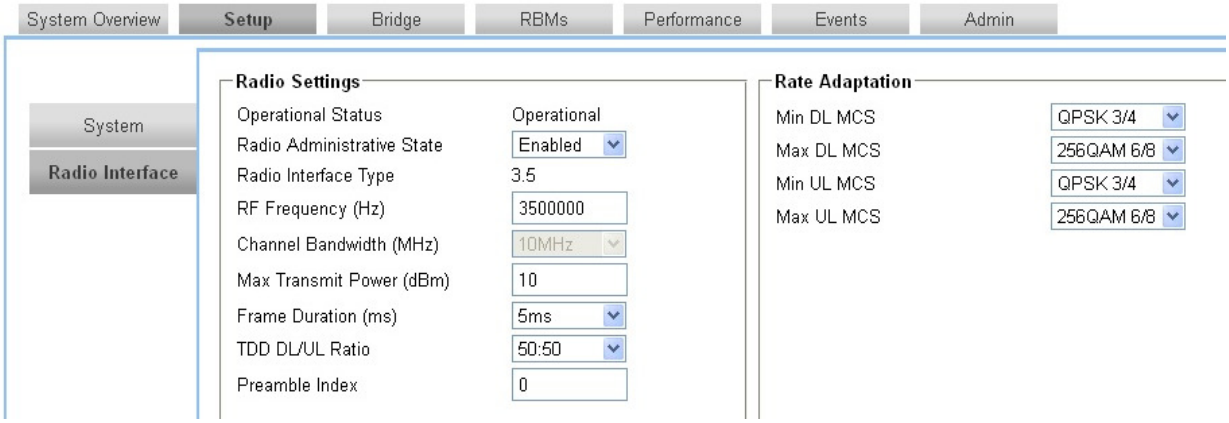
Management Interface:

Current IP Address: xxx.xxx.xxx.xxx (Read only)
Mgmt IP Address: DHCP/Static, set as desired
If "Static" set the following:

- Gateway: If this is to be used, set check box and enter gateway IP address
- IP Address: Set to Hub IP address (if not so already)
- Netmask: Set to subnet mask address
- Mgmt VLAN: Enable/Disable (if set to Enable enter ID)

10.3.4 Setup Page (Radio Interface)

This sub-page handles configuration of the radio operation for the Hub Module.



Radio Settings:

Operational Status: Operational/Down (Read only)
Radio Administrative State: Enabled/Disabled
Radio Interface Type: 3.5 (Read Only)
RF Frequency: Set as appropriate
Channel Bandwidth: 10 MHz (Read Only)
Max. Transmit Power: Enter between -18 dBm to 23 dBm for the 3.65 – 3.7 GHz non-exclusive licensed band.
Enter higher values for large Hub/RBM distances, and
lower values for smaller distances so that receiver does not saturate.
Frame Duration: 3.125[1] or 5 ms

[1]Not supported in current release.

TDD DL/UL Ratio: Set uplink to downlink bandwidth ratio to 50:50 or 65:35, as desired
Preamble Index: Enter preamble index value 0 to 31 (factory default is 0); refer to

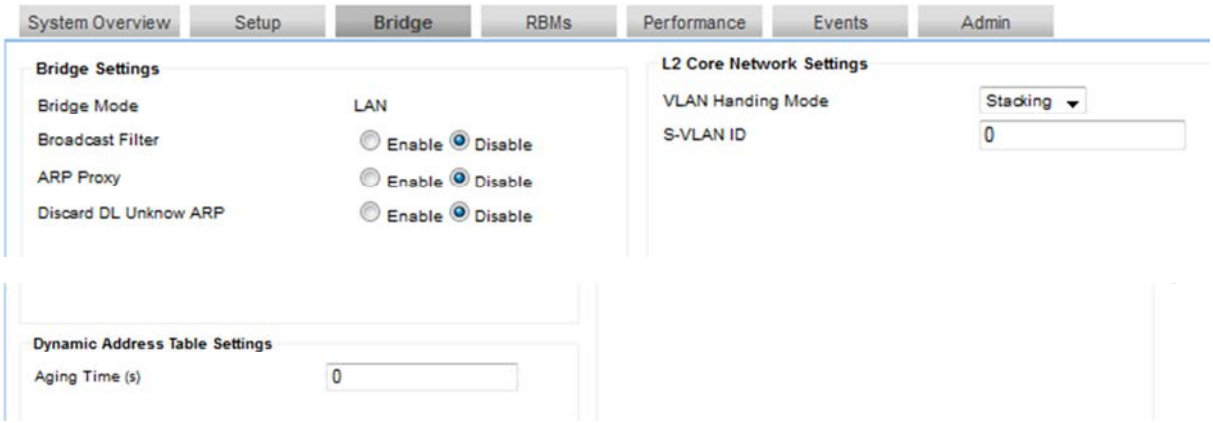
Chapter 14 for more information on use of preamble indices

Rate Adaptation:
Minimum and Maximum Uplink and Downlink Modulation and Coding Scheme (MCS)
For each, set to one of the following (as applicable):

- QPSK3/4
- 16QAM 1/2
- 64QAM 1/2
- 64QAM 2/3
- 64QAM 3/4
- 256QAM 5/8
- 256QAM 6/8

10.3.5 Bridge Page

This page handles configuration of standard Layer 2 Ethernet bridging for the Hub Module.



Bridge Setttings
Bridge Mode: LAN (Read only)
Broadcast Filter: Enable/Disable
ARP Proxy: Enable/Disable
Discard DL Unknown ARP: Enable/Disable

L2 Core Network Settings
VLAN Handling Mode: None/Stacking (if set to Stacking enter ID)

(if set to Stacking enter ID)
S-VLAN ID

Dynamic Address Table Settings
Specifies and saves in the running configuration the amount of time that elapses before an entry in the

Layer 2 MAC dynamic address table is discarded.

Note: If you specify 0 (the default), MAC aging is disabled.

Aging Time (sec): Set as desired. Allowable entries: 0 to 65535 seconds (default is 0).

10.3.6 RBMs Page (RBM General)

The X-100 system is a connection-oriented wireless technology. As such, an RBM cannot transmit data until it has been allocated a channel from its associated Hub Module (HM). This is to provide strong support for Quality of Service (QoS). Each connection between an RBM and its associated Hub in the X-100 system is supported by two or more service flows (at least one in the downlink direction and one in the uplink direction). The default for each RBM connection in the X-100 system is one flow in the downlink direction and one in the uplink direction. Each HM can support up to 16 service flows in the downlink and uplink direction, respectively, for a total of 32 service flows, while up to four service flows can be configured per RBM in the downlink and uplink direction, respectively, for a total of eight service flows.

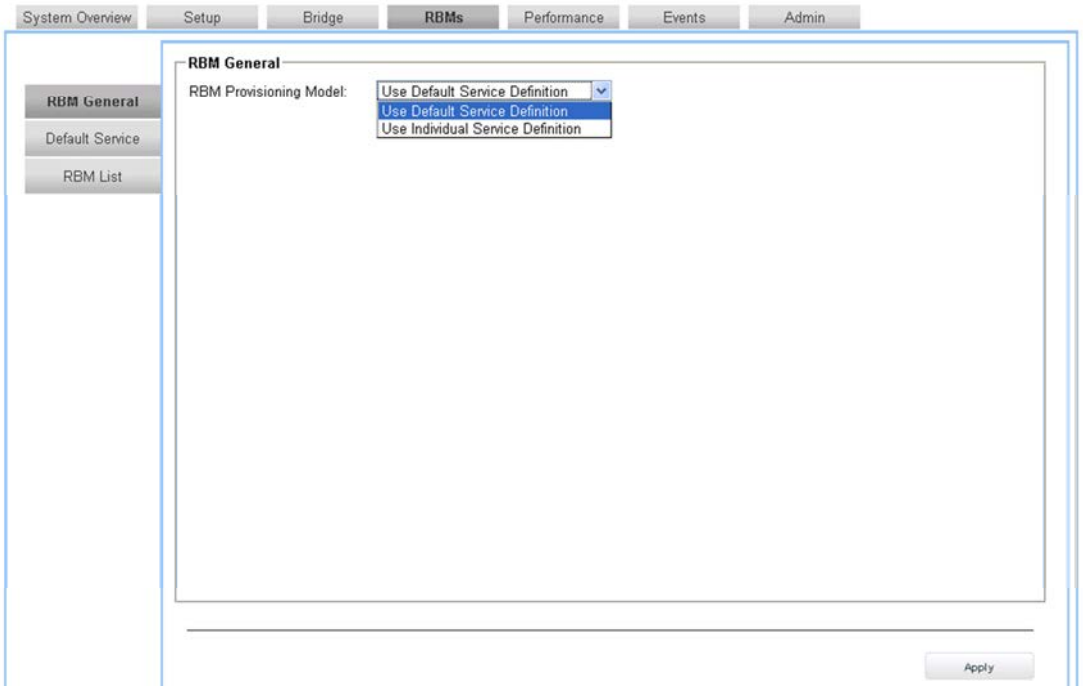
The RBM and Hub use a service flow with an appropriate QoS class (plus other parameters, such as priority and classifiers) to ensure that application data receives the QoS treatment appropriate to the user application. The QoS is supported by allocating each service flow a specific QoS class, of which there are two in the X-100 system: Guaranteed Bit Rate (GBR), and Best Effort (BE). The GBR class is for data streams for which the most stringent service scheduling is required, with guarantees on throughput, latency, and jitter. The BE class is for data streams for which no minimum service level is required and therefore may be handled on a space-available, no guarantee basis. Classifiers further define the scope of service flows.

On startup the X-100 system automatically finds all the RBMs connected to it. Through this sub-page you can make the HM either:

- apply the default service flow definition to all RBMs, as set through the ‘RBMs (Default Service)’ sub-page, by clicking **Use Default Service Definition** from the list box, or
- apply individual service flow definitions to these RBMs on an RBM-by-RBM basis, as set through the ‘RBMs (RBM List)’ sub-page, by clicking **Use Individual Service Definition** from the list box

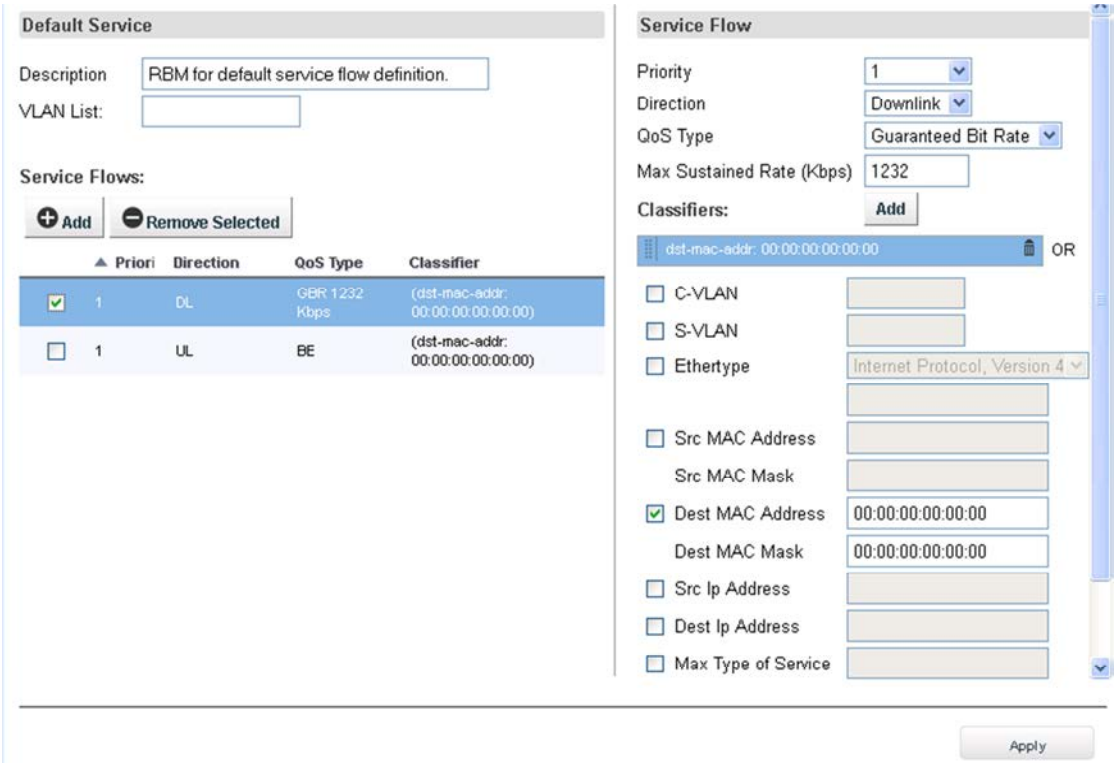
  Note: You can only use one RBM provisioning model at a time.

Click **Apply** for the chosen RBM provisioning model to take effect.



10.3.7 RBMs Page (Default Service)

On this sub-page you can edit the RBM configuration data for the default service flow definition. Click **Apply** for the changes to take effect.



Service Flow

Select a Service Flow from the list at the left. Details appear on the right where they can be edited. To delete a Service Flow, click on a check box on the list at the left and click on the **Remove Selected** button. Add a Service Flow by clicking on the **Add** button. Up to four service flows can be configured per RBM in the downlink and uplink direction, respectively.

Editing a Service Flow

Priority: If more than one service flow is defined for an up or down link, set priority (0 is highest, 7 is lowest)

Direction: Downlink/Uplink

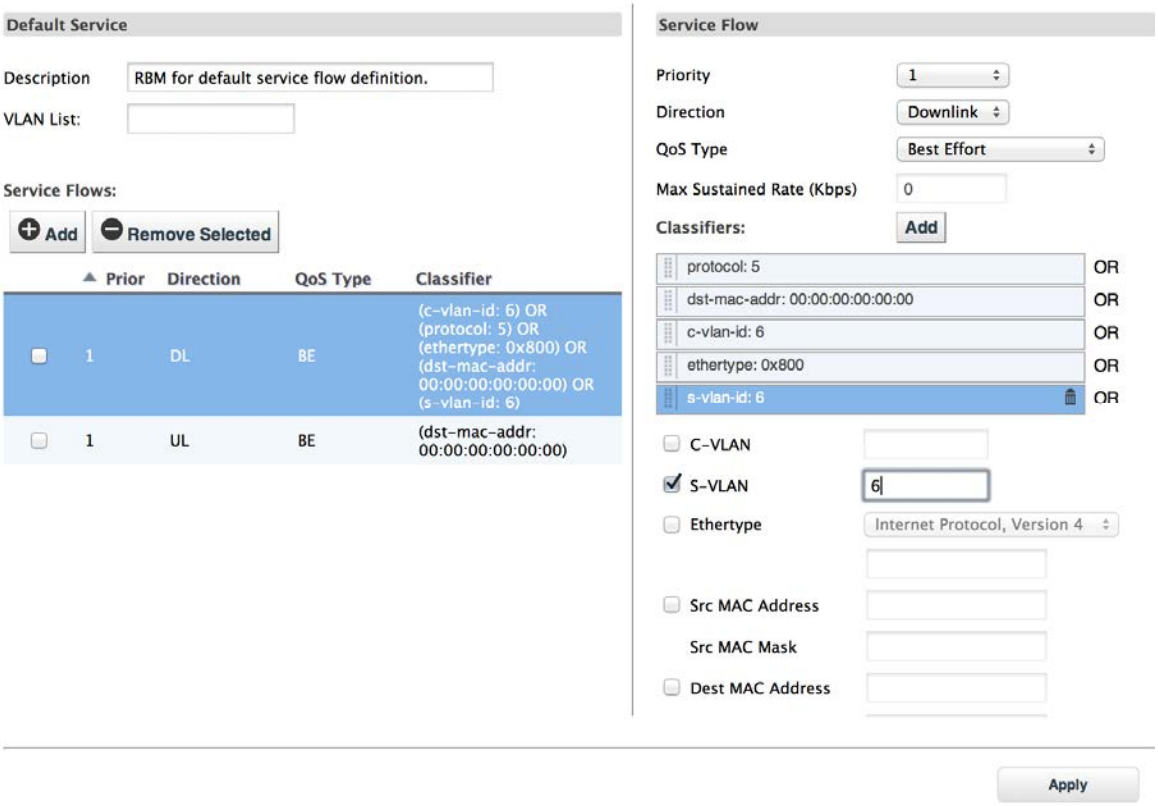
QoS Type: Best Effort/Guaranteed Bit Rate

If "Guaranteed Bit Rate" set:

Max Sustained Rate (kbps)

Classifiers for a Service Flow

Classifiers further define the scope of service flows.



Modify an existing Classifier by clicking on it. The Classifier becomes blue. Set the parameters below it as appropriate. Each check box that is clicked adds an additional requirement for transmission to occur for that Classifier, that is, Boolean AND logic is in effect on each Classifier in a service flow. Changes are detailed on both the left and right of the window.

Add a new Classifier by clicking on **Add**. A new Classifier appears in blue. Set the parameters below it as

appropriate. Up to eight Classifiers can be configured per service flow, with Boolean OR logic in effect on multiple Classifiers in a service flow.

Change the order and priority of Boolean OR operations for multiple Classifiers by drag and drop. The higher up the order the Classifier is, the higher its priority within Boolean OR operations.

To delete a Classifier, click on the trash can icon next to it.

