



BLiNQ Networks Inc.

X-1200 Intelligent Wireless Backhaul System

User Guide

Release D 0.1

Issue D01

November 2013

Revision History

Date	Release	Issue	Reason for Issue
November 2013	Release D 0.1	Issue D01	Initial Draft (still in development)

Contact Information:

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

Web Site:

<http://www.blingnetworks.com>

Sales Inquiries:

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

Customer Support:

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

Table of Contents

1	X-1200 System Overview	1
2	X-1200 System Description	5
3	Technical Specifications	9
3.1	System Parameters	9
3.2	OFDMA and Frame Parameters	10
3.3	Integrated RBM Antenna Performance	10
3.4	Optional Cavity Filters	11
3.5	System Enclosure	11
4	System Synchronization	13
4.1	Synchronization Services	13
5	System Throughput Performance	15
6	Element and Network Management	16
7	Ethernet Bridge Support	19
8	Using the X-1200 WebUI	21
8.1	Requirements	21
8.2	Common X-1200 WebUI Page Items	21
8.2.1	General	21
8.2.2	System Status Messages	22
8.3	Configuring Hub Modules	23
8.3.1	Logging In	24
8.3.2	System Overview Page	25
8.3.3	Setup - System Page	26
8.3.4	Setup - Radio Interface Page	27
8.3.5	Bridge Page	29
8.3.6	RBMs - General RBM Page	30
8.3.7	RBMs - Default Service Page	32
8.3.8	RBMs - RBM List Page	38
8.3.9	Performance - HM Page	39
8.3.10	Performance - RBMs Page	40
8.3.11	PM History Page	42
8.3.12	Events - Alarms Page	44
8.3.13	Events - History Page	44
8.3.14	Admin - Management Interface Page	45
8.3.15	Admin - User Manager Page	46
8.3.16	Admin - SNMP Settings Page	48
8.3.17	Admin - Performance Settings Page (HM Only)	50

8.3.18	Admin - Software Upgrade Page.....	51
8.3.19	Admin - Configuration Management Page	52
8.3.20	Admin - Syslog Server Page.....	53
8.4	Configuring RBMs.....	54
8.4.1	Logging In	54
8.4.2	System Overview Page.....	55
8.4.3	Setup - System Page.....	55
8.4.4	Setup - Radio Interface Page.....	56
8.4.5	Performance Page.....	56
8.4.6	Events Page	57
8.4.7	Admin Page	57
9	Alarms and Events (Fault Management).....	58
10	Using the X-1200 Command Line Interface.....	62
10.1	Overview	62
10.2	X-1200 CLI Command Line Prompts.....	62
10.3	X-1200 CLI Keywords and Parameters	63
10.3.1	Keywords.....	63
10.3.2	Parameters.....	63
10.3.3	Keywords and Parameters Together	64
10.4	Identify Command Context.....	64
10.5	X-1200 CLI Command Structure.....	65
10.6	Logging On to the X-1200 CLI.....	66
10.7	Privileged EXEC Commands	67
10.8	Global CONFIG Commands	68
10.8.1	Radio CONFIG Mode	69
10.8.2	User CONFIG Mode	70
10.8.3	RBM CONFIG Mode (Hub Modules Only)	71
10.9	Saving Configuration Changes Made Via X-1200 CLI	74
10.10	Writing and Running X-1200 CLI Scripts.....	75
10.11	Using Help	75
10.11.1	? (QUESTION MARK Key).....	76
10.11.2	help Command	79
10.11.3	Partial-keyword - TAB	81
10.12	Upgrading System Software through the X-1200 CLI	82
10.13	Show Command Options	83
11	System Provisioning.....	89
11.1	Initial System Setup and IP Configurations.....	89
11.1.1	Assigning a Management IP Address.....	90
11.1.2	Configuring the Radio Interface.....	91

11.2	Adding Users	92
11.2.1	Add Users using X-1200 WebUI	92
11.2.2	Add Users using the X-1200 CLI	93
11.3	Provisioning Default Versus Individual Service Flows.....	93
11.4	Configuring and Adding Individual RBMs.....	94
11.4.1	Using the X-1200 WebUI.....	94
11.4.2	Using the X-1200 CLI	98
12	Preambles, Flows, and Network Provisioning.....	99
12.1	Preamble Functional Description.....	99
12.2	Preamble Operational Description	100
12.3	Provisioning Preambles.....	100
12.4	Provisioning HM Service Flow Definitions	102
12.5	Provisioning Multiple Clusters within the Same Area.....	102
12.5.1	Provisioning Multiple Clusters with the X-1200 WebUI.....	102
12.5.2	Provisioning Multiple Clusters with the X-1200 CLI	103
13	Appendices.....	104
13.1	BLiNQ Wireless Devices and RF Safety.....	104
13.2	Equipment Compliance.....	105
13.2.1	Federal Communications Commission (FCC) Notices	105
13.2.2	Industry Canada Notice.....	106
13.3	List of Acronyms.....	107

List of Figures

FIGURE 1	BLiNQ X-1200 SYSTEM IN A WIRELESS BACKHAUL APPLICATION	1
FIGURE 2	HUB MODULE	3
FIGURE 3	REMOTE BACKHAUL MODULE	3
FIGURE 4	X-1200 SYSTEM 1024 SUB-CARRIER OFDM PHYSICAL LAYER	5
FIGURE 5	DYNAMIC BANDWIDTH SHARING (DBS) AUTOMATICALLY ALLOCATING CAPACITY ON PER RBM BASIS	6
FIGURE 6	HUB MODULE (HM) (FRONT AND BACK RESPECTIVELY).....	11
FIGURE 7	REMOTE BACKHAUL MODULE (RBM) (FRONT AND BACK RESPECTIVELY)	11
FIGURE 8	SYSTEM SYNCHRONIZATION THROUGH GPS	14
FIGURE 9	SYSTEM SYNCHRONIZATION THROUGH IEEE 1588V2	14
FIGURE 10	L2 TRANSPARENT BRIDGE FUNCTIONALITY OF X-1200 SYSTEM	19
FIGURE 11	X-1200 WEBUI SYSTEM STATUS MESSAGE (SUCCESS MESSAGE SHOWN)	22
FIGURE 12	X-1200 WEBUI WARNING MESSAGE	22
FIGURE 13	X-1200 WEBUI ERROR MESSAGE	23

List of Tables

TABLE 1 OVERVIEW OF MAIN X-1200 SYSTEM CHARACTERISTICS	2
TABLE 2 GENERAL X-1200 SYSTEM PARAMETERS	9
TABLE 3 OFDMA AND FRAME PARAMETERS FOR A 10 MHz CHANNEL BANDWIDTH.....	10
TABLE 4 SYSTEM THROUGHPUT PERFORMANCE	15
TABLE 5 LIST OF ALARMS	58
TABLE 6 LIST OF EVENTS	60
TABLE 7 HELP COMMANDS	75
TABLE 8 LIST OF ACRONYMS.....	107

1 X-1200 System Overview

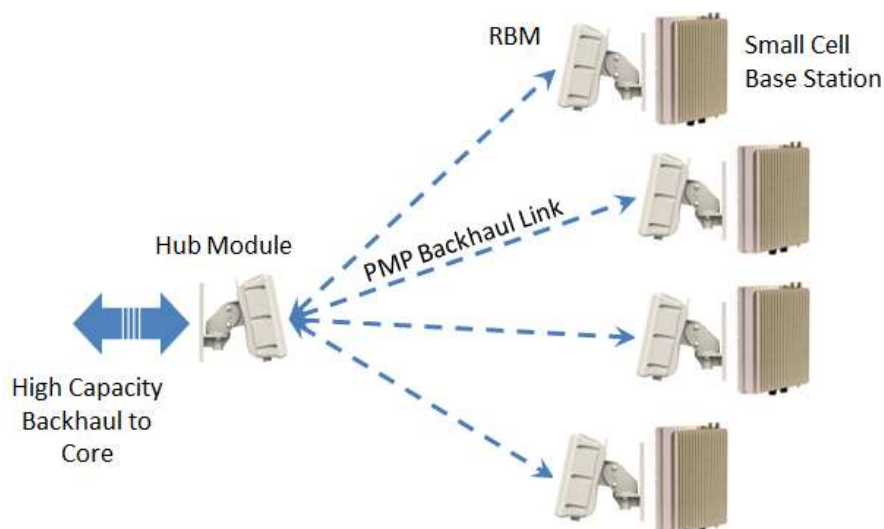


Figure 1 BLiNQ X-1200 System in a Wireless Backhaul Application

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-1200 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 (PHY) and Media Access Control (MAC) layer algorithms and techniques. BLiNQ Networks 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-1200 system delivers 11 bps/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 up to 440 Mbps of throughput in dual 2x20 MHz channels.

The X-1200 system operates in the licensed Time Division Duplexing (TDD) bands including 3.6 – 3.70 GHz band in both Point-to-Point (PTP) and Point-to-Multipoint (PMP) configurations. Other supported frequency bands include 5.725 – 5.825 GHz. Some of the main product characteristics are shown in Table 1. The X-1200 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-1200 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 yield 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-1200 system the cyclic prefix is only a small fraction of the total bandwidth.

Table 1 Overview of Main X-1200 System Characteristics

Operating Mode	Time Division Duplexing (TDD)
Physical Layer	Cyclic Single Carrier Frequency Doman Equalized
Antenna System	2x2 MIMO, Spatial Multiplexing / Tx & Rx Diversity Remote Backhaul Module: Integral antenna, 14 dBi Hub Module: Integral antenna, 17 dBi; Plasma (optional)
Operation Configuration	Point-to-Point (PTP) Point-to-Multipoint (PMP)
Throughput	Up to 400 Mbps, L2 aggregate UL and DL
Frequency of Operation	3.65 – 3.7 GHz (non-exclusive license band in US/Canada) 5.725 – 5.825 GHz
Channel Bandwidth	20 MHz (5/10 MHz ¹)
Network Interface	Ethernet (Fiber optional for Hub)
Quality of Service (QoS)	Two classes: Unsolicited Grant Service (UGS) and Best Effort (BE)
Form Factor	All-outdoor; zero-footprint

¹ Future Software Release

The X-1200 system has a small, all-outdoor, zero-footprint form factor that is easily deployed on towers, poles, building sidewalls, or rooftops unobtrusively. It consists of the following modules:

- **Hub Module (HM):** A sector controller that controls several Remote Backhaul Modules (RBMs). Hub Modules feature two RF connectors for an external user defined sectored antenna, a Small Form-factor Pluggable [SFP] housing for the optional fiber optical Gigabit Ethernet interface, and an integrated Global Positioning System (GPS) antenna.



Figure 2 Hub Module

- **Remote Backhaul Module (RBM):** A subscriber unit that is installed outdoors on customer premises, including public infrastructure assets such as light and utility poles in mobile backhaul applications. RBMs feature an integrated antenna. The RBM mechanical enclosure is similar to the Hub Module, except that the RF connectors, SFP housing and integrated GPS antenna are absent.



Figure 3 Remote Backhaul Module

- **Configuration System:** This consists of the X-1200 WebUI tool and X-1200 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).

2 X-1200 System Description

The BLiNQ X-1200 system meets 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 follow.

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.

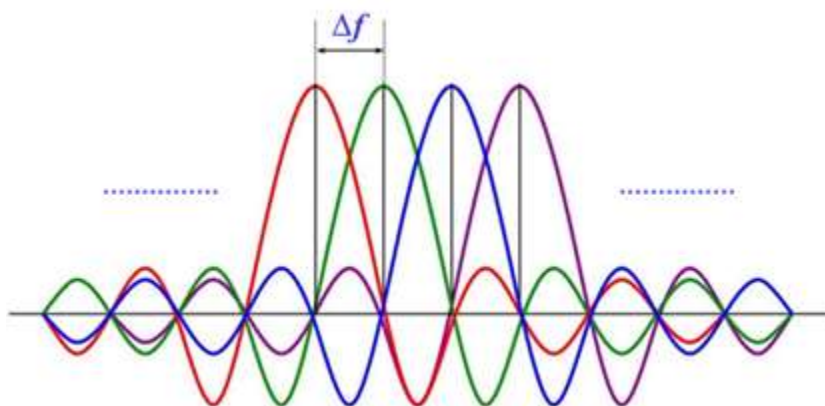


Figure 4 X-1200 System 1024 Sub-Carrier OFDM Physical Layer

Time Division Duplex (TDD): The X-1200 system features TDD access mode with variable frame length (user selectable 3.125¹ 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. Multiple settings are possible: 50:50, 65:35, 75:25, 35:65 and 25:75 downlink to uplink ratio.

Multiple Input Multiple Output (MIMO): The X-1200 system features spatial multiplexing on two antennas (2x2) for high capacity.

Adaptive Modulation with Link Adaptation: The X-1200 system supports QPSK, 16QAM, 64QAM and 256QAM on both the downlink and uplink path to achieve high capacity in limited channel bandwidth (83 Mbps² Ethernet layer throughput in a 10 MHz channel for combined downlink and uplink traffic).

Intelligent Interference Management: The X-1200 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.

¹ Not supported in current release.

² Total of 71.5 Mbps throughput is in effect in current release.

Backhaul Self-Organizing Networks: The X-1200 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-1200 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-1200 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) 4 and 5 mask requirements and 15 dB below ETSI DN 2 mask requirements.

Point-to-Multipoint (PMP) with Dynamic Bandwidth Sharing (DBS): The X-1200 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). This feature is known as Dynamic Bandwidth Sharing (DBS) and works to allocate additional capacity to RBMs experiencing a surge in throughput demand from modules that have excess capacity to spare.