Layer 2 Classifier parameters include:

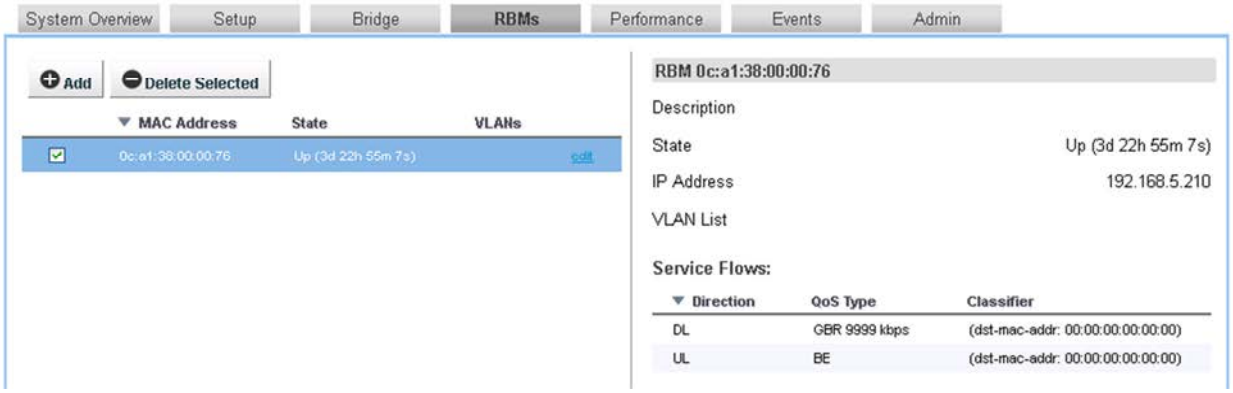
- Source MAC Address/Mask
- Destination MAC address/Mask

Layer 3 Classifier parameters include:

- Source IP Address
- Destination IP Address

10.3.8 RBMs Page (RBM List)

On this sub-page you can review RBM information on an RBM-by-RBM basis, as well as add or delete RBMs from the Hub. You can also edit RBM configuration data for individual service flow definitions on an RBM-by-RBM basis. The RBMs are referred to by their MAC address.



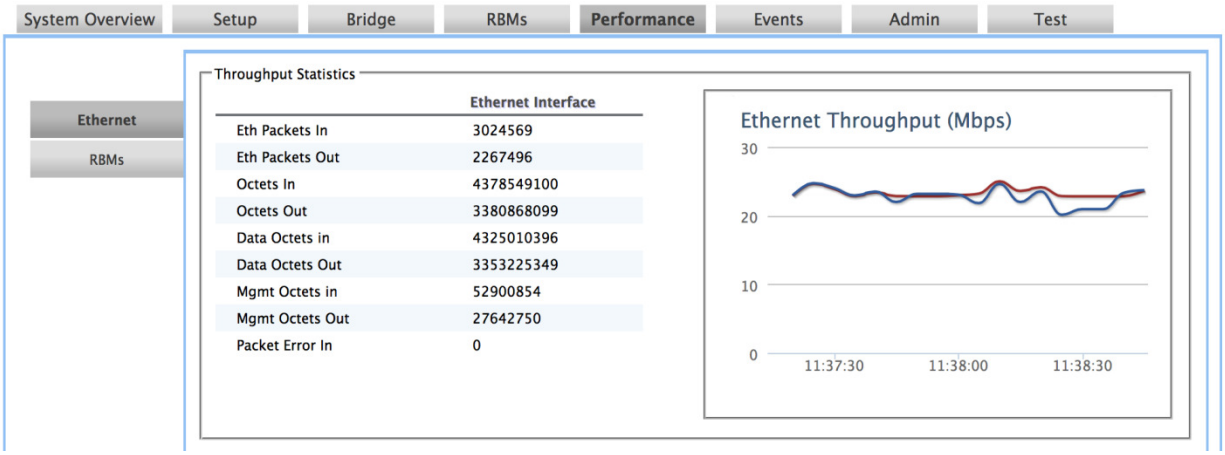
Sort the list on the left by ascending or descending MAC address, or by state by clicking on the column header. Select:

Add an RBM:	Click **Add** to add an RBM. In the dialog box that appears enter its MAC address. If desired, copy a service flow definition from an existing RBM by entering its MAC address, or start from a blank one. Click **OK**. Then edit the RBM.
Delete an RBM:	On the left, activate check box(es) of desired RBMs and click on **Delete Selected**.
Edit service flow definition:	Click on **edit** to the right of the RBM MAC address. The sub-page that appears is the same one as for the default service flow definition, except that now it applies to this specific RBM only. Refer to section 9.3.7 for details.

10.3.9 Performance Page (Ethernet)

This read-only sub-page for Hub Ethernet performance visualizes the incoming and outgoing traffic for the Ethernet interface connections using two graph lines. This allows the user to see traffic and bandwidth usage for the Ethernet interfaces in a real-time, graphical format, and monitor the current download/upload throughput speeds. It also lists the current throughput performance statistics for the Ethernet interfaces.

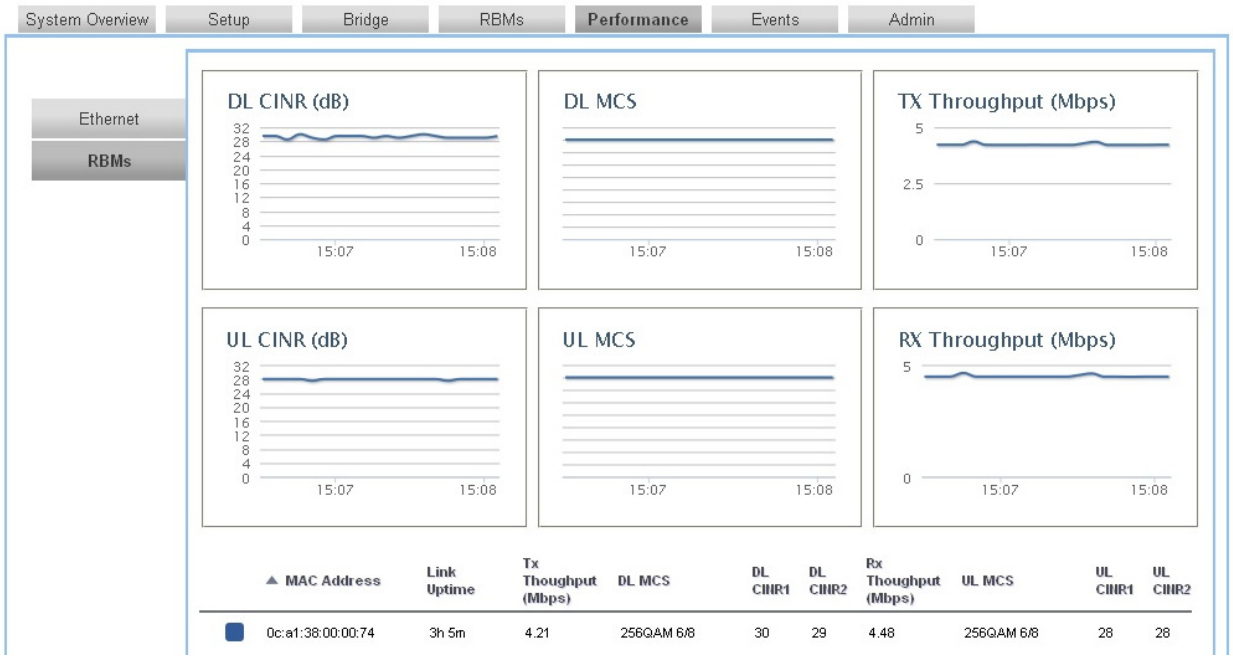
Note: The blue graph line represents the receive throughput rate, while the red graph line represents the transmit throughput rate. Screen refresh interval is every 5 seconds.



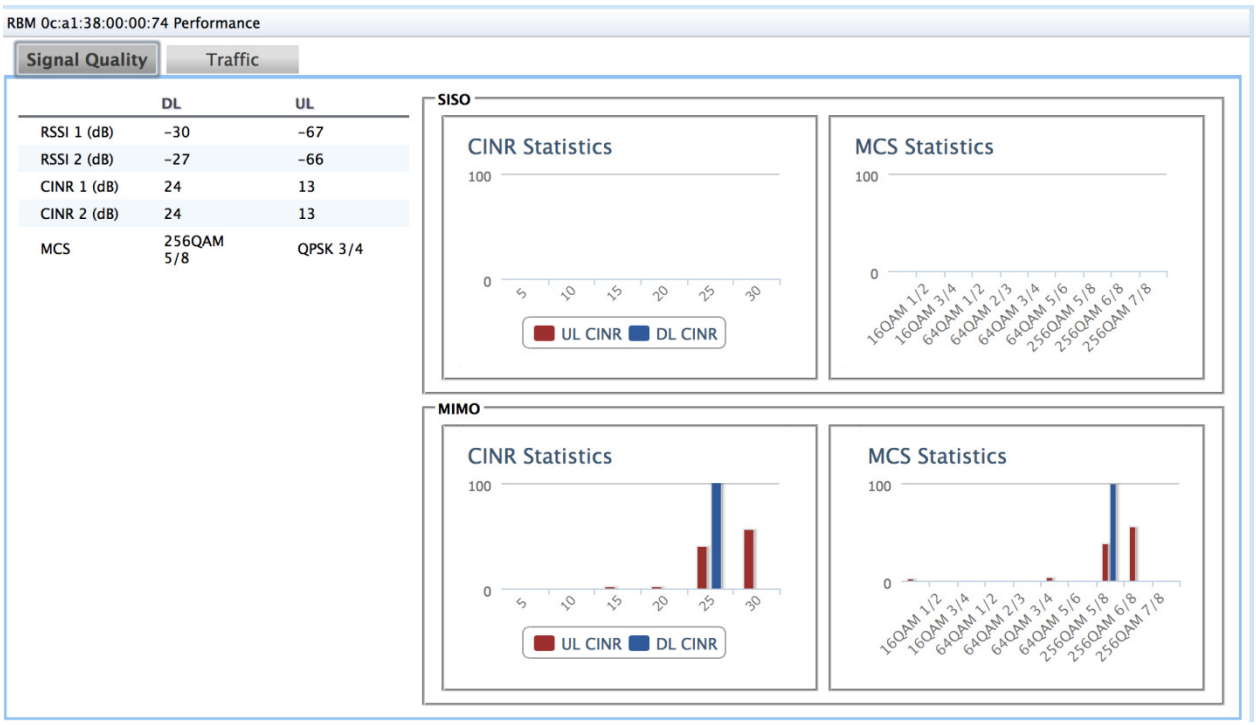
10.3.10 Performance Page (RBMs)

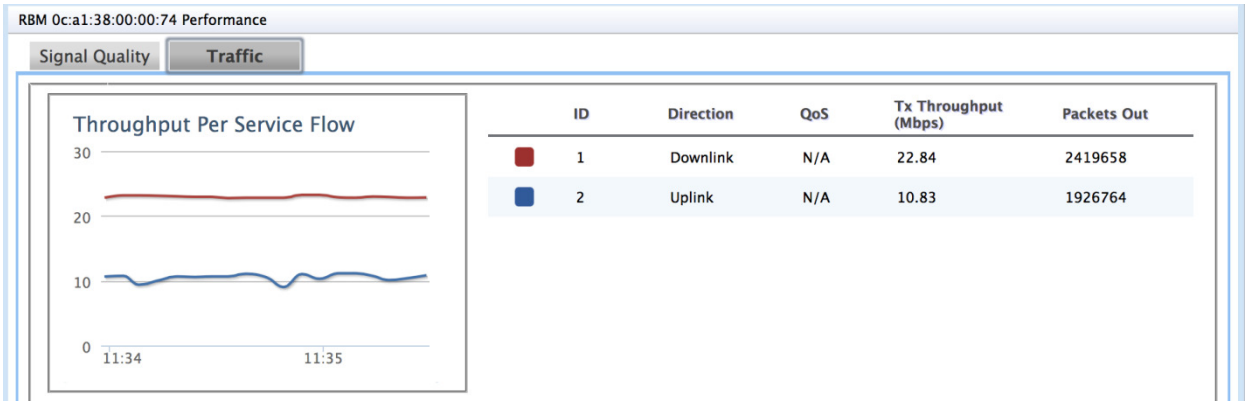
This read-only sub-page for RBM performance contains graphs and statistics for the downlink/uplink Carrier to Interference-plus-Noise (CINR), downlink/uplink MCS, and downlink/uplink throughput. It visualizes the incoming and outgoing traffic for the system RBMs using graph lines. This allows the user to see traffic and bandwidth usage for RBMs in a real-time, graphical format, and monitor the current download/upload throughput speeds.

Note: Screen refresh interval is every 5 seconds.



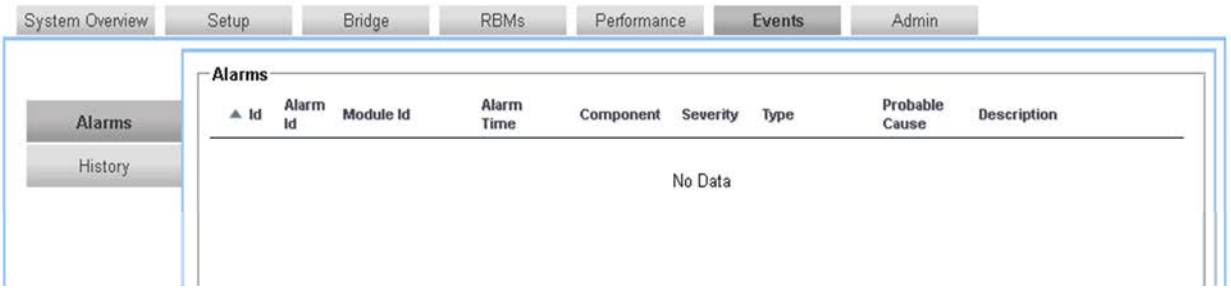
Click on an RBM on the list at the bottom to view the statistics on signal quality and throughput (per service flow) performance for that RBM.





10.3.11 Events Page (Alarms)

This read-only sub-page lists current alarms and events along with their details. For a list of alarms and events see Chapter 10. Reorder the alarms and events as desired by clicking on any of the column headers.



10.3.12 Events Page (History)

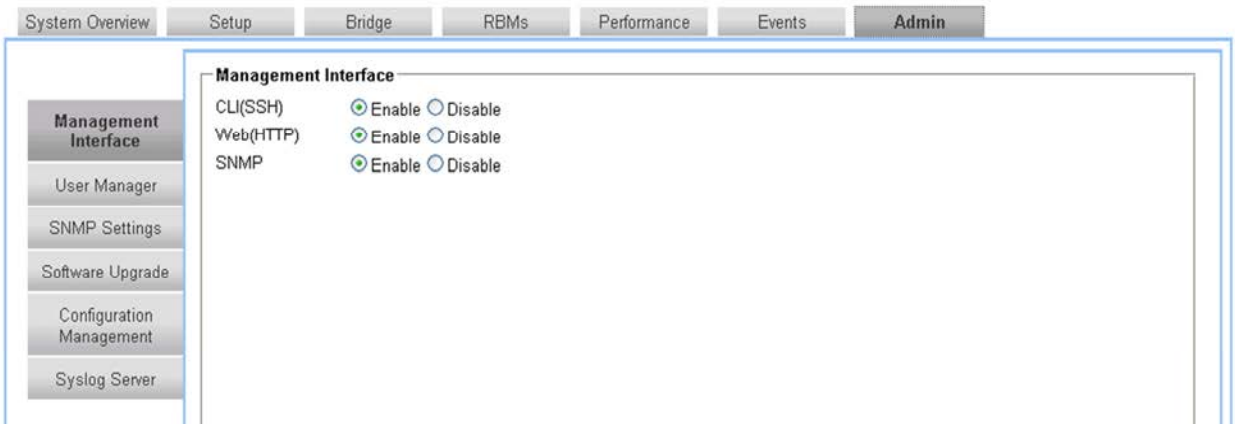
This read-only sub-page lists a chronological history of alarms and events along with their details. For a list of alarms and events see Chapter 10. Reorder the alarms and events as desired by clicking on any of the column headers.

Note: Clicking **Clear Table** completely clears the current alarms and events history from the X-100 event logging infrastructure. The only way to retrieve this history afterward is from Syslog (if provisioned).

10.3.13 Admin Page (Management Interface)

On this sub-page the administrator can select the types of management interfaces to use (CLI, Web, SNMP) using the radio buttons. One, two or all three can be selected.

Note: If you disable the Web option, the X-100 WebUI becomes unusable. You will have to enable it again using either the X-100 CLI or SNMP. It is not possible, however, to lock yourself out of all three options; at least one option is always be available.

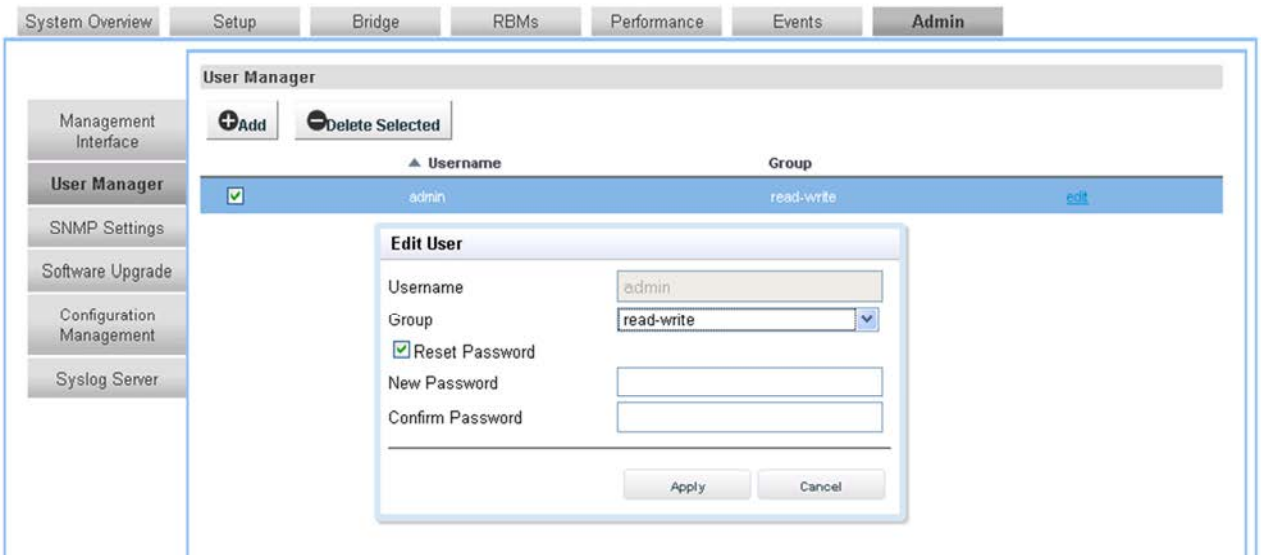


10.3.14 Admin Page (User Manager)

On this sub-page, by clicking on **edit** at the right of the list the administrator can add and delete users, set passwords, and set access privileges (that is, read-only versus read/write) to manage user access to the Hub.

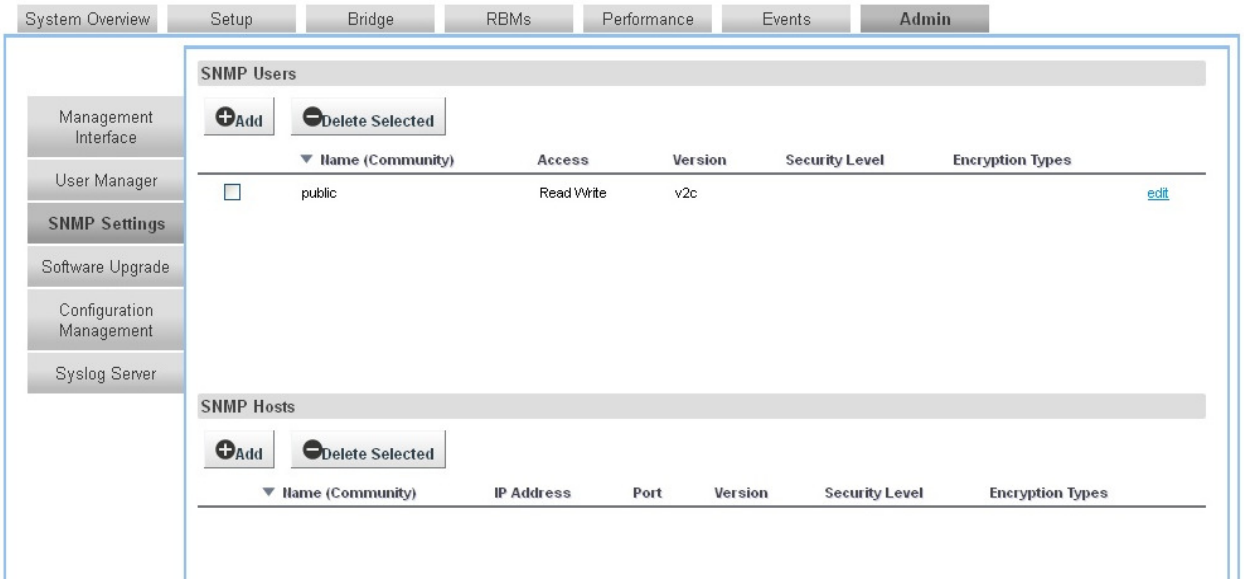
Note:

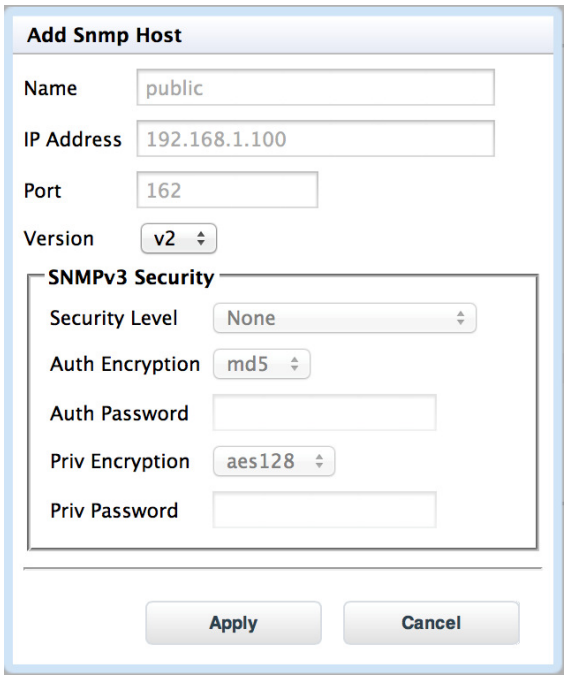
- User names must start with a letter and may be composed of alphanumeric characters only.
- Passwords are case sensitive, may be composed of alphanumeric characters and special characters, and must contain at least one letter and one digit.
- At least one user with read/write privileges needs to exist in the X-100 system.
- If you cannot login due to a forgotten user name or password, contact another user with read/write access privileges to have them reset your login credentials. If you have lost all read/write login credentials, contact your supplier.



10.3.15 Admin Page (SNMP Settings)

On this sub-page the administrator can add, delete, or edit SNMPv2C or SNMPv3 users and hosts if desired.

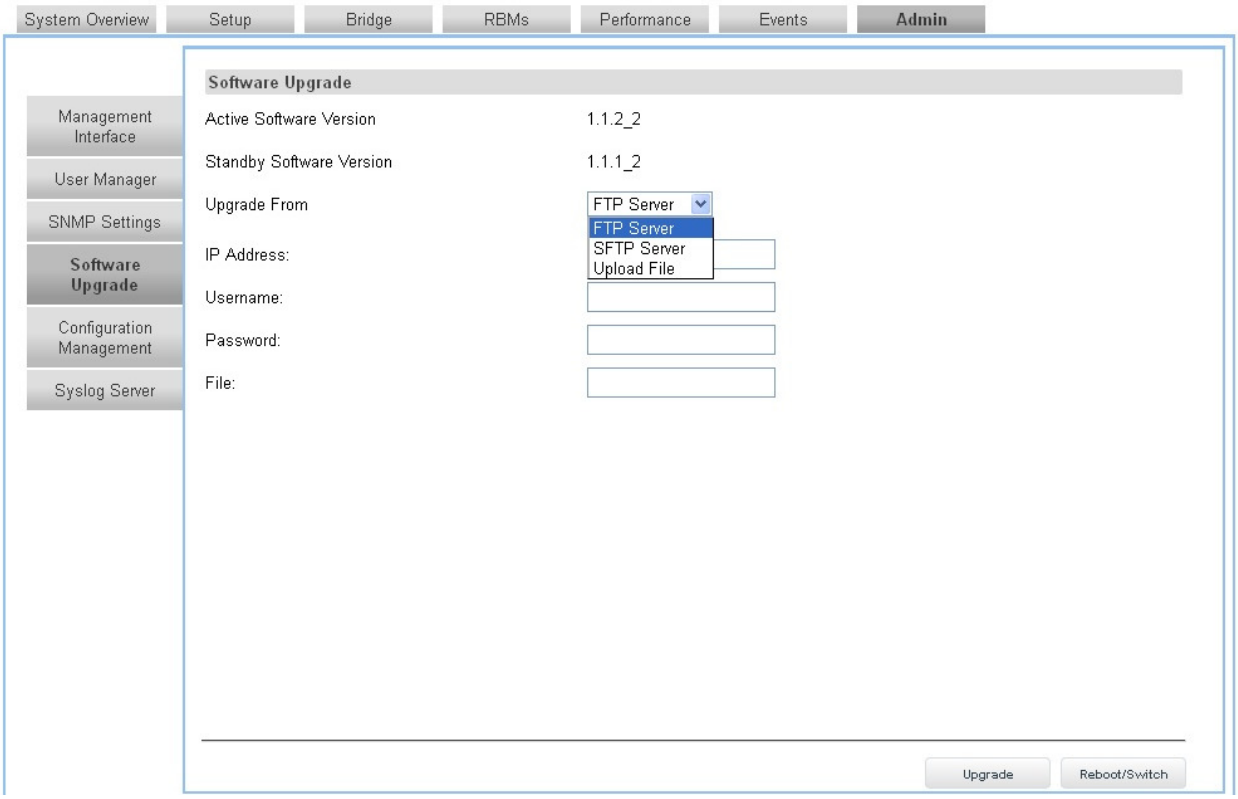




10.3.16 Admin Page (Software Upgrade)

On this sub-page the administrator can perform system software upgrade activities.

As shown, active and standby software image versions can coexist simultaneously on the HM (and RBM).



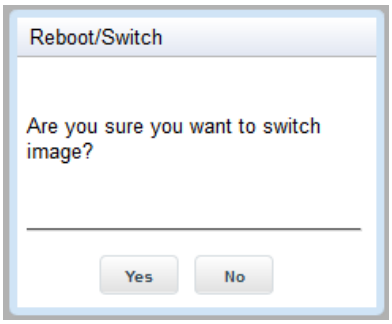
Software upgrades can occur either from an FTP server, SFTP server, or from your hard disk. To upgrade the software, do the following:

1. Select either 'FTP Server'or 'SFTP Server' and enter the details, or select 'Upload File' and browse for the file on your hard disk.

2. Click on **Upgrade** at the bottom right hand corner of the page. A progress bar appears at the bottom of the page.

3. If the software download succeeds, the banner at the top of the page indicates this. The 'Standby Software Version' field then shows the new software load image version.

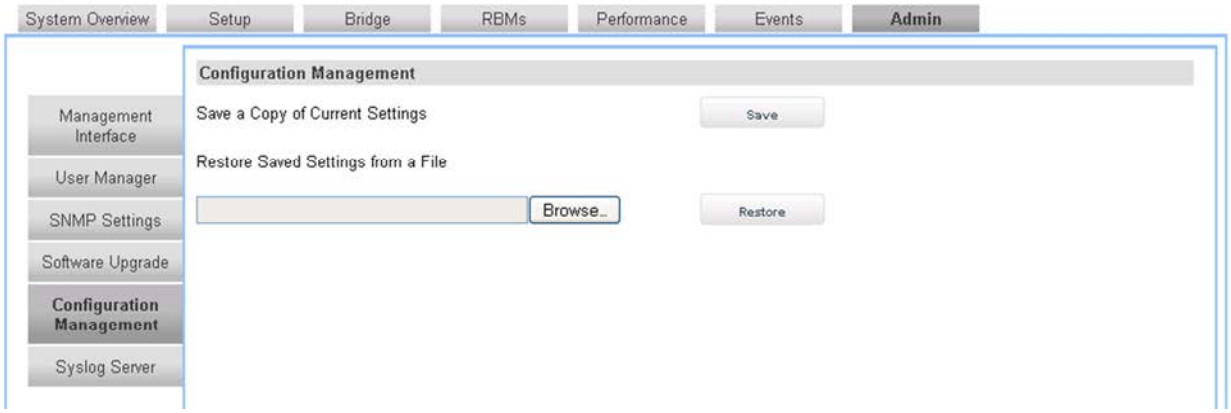
4. To make the standby software load image the active image on the module, click on **Reboot/Switch** at the bottom of the page. Then click on **Yes** at the prompt. The system restarts using the new software image. If the banner at the top indicates that this was successful you have finished this software upgrade procedure.



5. If the software upgrade fails (due normally to a corrupt load), the system restarts again using the old software image. The banner at the top of the page indicates that this has happened. In this case, select a different version of the new software and repeat this procedure from Step 1.

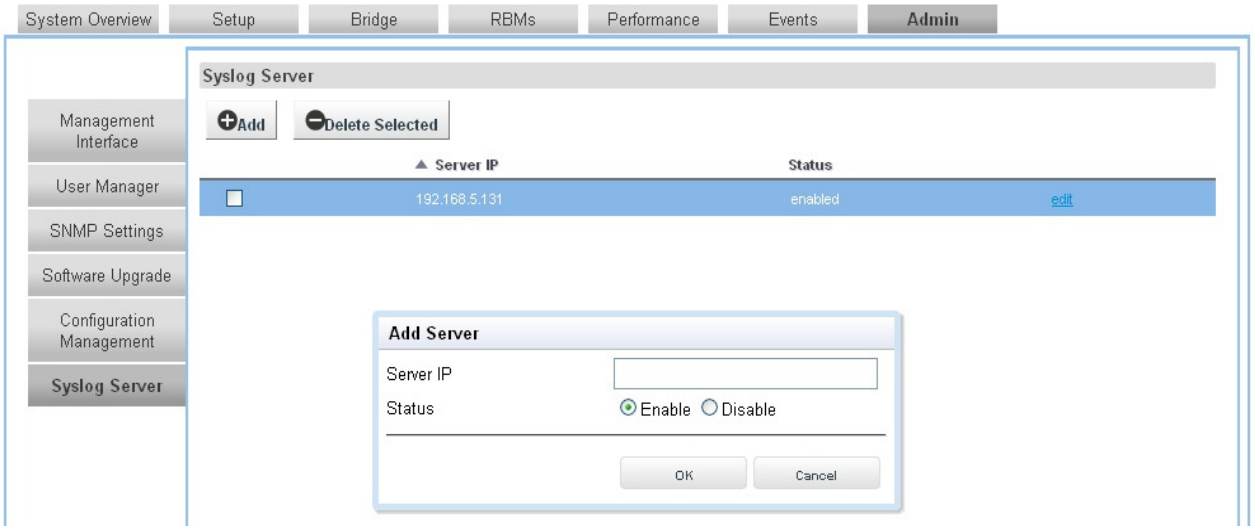
10.3.17 Admin Page (Configuration Management)

On this sub-page the administrator can save the current configuration to a file on their hard disk. Configuration files can then later be uploaded to restore previous settings.



10.3.18 Admin Page (Syslog Server)

On this sub-page the administrator can add and delete Syslog Servers, and set or change their operational status.

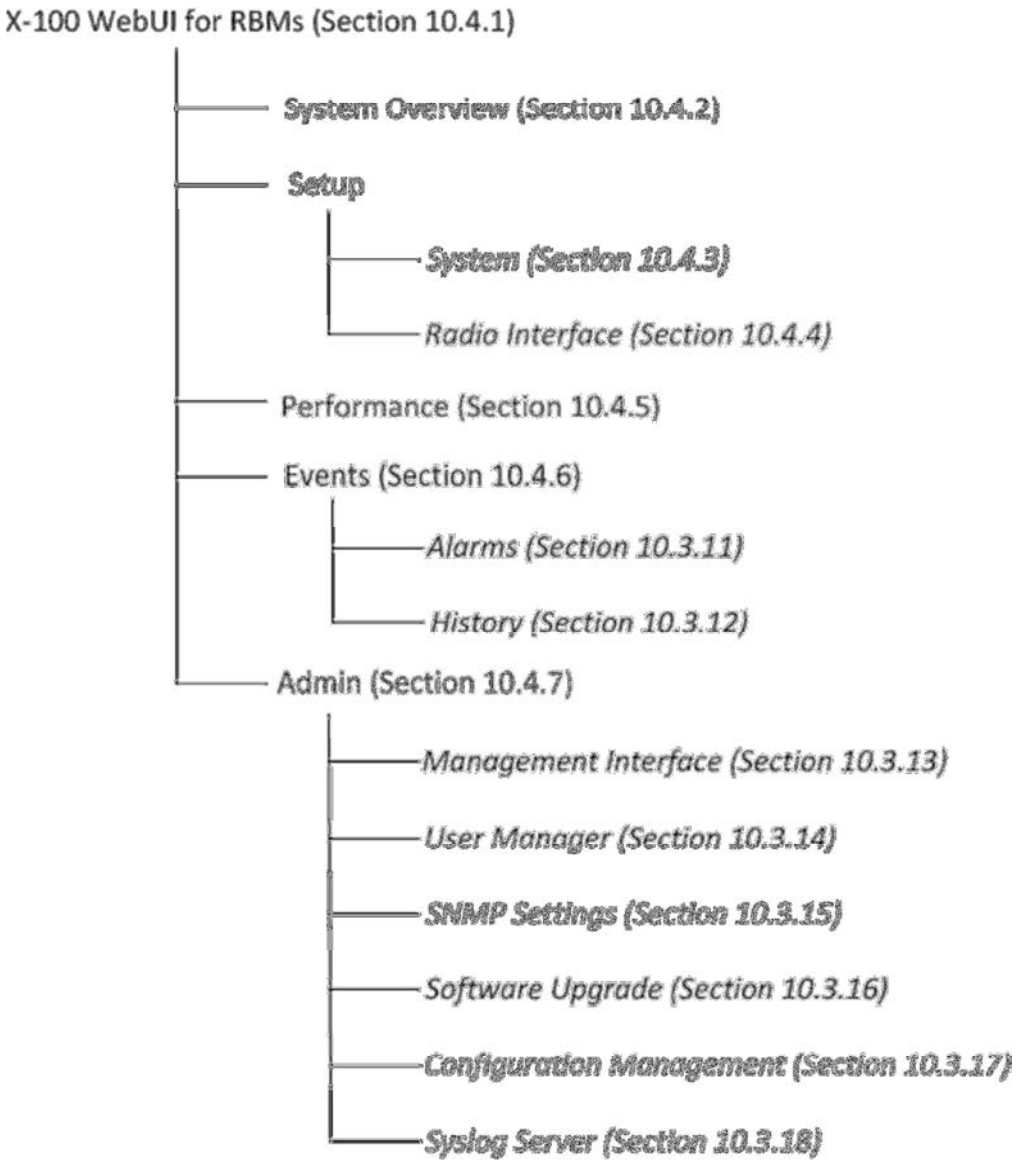


Click on **Add** to add a new Syslog server to the list displayed. In the dialog box that appears use the radio buttons to toggle its status: 'Enable' or 'Disable'. Its status can be changed later by clicking on **edit** at the right of the list and using the radio buttons again. Delete a server by checking the box next to it and clicking on **Delete Selected**.