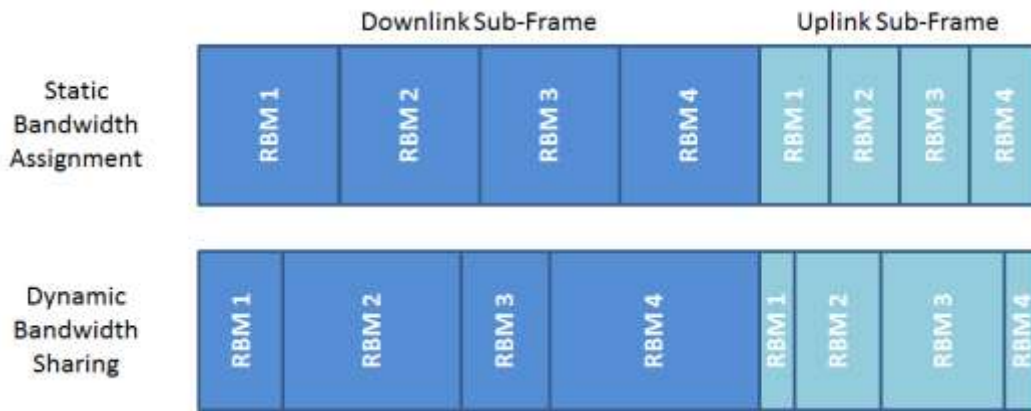


Figure 5 Dynamic Bandwidth Sharing (DBS) Automatically Allocating Capacity on Per RBM Basis

Quality of Service (QoS): Two levels of QoS are defined in the X-1200 system for traffic classification: Unsolicited Grant Service (UGS) and Best Effort (BE). Through service-level agreements (SLAs), customers can subscribe to the service class desired for their application.

Service Class		Description
UGS	Unsolicited Grant Service	Provides real-time data streams that are comprised of fixed-size data packets issued at periodic intervals.
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 based on Virtual Local Area Network (VLAN) tag and mapped according to the associated service class type. Payloads may also be classified by 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, Layer 3 (L3) IP source and destination address, and Layer 4 (L4) Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port number. QinQ/1802.1ad is supported. Traffic ‘hairpinning’ at the HM automatically forwards traffic addressed to one RBM to a peer RBM.

Multiple Frame Size: The X-1200 system supports Ethernet frame sizes up to 2016 bytes.

Security: The X-1200 system uses Advanced Encryption Standard (AES) encryption mode with 256-bit key.

Form Factor: The all-outdoor, zero-footprint Hub Module (HM) and RBMs are built to IPX2 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-1200 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-1200 system, which reduces the total cost of ownership of the solution while simplifying and accelerating installation.

The X-1200 system is small in size (31x21x8 cm) and low in weight (3.5 kg) so it easily mounts 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-1200 system also provides the following network management features:

- **Fault and Performance Management:** The X-1200 system incorporates fault and performance management through a standard Simple Network Management Protocol (SNMP)v2c/v3 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/NMSSs), thereby providing access to key information on X-1200 service availability and performance.

- **Configuration Management:** BLiNQ products minimize the configuration effort by the network operator. For example, when deployed in the field, the X-1200 system can obtain its IP address through DHCP rather than have it statically assigned by the user. Further, the X-1200 system provides a web-based configuration tool called the X-1200 WebUI and a standard Command Line Interface (CLI) that run directly on the X-1200 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 lists general X-1200 system parameters.

Table 2 General X-1200 System Parameters

RADIO SPECIFICATIONS	
Frequency Band	3.65 – 3.70 GHz, Unrestricted mode & 5.725-5.825 GHz band
Tuning Resolution	50 kHz, minimum
Transmit Power, 3.65 GHz	-15 dBm to +27 dBm per port, 0.25 dB resolution
Transmit Power, 5.8 GHz	-15 dBm to +23 dBm per port, 0.25 dB resolution
Channel Bandwidth	20 MHz (5/10 MHz ¹)
Receiver Sensitivity	-92 dBm with QPSK @ 1e-03 PER (typ.)
Modulation & Coding	QPSK/16QAM/64QAM/256QAM, bi-directional, fully adaptive
PERFORMANCE	
Throughput	Up to 400 Mbps, L2 aggregate uplink and downlink
Spectral Efficiency	11 bps/Hz
Physical Layer	Cyclic Single Carrier Frequency Domain Equalized
Operating Mode	TDD
Latency	3.5 msec for 4 RBM's assigned to Hub
Traffic ratios	50:50, 65:35, 75:25, 35:65, 25:75; user configurable
Frame Size	Up to 2016 bytes
Antenna System	2x2 MIMO, Spatial Multiplexing / Tx & Rx Diversity Remote Backhaul Module: Integral antenna, 14 dBi Hub Module: Integral antenna, 17 dBi; Plasma (optional)
Configuration	PTP or PMP up to 8 Remotes
Power Consumption	< 55 W
Power	-48 VDC nominal, -36 to -60 VDC range
Connectivity	Copper 1000BaseT Optional Fiber Gig-E (Hub only)
Synchronization	Integral GPS antenna and receiver, 1588v2, SyncE
QoS	8 queues per service flow, 4 SF's per RBM per direction
Security	AES-256
NETWORKING	
Configuration	Ethernet bridge
Attributes	802.1Q, 802.1ad, DSCP/ToS/802.1p (IPv4/IPv6)
Features	Per RBM service flows, Dynamic Bandwidth Sharing

¹ Future Software Release

OPERATIONS, ADMINISTRATION AND MANAGEMENT (OAM)	
Configuration	WebUI / CLI, radio and Ethernet performance monitoring
EMS Integration	SNMP v2c/v3
OAM Protocols	HTTP(S), TCP/IP, UDP, (S)FTP, SSH
MECHANICAL/ENVIRONMENTAL/COMPLIANCE	
RBM Dimensions	12.6" x 8.3" x 5.1" (32 x 21 x 13 cm)
Hub Dimensions	15.0" x 18.0" x 5.1" (38 x 46 x 13 cm)
Weight (Hub & RBM)	RBM < 8.8 lbs. (4.0 kg); Hub < 15.5 lbs. (7.0 kg)
Temperature Range	-45°C to +55°C (-49°F to 131°F)
Enclosure protection	IP67
Compliance	EMC: FCC Part 15 Subpart B, C, E; ICES-003 Class B Radio: FCC Part 90z, RSS 197 Safety: UL/CSA 60950-1,-22

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-1200 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 ¹	
Frames per Second	200		320	
Cyclic Prefix	1/8 ¹	1/16	1/8 ¹	1/16
Number of Symbols	48 ¹	51	30 ¹	32

¹Not supported in current release.

3.3 Integrated RBM Antenna Performance

The Remote Backhaul Module (RBM) features a high-gain antenna that has very low side lobes (-30 dBc) to minimize interference. This allows greater scalability of deployment of BLiNQ X-1200 system modules in a market and allows smaller frequency reuse factor for higher spectrum utilization. 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.

3.4 Optional Cavity Filters

Sharp roll-off cavity filters that comply with European Communications Committee (ECC) Recommendation (04)05 and Wireless Communication Services (WCS) band spectral-mask requirements can be optionally fitted into the product enclosure to provide very high isolation to adjacent bands.

The cavity filters are provisioned into the product mechanical enclosure to maintain a compact form factor for deployment on poles and other light infrastructure assets.

3.5 System Enclosure

The enclosure for both the Hub and RBM is a rugged IPX2 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. These cases allow for full flexibility in the range of orientation to establish best connectivity between the Hub and RBMs.



Figure 6 Hub Module (HM) (front and back respectively)

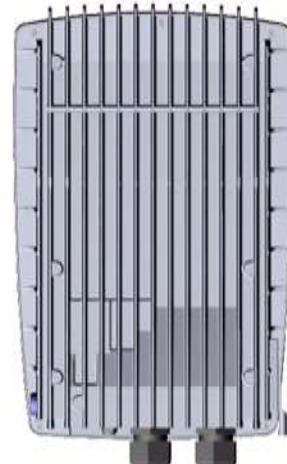


Figure 7 Remote Backhaul Module (RBM) (front and back respectively)

The mechanical enclosure for the HM has two RF port connectors for an external user-defined sectored antenna. There are two connectors 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 on the top (flat square patch). Therefore, there is no need for additional synchronization equipment which reduces 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 System Synchronization

The X-1200 system is a Time Division Multiplexed (TDM) radio system. Therefore, X-1200 networks require proper synchronization of the air interface to provide optimal service. The X-1200 system provides flexible synchronization options as well as providing a high-performance extension to existing synchronization networks which delivers quality clock services to downstream devices such as small-cells.

The Hub Module (HM) synchronizes the X-1200 system using one of two standard synchronization mechanisms: Global Positioning System (GPS) or IEEE 1588v2¹.

When configured to synchronize via GPS, the X-1200 system uses its internal GPS antenna and receiver module to synchronize to the GPS network. This allows all X-1200 HMs deployed in the network to accurately synchronize their transmit and receive operations on the air interface. The GPS system also allows the X-1200 system to determine accurate time of day and date information. This time information together with a user configured time zone setting is used to tell time across the system and is essential in functions such as fault management (for example, event and alarm time stamping) and historical performance (for example, performance indicator processing and performance file creation). The HM automatically transmits time information to any Remote Backhaul Module (RBM) associated to that HM.

When configured to synchronize on IEEE 1588v2, the X-1200 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)¹ 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-1200 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 provides 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 been 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-1200 systems.

4.1 Synchronization Services

Based on its high-performance internal synchronization mechanisms, the X-1200 system provides 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 time stamping, necessary for high-performance synchronization applications.

The X-1200 system supports two operating modes for synchronization services, depending on the primary clock reference used at the HM (that is, 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 to the

¹ Not supported in current release.

RBM and therefore the entire cluster implements the behavioral requirements of an IEEE 1588v2 master clock. The X-1200 system allows the configuration of the main IEEE 1588v2 master clock parameters such as transport protocol and messaging intervals.

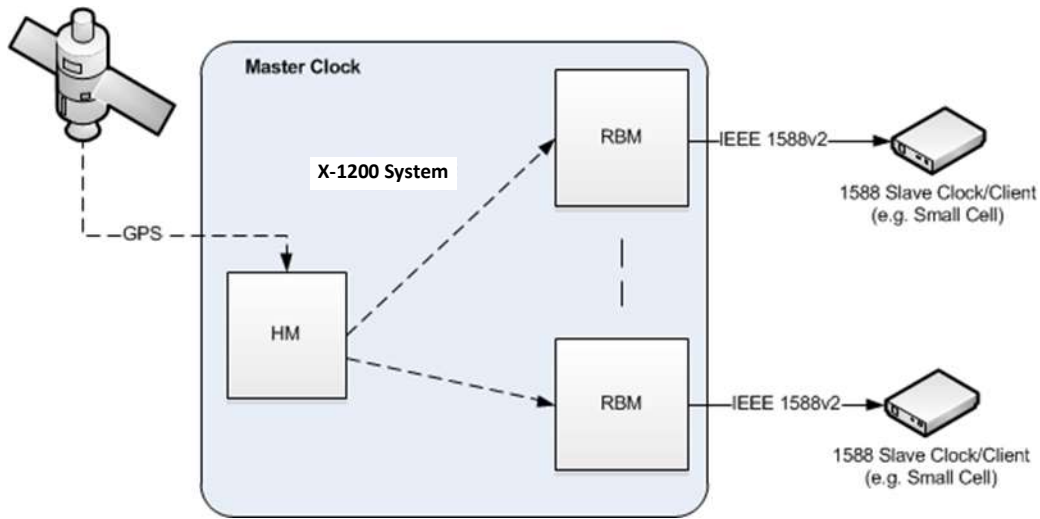


Figure 8 System Synchronization through GPS

In the second mode, the HM is configured to synchronize using the IEEE 1588v2 network, making the X-1200 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.

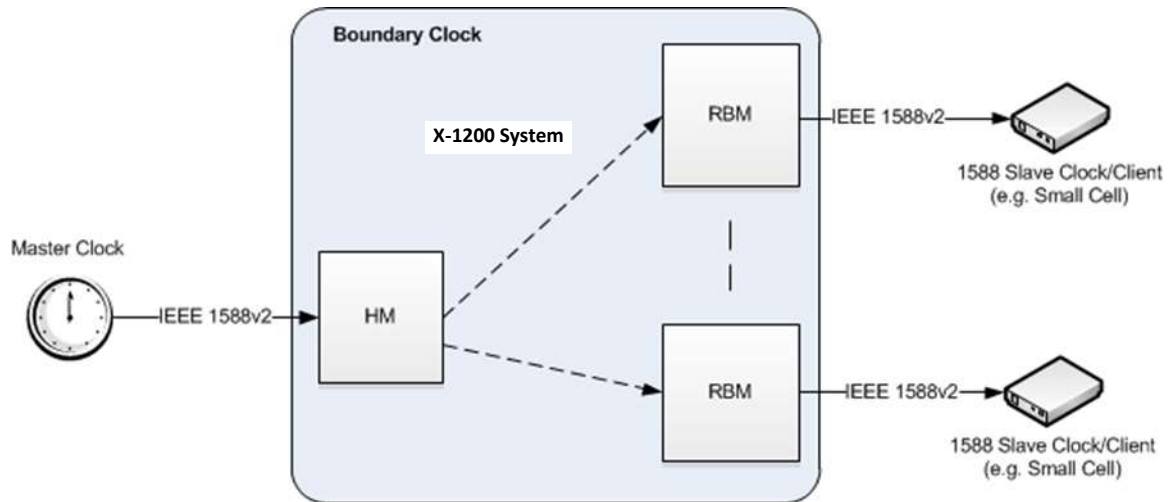


Figure 9 System Synchronization through IEEE 1588v2

5 System Throughput Performance

The X-1200 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 (3.125¹ 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 Scheme (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.

Table 4 shows the maximum link throughput for the X-1200 system assuming 10 MHz channel MIMO operation which doubles the channel throughput by transmitting two independent code words on each antenna.

Note: System throughput is set using the X-1200 WebUI Setup Page for the Radio Interface. See section 8.3.4, “Setup - Radio Interface Page” for details.

Table 4 System Throughput Performance

TDD Frame Length, DL/UL	5 ms, 50/50				3.125 ms, 12/12 ¹			
MCS	1 RBM	2 RBMs	3 RBMs	4 RBMs	1 RBM	2 RBMs	3 RBMs	4 RBMs
256-QAM 7/8¹	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

¹Not supported in current release.

Throughput performance depends on a number of factors, including system configuration parameters and deployment. Factors include, but are not limited to:

- Number of Remote Backhaul Modules (RBMs) per Hub Module (HM).
- The frame size and downlink/uplink traffic ratio setting.
- The packet size.
- The cyclic prefix (guard time interval).
- MIMO-SM or transmit diversity mode of transmission.
- Signal quality.
- The deployment scenario and RF propagation environment.

¹ Not supported in current release.