10.4 Configuring RBMs

The X-100 WebUI interface for configuring RBMs is similar to that for Hubs. *This section focusses on differences only.* Moreover, sections that are read-only are not discussed; some of these omit data not appropriate to RBMs and add other data not shown on the X-100 WebUI pages for Hubs.

Note: For all RBM X-100 WebUI configuration items not discussed here, see the corresponding Hub item in section 9.3 for details.



10.4.1 Logging In

To log in and access the X-100 WebUI interface for configuring RBMs, do the following:

1. Launch your web browser and set it to allow pop ups (as some screen functions in the X-100 WebUI require pop ups).

   For Firefox: Click on **Tools > Options > Content** and uncheck **Block pop-up windows**. Alternatively, click on the **Exceptions** button and enter a list of Hub IP addresses you will be configuring.

2. If there is a direct connection to the RBM (that is, not over a network), use your browser to go to http://169.254.1.1.
3. If connecting over a network to the RBM (that is, not locally), use your browser to connect to the management IP address of the RBM. Note, however, that the management IP address of the RBM is only accessible from behind the HM.

Note: To successfully log in and access the X-100 WebUI on an RBM over a network, its HM must be connected to the network, and the radio link from the Hub to the RBM must be up. This is because network communication with an RBM occurs through its associated Hub over the radio link.

For more information, refer to section 10.3.1.

10.4.2 System Overview Page

This read-only page gives information on the particular RBM you are logged in to as well as current alarm information.

10.4.3 Setup Page (System)

This sub-page handles configuration of system parameters that govern basic RBM operation and is the same sub-page as for Hub, except:

System Clock Source: Cannot be set from the RBM
Mgmt VLAN: Cannot be set from the RBM

For more information, refer to section 10.3.3 for the corresponding Hub page.

10.4.4 Setup Page (Radio Interface)

This sub-page handles configuration of the radio operation of the RBM and is the same sub-page as for Hub, except:

Preamble Series: Check 'All' or enter preamble index value 0 to 31 (factory default is 'All'); refer to Chapter 14 for more information on use of preamble indices

Pointing Mode (BSI): Enabled/Disabled

Pointing Mode or Best Signal Indicator (BSI) is an RBM operating mode which allows the installer to easily determine the direction of the best quality signal from the best serving HM. While in BSI mode, the RBM makes a buzzing noise to reflect the quality/strength of the RF signal it receives from the HM. The higher the quality of RF signal is from the HM, the louder and higher the frequency of the buzzer from the RBM. The installer moves the RBM on its axis and locks it down to its mount when the loudest and highest frequency buzzer noise is heard—indicating the best signal from the best serving HM has been found. The radio link can then be created by inserting an Ethernet cable into the Ethernet port on the RBM. This allows the RBM to lock on to the signal and exit BSI mode.

Note: While the RBM is in BSI mode it cannot create a radio link.

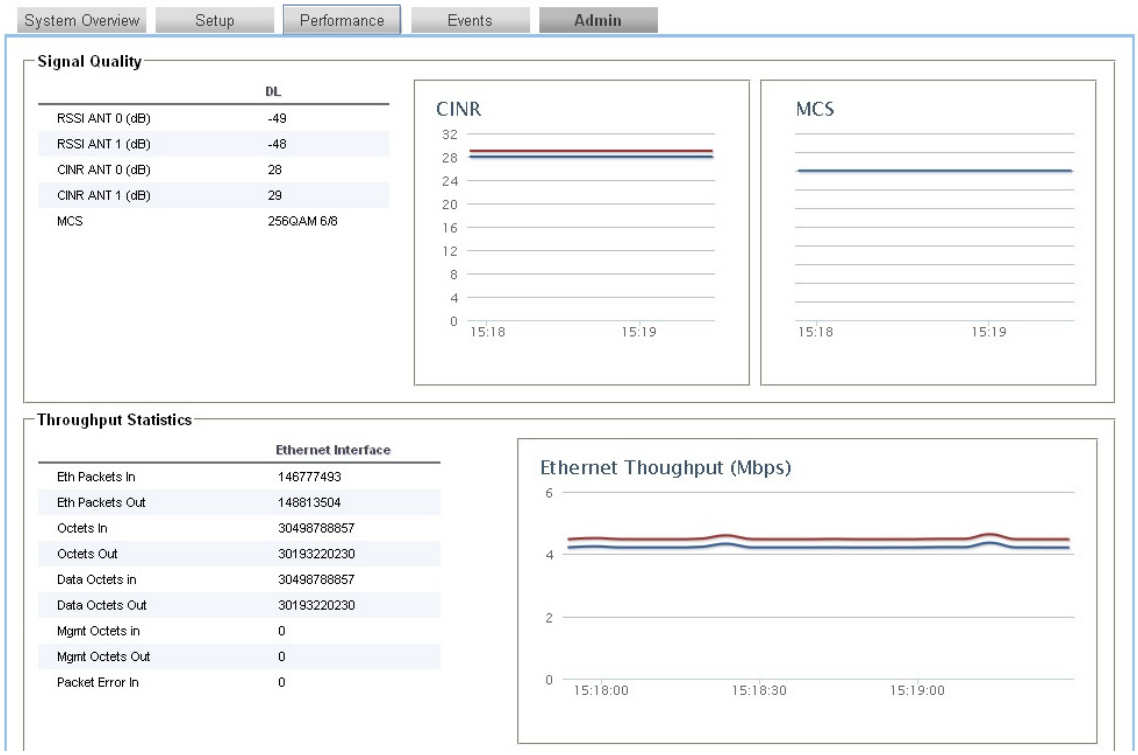
When initially configuring the RBM prior to being installed, set 'Pointing Mode (BSI)' to Enabled so that when the RBM restarts next with no Ethernet cable attached, it enters BSI mode and the installer can then find the optimum position for the RBM on its mount based on the signal quality from the HM. Once the installer plugs the Ethernet cable into the Ethernet port on the RBM to create the radio link to the Hub, the RBM exits BSI mode, and 'Pointing Mode (BSI)' can be set to Disabled. This prevents the RBM from entering BSI mode again while up on its mount due to, for example, the base station losing power and in turn not seeing the Ethernet connection to the RBM, causing the RBM to enter BSI mode again.

For more information, refer to section 10.3.4 for the corresponding Hub page.

10.4.5 Performance Page

This read-only sub-page for RBM performance contains graphs and statistics for the downlink/uplink Carrier to Interference-plus-Noise (CINR), downlink/uplink MCS, and downlink/uplink throughput. It visualizes the incoming and outgoing traffic for the RBM using graph lines. This allows the user to see traffic and bandwidth usage for the RBM in a real-time, graphical format, and monitor the current download/upload throughput speeds.

Note: Graph update interval is every 5 seconds.



10.4.6 Events Page

Same page and sub-pages as for Hub. Refer to sections 10.3.11 and 10.3.12 for details.

10.4.7 Admin Page

Same page and sub-pages as for Hub. Refer to sections 10.3.13 through **Error! Reference source not found.** for details.

11 Alarms and Events (Fault Management)

This chapter lists the alarms and events for the BLiNQ X-100 system.

The X-100 system issues an alarm notification when a fault condition occurs. Alarms issued are presented to users through the X-100 WebUI Events page and require operation and maintenance actions to restore functionality, or prevent a more serious situation from developing.

The X-100 system issues an event notification when something of importance happens that does not trigger an alarm, but is considered significant enough to be presented to users through the X-100 WebUI Events page.

Table 11 lists 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).

Table 12 lists 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 10 List of Alarms

ID	Name	Description/Comments	Type	Severity
6004	Radio Card Failure	—	Equip.	One card down (degraded performance): Major; Two cards down (no service): Critical
6005	Hardware Failure	—	Equip.	Critical
6006	Temperature Too High	Recovers when the temperature falls below threshold	Equip.	Critical
4001	Ethernet Port Down	Recovers when Ethernet link is reestablished	Comms.	Critical
5006	Radio Module Down	Two possible causes: a) Radio Driver lost connection with OAM Proxy and cannot reestablish connection. Alarm is followed by the Driver issuing a hardware reset to the Radio Module subsystem.	Equip.	Critical

ID	Name	Description/Comments	Type	Severity
		b) The Radio Driver is expecting the Radio Module to boot (for example, following a soft reset or after unit restart) and the DAN Driver fails to establish connection with the Radio Module after a certain time. Recovers when Radio Driver reestablishes connection with the Radio OAM Proxy.		
5007	RF Port Open	The system has detected an open RF port. Recovers when the system detects the port is no longer open.	Equip.	Critical
5010	Invalid RF Card Calibration Data	Recovers when the system detects the port is no longer open	Equip.	Critical
5009	Power Detector Fault	The system has detected a power fault. Recovers when the system detects the power fault is no longer present	Equip.	Major
7001	GPS Synchronization Lost	GPS receiver lost its synchronized status. Upon Hub reset, this alarm is not raised until 60 sec after reset and if synchronization still is not achieved. After hold-over time expires (10 minutes), GPS transitions to unsynchronized state.	Comms.	Major
7002	GPS Synchronization Failed	GPS transitioned from hold-over to un-synchronized state. System stops transmitting.	Equip.	Critical
4002	All RBM Links Down	Hub has lost all RBM connections. Upon Hub reboot, alarm occurs only if no RBM has established connection within 20 secs from the time the Hub radio is operational.	Comms.	If any RBM is configured as “Emit alarm when down”: Critical Otherwise: Major
4003	RBM Link Down	Hub has lost connection to an RBM that is configured to “Emit alarm when down.” Upon Hub reboot, alarm occurs only if RBM has not established connection within 20 secs from the time the Hub radio is operational.	Comms.	Critical
3004	Software Boot Failure	Switchover software versions after a failed boot attempt. Probably a storage capacity problem.	Equip.	Major
2002	Management Address Lease Renew Failed	Cannot renew its DHCP lease when unit is configured to use DHCP for the Management IP Address. Recovers when lease renewed.	Equip.	Minor

Table 11 List of Events

ID	Name	Description/Comments	Type	Severity
6001	Cold Start	Unplanned restart	Equip.	Information
6002	Warm Start	Planned restart	Equip.	Information
5001	Radio Module Initialized	Radio driver established communication with the OAM Proxy	Equip.	Information
5002	Radio Module Entering Pointing Mode	No transmitting occurs in this mode; it is “receive only” radio operation	Equip.	Information
5003	Radio Module Entering Operational Mode	Normal send/receive operation	Equip.	Information
5004	Radio Module Disabled	Radio Module is initialized and received an administrative disable configuration	Equip.	Information
5005	Radio Module Initializing	Radio Module intentionally reset	Equip.	Information
7003	GPS Lock Acquired	GPS entered synchronized state	Equip.	Information
3001	Software Download Initiated	Software download procedure initiated	Equip.	Information
3002	Software Download Successful	Software download successfully completed	Equip.	Information
3003	Software Download Failed	Either: transfer, file validation or file persistence error	Equip.	Major
2001	Startup Configuration Changed	Changes to the system running configuration have been saved to the startup configuration	Equip.	Information
8001	Authentication Failed	Attempt to authenticate on one of the management interfaces of the equipment failed	Process -ing Error	Minor

12 Using the X-100 Command Line Interface

The BLiNQ X-100 Command Line Interface (CLI) is a text-based interface to the BLiNQ X-100 system.

12.1 Overview

The X-100 CLI provides commands that the network administrator can use to perform various tasks, including configuring, provisioning, monitoring and troubleshooting the module software, hardware, and network connectivity.

Using a Secure Shell (SSH) connection, you can access the X-100 CLI over the network.

The commands in the X-100 CLI let you display information and perform configuration tasks and make configuration changes to the X-100 system. The CONFIG level contains, for example, sub-levels for Ethernet port setting, management interface settings, and other configuration areas such as global default CLI session parameters.

To display a list of the available X-100 CLI commands or command options, enter **?**.

The X-100 CLI supports command completion, so you do not need to enter the entire name of a command or option. If you enter part of a command, then press **Tab** or **<space>**, the CLI lists the options you can enter at that point in the command string. As long as you enter enough characters of the command or option name to avoid ambiguity with other commands or options, the CLI understands what you are typing and completes it.

Note: Command comments can be entered directly in the X-100 CLI by identifying them with an exclamation mark (!) at the start of a line. This tells the X-100 system that the information is a comment and is to be ignored.

12.2 Identify Command Context

Command levels set a context for the X-100 CLI. Command context helps you:

- determine where you are in CONFIG command levels
- determine what you are configuring
- go to other CLI command levels

Each command level has its own distinct CLI command prompt so that you know which level you are in. By recognizing the command line prompt, you can identify where you are in the CLI and the context at any given point. This helps to prevent you from making configuration mistakes that could adversely affect the operation of the X-100 system.

The X-100 CLI command prompt changes at each level of the command structure to easily identify the current level:

`localhost#`	Privileged EXEC Level Command
`localhost(config)#`	Global CONFIG Level Command

12.3 Logging On to the X-100 CLI

Note: The CLI has an inactivity timer which logs out inactive users. This inactivity time is automatically invoked if no commands are entered for several minutes. You cannot change the inactivity timer configuration.

Once an IP address is assigned to a module, you can log on to the X-100 CLI using a Secure Shell (SSH) connection (SSH is an application for opening a secure socket connection to an IP device). However, SSH version 2.0 client software must be installed on your host computer (SSH version 1.0 can be used, but is not recommended).

After initial log on, once CLI connectivity to the X-100 system is established, you see a CLI banner and prompt similar to:

```
BLiNQ X100 CLI
admin connected from 192.168.5.100 using ssh on localhost
localhost#
```

At this prompt (#), you are at the Privileged EXEC level of the CLI command structure. This is the first level that you have access to when connected to the X-100 system through the X-100 CLI.

To reach the Global CONFIG Level, the uppermost level of the CONFIG commands, enter the **config** Privileged EXEC command. You can then reach all the other levels of the CONFIG command structure from this point.

```
BLiNQ X100 CLI
admin connected from 192.168.5.100 using ssh on localhost
localhost# config terminal
Entering configuration mode terminal
localhost(config)#
```

The CLI is now at the Global CONFIG level.

12.4 Privileged EXEC Commands

The Privileged EXEC level commands primarily enable you to review information on the system configuration, monitor features globally on an X-100 system (through show commands), perform and configure basic user operations, transfer and store configuration files, and verify system connectivity. It does not allow you to make changes to the system configuration.

```
localhost# <Tab>
Possible completions:
  autowizard              Automatically query for mandatory elements
  clear                   Clear parameter
  compare                 Compare running configuration to another
                          configuration or a file
  complete-on-space       Enable/disable completion on space
  config                  Manipulate software configuration information
  copy                    Copy configuration from one store to another
  display-level           Configure show command display level
```

```
  event-history
  exit                    Exit the management session
  file                    Perform file operations
  help                    Provide help information
  history                 Configure history size
  id                      Show user id information
  idle-timeout            Configure idle timeout
  ignore-leading-space    Ignore leading whitespace (true/false)
  job                     Job operations
  logout                  Logout a user
  no                      Negate a command or set its defaults
  output-file             Copy output to file or terminal
  paginate                Paginate output from CLI commands
  prompt1                 Set operational mode prompt
  prompt2                 Set configure mode prompt
  quit                    Exit the management session
  screen-length           Configure screen length
  screen-width            Configure screen width
  send                    Send message to terminal of one or all users
  show                    Show information about the system
  show-defaults           Show default values when showing the configuration
  source                  File to source
  system
  terminal                Set terminal type
  who                     Display currently logged on users
  write                   Write configuration
```

12.5 Global CONFIG Commands

The Global CONFIG commands allow you to globally apply or modify configuration parameters for an X-100 system:

```
localhost# config terminal
Entering configuration mode terminal
localhost(config)# <Tab>
Possible completions:
  admin           Administrative settings and commands
  alias           Create command alias.
  ethernet        Ethernet port settings
  event-history
  mgmt            Management interface settings
  radio           Radio Interface Settings
  session         Global default CLI session parameters
  system          System settings
  user
  ---
  abort           Abort configuration session
  clear           Remove all configuration changes
  commit          Commit current set of changes
  copy            Copy a dynamic element
  do              Run an operational-mode command
  end             Terminate configuration session
  exit            Exit from current mode
  help            Provide help information
  insert          Insert a parameter
```

```
load            Load configuration from an ASCII file
move            Move a parameter
no              Negate a command or set its defaults
pwd             Display current mode path
rename          Rename an identifier
resolved        Conflicts have been resolved
revert          Copy configuration from running
rollback        Roll back database to last committed version
save            Save configuration to an ASCII file
service         Modify use of network based services
show            Show a parameter
top             Exit to top level and optionally run command
validate        Validate current configuration
```

Within the Global CONFIG level you can:

- Apply features globally to an X-100 system
- Enable/disable a feature or function
- Configure a feature or function
- Access all other CONFIG level modes (for example, Radio CONFIG, User CONFIG, RBM Config)

12.5.1 Radio CONFIG Mode

```
localhost(config)# radio
localhost(config-radio)# <Tab>
Possible completions:
  admin-state       Radio enable/disable
  bandwidth         Bandwidth
  bsi-admin-state   Pointing mode enable/disable
  frame-duration    Frame duration
  frequency         Center frequency
  preamble          Preamble configuration
  transmit-power    Maximum transmit power
  ---
  commit            Commit current set of changes
  exit              Exit from current mode
  help              Provide help information
  no                Negate a command or set its defaults
  pwd               Display current mode path
  top               Exit to top level and optionally run command
localhost(config-radio)#
```

12.5.2 User CONFIG Mode

```
localhost(config)# admin <Tab>
Possible completions:
  cli     Command Line Interface settings
  snmp    SNMP agent settings
  users   CLI and WebUI users
localhost(config)# admin users user <Tab>
Possible completions:
  User name ([A-Za-z_][A-Za-z0-9_-]*)  admin
localhost(config)# admin users user admin
```

```
localhost(config-user-admin)# <Tab>
Possible completions:
  group      Group the user belongs to
  password   User password
  ---
  commit     Commit current set of changes
  exit       Exit from current mode
  help       Provide help information
  no         Negate a command or set its defaults
  pwd        Display current mode path
  top        Exit to top level and optionally run command
localhost(config-user-admin)#


localhost(config)#
localhost(config)# admin users user roy <Tab>
Value for 'password' (<MD5 digest string>): ********
Value for 'group' [read-only,read-write]: read-write
localhost(config-user-roy)# ?
Possible completions:
  group      Group the user belongs to
  password   User password
  ---
  commit     Commit current set of changes
  exit       Exit from current mode
  help       Provide help information
  no         Negate a command or set its defaults
  pwd        Display current mode path
  top        Exit to top level and optionally run command
localhost(config-user-roy)#
```

12.5.3 RBM CONFIG Mode (Hub Modules Only)

```
HUB_traffic#
HUB_traffic# config terminal
Entering configuration mode terminal
HUB_traffic(config)# ?
Possible completions:
  admin            Administrative settings and commands
  alias            Create command alias.
  bridge           L2 Bridge Settings
  ethernet         Ethernet port settings
  event-history
  mgmt             Management interface settings
  radio            Radio Interface Settings
  rbm-table        RBM Table
  session          Global default CLI session parameters
  system           System settings
  user
  ---
  abort            Abort configuration session
  clear            Remove all configuration changes
  commit           Commit current set of changes
  copy             Copy a dynamic element
  do               Run an operational-mode command
```

```
  end             Terminate configuration session
  exit            Exit from current mode
  help            Provide help information
  insert          Insert a parameter
  load            Load configuration from an ASCII file
  move            Move a parameter
  no              Negate a command or set its defaults
  pwd             Display current mode path
  rename          Rename an identifier
  resolved        Conflicts have been resolved
  revert          Copy configuration from running
  rollback        Roll back database to last committed version
  save            Save configuration to an ASCII file
  service         Modify use of network based services
  show            Show a parameter
  top             Exit to top level and optionally run command
  validate        Validate current configuration
HUB_traffic(config)#
HUB_traffic (config)# rbm-table rbm ?
Possible completions:
  MAC address
  0c:a1:38:00:00:4f   RBM 3
  0c:a1:38:00:00:56   RBM 2
  0c:a1:38:00:00:63   RBM 4
  0c:a1:38:00:00:81   RBM 1
HUB_traffic(config)# rbm-table rbm 0c:a1:38:00:00:81
HUB_traffic(config-rbm-0c:a1:38:00:00:81)# ?
Possible completions:
  description     Description/label
  service-flows   Service flows list
  vlan-table      VLAN table
  ---
  commit          Commit current set of changes
  exit            Exit from current mode
  help            Provide help information
  no              Negate a command or set its defaults
  pwd             Display current mode path
  top             Exit to top level and optionally run command
HUB_traffic(config-rbm-0c:a1:38:00:00:81)# service-flows service-flow ?
Possible completions:
  Service flow ID  0  1  range
HUB_traffic(config-rbm-0c:a1:38:00:00:81)# service-flows service-flow 1
HUB_traffic(config-service-flow-1)# classification rule 0
HUB_traffic(config-rule-0)# show full
rbm-table rbm 0c:a1:38:00:00:81
 service-flows service-flow 1
  classification rule 0
   dst-mac-addr 00:00:00:00:00:00
   dst-mac-mask 00:00:00:00:00:00
  !
 !
!
HUB_traffic(config-rule-0)# ?
Possible completions:
  c-vlan-id         Inner (C-VLAN) tag VLAN ID
  c-vlan-priority   Inner (C-VLAN) tag priority bit
  dst-ip            Destination IP address
```

```
  dst-mac-addr      Destination MAC address
  dst-mac-mask      Destination MAC address mask
  ethertype         Ethertype
  max-tos           Type of Service (ToS) maximum value
  min-tos           Type of Service (ToS) minimum value
  priority          Rule priority
  protocol
  s-vlan-id         Outer (S-VLAN) tag VLAN ID
  s-vlan-priority   Outer (S-VLAN) tag priority bit
  src-ip            Source IP address
  src-mac-addr      Source MAC address
  src-mac-mask      Source MAC address mask
  ---
  commit            Commit current set of changes
  exit              Exit from current mode
  help              Provide help information
  no                Negate a command or set its defaults
  pwd               Display current mode path
  top               Exit to top level and optionally run command
```

12.6 X-100 CLI Command Structure

To get a quick display of available options at a CLI level or for the next option in a command string, enter a single question mark **?** at the prompt, press **Tab**, or press **<space>**.

When an item is bracketed with < > symbols, the information requested is a variable and required.

When an item is enclosed with [ ] symbols, it shows the current value of the variable.

When an item is not enclosed by < > or [ ] symbols, the item is a required keyword.

When two or more options are separated by a / symbol, you must enter one of the options as part of the command.

Example 1:

```
localhost(config)# mgmt <Tab>
Possible completions:
  default-gateway
  interfaces        Management interfaces administrative state
  ip                Management IP address and netmask
  ip-config-mode    Management IP mode
  syslog            Syslog server settings
localhost(config)# mgmt ip-config-mode <Tab>
Possible completions:
  dhcp  static
```

Example 2:

```
localhost# terminal ?
Possible completions:
  <generic/xterm/vt100/ansi/linux>
localhost# terminal
```

Example 3:

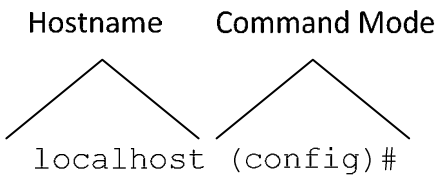
To view possible show command offerings, enter the following:

```
localhost# show ?
Possible completions:
  active-alarms    Active alarms list
  cli              Display cli settings
  configuration
  ethernet         Ethernet port settings
  event-history
  history          Display CLI command history
  mgmt             Management interface settings
  pm               Performance measurements
  radio            Radio Interface Settings
  running-config   Display current configuration
  startup-config   Display startup configuration
  system           System settings
localhost# show
```

12.7 X-100 CLI Command Line Prompts

Within the X-100 CLI, the command line prompt identifies both the hostname and the command mode. The hostname is the name of your X-100 system; the command mode indicates your location within the CLI command structure.

For example:



For some actions, the X-100 CLI prompts you for a response. The acceptable default responses are the following:

- You can press <Enter> to agree with the prompt and continue.
- You can press any other key to disagree with the prompt and cancel the action.

12.8 X-100 CLI Keywords and Parameters

X-100 CLI commands are made up of two primary elements: keywords and parameters.

12.8.1 Keywords

Every command requires at least one keyword; however, a command can contain other optional keywords. The keyword(s) must be typed into the CLI accurately for it to be recognized. These are examples of keywords:

- clear
- config
- exit
- load
- revert
- show

Keywords identify the operation to be performed. You can abbreviate keywords; however, you must enter enough initial characters to unambiguously identify the command. For example, if the keyword you want to specify is **session** and you enter only **s**, a list of possible completions appears. This list indicates that one or more possible keywords begin with **s**, thus making your entry ambiguous.

```
localhost(config)# s
Possible completions:
  session    Global default CLI session parameters
  system     System settings
  ---
  save       Save configuration to an ASCII file
  service    Modify use of network based services
  show       Show a parameter
```

12.8.2 Parameters

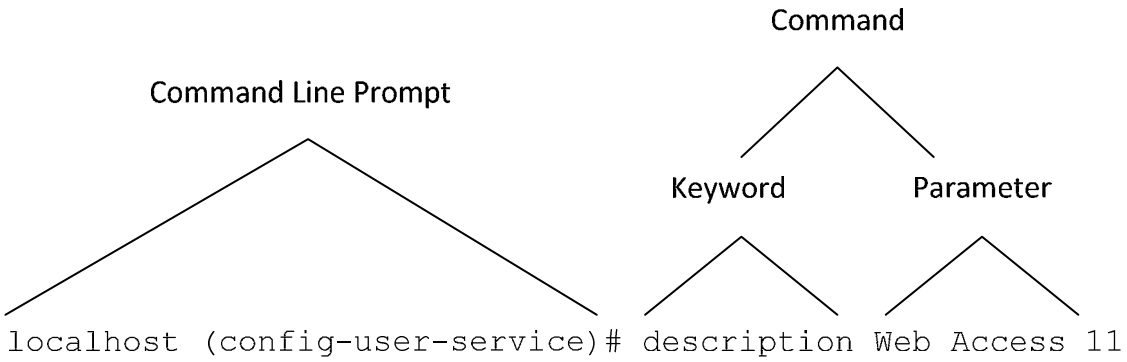
Parameters are often required elements of a command; however, for some commands, parameters are not required. A parameter is most often a value that you specify after the keyword. There are different types of parameters, such as strings, integers, or IP addresses. The X-100 CLI indicates the type of parameter that you must enter. When you see a range of numbers or uppercase letters, it indicates that you must specify a value.

12.8.3 Keywords and Parameters Together

By combining keywords and parameters in the correct sequence, you can begin using the X-100 CLI to configure and monitor your X-100 system. For example, you could specify the Global CONFIG command **user service** to add a description of the user service to the X-100 system by entering a keyword and a parameter. You need to type only the portion of the keyword that makes it unambiguous, such as **des**. Here, the value of the parameter, which is the description you assign to the user service (for example, "Web Access 1"), is a string of up to 64 characters.

For example:

```
localhost(config)# user service
localhost(config-user-service)# ?
Possible completions:
  alias         Create command alias.
  description   User description
  session       User specific default CLI session parameters
  ---
  commit        Commit current set of changes
  exit          Exit from current mode
  help          Provide help information
  no            Negate a command or set its defaults
  pwd           Display current mode path
  top           Exit to top level and optionally run command
localhost(config-user-service)# des
(<string>):
```



12.9 Saving Configuration Changes Made Through the X-100 CLI

When using the X-100 CLI to change parameters on the X-100 system configuration, the changes do not take effect immediately. This example shows the full process to follow to have system configuration changes made through the X-100 CLI take effect on the X-100 system and have them saved across system restarts.

For example, to change the radio frequency on the X-100 system, you run the **radio** Global CONFIG command:

```
localhost#
localhost# config terminal
localhost(config)# radio
localhost(config-radio)# frequency 2310000
localhost(config-radio)#
```

While you have entered a new value for the radio frequency to be 2310000, this configuration change has not taken effect (if you were to measure the frequency it would still be at the original value). For this change to take effect, you need to run the **commit** Global CONFIG command:

```
localhost(config-radio)# commit
#commit complete
localhost(config-radio)#
```

Now your change has taken effect and the radio frequency is actually operating at the 2310000 frequency on the X-100 system.

However, this has only made a change to the current running configuration of the X-100 system—not the startup configuration (the startup configuration is loaded upon booting the system). This means that if the system is restarted, the running configuration changes are lost unless they have been previously saved to the startup configuration. To do this, copy the running configuration to the startup configuration on the X-100 system by using the **copy** Privileged EXEC command:

```
localhost(config-radio)# exit
localhost(config)# exit
localhost# copy running-configuration startup-configuration
localhost#
```

Through the X-100 CLI, by way of this example you have now successfully made a change to the X-100 system configuration, committed this change to the running configuration, and copied the running configuration to the startup configuration, thereby saving the configuration change across system restarts.

12.10 Writing and Running X-100 CLI Scripts

To simplify the loading of common or repetitive configuration setups, the X-100 CLI has a basic scripting facility that enables you to define and run scripts that run multiple CLI commands in series to completion. Depending on your needs, you might want to store all of your CLI commands in one script file, or group script files by function.

To run a basic CLI script file on the X-100 system, save the script as text, then copy and paste it directly into the X-100 CLI at the Global CONFIG level. The script then runs on the X-100 system. Ordinarily, when a CLI script is run, it is run to completion, even if errors are encountered.

Always observe these key points when writing or running CLI scripts:

- The commands in the script must be valid in the current operating mode.
- If a command inside a script contains a syntax error, or fails for some other reason, the remainder of the commands in the file are still run (that is, script execution does not abort on failure).
- A script does not require an **exit** or **logout** command at the end. If present, these commands are run normally, such that if run in user mode the CLI session is exited.
- Comments can be included directly in the CLI script file itself and are identified with an exclamation mark (!) at the start of a line. This tells X-100 modules that the information is a comment and should not be displayed or parsed. Comments do not require an end tag.

Note: If you decide to include comments, anyone who reads or edits your CLI script may read them. Any application that parses or validates your CLI script ignores commented information.

12.11 Using Help

The X-100 CLI provides a variety of useful context-sensitive help features. An important thing to remember about using the help features is that the use of a space or the lack of a space before the **?** gives different results. Table 13 summarizes the help system.

Table 12 Help Commands

Command	Description
?, help, <Tab>	Lists all commands or command options available in the current CLI level.
partial-command<Tab>	Completes the partial command you entered, if you have provided an unambiguous abbreviation. Otherwise, if ambiguous, the CLI lists the available command options.
Command<space>?	Gives detailed help on the specific command and its available parameters in the current CLI level.

12.11.1 ? (Question Mark Key)

You can enter the question mark (**?**) key whenever you need additional information. When you enter **?**, all available choices for the CLI level are displayed. When you enter **?** on a line by itself or when it is preceded by one or more spaces, a list of all next available choices is displayed. Refer to Example 1.

Example 1

From the prompt, you can enter **?** to display the online help:

```
BLiNQ X100 CLI
admin connected from 192.168.5.100 using ssh on localhost
localhost# ?
Possible completions:
  autowizard              Automatically query for mandatory elements
  clear                   Clear parameter
  compare                 Compare running configuration to another
                          configuration or a file
  complete-on-space       Enable/disable completion on space
  config                  Manipulate software configuration information
  copy                    Copy configuration from one store to another
  display-level           Configure show command display level
  event-history
  exit                    Exit the management session
  file                    Perform file operations
  help                    Provide help information
  history                 Configure history size
  id                      Show user id information
  idle-timeout            Configure idle timeout
  ignore-leading-space    Ignore leading whitespace (true/false)
  job                     Job operations
  logout                  Logout a user
  no                      Negate a command or set its defaults
  output-file             Copy output to file or terminal
  paginate                Paginate output from CLI commands
  prompt1                 Set operational mode prompt
  prompt2                 Set configure mode prompt
  quit                    Exit the management session
  screen-length           Configure screen length
  screen-width            Configure screen width
  send                    Send message to terminal of one or all users
  show                    Show information about the system
  show-defaults           Show default values when showing the configuration
  source                  File to source
  system
  terminal                Set terminal type
  who                     Display currently logged on users
  write                   Write configuration

localhost# config terminal
Entering configuration mode terminal
localhost(config)# ?
Possible completions:
  admin           Administrative settings and commands
  alias           Create command alias.
```

```
  ethernet          Ethernet port settings
  event-history
  mgmt              Management interface settings
  radio             Radio Interface Settings
  session           Global default CLI session parameters
  system            System settings
  user
  ---
  abort             Abort configuration session
  clear             Remove all configuration changes
  commit            Commit current set of changes
  copy              Copy a dynamic element
  do                Run an operational-mode command
  end               Terminate configuration session
  exit              Exit from current mode
  help              Provide help information
  insert            Insert a parameter
  load              Load configuration from an ASCII file
  move              Move a parameter
  no                Negate a command or set its defaults
  pwd               Display current mode path
  rename            Rename an identifier
  resolved          Conflicts have been resolved
  revert            Copy configuration from running
  rollback          Roll back database to last committed version
  save              Save configuration to an ASCII file
  service           Modify use of network based services
  show              Show a parameter
  top               Exit to top level and optionally run command
  validate          Validate current configuration
```

Alternatively, the user can terminate a command with a ? to display the complete help on that command. This feature is most powerful when the command keyword is known, but the list and format of parameters is not. Refer to Example 2.

Example 2

You can terminate an X-100 CLI command with a **?** to display the complete help on that command:

```
localhost(config)# mgmt ?
Possible completions:
  default-gateway
  interfaces        Management interfaces administrative state
  ip                Management IP address and netmask
  ip-config-mode    Management IP mode
  syslog            Syslog server settings
```

12.11.2 help Command

From the prompt, you can enter the **help** command when you want to display a brief description of the X-100 CLI help system.

```
localhost# help
```

```
Possible completions:
  autowizard              Automatically query for mandatory elements
  clear                   Clear parameter
  compare                 Compare running configuration to another
                          configuration or a file
  complete-on-space       Enable/disable completion on space
  config                  Manipulate software configuration information
  copy                    Copy configuration from one store to another
  display-level           Configure show command display level
  event-history
  exit                    Exit the management session
  file                    Perform file operations
  help                    Provide help information
  history                 Configure history size
  id                      Show user id information
  idle-timeout            Configure idle timeout
  ignore-leading-space    Ignore leading whitespace (true/false)
  job                     Job operations
  logout                  Logout a user
  no                      Negate a command or set its defaults
  output-file             Copy output to file or terminal
  paginate                Paginate output from CLI commands
  prompt1                 Set operational mode prompt
  prompt2                 Set configure mode prompt
  quit                    Exit the management session
  screen-length           Configure screen length
  screen-width            Configure screen width
  send                    Send message to terminal of one or all users
  show                    Show information about the system
  show-defaults           Show default values when showing the configuration
  source                  File to source
  system
  terminal                Set terminal type
  who                     Display currently logged on users
  write                   Write configuration
```

12.11.3 Partial-keyword <Tab>

At any point in the command line, the user can press **<Tab>** to display the valid inputs onward.