6 Element and Network Management

Designed to provide comprehensive Fault, Configuration, Accounting, Performance, and Security (FCAPS) functionality, the X-1200 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-1200 system supports the following network management Interfaces:

- **X-1200 Command Line Interface (CLI).** Accessible via Secure Shell protocol (SSH), the X-1200 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-1200 Web Interface (WebUI).** Accessible via HTTP(S), the X-1200 WebUI provides an interactive visual toolset that allows an operator to modify the full configuration of the X-1200 system as well as view state, fault, and performance indicators. The X-1200 WebUI displays performance data 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 provide complete access to configuration, state, performance and fault information in the X-1200 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-1200 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-1200 system are accessible via Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/IP (UDP/IP). The X-1200 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). You use this address in situations where the Management IP Address (see below) is not configured or is unavailable, including initial commissioning and field troubleshooting scenarios. Typically, the Local Craft IP Address is accessed by a technician by plugging directly into the RJ45 Ethernet port of the module.

Note: The RJ45 port has priority over the optional optical connector on the HM. If the latter is installed and the operator plugs into the RJ45 port, the fiber connection is disabled as long as the RJ45 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). An operator-configurable Virtual Local Area Network (VLAN) encapsulates all traffic to and from the management IP address.

The X-1200 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.

- 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 either 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.
- Bridge Configuration parameters control the Ethernet bridge and core network data behavior of the X-1200 cluster.
- Security Configuration parameters allow the operator to secure access or disable specific management interfaces and perform various unit administrative operations.
- **Fault Management.** The X-1200 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-1200 CLI or X-1200 WebUI.

- **Performance Management.** The X-1200 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-1200 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-1200 WebUI (that is, the operator uploads a software package file to the system modules using the X-1200 WebUI). The X-1200 system also supports remote configuration backups and backup restoration.

7 Ethernet Bridge Support

Designed to seamlessly integrate into existing Ethernet backhaul or general purpose networks, the X-1200 system is built for Ethernet services and provides network functionality as a standard Layer 2 (L2) Transparent Bridge (IEEE 802.1d), whereby the X-1200 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.

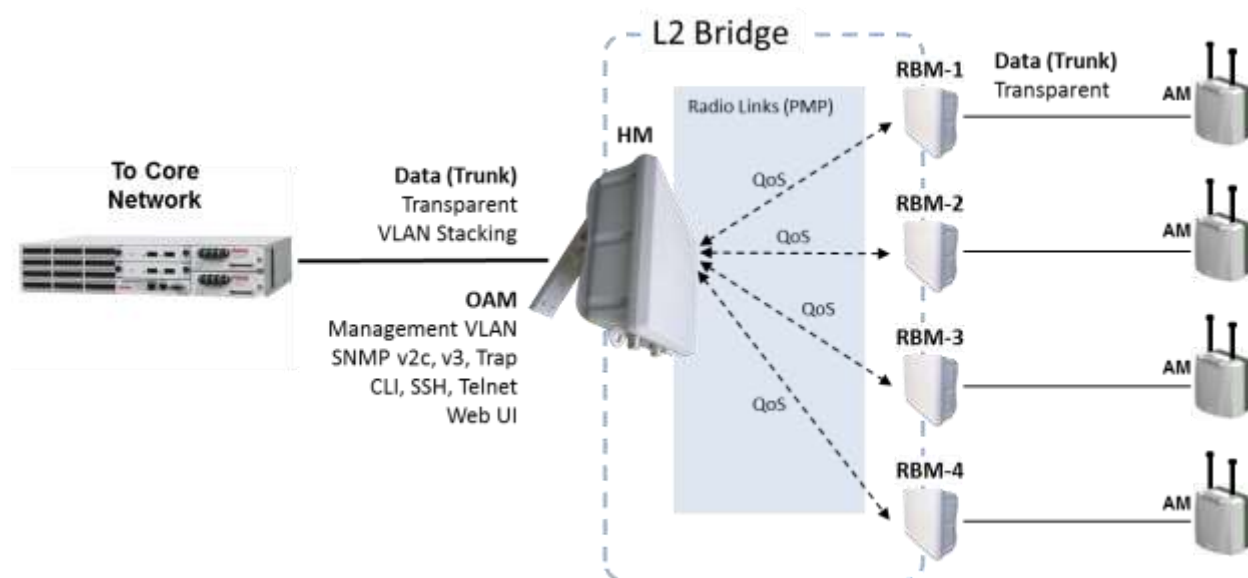


Figure 10 L2 Transparent Bridge Functionality of X-1200 System

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-1200 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.

Further, the X-1200 system supports traffic ‘hairpinning’ at the HM—the ability to automatically forward traffic addressed to one RBM on to another peer RBM without requiring the forwarding decision to be done on the core network, thereby minimizing latency. This ensures that RBM to RBM traffic is handled with minimal overhead and facilitates such use cases as inter-base station coordination when the RBMs serve to connect small cells to a core operator network.

The X-1200 scheduler supports two Classes of Service (CoS): Unsolicited Grant Service (UGS) and Best Effort (BE). The UGS CoS is 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-1200 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-1200 classification engine allows the operator to define complex classification rules (known as 'Classifiers') to further define the scope of service flows using basic Boolean logic constructs and packet field matching criteria. The following fields are supported:

- L2 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 (L3) Internet Protocol (IP) packet fields: source/destination IP address with masking option, Type of Service (ToS).

The X-1200 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-1200 system can transport standard Ethernet frames (up to 1518 bytes) as well as mini Jumbo frames of up to 2048 bytes.

8 Using the X-1200 WebUI

8.1 Requirements

The X-1200 WebUI is the configuration tool for use with X-1200 Hub Modules (HMs) and Remote Backhaul Modules (RBMs). It is a standard web application that runs directly on the X-1200 equipment through the default port for HTTP (80), and is accessible at URL <http://<ip of the node>>.

Browser support for X-1200 WebUI:

- Mozilla Firefox
- Internet Explorer 9 (IE9)
- WebKit-based browsers, for example:
 - Apple Safari
 - Google Chrome

Operating System (OS) support for X-1200 WebUI:

- Windows
- Mac OS X
- Linux

Note: With the exception of IE9, both web browser and OS support for the X-1200 WebUI always refer to the most recent versions.

All required X-1200 system configuration tasks can be performed using the X-1200 WebUI.

As an alternative, you can use the X-1200 Command Line Interface (CLI) for system monitoring and configuration tasks. See Chapter 10, *Using the X-1200 Command Line Interface* for details.

8.2 Common X-1200 WebUI Page Items

8.2.1 General

Most X-1200 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.

Changes made to the running configuration of the X-1200 system are lost when the system is restarted—unless they are saved to the startup configuration by clicking **Save Config**. Clicking the **Save Config** button copies the current running configuration to the startup configuration, thereby saving

configuration changes across system restarts. The **Save Config** button remains grayed out until changes are applied via the **Apply** button.

End each session by clicking on **Logout**, located in the top right hand corner.



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.



The X-1200 system displays the serial number, software version, and current IP address along the bottom of each main page. For example:



8.2.2 System Status Messages

The X-1200 WebUI outputs the following types of real-time messages to report on X-1200 system status:

Success Message (Green):

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



Figure 11 X-1200 WebUI System Status Message (Success Message Shown)

Warning Message (Yellow):

- A Warning message in yellow is usually shown to advise of a validation error. For example, if there are problems with inputted data then a Warning message in yellow appears to explain the issue.
- Warning messages must be clicked to be dismissed. They do not disappear automatically.



Figure 12 X-1200 WebUI Warning Message

Error Message (Red):

- An Error message in red is usually shown to advise, for example, when the server is returning an error.
- Error messages typically require troubleshooting of the X-1200 system to resolve.
- Error messages must be clicked to be dismissed. They do not disappear automatically.



Figure 13 X-1200 WebUI Error Message

8.3 Configuring Hub Modules

The following sections show the structure of the X-1200 WebUI with respect to configuring Hub Modules (HM):

- Logging In to the X-1200 WebUI — See 8.3.1, *Logging In*
- System Overview — See 8.3.2, *System Overview Page*
- Setup
 - System Page — See 8.3.3, *Setup - System Page*
 - Radio Interface — See 8.3.4, *Setup - Radio Interface Page*
- Bridge — See 8.3.5, *Bridge Page*
- RBMs
 - General RBM — See 8.3.6, *RBMs - General RBM Page*
 - Default Service — See 8.3.7, *RBMs - Default Service Page*
 - RBM List — See 8.3.8, *RBMs - RBM List Page*
- Performance
 - HM — See 6,
 - *Performance - HM Page*
 - RBMs — See 8.3.10, *Performance - RBMs Page*
- Performance History — See 8.3.11, *PM History Page*
- Events
 - Alarms — See 8.3.12, *Events - Alarms Page*
 - History — See 8.3.13, *Events - History Page*
- Admin
 - Management Interface — See 8.3.14, *Admin - Management Interface Page*
 - User Manager — See 8.3.15, *Admin - User Manager Page*
 - SNMP Settings — See 8.3.16, *Admin - SNMP Settings Page*
 - Performance Settings — See 8.3.17, *Admin - Performance Settings Page (HM Only)*
 - Software Upgrade — See 8.3.18, *Admin - Software Upgrade Page*
 - Configuration Management — See 8.3.19, *Admin - Configuration Management Page*

- Syslog Server — See 8.3.20, *Admin - Syslog Server Page*

8.3.1 Logging In

To log in and access the X-1200 WebUI interface for configuring Hub Modules (HMs):

1. Launch your web browser and set it to allow pop ups for your specific web browser (for instance Firefox, Chrome, Internet Explorer, etc.). Some screen functions in the X-1200 WebUI require pop ups.
2. If connecting locally to the HM (that is, not over a network), use your browser to connect to the local Craft IP address of the unit: **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 unit—an operator assigned, static or Dynamic Host Configuration Protocol (DHCP) IP address used for remote management of the units. Refer to Chapter 6, “**Element and Network Management**” for more information.
4. Log on to the system. The default username and password are **admin**.

User Name: **admin**

Password: **admin**



The image shows a screenshot of the BLiNQ Networks login interface. At the top, the BLiNQ Networks logo is displayed. Below the logo is a light blue rectangular box containing the login form. The form has two input fields: 'User Name:' with the text 'admin' entered, and 'Password:' with five dots representing a masked password. Below these fields is a 'Log In' button.

Note:

- User names and passwords are administered through the X-1200 WebUI using the User Manager Admin page and can be changed anytime (see section 8.3.15, “*User Manager Page*” 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-1200 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 required, see section 11.2.1, “*Add Users using X-1200 WebUI*” for more information on resetting a password). If you have lost all read/write login credentials, contact your supplier.

8.3.2 System Overview Page

This read-only page gives general system information on the particular Hub into which you are logged. 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. The screen refresh interval is every 5 seconds. For system statistics based on these graphs, see section 6, “

Performance - HM Page” for Ethernet statistics and section 8.3.10, “Performance - RBMs Page” for RBMS statistics.

The screenshot displays the BLiNQ Networks web interface. At the top, there are navigation buttons for 'Save Config' and 'Reboot', and a user greeting 'Welcome admin | Logout'. Below this is a menu bar with tabs for 'System Overview', 'Setup', 'Bridge', 'RBMs', 'Performance', 'Performance History', 'Events', and 'Admin'. The 'System Overview' tab is active.

The main content area is divided into three sections:

- Information:** A list of system details including System Name (HUB_NW), System Location (Roof NW), Uptime (0 days, 0 hours, 12 minutes, 39 seconds), Active SW Version (1.1.12_2), MAC Address (0c:a1:38:00:00:92), Model (X-100), Radio Interface Type (3.5), RF Frequency (3680000), Bandwidth (10MHz), Frame Duration (5ms), TDD DL/UL Ratio (50:50), and Preamble Index (0).
- Performance:** Two line graphs. The left graph, 'RBM(s) Throughput (Mbps)', shows three lines (red, green, blue) representing different RBMs, with values fluctuating between 0 and 5 Mbps. The right graph, 'Ethernet Throughput (Mbps)', shows two lines (red, blue) representing uplink and downlink, with values around 60-70 Mbps.
- RBMs:** A table listing three RBMs with their MAC addresses, IP addresses, and current throughput rates.
- Alarms:** A table with columns for Id, Alarm Id, Module Id, Alarm Time, Component, Severity, Type, Probable Cause, and Description. It currently shows 'No Data'.

MAC Address	IP Address	TX throughput (Mbps)	RX throughput (Mbps)	Link Uptime
0c:a1:38:00:00:91	192.168.5.234	0.00	0.00	8m
0c:a1:38:00:00:79	192.168.5.231	0.00	0.00	8m
0c:a1:38:00:00:77	192.168.5.233	0.00	0.00	8m

8.3.3 Setup - System Page

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

8.3.3.1 System Identification Area

Enter information here to aid in 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. You can also include @ for an email address.
- **System Description:** Description of the module; composed of alphanumeric characters, underscores, and dashes.

8.3.3.2 Ethernet Port Configuration Area

- **Operational State:** Up/Down (Read only)
- **Operational Speed/Duplex:** e.g. 100M Full Duplex (Read only)
- **Auto-Negotiation:** On/Off

If auto-negotiation is set to **Off**, the following options appear; set as applicable:

- **Configured Speed:** 10M/100M
- **Configured Duplex:** Full/Half

8.3.3.3 System Time Configuration Area

- **Sync State (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: FreeRun mode is intended only for isolated trial or laboratory testing of the X-1200 system only. Networks of X-1200 systems depend on proper synchronization through either GPS or IEEE 1588v2¹ 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.

8.3.3.4 Management Interface Area

- **Current IP Address:** xxx.xxx.xxx.xxx (Read only)
- **Mgmt IP Address:** DHCP/Static, set as desired

If “Static” set the following:

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

Note: If **Mgmt VLAN** is enabled, the ID entered for the Management (Mgmt) VLAN must not match the ID entered for any other VLAN passing data traffic. If the IDs match, data traffic does not pass since the X-1200 system then sees all data traffic as destined for the Management interface.