When you cannot recall a complete command name or keyword, type in the first few letters, press **<Tab>**, and the system completes your partial entry. However, you must type enough characters to

provide a unique abbreviation. If your partially entered command is not unique, the CLI presents you with a list of valid options.

For example:

```
localhost# show run <Tab>
```

A subsequent **<Tab>** will then display the valid parameters for the command / argument pair:

```
localhost# show running-config <Tab>
Possible completions:
  admin      Administrative settings and commands
  alias      Create command alias.
  ethernet   Ethernet port settings
  mgmt       Management interface settings
  radio      Radio Interface Settings
  session    Global default CLI session parameters
  system     System settings
  user
  |          Output modifiers
  <cr>
```

12.12 Upgrading System Software Through the X-100 CLI

Active and standby software image versions can coexist simultaneously on the HM and RBM.

Entering the **show system software** Privileged EXEC command displays the 'running-version', 'restart-version', and 'available-version' software images currently on the HM or RBM. The running and restart versions represent the currently 'active' system software images, while the available version represents the 'standby' system software image. For example:

```
localhost# show system software
system software running-version 1.0.10_1
system software restart-version 1.0.10_1
system software available-version 1.0.7_1
localhost#
```

To ugrade the software through the X-100 CLI, do the following:

1. Run the **systems software download** Privileged EXEC command to download a new software image onto the HM or RBM from an FTP server. If the software download is successful, the command output indicates "Upgrade was successful". For example:

```
localhost# system software download ftp blinq1 blinq1
169.254.1.27 BLiNQ_X100_0.13.0_2.bin
Downloading BLiNQ_X100_0.13.0_2.bin from 169.254.1.27 using
FTP.....
ftp succeeded.
Verifying the checksum of the image.......
Checksums are equal
checksum is valid
Uncompressing image.........
We are running from partition 0
Applying the app directory
Applying the os directory
Applying the radio directory
./kernel/
./kernel/vmlinux
Kernel is present
Putting Kernel in Boot Partition 1
22544628 bytes
File stored in partition 1
Upgrade was successful
```

2. Run the **show system software** Privileged EXEC command. The 'available-version' field (that is, the 'standby' system software image) should show the new software load image version:

```
localhost# show system software
system software running-version 1.0.10_1
system software restart-version 1.0.10_1
system software available-version BLiNQ_X100_0.13.0_2.bin
localhost#
```

3. To make the 'available-version' software (that is, the 'standby' software load image) the active software on the module, run the **system software switchover** Privileged EXEC command:

```
localhost# system software switchover
```

On completion, the HM or RBM resets and the user is forced out of the X-100 CLI. Log in again once the X-100 system is back up and running.

4. If the software upgrade fails (due normally to a corrupt load), the system restarts again using the old software image. The command output from the **systems software download** command indicates that this has happened. In this case, select a different version of the new software and repeat this procedure from Step 1.

13 System Provisioning

This chapter describes the tasks associated with preparing an X-100 system to allow it to provide network services to its users. Each section in the chapter covers a different task:

- Initial System Setup and IP Configurations
- Adding Users
- Provisioning Default Versus Individual Service Flows
- Configuring and Adding Individual RBMs

13.1 Initial System Setup and IP Configurations

When you receive a new X-100 system from the factory with no configuration on it, you must connect to the management interface so that you can change the management IP address of the Hub Module (HM) and configure other management parameters for the system, as follows:

1. Connect your computer directly to the HM through an Ethernet cable. Once you have the cable connected to the HM, check your connectivity to the management interface IP address by pinging the HM. There are two IP addresses you can use for this:
    - 192.168.26.2/24, the default IP address given to all X-100 systems from the factory
    - 169.254.1.1/16, the debug IP address that is always accessible as it cannot be changed by the user
2. Ensure that the NIC on your computer has been assigned an address within one of the subnets for these two IP addresses.

    Note: If you cannot access the 192.168.26.2 address, it is possible that someone has changed this IP. When you are unsure of the IP address of the module, use the 169.254.1.1 address as it cannot be changed.
3. After successfully pinging either of two IP addresses above, either:
    a. Open a web browser and navigate to the IP address that you pinged to bring up the X-100 WebUI.
    b. Use a Secure Shell (SSH) client to log on to the X-100 CLI using an SSH connection to the IP address that you pinged. However, SSH version 2.0 client software must be installed on your host computer (SSH version 1.0 can be used, but is not recommended).
4. When prompted for login credentials, enter the default username and password **admin**.

Once logged on to the HM, you can change the IP address of the management interface. This can be done by one of two methods. You can choose to either statically assign the IP address for the management interface, or you can use the Dynamic Host Configuration Protocol (DHCP) to configure this IP address.

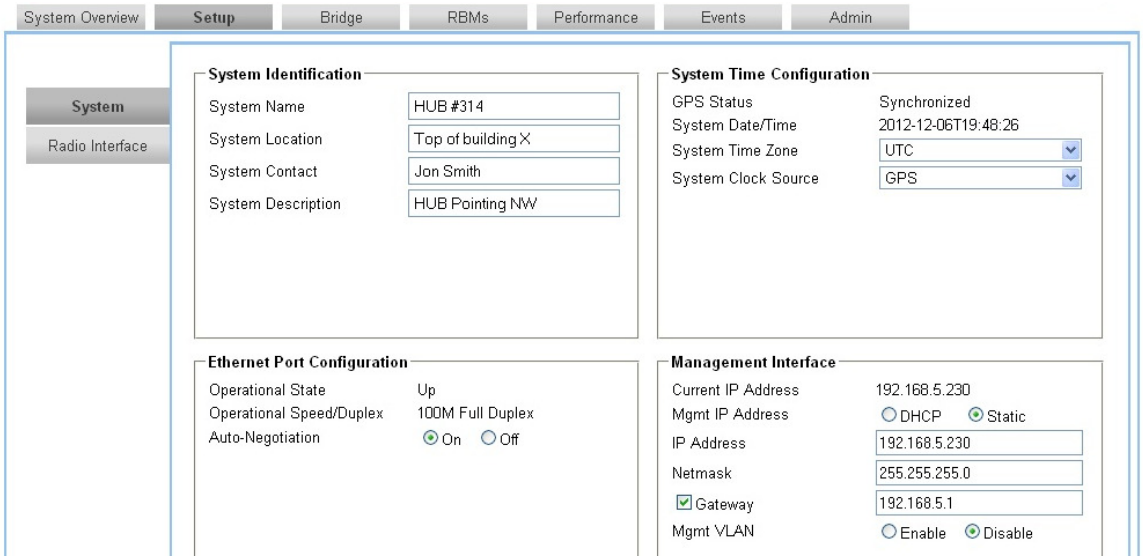
Note: To have DHCP properly assign an address to your X-100 system, the system must have network access to a DHCP server on your local network. This DHCP server must have available addresses in its address pool, which are in the desired subnet you wish to assign to the system.

By default, the X-100 system is configured to get an IP address for the management interface through DHCP. If desired, change it to a static user-assigned IP address using the X-100 WebUI, as follows:

1. Navigate to the "Setup Page (System)" sub-page of the X-100 WebUI.

   In the bottom right corner, under "Management Interface", are all the configurable options for the management interface.

2. Change the "Mgmt IP Address" selection from "DCHP" to "Static".
3. Enter an IP address, netmask, and optionally an address for the default gateway (local router).
4. Click "Apply" in the bottom right corner for the changes to take effect.



Alternately, if you wish to use the X-100 CLI to change this management IP to a static user-assigned IP address (for example, 192.168.1.1/24), enter these commands:

```
localhost#
localhost# config
Entering configuration mode terminal
localhost(config)# mgmt ip-config-mode static
localhost(config)# mgmt ip 192.168.1.1/24
localhost(config)# commit
Commit complete.
```

To allow for a radio link to be created between an HM and RBM, you must at a minimum initially configure the following for the X-100 system, as follows:

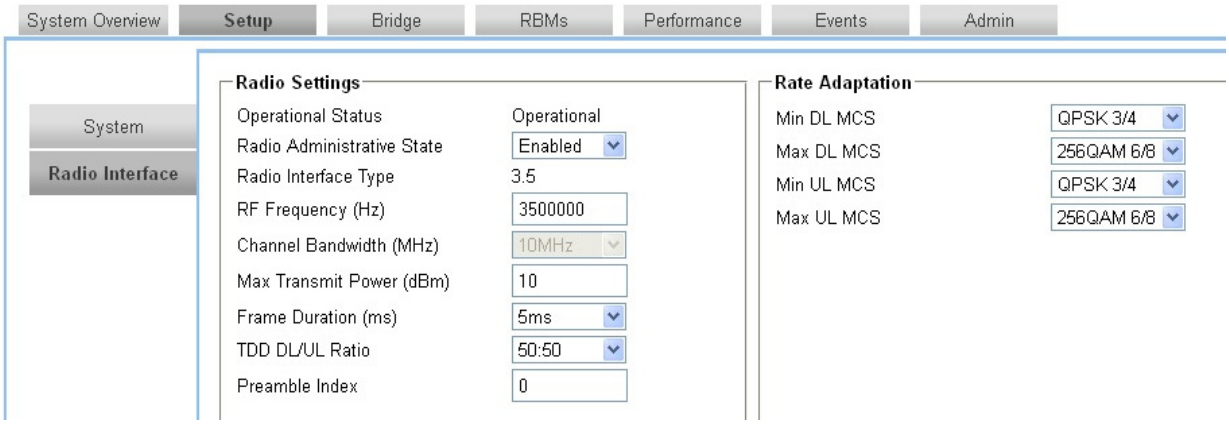
1. Navigate to the “Setup Page (Radio Interface)” sub-page of the X-100 WebUI.
2. Set the Radio Administrative State to “Enabled”.
3. Ensure both the HM and RBM have their radio frequencies set to matching values that are within the range of usable frequency for the X-100 system.

   Note: The radio frequency tuning granularity is 1 kHz.

4. Click “Apply” in the bottom right corner for the changes to take effect.

General notes:

- The following RF parameters must match between an HM and RBM for a radio link to be created:
  - frequency
  - preamble index value (for more information on preambles, refer to Chapter 14)
- Since the RBM factory default value for the preamble index is “All”, it automatically accepts preambles from any HM. Other preamble index values can be configured provided the HM and RBM preamble index values match.
- These RF parameters are passed from the HM to the RBM:
  - TDD DL/UL ratio
  - Frame Duration (that is, size)
  - Max/Min DL MCS
  - Max/Min UL MCS



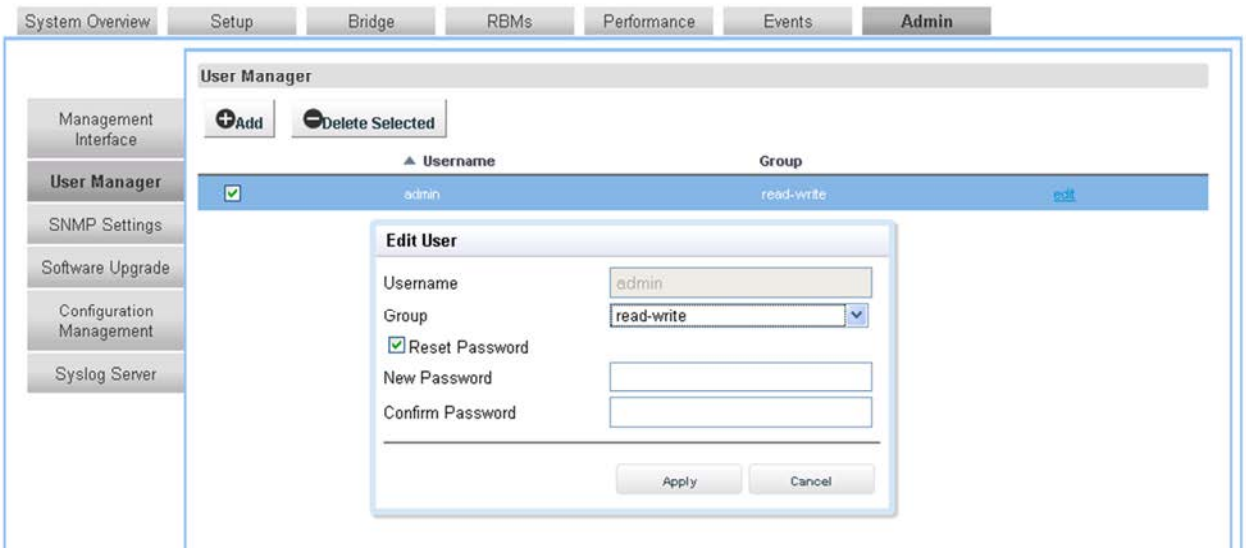
13.2 Adding Users

Adding users to the X-100 system can be done through either the X-100 WebUI or the X-100 CLI.

To add users to the X-100 system using the X-100 WebUI:

1. Navigate to the “Admin Page (User Manager)” sub-page of the X-100 WebUI.
1. Choose “User Manager” from the tabs on the left side of the page.
2. Click “+Add” to add a user.
3. From the prompt you can now enter a username, password, and choose the access privilege group you wish the user to belong to (either read-only or read/write).

   Note:
   - User names must start with a letter and may be composed of alphanumeric characters only.
   - Passwords are case sensitive, may be composed of alphanumeric characters and special characters, and must contain at least one letter and one digit.
   - At least one user with read/write privileges needs to exist in the X-100 system.
   - If you cannot login due to a forgotten user name or password, contact another user with read/write access privileges to have them reset your login credentials. If you have lost all read/write login credentials, contact your supplier.
4. Click “Apply” for the changes to take effect.



To add users to the X-100 system using the X-100 CLI, enter these commands:

```
localhost#
localhost# config
Entering configuration mode terminal
```

```
localhost(config)# admin users user <user name> password <password> group
<read-only or read/write>
localhost(config-user-<username>)# commit
Commit complete.
```

This command string creates a user with the given username, password, and access privilege based on the group.

13.3 Provisioning Default Versus Individual Service Flows

The HM has two service flow definitions for allowing communication to be established with a RBM, set through the 'RBMs (RBM General)' X-100 WebUI sub-page for HMs:

- Use Default Service Definition
- Use Individual Service Definition

If **Use Default Service Definition** is set, you can define up to four unidirectional default service flow definitions for that HM as set through the 'RBMs (Default Service)' sub-page. All RBMs connecting to this HM then are assigned this service flow definition profile and it is not necessary to enter MAC addresses for the RBMs as the HM automatically discovers them. Use of this definition is best associated with the Automatic Scan Mode for RBMs because any RBM can then automatically connect to an HM, and the HM does not need to know the MAC address of the RBM.

Note: You cannot use individual service definition profiles on a per RBM basis If **Use Default Service Definition** is set since all the RBMs then have the same default service flow assigned as defined in the HM.

If **Use Individual Service Definition** is set, you can define and assign up to four downlink and four uplink service flows for each RBM (for a total of 32 per HM) through the 'RBMs (RBM List)' sub-page. The assignment is done based on the MAC address of each RBM, so use of this definition requires you to manually provision the HM with the MAC addresses of the RBMs. The RBM preamble operating mode must in turn either be set to Automatic Scan Mode, or its preamble series index value must be set to match that of the HM through the Defined Preamble Mode.

In summary, the typical use cases for the HM service flow definitions are:

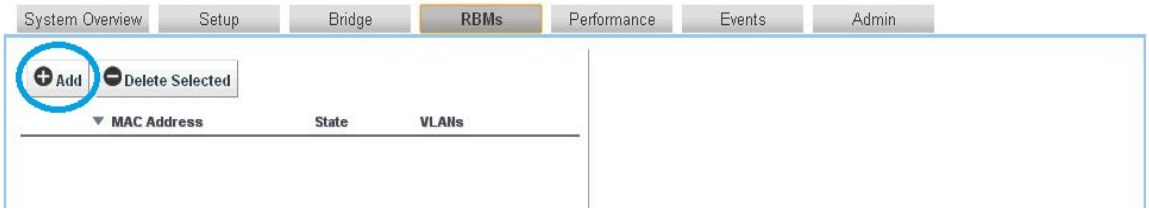
- Use Case 1—If the operator has one service flow definition that applies to all RBMs in the cluster, set the HM service flow definition to **Use Default Service Definition**. There is then no need to provision the HM with the MAC addresses of the RBMs as the HM automatically discovers the RBM MAC addresses.
- Use Case 2—If the operator wants to configure individual service flow definitions for each RBM in the cluster on an RBM-by-RBM basis, set the HM service flow definition to **Use Individual Service Definition**. This requires you to manually provision the HM with the MAC address for each RBM in its cluster, as described in section 13.4 "Manually Adding and Configuring Individual RBMs".

13.4 Configuring and Adding Individual RBMs

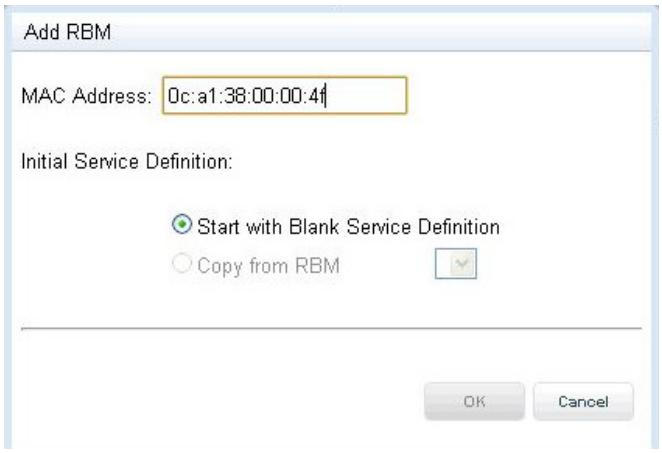
With the HM service flow definition set to **Use Individual Service Definition**, you must configure each RBM service flow and add the RBMs to the X-100 system on an RBM-by-RBM basis. This can be done through either the X-100 WebUI or the X-100 CLI.