8.3.4 Setup - Radio Interface Page

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

System Overview	Setup	Bridge	RBM	Performance	Performance History	Events	Admin																										
<div style="display: flex; justify-content: space-between;"> <div style="width: 20%;"> <p>System</p> <p>Radio Interface</p> </div> <div style="width: 80%;"> <h4>Radio Settings</h4> <table border="0"> <tr><td>Operational Status</td><td>Operational</td></tr> <tr><td>Radio Administrative State</td><td>Enabled <input type="button" value="v"/></td></tr> <tr><td>Radio Interface Type</td><td>3.5</td></tr> <tr><td>RF Frequency (kHz)</td><td><input type="text" value="3680000"/></td></tr> <tr><td>Channel Bandwidth (MHz)</td><td><input type="button" value="10MHz"/></td></tr> <tr><td>Max Transmit Power (dBm)</td><td><input type="text" value="0"/></td></tr> <tr><td>Frame Duration (ms)</td><td>5ms <input type="button" value="v"/></td></tr> <tr><td>TDD DL/UL Ratio</td><td>50:50 <input type="button" value="v"/></td></tr> <tr><td>Preamble Index</td><td><input type="text" value="0"/></td></tr> </table> </div> </div>		Operational Status	Operational	Radio Administrative State	Enabled <input type="button" value="v"/>	Radio Interface Type	3.5	RF Frequency (kHz)	<input type="text" value="3680000"/>	Channel Bandwidth (MHz)	<input type="button" value="10MHz"/>	Max Transmit Power (dBm)	<input type="text" value="0"/>	Frame Duration (ms)	5ms <input type="button" value="v"/>	TDD DL/UL Ratio	50:50 <input type="button" value="v"/>	Preamble Index	<input type="text" value="0"/>	<h4>Rate Adaptation</h4> <table border="0"> <tr><td>Min DL MCS</td><td><input type="button" value="QPSK 3/4"/></td></tr> <tr><td>Max DL MCS</td><td><input type="button" value="256QAM 6/8"/></td></tr> <tr><td>Min UL MCS</td><td><input type="button" value="QPSK 3/4"/></td></tr> <tr><td>Max UL MCS</td><td><input type="button" value="256QAM 6/8"/></td></tr> </table>						Min DL MCS	<input type="button" value="QPSK 3/4"/>	Max DL MCS	<input type="button" value="256QAM 6/8"/>	Min UL MCS	<input type="button" value="QPSK 3/4"/>	Max UL MCS	<input type="button" value="256QAM 6/8"/>
Operational Status	Operational																																
Radio Administrative State	Enabled <input type="button" value="v"/>																																
Radio Interface Type	3.5																																
RF Frequency (kHz)	<input type="text" value="3680000"/>																																
Channel Bandwidth (MHz)	<input type="button" value="10MHz"/>																																
Max Transmit Power (dBm)	<input type="text" value="0"/>																																
Frame Duration (ms)	5ms <input type="button" value="v"/>																																
TDD DL/UL Ratio	50:50 <input type="button" value="v"/>																																
Preamble Index	<input type="text" value="0"/>																																
Min DL MCS	<input type="button" value="QPSK 3/4"/>																																
Max DL MCS	<input type="button" value="256QAM 6/8"/>																																
Min UL MCS	<input type="button" value="QPSK 3/4"/>																																
Max UL MCS	<input type="button" value="256QAM 6/8"/>																																

8.3.4.1 Radio Settings Area

- **Operational Status:** Operational/Down/Fault (Read only)
- **Radio Administrative State:** Enabled/Disabled
- **Radio Interface Type:** 3.5 (Read Only)
- **RF Frequency (kHz):** Set as appropriate
- **Channel Bandwidth (MHz):** 5, 10, 20 MHz (Read Only)
- **Max. Transmit Power (dBm):**
 - Enter between -15 dBm to +27 dBm for the 3.65 – 3.7 GHz bands, non-exclusive licensed band.
 - Enter between -15 dBm to +23 dBm for the 5.725 – 5.825 GHz.
 - Enter higher values for large Hub/RBM distances and lower values for smaller distances so that receiver does not saturate.
- **Frame Duration (ms):** 5 ms or 6 ms
- **TDD DL/UL Ratio:** Set uplink to downlink bandwidth ratio to 50:50 or 70:30, as desired
- **Preamble Index:** Enter preamble index value 0 to 31 (factory default is 0); refer to Chapter 12, *“Preambles, Flows, and Network Provisioning”* for more information on the use of preamble indices

8.3.4.2 Rate Adaptation Area

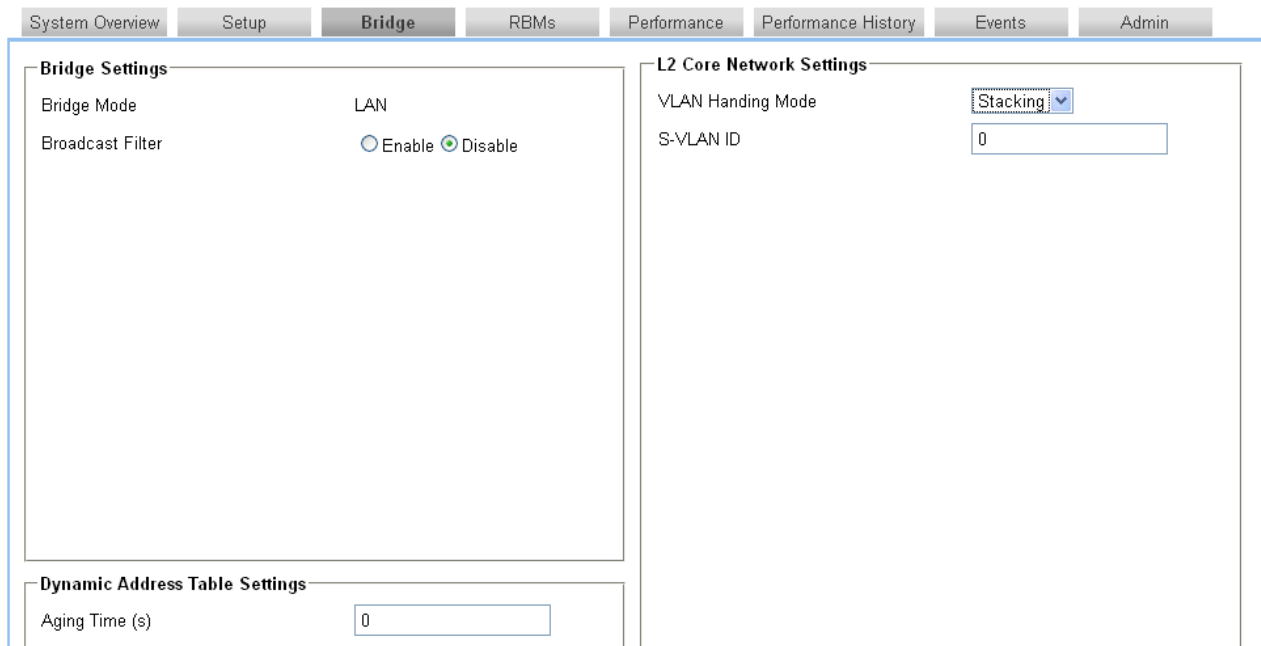
- **Min DL MCS:** Minimum Downlink Modulation and Coding Scheme (MCS)
- **Max DL MCS:** Maximum Downlink Modulation and Coding Scheme (MCS)
- **Min UL MCS:** Minimum Uplink Modulation and Coding Scheme (MCS)
- **Max UL MCS:** Maximum Uplink Modulation and Coding Scheme (MCS)

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

8.3.5 Bridge Page

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



The screenshot shows the configuration page for the Bridge module. At the top, there is a navigation bar with tabs: System Overview, Setup, Bridge (selected), RBMs, Performance, Performance History, Events, and Admin. Below the navigation bar, the page is divided into three main sections:

- Bridge Settings:** Contains two settings: Bridge Mode (set to LAN) and Broadcast Filter (radio buttons for Enable and Disable, with Disable selected).
- L2 Core Network Settings:** Contains two settings: VLAN Handling Mode (dropdown menu set to Stacking) and S-VLAN ID (text input field with 0).
- Dynamic Address Table Settings:** Contains one setting: Aging Time (s) (text input field with 0).

8.3.5.1 Bridge Settings Area

- **Bridge Mode:** AN (Read only)
- **Broadcast Filter:** Enable/Disable

8.3.5.2 Dynamic Address Table Settings Area

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 (s):** Set as desired. Allowable entries: 0 to 65535 seconds (default is 0).

8.3.5.3 L2 Core Network Settings Area

- **VLAN Handling Mode:** None/Stacking (if set to Stacking, the S-VLAN ID option appears)
- **S-VLAN ID:** Enter S-VLAN id

8.3.6 RBMs - General RBM Page

The X-1200 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-1200 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-1200 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.

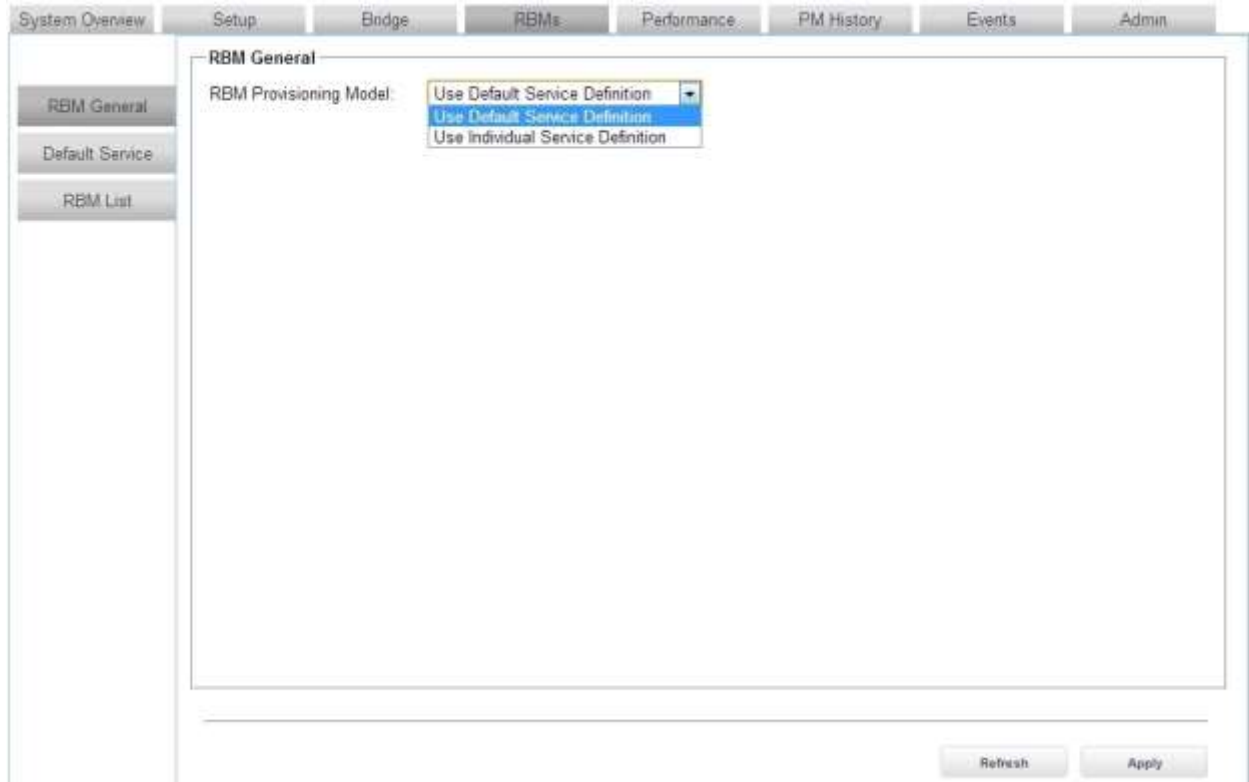
The RBM and Hub use a service flow with an appropriate QoS class (plus other parameters, such as priority and classifiers) to ensure that application data receives the QoS treatment appropriate to the user application. The QoS is supported by allocating each service flow a specific QoS class, of which there are two in the X-1200 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.

When the X-1200 system starts, it automatically finds all the RBMs connected to it. Through this page you can make the HM either:

- apply the default service flow definition to all RBMs, as set through the **RBMs > Default Service** 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** 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.



8.3.7 RBMs - Default Service Page

On the **Default Service Flow Provisioning Profile** page, you can add and remove service flows for the specified RBM. You identify the specified RBM by its MAC address, just below the **Default Service Flow Provision Profile:** title. Click the **Apply** button for the changes to take effect. Use the **Cancel** button to cancel any changes.

The screenshot displays the 'Default Service Flow Provisioning Profile' configuration page. The top navigation bar includes 'System Overview', 'Setup', 'Bridge', 'RBMs', 'Performance', 'PM History', 'Events', and 'Admin'. The left sidebar has 'RBM General', 'Default Service', and 'RBM List'. The main content area is titled 'Default Service Flow Provisioning Profile:' and shows a MAC address '00:00:00:00:00:00' with a blue arrow pointing to it from the label 'RBM Address'. Below this is the 'RBM Details' section with a 'Description' field containing 'RBM for default service flow definiti' and an empty 'VLAN' field. The 'Service Flows' section has 'Add' and 'Remove' buttons and a table with the following data:

ID	Priority	Direction	QoS Type	Queue Classification
1	1	Downlink	Best Effort	802.1p
2	1	Uplink	Best Effort	802.1p

At the bottom right, there are 'Cancel' and 'Apply' buttons.

8.3.7.1 RBM Details Area

- **Description:** Describes the RBM setting chosen from the **RBMS > RBM General** page.
- **VLAN:** This box is where you can specify the Virtual Local Area Network (VLAN) for the RBM, if applicable.

8.3.7.2 Service Flows Area

The available service flows for the RBM appear in this list detailing the ID number, Priority, Direction, Qos Type and the Queue Classification.

Up to four (4) service flows can be configured per RBM in the downlink and uplink direction, respectively; and up to eight (8) if set to bi-directional.

1. Add a Service Flow by clicking on the **Add** button. A **Service Flow:** page appears where you can assign settings to that RBMs service flow (see section 8.3.7.3, "Service Flow: Page").
2. To delete a Service Flow, click on the check box beside the desired service flow and click on the **Remove** button. The service flow disappears from the list.
3. Selecting the **ID** number of the Service Flow allows you to edit that Service Flow. The **Service Flow:** page for that ID number appears (see section 8.3.7.3, "Service Flow: Page").

8.3.7.3 Service Flow: Page

This is the page where you add and/or edit the service flow of the selected RBM. You can identify which service flow you are observing by the **ID** number just below the **Service Flow:** page title. Also in the upper right hand corner, there are up and down arrows which allow you to scroll through the currently active service flows. You can also return to the previous screen by selecting the **Return to RBM** hyperlink or select the **Done** button in the bottom right hand corner.

8.3.7.3.1 Service Flow Details Area

The Service Flow Details area allows you to add and edit a Service Flow for the selected RBM. The service flow settings are:

- **ID:** Identification number for this service flow. Only the unassigned identification numbers are available from the list (0-7; 8 total)
- **Priority:** If more than one service flow is defined for an up or down link, set priority (0 is highest, 7 is lowest)
- **Direction:** Uplink/Downlink/ Bi-Directional
- **Queue Classification:** 802.1p/Advanced
- **QoS Type:** Best Effort/Unsolicited Grant Service
- **Min Reserved Rate:** ?? Kbps
- **Max Sustained Rate:** Set the maximum sustained throughput rate (value between 1 Kbps and 150000 Kbps).

8.3.7.3.2 Flow Classification Area

This area of the **Service Flow** page shows the currently defined flow classifications. The **Edit** button under the **Flow Classification** area opens the **Flow Classification** page.

▼ Flow Classification


[Edit](#) (dst-mac-addr: 00:00:00:00:00:00)

Flow Classification: Page

The Flow Classification page is where you can further define the scope of service flows. You can also return to the previous screen by selecting the **Return to Service Flow** hyperlink (upper right hand side of page) or select the **Done** button in the bottom right hand corner.

Classification parameters include:

- C-VLAN, along with C-VLAN Priority
- S-VLAN, along with S-VLAN Priority
- Ethertype:
 - Internet Protocol Version 4 (IPv4)
 - Internet Protocol, Version 6 (IPv6)
 - Address Resolution Protocol (ARP)
 - Reverse Address Resolution Protocol (RARP)
 - VLAN-tagged frame (IEEE 802.1Q)
 - Simple Network Management Protocol (SNMP)

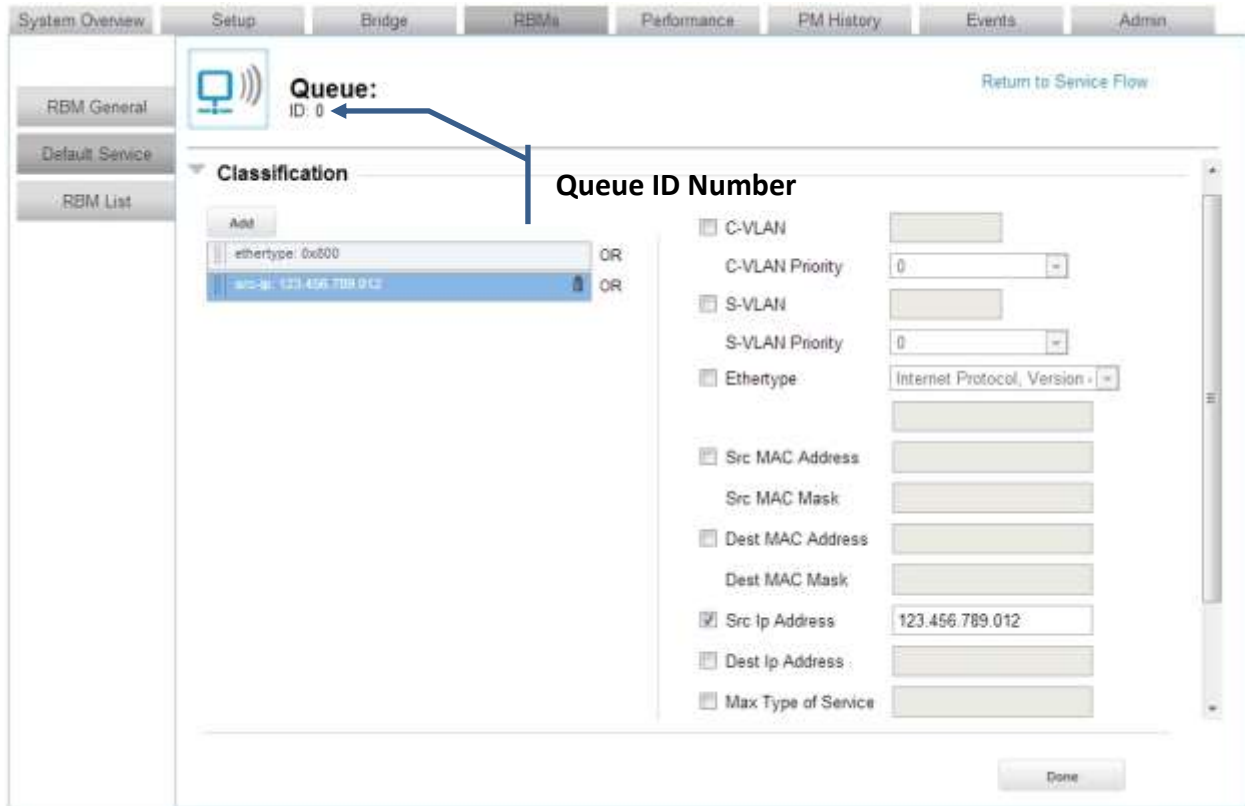
- Slow Protocol
 - MPLS (Multiprotocol Label Switching)
 - Jumbo Frames
 - Provider Bridging (IEEE 802.1ad)
 - LLDP (Link Layer Discovery Protocol)
 - MAC Security (IEEE 802.1AE)
 - Precision Time Protocol (IEEE 1588)
 - Q-in-Q
 - Other
 - Source (Src) MAC Address/Mask
 - Destination (Dest) MAC Address/Mask
 - Source (Src) IP Address
 - Destination (Dest) IP Address
 - Maximum (Max) Type of Service
 - Minimum (Min) Type of Service
 - Protocol
1. Modify an existing classification by clicking on it. The classification changes to blue showing that it is the selected classification. Set/change the parameters as appropriate. Each check box that is selected adds an additional requirement for transmission to occur for that classification, that is, Boolean AND logic is in effect on each classification in a service flow. Changes are detailed on both the left and right of the window.
 2. Add a new flow classification by clicking on the **Add** button. A new classification appears in blue. Set the parameters as appropriate. Up to eight classifications can be configured per service flow, with Boolean OR logic in effect on multiple classifications in a service flow.
 3. Change the order and priority of Boolean OR operations for multiple classifications by using drag and drop. This feature activates when you place your cursor over the left-hand side of the classification; the cursor changes to  which indicates that you can move this classification up or down in the list. The higher up the order the classification is, the higher its priority within Boolean OR operations.
 4. To delete a classification, select the classification and then click on the trash can icon on the same line.

8.3.7.3.3 Queues

The **Queues** area shows a queuing list of available service flows. You can further classify a service flow by assigning a queue to the selected service flow – the queuing is based on even more specified queue classifications. You can add or remove queue classifications to the specified service flow via the **Add** and **Remove** buttons.




You can identify which queue you are observing by the **ID** number just below the **Queue:** page title. You can also return to the previous screen by selecting the **Return to Service Flow** hyperlink (upper right hand side of page) or select the **Done** button in the bottom right hand corner.



1. While on the **Service Flow:** page, modify an existing Queue Classification by clicking on the ID number. The **Queue:** page appears where you can edit the currently set parameters. Set the parameters as appropriate. Each check box that is selected adds an additional requirement for transmission to occur for that queue classification, that is, Boolean AND logic is in effect on each queue classification in a service flow.

Queue classification parameters include:

- C-VLAN, along with C-VLAN Priority
- S-VLAN, along with S-VLAN Priority
- Ethertype:
 - Internet Protocol Version 4 (IPv4)
 - Internet Protocol, Version 6 (IPv6)
 - Address Resolution Protocol (ARP)
 - Reverse Address Resolution Protocol (RARP)
 - VLAN-tagged frame (IEEE 802.1Q)
 - Simple Network Management Protocol (SNMP)
 - Slow Protocol
 - MPLS (Multiprotocol Label Switching)

- Jumbo Frames
 - Provider Bridging (IEEE 802.1ad)
 - LLDP (Link Layer Discovery Protocol)
 - MAC Security (IEEE 802.1AE)
 - Precision Time Protocol (IEEE 1588)
 - Q-in-Q
 - Other
 - Source (Src) MAC Address/Mask
 - Destination (Dest) MAC Address/Mask
 - Source (Src) IP Address
 - Destination (Dest) IP Address
 - Maximum (Max) Type of Service
 - Minimum (Min) Type of Service
 - Protocol
2. Add a new queue classification by clicking on the **Add** button on the **Service Flow** page. The **Queue** page opens and a new classification appears in blue. Set the parameters as appropriate. Up to eight classifications can be configured per service flow, with Boolean OR logic in effect on multiple classifications in a service flow.
 3. Change the order and priority of Boolean OR operations for multiple classifications by using drag and drop. This feature activates when you place your cursor over the left-hand side of the queue classification; the cursor changes to  which indicates that you can move this queue classification up or down in the list. The higher up the order the queue classification is, the higher its priority within Boolean OR operations.
 4. To delete a queue classification from within a queue: while on the **Queue** page, click on the queue classification and select the trash can on the same line.

OR to remove a queue from the service flow: while on the **Service Flow** page: select the check mark beside the queue classification and then click on the **Remove** button.

8.3.8 RBMs - RBM List Page

On this 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.

System Overview Setup Bridge RBMs Performance PM History Events Admin

RBM General
Default Service
RBM List

Remote Backhaul Module Provisioning Profiles:

Below is a list of the service provisioning profiles for each RBM.
Note: These profiles will only be used if the Service Provision model is set to Individual Service Definition.

RBM Profile List

Add Remove

	MAC Address	Description	VLANs
<input type="checkbox"/>	12.34.56.78.90.00	test	
<input type="checkbox"/>	12.34.56.78.99.0a	test 2	
<input type="checkbox"/>	12.34.56.78.99.0b	test 3	

1. Sort the **RBM Profile List** by ascending or descending MAC address, by clicking on the column header.
2. To add an RBM: Click the **Add** button; the **Remote Backhaul Module:** page appears. Enter the RBMs MAC address, and if desired, a description for that RBM (i.e., location) and the VLAN, if applicable. If desired, you can add a service flow definition to this RBM by going to the **Service Flows** area (Refer to section 8.3.7.3, “*Service Flow: Page*” for details). Click **Apply** to add this RBM or **Cancel** to abandon.

System Overview Setup Bridge RBMs Performance PM History Events Admin

RBM General
Default Service
RBM List

Remote Backhaul Module: NEW RBM 2 of 2
[Return to RBM List](#)

RBM Details

MAC Address:

Description:

VLAN:

Service Flows

Add Remove

ID	Priority	Direction	QoS Type	Queue Classification
----	----------	-----------	----------	----------------------

Cancel Apply

- To delete an RBM: In the **Remote Backhaul Module Provisioning Profiles > RBM Profile List** area, activate the check box(es) beside the desired RBM(s) and click on the **Remove** button. The RBM(s) disappear from the list.
- To edit an RBM: In the **Remote Backhaul Module Provisioning Profiles > RBM Profile List** area, select the **MAC Address** of the desired RBM. The **Remote Backhaul Module: [ID number]** page appears. Change the desired features, select **Apply** to save your changes or **Cancel** to abandon.

- To edit that RBM's service flow definition: In the **Service Flows** area; click on the service flow **ID** number. The page that appears is the same one as for the **RBMs > Default Service Flows** area, except that now it applies to this specific RBM only. Refer to section 8.3.7.3, "Service Flow: Page" for details.

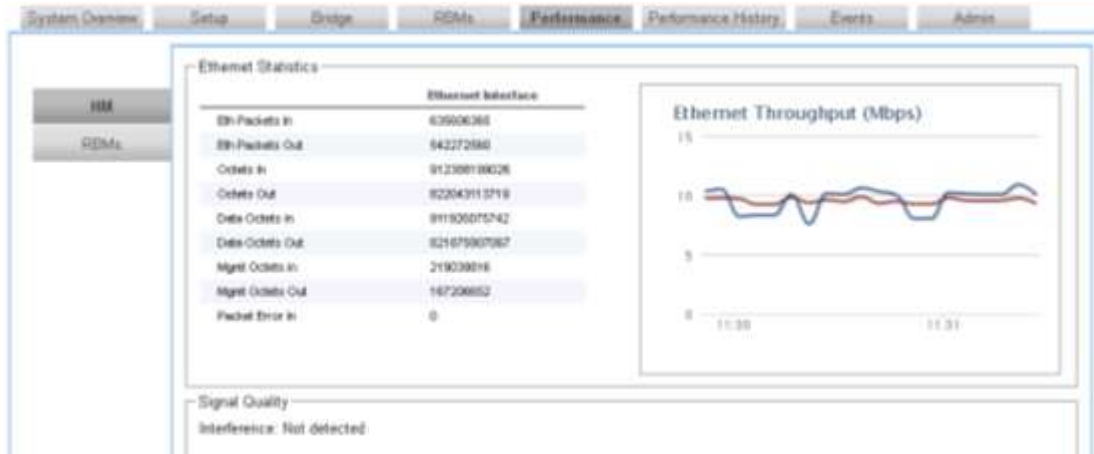
You can also sort the service flows by clicking on the **ID** area at the top of the column.

- In the upper right hand corner of this page, use the **Return to RBM List** hyperlink to return to the **RBM List** page or use the up and down arrows to scroll through the available RBMs.

8.3.9 Performance - HM Page

This read-only page for HM 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.



8.3.10 Performance - RBMs Page

This read-only 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.