For example, to configure a default, pass-all, bidirectional service flow on the HM for one RBM on the X-100 system using the X-100 WebUI:

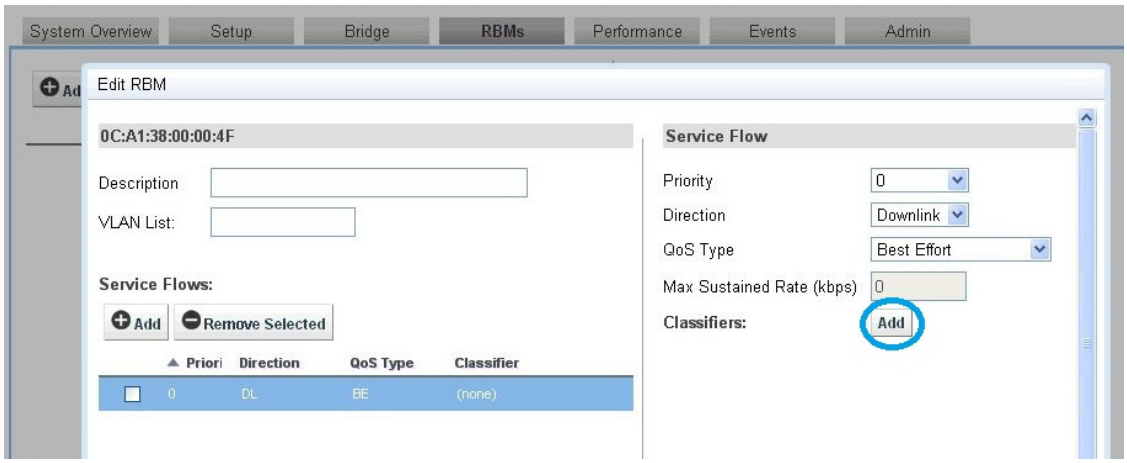
1. Navigate to the RBMs page of the X-100 WebUI.
2. Click **Add** to add an RBM.



3. In the Add RBM prompt, enter the MAC address for your RBM and click **OK**.

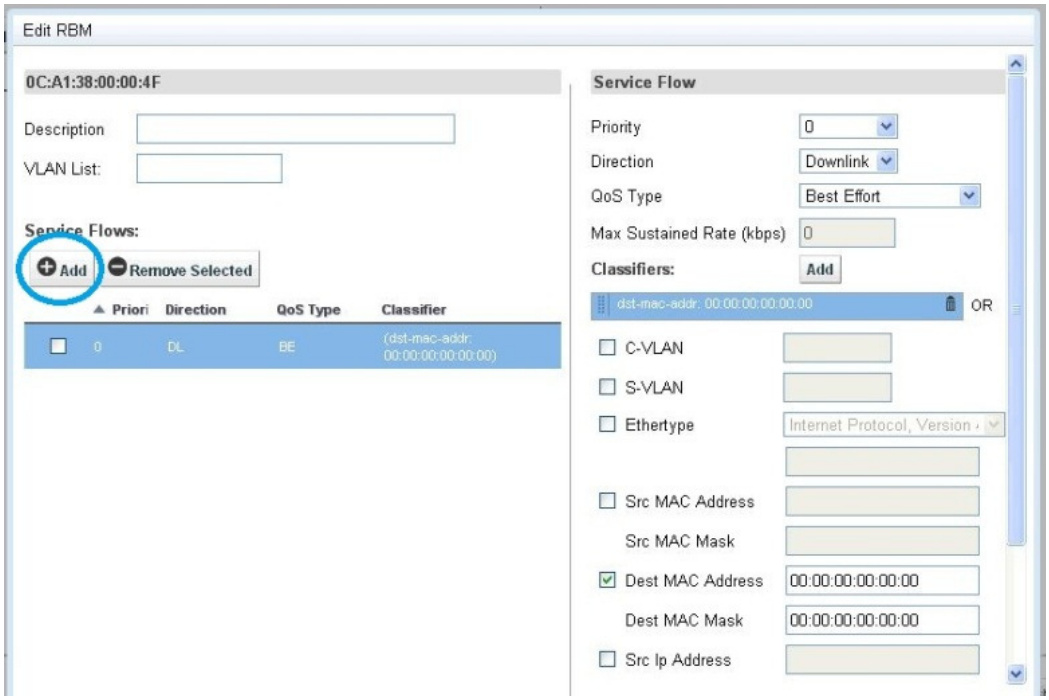


4. From the Edit RBM prompt, click **Add** to add a service flow.
5. Leave the Direction and QoS Type as their defaults. Click **Add** next to Classifiers to add a classification rule.

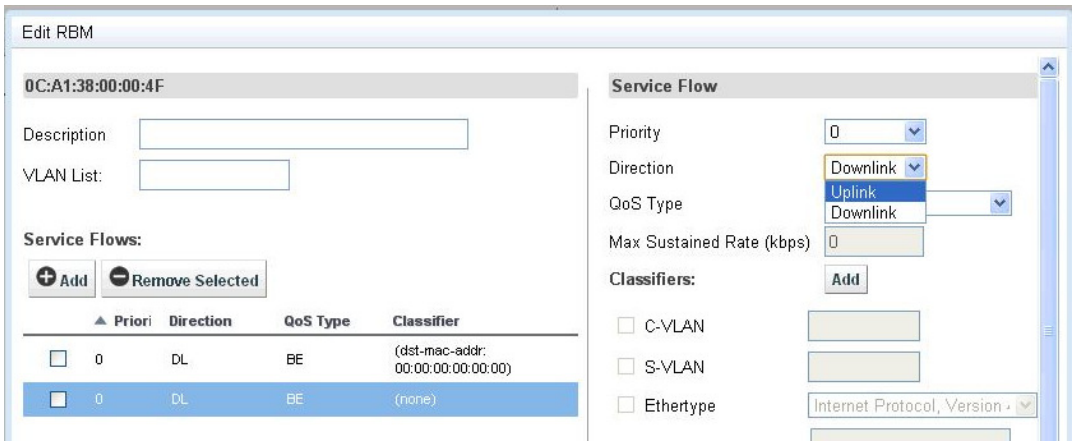


6. Select the “Destin MAC Address” box and set both values to 00:00:00:00:00:00 to allow for any destination MAC Address.

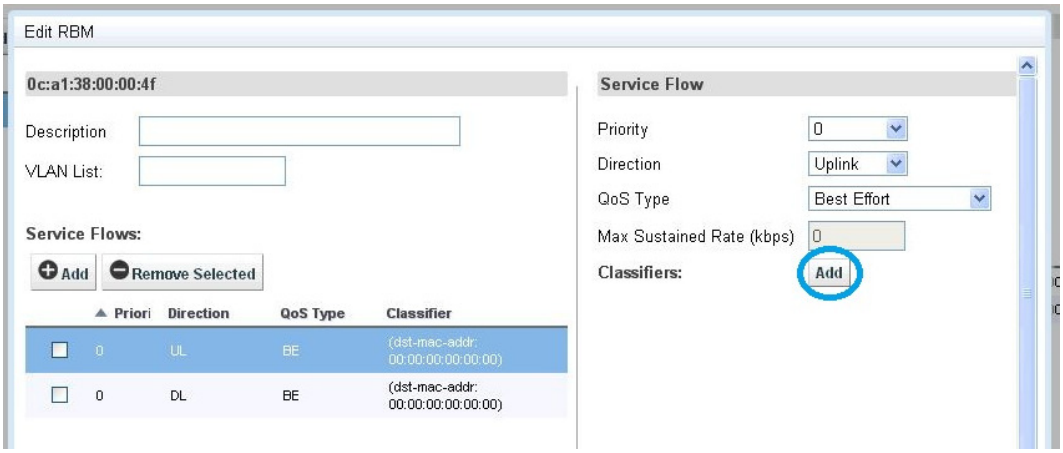
7. Click **Add** to add another service flow for the other direction.



8. Change the direction of this service flow to Uplink.

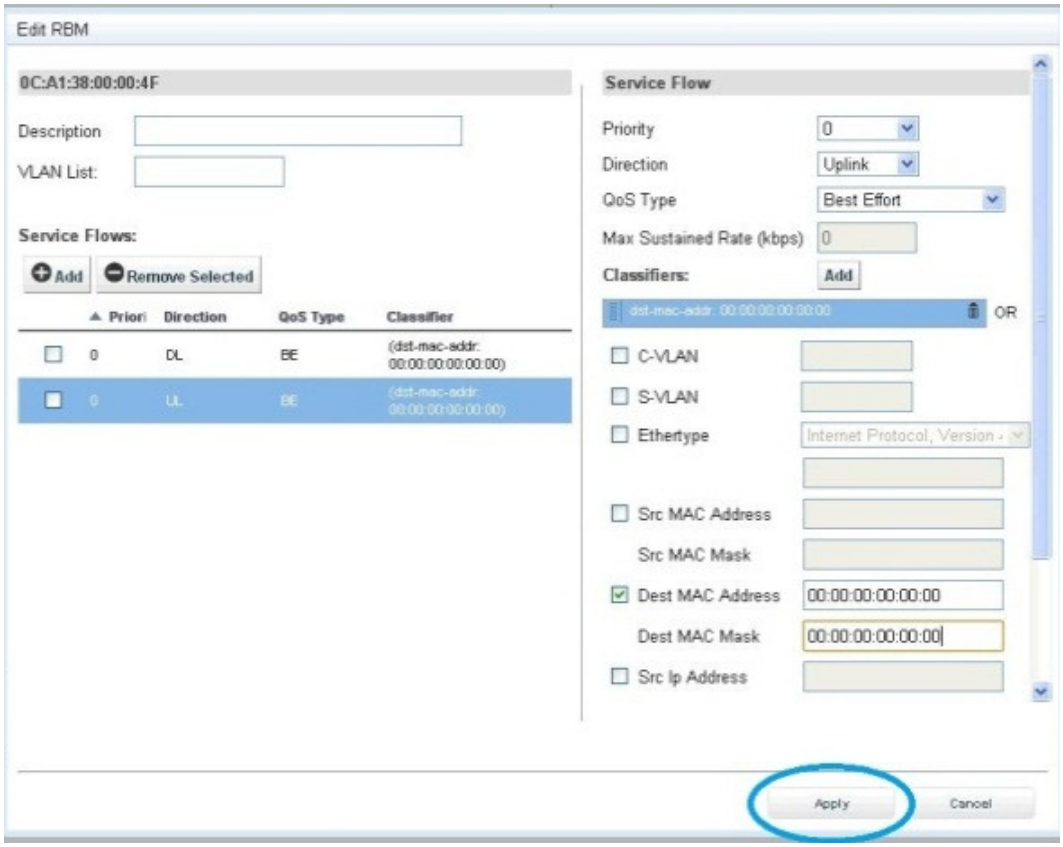


9. Click **Add** to add a classification rule for this service flow.



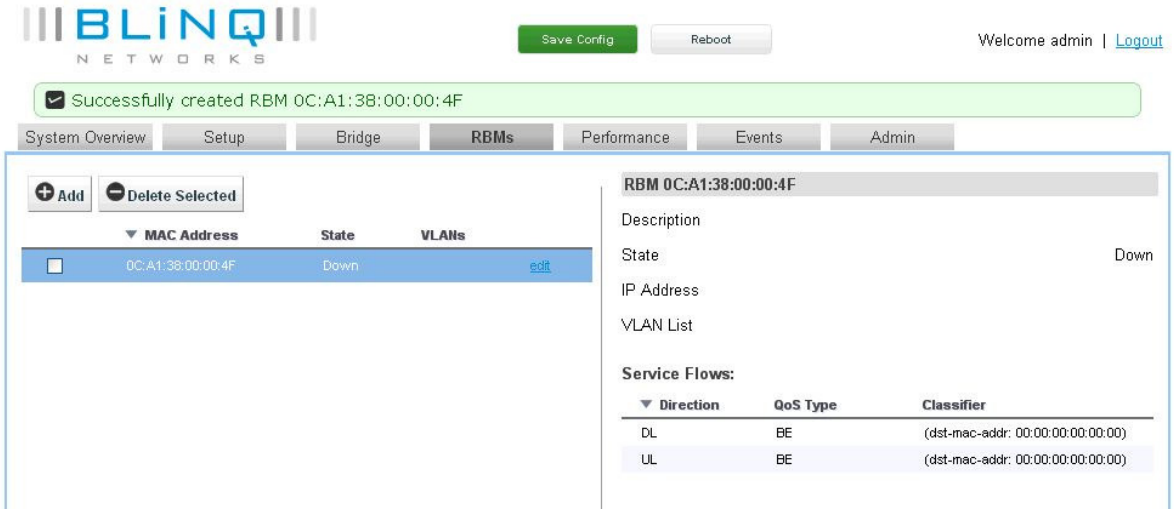
10. Select the Dest MAC Address checkbox and set both values to 00:00:00:00:00:00 to allow for any destination MAC Address.

11. Click **Apply** for the changes to take effect.

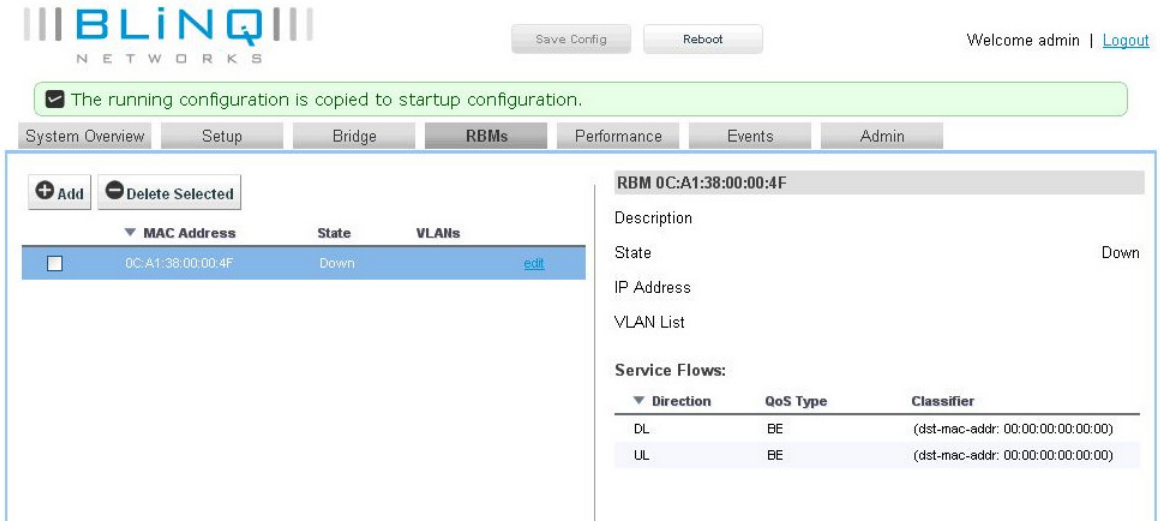


You should now see a message that the RBM was successfully created and is now in the RBM table.

13. Select the green **Save Config** button.



14. The system should notify you that the running configuration has been successfully copied to the startup configuration.



Alternately, for example, to configure a default pass-all, bidirectional service flow on the HM for one RBM on the X-100 system using the X-100 CLI, enter these commands:

```
localhost#

localhost# config terminal                          //Enter configuration mode
Entering configuration mode terminal
localhost(config)# rbm-table rbm <MAC-ADDRESS       //Add the MAC of the RBM to the RBM table
OF RBM>
```

```
localhost(config-rbm-0c:a1:38:00:00:4f)#
service-flows service-flow 1
Value for 'direction' [downlink,uplink]:
downlink

Value for 'priority' (<unsignedByte>): 0

Value for 'qos service-type' [best-
effort,guaranteed-bit-rate]: best-effort
```

//Create the first service flow for one direction

```
localhost(config-service-flow-1)#
classification rule 1

localhost(config-rule-1)# dst-mac-addr
00:00:00:00:00:00
localhost(config-rule-1)# dst-mac-mask
00:00:00:00:00:00
localhost(config-rule-1)# exit
localhost(config-service-flow-1)# exit
```

//Add the classification rule that allows for any destination MAC address

```
localhost(config-rbm-0c:a1:38:00:00:4f)#
service-flows service-flow 2
Value for 'direction' [downlink,uplink]:
uplink
Value for 'priority' (<unsignedByte>): 0
Value for 'qos service-type' [best-
effort,guaranteed-bit-rate]: best-effort
```

//Create the second service flow for the other direction

```
localhost(config-service-flow-2)#
classification rule 1
localhost(config-rule-1)# dst-mac-addr
00:00:00:00:00:00
localhost(config-rule-1)# dst-mac-mask
00:00:00:00:00:00
```

//Add the classification rule that allows for any destination mac address

```
localhost(config-rule-1)# commit


Commit complete.
localhost(config-rule-1)# end
```

//Commit the commands so that they take effect

```
localhost# copy run start
```

//Copy the running configuration to the startup-configuration so that upon reboot this configuration will be loaded

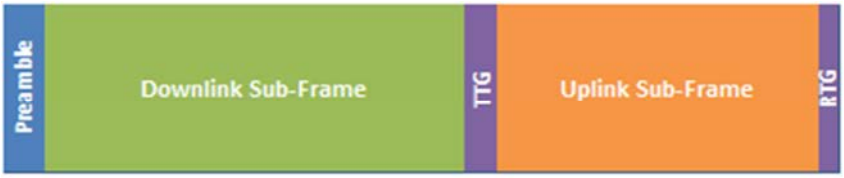
14 Preambles, Flows, and Network Provisioning

This chapter describes the role and use of preamble series indices and service flows in provisioning multiple X-100 clusters—a cluster being one Hub Module (HM) configured with its group of up to four Remote Backhaul Modules (RBMs) (referred to as 1:2, 1:3, or 1:4 clusters), as well as the provisioning tasks to follow for determining which RBMs from which clusters are allowed to register with a particular HM.

- Preamble Functional Description
- Preamble Operational Description
- Provisioning Preambles
- Provisioning HM Service Flow Definitions
- Provisioning Multiple Clusters Within the Same Area

14.1 Preamble Functional Description

The X-100 system uses Time Division Duplex (TDD) to transport wireless traffic data. TDD divides the data stream into frames. There are two frame size options: 3.125 msec and 5 msec. The frame consists of a number of Orthogonal Frequency-Division Multiplexing (OFDM) symbols. Each OFDM symbol is 97.1 µsec long with a 1/16 cyclic prefix option (91.4 µsec useful symbol time plus 6.25 µsec cyclic prefix; cyclic prefix of 1/8 is optional). The TDD frame is divided into a downlink sub-frame and an uplink sub-frame. The downlink to uplink ratio is user selectable through the Web UI or CLI: 50:50 or 65:35.



TTG: Transmit Transition Gap
RTG: Receive Transition Gap

The first symbol of the TDD frame is the ‘preamble’. This symbol is used for physical layer procedures such as synchronization, initial channel estimation, and noise and interference estimation. It is repeated in every frame. The preamble carries a uniquely defined signaling sequence. Up to 32 unique preamble indices can be configured on the X-100 system.

Preamble indices identify and separate clusters of X-100 modules from each other, and enhance the receive operation performance of the X-100 system when different clusters are deployed in close geographical and/or RF proximity (RF proximity in this context is defined as two clusters that may or may not be geographically close, but significant power from one cluster is received by modules of the second cluster).

Note: BLiNQ recommends that clusters in close geographic and RF proximity be identified with different preamble indices by assigning the HM a different preamble index from that of its RF neighbor.

14.2 Preamble Operational Description

A Hub and RBM only register and talk to each other if they have the same preamble series value. If the RBM preamble index value does not match that of any HM, the RBM cannot connect or communicate to any HM.

General notes:

- A Hub can only have up to four RBMs registered at any one time.
- There are 32 possible X-100 preamble series index values: 0 to 31.
- HMs default to a preamble series value of '0' (factory default).
- RBMs default to a preamble series of 'all'. That is, by default RBMs accept and register with any Hub preamble series index value (factory default).
- Hub modules can only be configured with one preamble series index value, while RBMs can be configured to either a specific index value to match a Hub, or to automatically scan multiple index values to search for the best serving Hub

Hubs default to a preamble series value of '0', while RBMs default to a preamble series of 'all'. Thus, by factory default, RBMs accept X-100 system service from and register with the best serving Hub pointed in their direction using any preamble series index value.

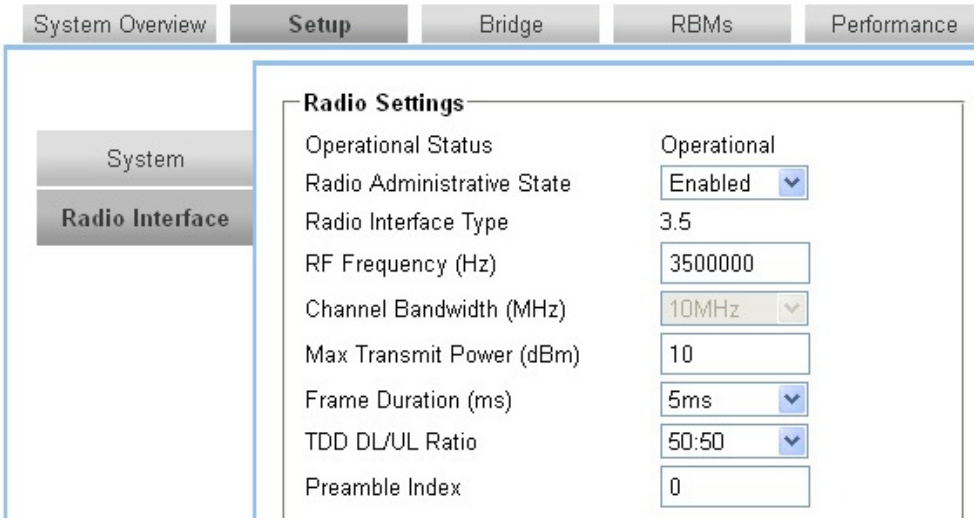
With 32 preamble series index values available, you can provision up to 32 neighboring clusters within the same geographic area using, for example, preamble series index value 0 for the first 1x4 cluster, preamble series index value 1 for the second 1x4 cluster, preamble series index value 2 for the third 1x4 cluster, and so forth, all the way up to preamble series index value 31 for the 32nd 1x4 cluster. Such a configuration runs no risk of Hub-to-RBM registration faults between neighboring clusters.

Note: Best Signal Indicator (BSI) is an RBM operating mode which allows the installer to easily determine the direction of the best quality signal from the best serving HM (refer to section 10.4.4 for details). When the field technician mounts the RBM and is in the process of searching for the optimum direction of the best serving HM using BSI, the RBM cycles through all preambles in Automatic Scan Mode (by factory default, unless set otherwise). Once the RBM identifies the preamble value for the best serving available HM, it locks on to that preamble value to allow the installer to pinpoint the best direction for the RBM to communicate with that HM.

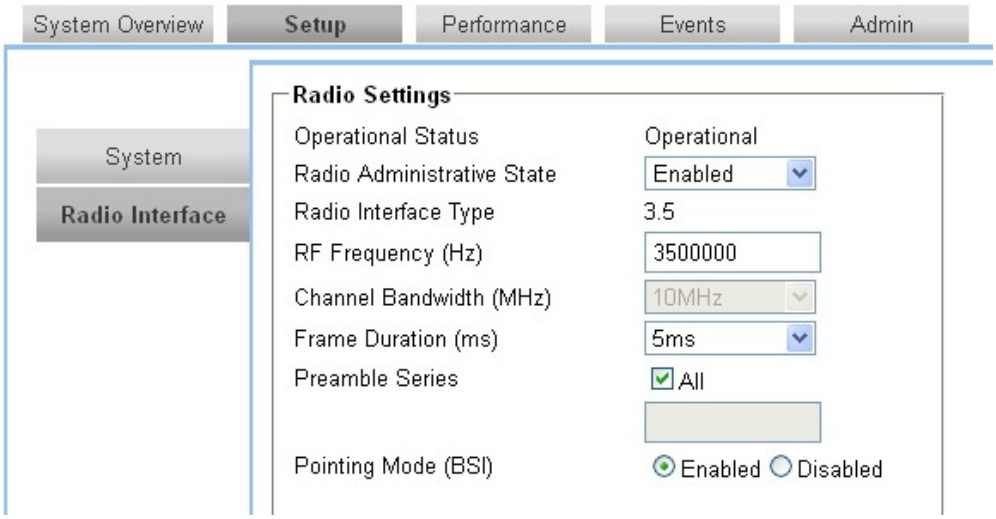
14.3 Provisioning Preambles

The default Preamble Series index settings can be seen in the 'Setup (Radio Interface)' sub-page of the X-100 WebUI for HMs and RBMs, respectively, under Radio Settings.

Hub Radio Settings show the factory default of '0' for Preamble Series, but can be set to use any single unique preamble index value from 0 to 31:



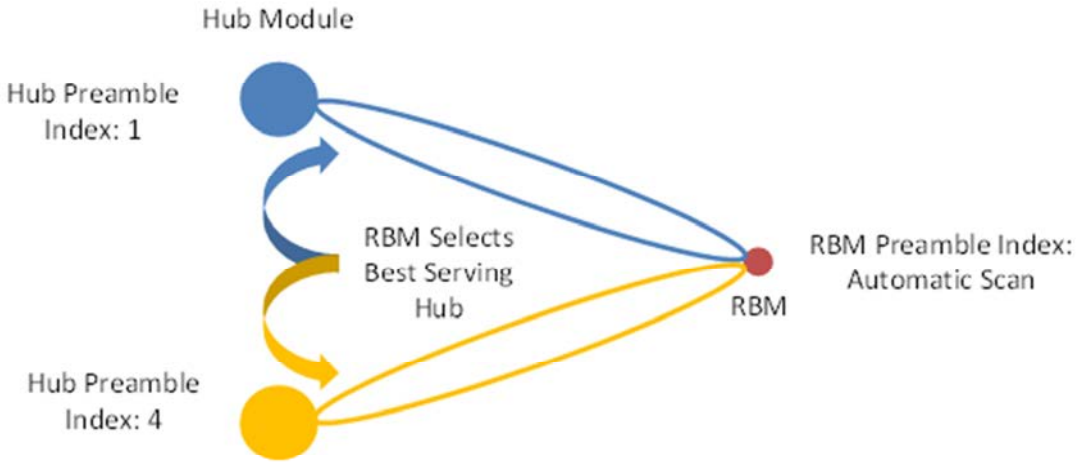
RBM Radio Settings show the factory default of 'All' for Preamble Series, but the box below the 'All' checkbox can be set to use any single unique preamble index value from 0 to 31:



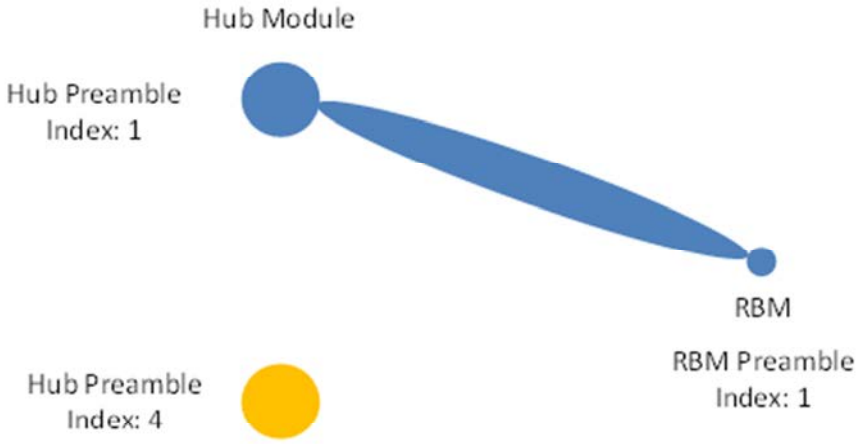
RBMs can also be set to two different preamble operating modes through the 'Setup (Radio Interface)' X-100 WebUI sub-page for RBMs:

- Automatic Scan Mode—When the RBM preamble series index is set to "All" (the system default), the RBM scans the full range of preamble values to automatically determine the best serving HM available to it within its cluster.
- Defined Preamble Mode—When the RBM preamble series index is set to a value between 0 to 31, it searches and seeks to connect and register to the best serving HM pointed in its direction within its cluster that matches its RBM preamble value setting.

  Note: Registering with the best serving HM through the Defined Preamble Mode can serve to reduce overall network interference because selecting the best RF server usually results in reduced transmitted power and consequently reduced network interference between clusters.



RBM Preamble Index set to Automatic Scan selects the best serving HM



RBM configured to Preamble Index 1 only connects to a hub module with Preamble Index 1

The Defined Preamble Mode is typically used when the operator seeks to connect to a specific hub module. For normal network operation, BLiNQ recommends that the preamble on RBMs be set to a specific index value using the Defined Preamble Mode rather than use Automatic Scan Mode. In Automatic Scan Mode an RBM can register with a weaker serving HM based on its initial startup orientation—completely missing a better serving HM for its location later on.

Note: If an RBM loses communication with its HM (for example, in case the HM fails), if set to Automatic Scan Mode it attempts to identify and connect to another HM. Otherwise, if set to Defined Preamble Mode, the RBM scans for and identifies the best HM in its direction that matches its set preamble series definition value.

14.4 Provisioning HM Service Flow Definitions

As explained in Chapter 13 “System Provisioning”, the HM has two service flow definitions for allowing communication to be established with a RBM, set through the ‘RBMs (RBM General)’ X-100 WebUI sub-page for HMs:

- Use Default Service Definition
- Use Individual Service Definition

Refer to section 13.3 “Provisioning Default Versus Individual Service Flows” for details.

The typical use cases for the HM service flow definitions are:

- Use Case 1—If the operator has one service flow definition that applies to all RBMs in the cluster, set the HM service flow definition to **Use Default Service Definition**. There is no need to provision the HM with the MAC addresses of the RBMs as the HM automatically discovers the RBM MAC addresses.
- Use Case 2—If the operator wants to define individual service flow definitions for each RBM in the cluster on an RBM-by-RBM basis, set the HM service flow definition to **Use Individual Service Definition.**

14.5 Provisioning Multiple Clusters Within the Same Area

With 32 preamble series index values available, you can provision up to 32 neighboring clusters within the same geographic area.

Using ‘Use Case 2’ from section 14.4, you can, for example, provision three neighboring 1:4 clusters within the same geographic area using the X-100 WebUI:

First 1:4 Neighbor Cluster:

Using the X-100 WebUI for the HM:

1. Enter **0** in the ‘Preamble Series’ box of the Setup(Radio Interface) sub-page, under Radio Settings.
2. Click **Apply** for the changes to take effect.
3. Select the green **Save Config** button to copy the running configuration to the startup configuraton.

Using the X-100 WebUI for RBM 1, RBM 2, RBM 3, and RBM 4, respectively:

1. Enter **0** in the ‘Preamble Series’ box of the (Radio Interface) sub-page, under Radio Settings.
2. Click **Apply** for the changes to take effect.
3. Select the green **Save Config** button to copy the running configuration to the startup configuraton.

Second 1:4 Neighbor Cluster:

Repeat the steps done for the first 1x4 cluster, replacing the 'Preamble Series' value 0 with **1**.

Third 1:4 Neighbor Cluster:

Repeat the steps done for the first 1x4 cluster, replacing the 'Preamble Series' value 0 with **2**.

Alternately, using 'Use Case 2' from section 14.4, the same three neighboring 1x4 clusters can be provisioned within the same geographic area using the X-100 CLI:

First 1:4 Neighbor Cluster:

Using the X-100 CLI for the HM:

```
localhost(config)# radio
localhost(config-radio)# preamble series-index 0
```

Using the X-100 CLI for RBM 1, RBM 2, RBM 3, and RBM 4, respectively:

```
localhost(config-radio)# preamble scanning-mode scan-series-list
localhost(config-radio)# preamble series 0 value 0
```

Second 1:4 Neighbor Cluster:

Repeat the steps done for the first 1x4 cluster, replacing the 'preamble series' value 0 with **1**.

Third 1:4 Neighbor Cluster:

Repeat the steps done for the first 1x4 cluster, replacing the 'preamble series' value 0 with **2**.

Further, if applicable for your network, this can be repeated all the way up to preamble series index value 31 for the 32nd 1x4 cluster.

15 Appendices

15.1 BLiNQ Wireless Devices and RF Safety

All BLiNQ Networks products are evaluated to ensure they conform to the Radio Frequency (RF) energy emission safety limits adopted by the Federal Communications Commission (FCC). These evaluations are conducted 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 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 body.

To prevent unnecessary exposure to RF energy:

- Always install the X-100 system so as to provide and maintain a minimum separation distance from all persons.
- When the X-100 system is operational, avoid standing directly in front of Hub Module (HM) sectored antennas or in front of Remote Backhaul Modules (RBMs) and their internal antennas. RF energy fields may be present when the transmitter is on.
- Do not install the X-100 system in a location where it is possible for people to stand or walk inadvertently in front of an antenna.

15.2 List of Acronyms

Table 13 List of Acronyms

BE	Best Effort
BSI	Best Signal Indication
B-SON	Backhaul – Self-Organizing Network
CINR	Carrier to Interference plus Noise Ratio
CLI	Command Line Interface
CoS	Class of Service
CPE	Customer Premise Equipment
DARS	Digital Audio Radio Service
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DN	Directory Number
DNS	Domain Name System
ECC	European Communications Committee
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
F/B	Front to Back
FTP	File Transfer Protocol
GBR	Guaranteed Bit Rate
GPS	Global Positioning System
HM	Hub Module
IEEE	Institute of Electrical and Electronics Engineers
L2	Layer 2
LAN	Local Area Network
MAC	Media Access Control
MARA	Managed Adaptive Resource Allocation
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple Input Multiple Output
MIMO-SM	Multiple Output-Spatial Multiplexing
MRC	Maximal Ratio Combining
NLOS	Non Line-of-Sight
NMS	Network Management System
NOC	Network Operations Center
OAM	Operations, Administration & Maintenance
OFDM	Orthogonal Frequency Division Multiplexing
OSS	Operations Support System
PC	Personal Computer
PMP	Point-to-Multipoint
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation

QoS	Quality of Service
RBM	Remote Backhaul Module
RF	Radio Frequency
RFEC	Radio Frequency Environment Characterization
SFTP	Secure File Transfer Protocol
SISO	Single Input Single Output
SFP	Small form-factor pluggable
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
S-VLAN	Stacked VLAN
TDM	Time Division Multiplexed
TDD	Time Division Duplexing
ToS	Terms of Service
UL	Uplink
URL	Universal Resource Locator
VLAN	Virtual Local Area Network
VSWR	Voltage Standing Wave Ratio
VDC	Volts Direct Current
WCS	Wireless Communications Services