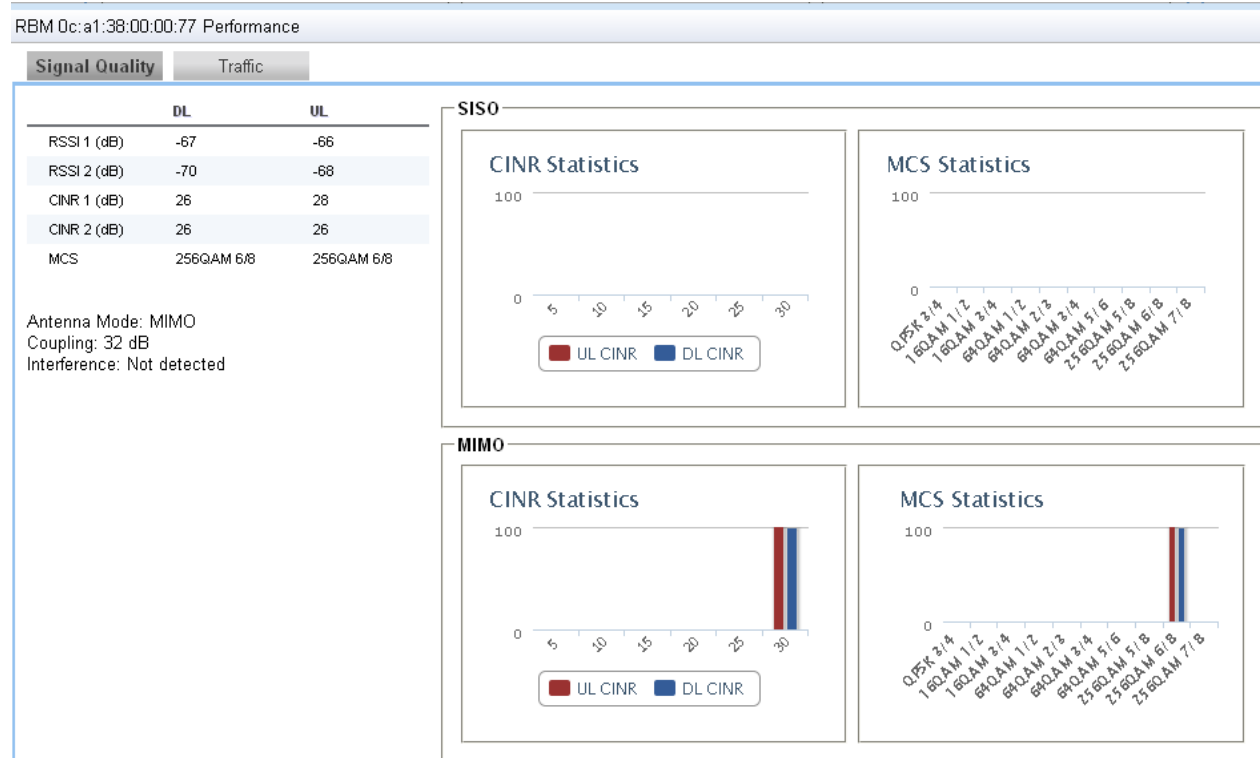
The coupling is a system measurement that indicates the probability of achieving a MIMO link for the current channel conditions. The system automatically chooses to use SISO mode whenever this value falls below 5dB.

The interference field provides a reading of the current external interference levels. External interference is measured in the gaps between the transmission and reception portions of the TDD frame and is generally caused by other systems present in the same or adjacent channels and which do not have the same transmission model or air frame structure as the X-1200 system.

Note: Screen refresh interval is every 5 seconds.



Click on an RBM on the list at the bottom. This opens a new page which allows you to view the statistics on signal quality and throughput (per service flow) performance for that RBM. To view signal quality, select the **Signal Quality** tab. To view the throughput performance, select the **Traffic** tab.





8.3.11 PM History Page

This read-only page is available on the HM only and displays aggregated performance history statistics for how the HM and its associated RBMs have been performing for the past 24 hours.

The HM stores a maximum of 96 performance history files over 24 hours before overwriting—one file for every 15 minutes of performance data. Each performance history file contains all the performance data for every active, linked RBM during the associated 15 minute period.



A list at the bottom of this page shows the available RBMs. Click on an RBM to view the performance history for that RBM. Clicking in turn through the tabs on the RBM performance history page displays data and statistics for **Traffic** (service flow throughput), **CINR and RSSI**, **CINR and MCS Statistics**, and **Coupling and Interference**.



Use the **Close** button to exit this page.

To zoom in on part of a graph, hold the **Left Mouse** button down and move the cursor to enclose the desired part of the performance history data. To return to the main graph, click on the **Reset Zoom** button.



8.3.12 Events - Alarms Page

This read-only page lists current alarms and events along with their details. For a list of alarms and events see Chapter 9, *Alarms and Events (Fault Management)*. Reorder the alarms and events as desired by clicking on any of the column headers.

Id	Alarm Id	Module Id	Alarm Time	Component	Severity	Type	Probable Cause	Description
No Data								

8.3.13 Events - History Page

This read-only page lists a chronological history of alarms and events along with their details. For a list of alarms and events see Chapter 9, *Alarms and Events (Fault Management)*. Reorder the alarms and events as desired by clicking on any of the column headers.

The screenshot shows the 'Events' tab in the X-1200 management interface. It features a navigation bar at the top with tabs for System Overview, Setup, Bridge, RBMs, Performance, Performance History, Events, and Admin. On the left, there are buttons for Alarms and History. The main area displays a table titled 'History' with the following data:

ID	Event Id	Module Id	Event Time	Component	Category	Severity	Type	Probable Cause	Description
16	4003	0c:af:38:00:00:05	2013-01-08 19:21:29Z	RBM OC:A1:38:00	Clear	Critical	Communications	Loss of Signal	RBM Link Up
17	7011	0c:af:38:00:00:05	2013-01-10 14:12:58Z	GPS	Message	Info	Equipment	Operating Mode	GPS state change to HCLDOVER
18	7001	0c:af:38:00:00:05	2013-01-10 14:13:03Z	SYNC	Set	Major	Equipment	Loss of Signal	System lost synchronization with timing source
19	7001	0c:af:38:00:00:05	2013-01-10 14:14:28Z	SYNC	Clear	Major	Equipment	Loss of Signal	CLEAR: System lost synchronization with timing source
20	7003	0c:af:38:00:00:05	2013-01-10 14:14:28Z	SYNC	Message	Info	Equipment	Operating Mode	System synchronized with timing source
21	7011	0c:af:38:00:00:05	2013-01-10 14:14:28Z	GPS	Message	Info	Equipment	Operating Mode	GPS state change to SYNC
22	5005	0c:af:38:00:00:05	2013-01-14 16:41:04Z	radio	Message	Info	Operational Status	Operating Mode	Radio reset due to configuration change.
23	5001	0c:af:38:00:00:05	2013-01-14 16:41:19Z	radio	Message	Info	Operational Status	Operating Mode	The radio has been successfully initialized.

At the bottom of the table, there is a 'Clear Table' button on the left, a message 'The Event History table only displays last 100 events' in the center, and a 'Refresh' button on the right.

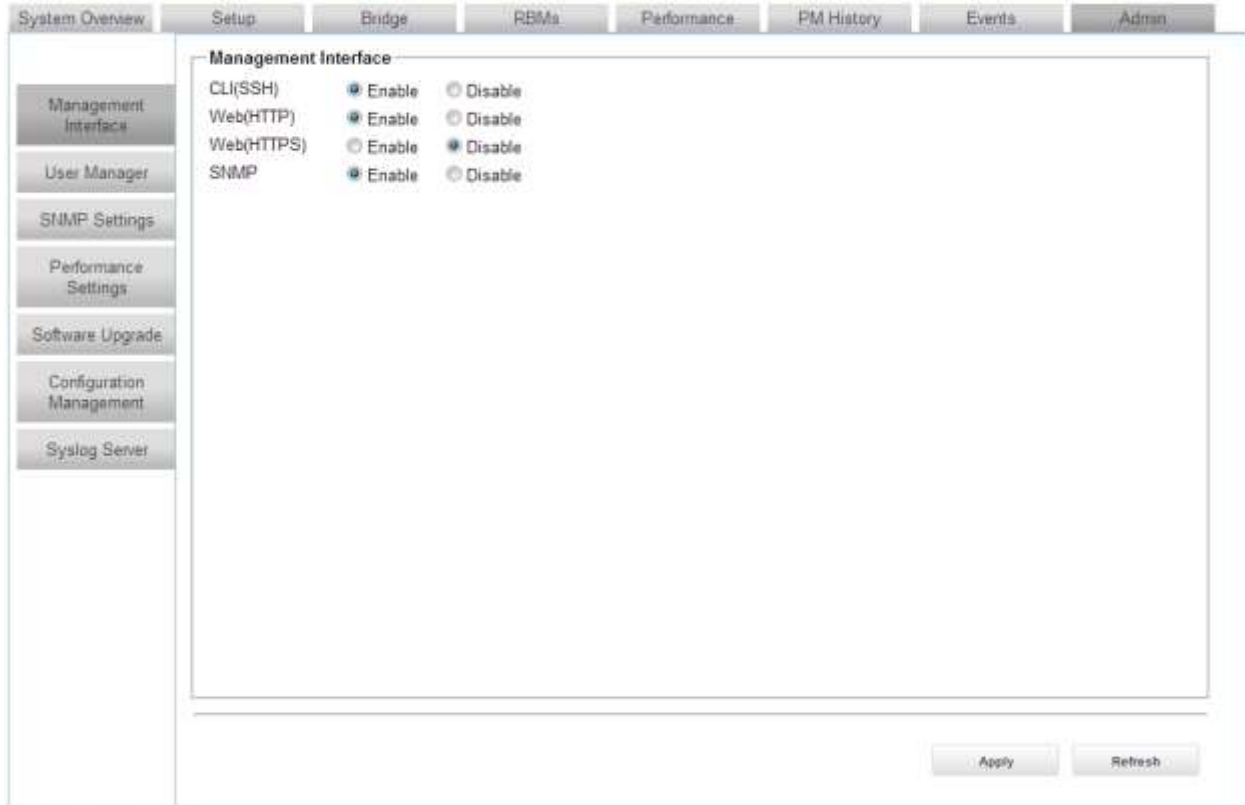
Note: Clicking **Clear Table** completely clears the current alarms and events history from the X-1200 event logging infrastructure. The only way to retrieve this history afterward is from Syslog (if provisioned).

Use the **Refresh** button to update the information on the screen.

8.3.14 Admin - Management Interface Page

On this page the administrator can enable or disable the types of management interfaces to use (CLI (SSH), Web (HTTP), Web (HTTPS), SNMP) using the option buttons. One, two or all three can be selected.

Note: If you disable the Web option, the X-1200 WebUI becomes unusable. You will have to enable it again using either the X-1200 CLI or SNMP. It is not possible, however, to lock yourself out of all three options; at least one option is always available.



8.3.15 Admin - User Manager Page

On this page, the administrator can add and delete users, set passwords, and set access privileges (read-only versus read/write) to manage user access to the Hub.

Note:

- User names must start with a letter and be composed of alphanumeric characters only.
- Passwords are case sensitive. It must be composed of alphanumeric characters, special characters, and must contain at least one letter and one number.
- At least one user with read/write privileges needs to exist in the X-1200 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 required, see section 11.2.1, “*Add Users using X-1200 WebUI*” for more information on resetting a password). If you have lost all read/write login credentials, contact your supplier.

1. To add a user, select the **Add** button, the **Add User** dialog window appears.

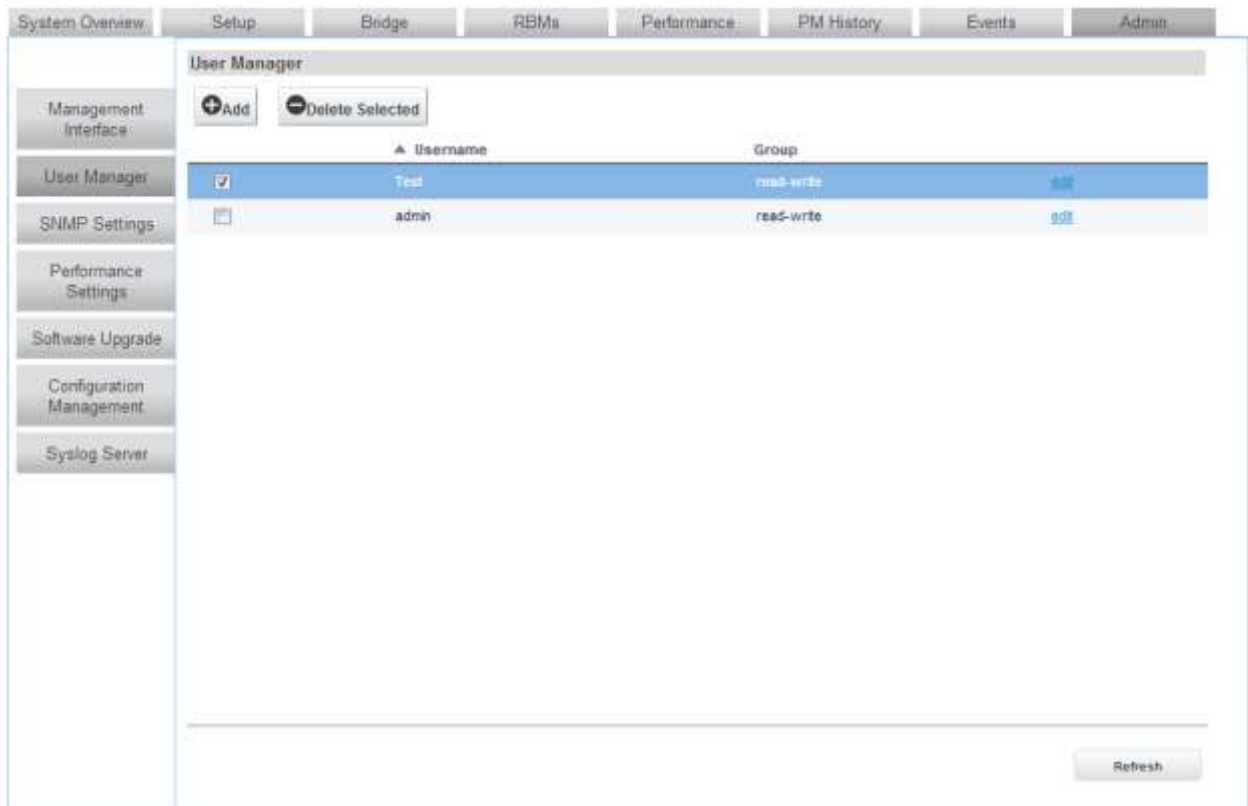


- Input a name for the user in the **Username** field. Select an access group (read-only, read-write) from the **Group** menu. Type a password for the user in the **Password** area and repeat the password again in the **Confirm Password** area. Select **Apply** to add the user or **Cancel** to abort this action.
- Change the user settings by selecting **edit** on the same line as the user that you want to modify. An **Edit User** dialog appears. You can change the access group and reset the password in this dialog.



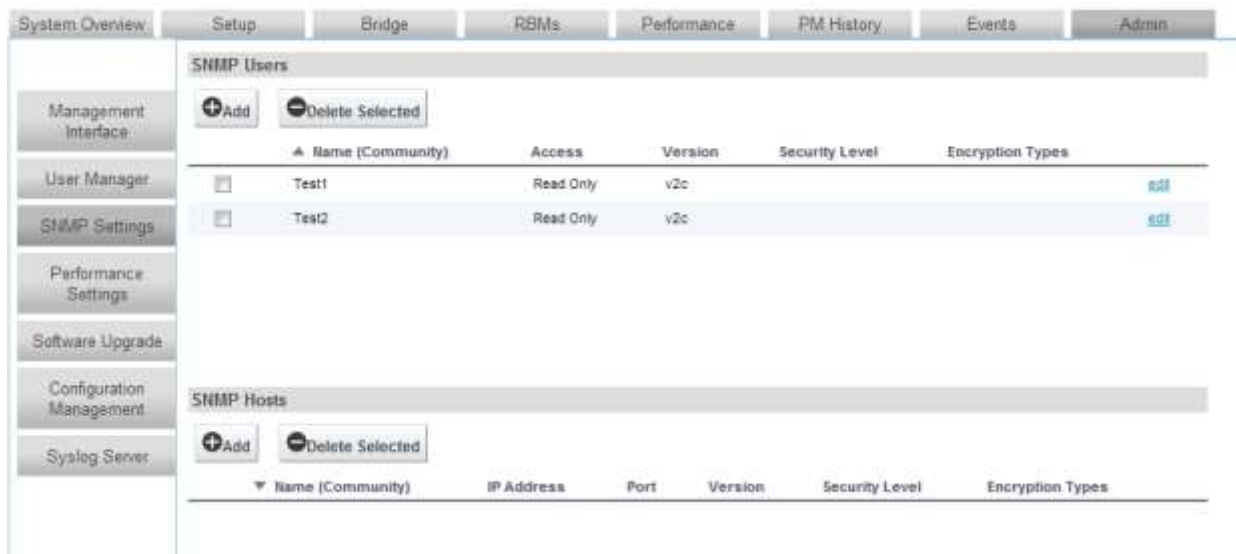
To change the user name, delete this user and re-input under a new name.

- To delete a user, select the check box beside the desired user, and then select the **Delete Selected** button. The user disappears from the list.
- To apply your changes, select the **Apply** button or use the **Cancel** button to abort these changes. Use the **Refresh** button to update the information on the screen.



8.3.16 Admin - SNMP Settings Page

On this page the administrator can add, delete, or edit SNMPv2c or SNMPv3 users and hosts.



To add or remove an SNMP user:

1. Access the **Admin>SNMP Settings; SNMP Users** area.
2. To add an SNMP user: select the **Add** button. An **Add SNMP User** dialog appears. Set the name of the user in the **Name** field. You can designate the access of the user by selecting either the **Read Only** or **Read Write** option buttons.

Add Snmp User

Name

Access Read Only Read Write

Version

SNMPv3 Security

Security Level

Auth Encryption

Auth Password

Priv Encryption

Priv Password

Version refers to the security protocol level for that user: **v2c** or a higher level security protocol of **v3**. With the **SNMPv3 Security** area, you can choose higher levels of security depending on the needs of your user and network.

- **Security Level** – sets the level of security: **None** (no options available), **Authentication**, **Authentication Privacy**
- **Auth Encryption** – sets the type of authentication encryption protocol: **md5** or **sha**

- **Auth Password** – sets the authentication password
 - **Priv Encryption** – sets the privacy encryption: **aes128** or **des56**; available only when **Authentication Privacy** option selected.
 - **Priv Password** - sets the privacy encryption password; available only when **Authentication Privacy** option selected.
3. If you need to edit an existing user, select the **edit** option on the right hand side of the desired user row. You cannot change the name field. If you do need to change the user name, delete that user and repeat the above steps with a new name.
 4. Select the **Apply** button to apply your changes or the **Cancel** button to abandon these changes.
 5. To remove an SNMP user: select the check box beside the user you want to delete. Select the **Delete Selected** button. The user disappears from the list.

To add or remove an SNMP host:

1. Access the **Admin>SNMP Settings; SNMP Hosts** area.
2. To add an SNMP host: select the **Add** button. An **Add SNMP Host** dialog appears. You need to know the **Name**, **IP Address** and **Port** for your SNMP host.

The screenshot shows a dialog box titled "Add Snmp Host". It contains the following fields and options:

- Name:** public
- IP Address:** 192.168.1.100
- Port:** 162
- Version:** v2
- SNMPv3 Security:**
 - Security Level:** None
 - Auth Encryption:** md5
 - Auth Password:** (empty field)
 - Priv Encryption:** aes128
 - Priv Password:** (empty field)

At the bottom of the dialog are two buttons: "Apply" and "Cancel".

Version refers to the security protocol level for that host: **v1**, **v2** or the higher level security protocol of **v3**. Under the **SNMPv3 Security** area, you can choose higher levels of security depending on the needs of your host when you select the **v3** option.

- **Security Level** – sets the level of security: **None** (no options available), **Authentication**, **Authentication Privacy**
- **Auth Encryption** – sets the type of authentication encryption protocol: **md5** or **sha**
- **Auth Password** – sets the authentication password
- **Priv Encryption** – sets the privacy encryption: **aes128** or **des56**; available only when **Authentication Privacy** option selected under **Security Level**.
- **Priv Password** - sets the privacy encryption password; available only when **Authentication Privacy** option selected under **Security Level**.

3. If you need to edit an existing SNMP host, select the **edit** option on the right hand side of the desired Host row. You cannot change the name field. If you do need to change the Host name, delete that host and repeat the above steps with a new name.
4. Select the **Apply** button to apply your changes or the **Cancel** button to abandon these changes.
5. To remove an SNMP host: select the check box beside the host you want to delete. Select the **Delete Selected** button. The host disappears from the list.

8.3.17 Admin - Performance Settings Page (HM Only)

The administrator uses this page to set the operational status for performance file uploads to an FTP server.

In the dialog box that appears, use the **Enabled** or **Disabled** option buttons to set the performance file upload configuration (default is **Disabled**). When set to **Enabled**, the X-1200 system automatically uploads the performance files collected by its Performance File Manager to the configured FTP server.

The screenshot shows the 'Performance File Auto Upload Configuration' dialog box. The 'Status' is set to 'Enabled'. The 'FTP Server' is '192.168.5.210', 'Username' is 'Bling', 'Password' is masked with asterisks, and 'Target Directory' is 'pm_unprocessed'. The 'Apply' and 'Refresh' buttons are visible at the bottom right.

Field	Value
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
FTP Server	192.168.5.210
Username	Bling
Password	*****
Target Directory	pm_unprocessed

As required, input the IP address of the desired **FTP Server**; including the **Username**, **Password** and **Target Directory** for the file on the FTP server (optional; only required if the destination directory is not the root FTP directory on the server).

8.3.18 Admin - Software Upgrade Page

On this 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).

The screenshot displays the 'Software Upgrade' configuration page. The interface includes a navigation menu on the left with options like 'Management Interface', 'User Manager', 'SNMP Settings', 'Performance Settings', 'Software Upgrade', 'Configuration Management', and 'Syslog Server'. The main content area shows the following fields and controls:

- Active Software Version:** 1.1.11_2
- Standby Software Version:** 1.1.10_2
- Upgrade From:** A dropdown menu currently showing 'FTP Server'.
- IP Address:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- File:** An empty text input field.

At the bottom right of the page, there are two buttons: 'Upgrade' and 'Reboot/Switch'.

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. If you have a file on your hard disk, select **Upload File** and browse for the file.
2. Click on the **Upgrade** button at the bottom right hand corner of the page. A progress bar appears at the bottom of the page.
3. A banner at the top of the page indicates if the software download succeeds.
4. The **Standby Software Version** field then shows the new software load image version.
5. To make the standby software load image the active image on the module, click on the **Reboot/Switch** button at the bottom of the page. A **Reboot/Switch** window appears. Select the **Yes** button at the prompt. The system restarts using the new software image. If the banner at the top indicates that this was successful, you have finished this software upgrade procedure. Select the **No** button, if you want to abort this update.

The 'Reboot/Switch' dialog box is a small window with a title bar. It contains the following text and controls:

- Title:** Reboot/Switch
- Text:** Are you sure you want to switch image?
- Buttons:** Yes and No

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



Note: You can only upgrade the X-1200 system software from one active browser session. This means you cannot open another browser session and start another upgrade process in parallel with the first. If you try this, you get a warning message and the system does not let you continue. Further, you must not close the browser once you start the upgrade. If you do, or if your computer crashes, you must reset the X-1200 system that was being upgraded and start the upgrade process over.

8.3.19 Admin - Configuration Management Page

On this 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.



1. To save a copy of the current configuration settings, select the **Save** button. A **Save** dialog box appears where you can save the file under a desired name (*.TAR format).
2. To restore a saved configuration file, use the **Choose File** button to locate and select your desired file (*.TAR). Select the **Restore** button to load this file. The X-1200 displays an error if the format is incorrect or a success message saying the configuration has been uploaded and applied.

8.3.20 Admin - Syslog Server Page

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



To Add a New Syslog Server:

1. Click on the **Add** button to add a new Syslog server IP address to the display list. In the **Add Server** dialog box that appears, input the **Server IP** address and use the option buttons to toggle its status: **Enable** or **Disable**. Select the **Ok** button to add the server or select the **Cancel** button to abort this action. You can change the server's status later by clicking on **edit** at the right of the list and using the option buttons again.

To Delete a Syslog Server:

1. Delete a server by choosing the check box next to it and then selecting the **Delete Selected** button. The selected syslog server disappears from the list.

8.4 Configuring RBMs

The X-1200 WebUI interface for configuring RBMs is similar to that for Hubs. *This section focusses on the differences only.* Moreover, sections that are read-only are not discussed; some of these omit data not applicable to RBMs and add other data not shown on the X-1200 WebUI pages for Hubs.

Note: For all RBM X-1200 WebUI configuration items not discussed here; see the corresponding HM item in section 8.3, “*Configuring Hub Modules*” for details.

- Logging In to X-1200 WebUI for RBMs — See section 8.4.1, “*Logging In*”
- System Overview — See section 8.4.2, “*System Overview Page*”
- Setup
 - System — See section 8.4.3, “*Setup - System Page*”
 - Radio Interface — See section 8.4.4, “*Setup - Radio Interface Page*”
- Performance — See section 8.4.5, “*Performance Page*”
- Events — See section 8.4.6, “*Events Page*”
 - Alarms — See section 8.3.12, “*Events - Alarms Page*”
 - History — See section 8.3.13, “*Events - History Page*”
- Admin — See section 8.4.7, “*Admin Page*”
 - Management Interface — See section 8.3.14, “*Admin - Management Interface Page*”
 - User Manager — See section 8.3.15, “*Admin - User Manager Page*”
 - SNMP Settings — See section 8.3.16, “*Admin - SNMP Settings Page*”
 - Software Upgrade — See section 8.3.18, “*Admin - Software Upgrade Page*”
 - Configuration Management — See section 8.3.19, “*Admin - Configuration Management Page*”
 - Syslog Server — See section 8.3.20, “*Admin - Syslog Server Page*”

8.4.1 Logging In

To log in and access the X-1200 WebUI interface for configuring RBMs:

1. Launch your web browser and set it to allow pop ups for your specific web browser (for instance Firefox, Chrome, Internet Explorer, etc.). Some screen functions in the X-1200 WebUI require pop ups.
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 locally to the RBM (that is, not over a network), use your browser to connect to the local Craft IP address of the unit: **http://169.254.1.1**.
4. 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—an operator assigned, static or Dynamic Host Configuration Protocol (DHCP) IP address used for remote management of the units. Note, however, that the management IP address of the RBM is only accessible from behind the HM. Refer to Chapter 6, “*Element and Network Management*” for more information.
5. Log on to the system. The default username and password are **admin**.

Note: To successfully log in and access the X-1200 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 8.3.1, “Logging In”.

8.4.2 System Overview Page

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

The screenshot displays the BLiNQ Networks System Overview page for an RBM. The page is titled "System Overview" and includes a navigation menu with options: Setup, Bridge, RBMs, Performance, Performance History, Events, and Admin. The main content area is divided into several sections:

- Information:**
 - System Name: HUB_NW
 - System Location: Roof NW
 - Uptime: 0 days, 0 hours, 12 minutes, 39 seconds
 - Active SW Version: 1.1.12_2
 - MAC Address: 0c:a1:38:00:00:92
 - Model: X-100
 - Radio Interface Type: 3.5
 - RF Frequency: 3680000
 - Bandwidth: 10MHz
 - Frame Duration: 5ms
 - TDD DL/UL Ratio: 50:50
 - Preamble Index: 0
- Performance:**
 - RBM(s) Throughput (Mbps):** A line graph showing throughput for three RBMs (green, red, blue) over time. The y-axis ranges from 0 to 5 Mbps. The x-axis shows time from 11:16 to 11:17. All three RBMs show a sharp increase in throughput starting around 11:16:30, peaking at approximately 4.5 Mbps, and then dropping back to 0 by 11:17:00.
 - Ethernet Throughput (Mbps):** A line graph showing Ethernet throughput over time. The y-axis ranges from 0 to 100 Mbps. The x-axis shows time from 11:16 to 11:17. The throughput starts at 0, rises sharply to about 60 Mbps at 11:16:30, and remains stable at that level until 11:17:00.
- RBM(s):** A table listing the status of three RBMs.

MAC Address	IP Address	TX throughput (Mbps)	RX throughput (Mbps)	Link Uptime
0c:a1:38:00:00:91	192.168.5.234	0.00	0.00	8m
0c:a1:38:00:00:79	192.168.5.231	0.00	0.00	8m
0c:a1:38:00:00:77	192.168.5.233	0.00	0.00	8m
- Alarms:** A table with columns: Id, Alarm Id, Module Id, Alarm Time, Component, Severity, Type, Probable Cause, and Description. The table is currently empty, displaying "No Data".

8.4.3 Setup - System Page

This page handles configuration of system parameters that govern basic RBM operation and is the same 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 8.3.3, “Setup - System Page” for the corresponding HM page.

8.4.4 Setup - Radio Interface Page

Under **Radio Settings** area, this page handles configuration of the radio operation of the RBM and is the same page as for Hub, except:



Preamble Series All

Pointing Mode (BSI) Enabled Disabled

- **Preamble Series:** Enter preamble index value 0 to 31; refer to Chapter 12, *Preambles, Flows, and Network Provisioning* for more information on use of preamble indices
- **Pointing Mode (BSI):** Select the Enabled or Disabled option.

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 RF signal from the HM. It is enabled and disabled through the X-1200 WebUI.

While in BSI mode, the RBM makes a buzzing tone 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 tone is heard—indicating the best signal from the 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 the **Pointing Mode (BSI)** option to **Enabled** so that when the RBM restarts next with no Ethernet cable attached, it automatically enters BSI mode. The installer can then find the optimum position for the RBM by moving it on its axis from 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. At this time, **Pointing Mode (BSI)** can be set to **Disabled**. This prevents the RBM from entering BSI mode again while up on its mount, for example, due to 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 8.3.4, “*Setup - Radio Interface Page*” for the corresponding HM page.

8.4.5 Performance Page

This read-only page for RBM performance contains graphs and statistics for the downlink/uplink Carrier to Interference-plus-Noise Ratio (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.

The coupling is a system measurement that indicates the probability of achieving a MIMO link for the current channel conditions. The system automatically chooses to use SISO mode whenever this value falls below 5dB.

Note: Graph update interval is every 5 seconds.



8.4.6 Events Page

The events for RBMs are the same as for the HM. Refer to sections 8.3.12, “Events - Alarms Page” and 8.3.13, “Events - History Page” for details.

8.4.7 Admin Page

The RBM administration pages are the same as the HM administration pages, with the exception of Performance Settings, which is HM only. Refer to sections 8.3.14, “Admin - Management Interface Page” through 8.3.20, “Admin - Syslog Server Page” for details.

9 Alarms and Events (Fault Management)

This chapter lists the alarms and events for the BLiNQ X-1200 system.

The X-1200 system issues an alarm notification when a fault condition occurs. You view alarms through the X-1200 WebUI **Events** page (See section 8.3.12, “*Events - Alarms Page*” for HMs and/or section 8.4.6., “*Events Page*” for RBMs). These alarms require operation and maintenance actions to restore functionality and/or to prevent a more serious situation from developing.

The X-1200 system issues an event notification when something of importance happens that does not trigger an alarm, but is considered significant enough to take note. You view these events through the X-1200 WebUI **Events** page (See section 8.3.13, “*Events - History Page*” for HMs and/or section 8.4.6, “*Events Page*” for RBMs).

Table 5, *List of Alarms* shows each alarm (whose name also represents the particular problem), the alarm ID, type, and explanation on the likely cause of the alarm and possible solution (as applicable).

Table 6, *List of Events* shows each event (whose name also represents the particular problem), the event ID, type, and explanation on the likely cause of the event.

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

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

Table 5 List of Alarms

ID	Name	Description/Comments	Type	Severity
2002	Management Address Lease Renew Failed	System cannot renew the Dynamic Host Configuration Protocol (DHCP) lease when unit is configured to use DHCP for the Management IP Address. It recovers when the lease is renewed.	Equip.	Minor
3004	Software Boot Failure	Switchover software versions after a failed boot attempt. Probably a storage capacity problem.	Equip.	Major
4001	Ethernet Port Down	System recovers when Ethernet link is reestablished.	Comms.	CRITICAL
4002	All RBM Links Down	Hub Module (HM) has lost all Remote Backhaul Module (RBM) connections. Upon HM reboot, alarm occurs only if no RBM has established connection within 20 s from the time the HM radio is operational.	Comms.	If any RBM is configured as <i>Emit alarm when down</i> : CRITICAL Otherwise: Major

ID	Name	Description/Comments	Type	Severity
4003	RBM Link Down	HM has lost connection to an RBM that is configured to <i>Emit alarm when down</i> . Upon HM restart, alarm occurs only if RBM has not established connection within 20 s from the time the HM radio is operational.	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. 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.	Equip.	CRITICAL
5007	RF Port Open	The system has detected an open Radio Frequency (RF) port. It recovers when the system detects the port is no longer open.	Equip.	CRITICAL
5009	Power Detector Fault	The system has detected a power fault. It recovers when the system detects the power fault is no longer present.	Equip.	Major
5010	Invalid RF Card Calibration Data	System recovers when it detects the port is no longer open.	Equip.	CRITICAL
5011	CBP threshold	Module is experiencing RF interference above the detected threshold (configurable from -90 to -31 dBm). System recovers when interference drops below the configured threshold. A minor alarm is generated when the percentage of contention frames exceeds 10%; a major alarm is generated when the percentage exceeds 50%.	QoS	Minor/Major
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	System recovers when the temperature falls below threshold.	Equip.	CRITICAL

ID	Name	Description/Comments	Type	Severity
7001	GPS Synchronization Lost	The Global Positioning System (GPS) receiver lost its synchronized status. Upon HM reset, this alarm is not raised until 60 s 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 unsynchronized state. System stops transmitting.	Equip.	CRITICAL
9001	Performance measurement forwarding failed	RBM cannot forward performance measurements to the HM. Indicates an issue with the RF link. System recovers when the RF link is restored.	Comms.	Minor
9004	Automatic PM file upload failed	Hub Module cannot upload PM files to the specified server. Indicates a server connectivity or access error. System recovers when connectivity/access to the PM server is restored.	Comms.	Minor

Table 6 List of Events

ID	Name	Description/Comments	Type	Severity
2001	Startup Configuration Changed	Changes to the system running configuration file have been saved to the startup configuration file.	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 file transfer, file validation, or file persistence error occurred.	Equip.	Major
3005	Switchover Failed	The system has failed to perform a software switchover (due to an unknown available software version or a configuration data migration error).	System	Major
4004	Unauthorized RBM	An RBM attempts to connect to an HM, but the RBM is not configured in the RBM table of the HM. Either add the RBM in question to the HM's RBM configuration table, or point the RBM to a different HM.	Security	Warning
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

ID	Name	Description/Comments	Type	Severity
5004	Radio Module Disabled	Radio Module is initialized and has received an administrative disable configuration.	Equip.	Information
5005	Radio Module Initializing	Radio Module intentionally reset.	Equip.	Information
6001	Cold Start	Unplanned restart.	Equip.	Information
6002	Warm Start	Planned restart.	Equip.	Information
7003	GPS Lock Acquired	GPS entered synchronized state.	Equip.	Information
7004	GPS State Change	The GPS state machine gained or lost GPS synchronization (specific state indicated by the comment text).	Equip.	Information
8001	Authentication Failed	Attempts to authenticate on one of the management interfaces of the equipment failed.	Security	Minor
9002	PM File Upload Complete	The system has completed a performance measurement (PM) file upload operation.	System	Information
9003	Performance File Manager Restart	The performance file manager application restarts during system operation. Used to correlate a missing PM file.	System	Warning

10 Using the X-1200 Command Line Interface

The BLiNQ X-1200 Command Line Interface (CLI) is a text-based interface to the BLiNQ X-1200 system.

10.1 Overview

The X-1200 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-1200 CLI over the network.

The commands in the X-1200 CLI let you display information and perform configuration tasks and make configuration changes to the X-1200 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-1200 CLI commands or command options, enter a single: QUESTION MARK (?) key.

The X-1200 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 the TAB key or SPACEBAR, 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-1200 CLI by identifying them with an EXCLAMATION MARK (!) at the start of a line. This tells the X-1200 system that the information is a comment and is to be ignored.

10.2 X-1200 CLI Command Line Prompts

Within the X-1200 CLI, the command line prompt identifies both the hostname and the command mode. The hostname is the name of your X-1200 system; the command mode indicates your location within the CLI command structure.

For example:

Hostname	Command Mode
localhost	(config) #

For some actions, the X-1200 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.

10.3 X-1200 CLI Keywords and Parameters

X-1200 CLI commands are made up of two primary elements:

- keywords and
- parameters.

10.3.1 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 you want to perform. 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.

For example:

```
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
```

10.3.2 Parameters

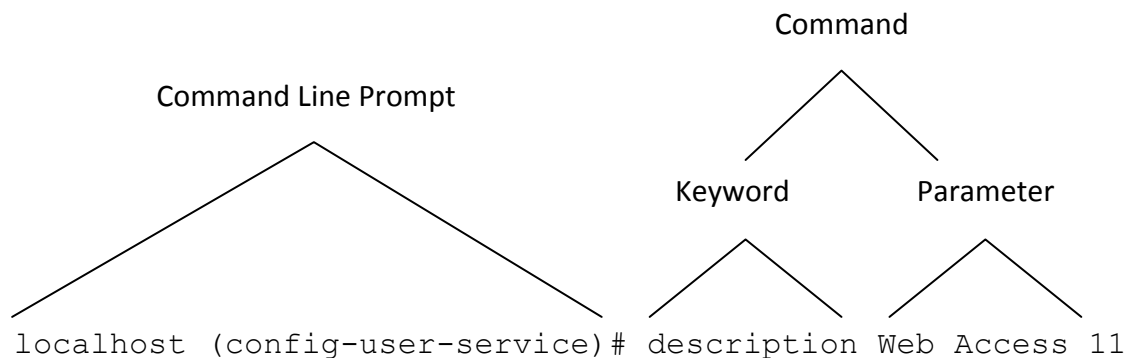
Parameters are often required elements of a command; however, for some commands, parameters are not required. A parameter is most often a value that you specify after the keyword. There are different types of parameters, such as strings, integers, or IP addresses. The X-1200 CLI indicates the type of parameter that you must enter. When you see a range of numbers or uppercase letters, it indicates that you must specify a value.

10.3.3 Keywords and Parameters Together

By combining keywords and parameters in the correct sequence, you can begin using the X-1200 CLI to configure and monitor your X-1200 system. For example, you could specify the Global CONFIG command **user service** to add a description of the user service to the X-1200 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 11”), 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>):
```



10.4 Identify Command Context

Command levels set a context for the X-1200 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-1200 system.

The X-1200 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
```

10.5 X-1200 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 (?) key) at the prompt, then press TAB or the SPACEBAR.

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

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

When an item is not enclosed by angle brackets (< >) or bracket ([]) symbols, the item is a required keyword.

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

Example 1:

```
localhost(config)# mgmt <TAB>
Possible completions:
  default-gateway  IP default gateway
  interfaces       Management interface control
  ip               Management IP address and netmask
  ip-config-mode   Management IP mode
  syslog           Syslog server settings
  traffic-tunneling Traffic tunneling enable/disable [HM only]
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      Historical event list
  history            Display CLI command history
  mgmt              Management interface settings
  pm                Performance measurements
  ptp               PTP settings
  radio             Radio interface settings
  running-config    Display current configuration
  startup-config    Display startup configuration
  system            System settings
localhost# show
```

10.6 Logging On to the X-1200 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-1200 CLI using a Secure Shell (SSH) connection (SSH is an application for opening a secure socket connection to an IP device). However, you must install SSH version 2.0 client software on your host computer (It is not recommended but you can use SSH version 1.0).

After initial log on, using the desired SSH client, and once CLI connectivity to the X-1200 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-1200 system through the X-1200 CLI.

To reach the Global CONFIG Level, the uppermost level of the CONFIG commands, enter the **config terminal** 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.

10.7 Privileged EXEC Commands

The Privileged EXEC level commands primarily enable you to review information on the system configuration, monitor features globally on an X-1200 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. At the terminal, the screen displays:

```
localhost# <TAB>
Possible completions:
  admin           Administrative settings and commands
  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   Historical event list
  exit            Exit the management session
  export-logs     Export debug logs to an FTP server for offline
                  analysis
  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
  license-key     Download a software license key and apply it to the
                  module.
  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
  ping           Debug network connectivity using ping
  pm              Performance measurements
  prompt1         Set operational mode prompt
  prompt2         Set configure mode prompt
  quit            Exit the management session
  radio           Radio interface settings
  screen-length   Configure screen length
  screen-width    Configure screen width
  send            Send message to terminal of one or all users
  shell           Debug shell.
  show            Show information about the system
  show-defaults   Show default values when showing the configuration
  source          File to source
  system          System commands
  terminal         Set terminal type
  timestamp       Enable/disable the display of timestamp
  who             Display currently logged on users
  write           Write configuration
```

10.8 Global CONFIG Commands

The Global CONFIG commands allow you to globally apply or modify configuration parameters for an X-1200 system. At the terminal, the screen displays:

```
localhost# config terminal
Entering configuration mode terminal
localhost(config)# <TAB>
Possible completions:
  admin           Administrative settings and commands
  alias           Create command alias.
  bridge          L2 bridge settings [HM only]
  ethernet        Ethernet port settings
  event-history   Historical event list
  mgmt            Management interface settings
  pm              Performance measurements
  ptp             PTP settings
  radio           Radio interface settings
  rbm-general-conf RBM provisioning settings[HM only]
  rbm-table       RBM configuration table[HM only]
  session         Global default CLI session parameters
  system          System settings
  user
  webui           Web UI specific configuration
  ---
  abort           Abort configuration session
  clear           Remove all configuration changes
  commit          Commit current set of changes
  compare         Compare configuration
  copy            Copy a list entry
  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-1200 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)

10.8.1 Radio CONFIG Mode

To access Radio CONFIG mode, input **radio** while in Global CONFIG level. At the terminal, the screen displays:

On the HM:

```
localhost(config)# radio <TAB>
Possible completions:
  rf      RF card statistics
localhost(config)# radio rf <TAB>
Possible completions:
  RF card identifier 0 range
localhost(config)# radio rf 0
localhost(config-rf-0)# <TAB>
Possible completions:
  antenna-method      Radio antenna method enabled/disabled
  dl-ul-ratio         TDD DL:UL ratio enabled/disabled
  frequency           Center frequency
  preamble-phase      Preamble phase index
  rate-adaptation     Rate Adaptation (RA) algorithm settings
  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)#
```

On the RBM:

```
localhost-RBM(config)# radio <TAB>
Possible completions:
  bsi-admin-state    Pointing mode enable/disable
  rf                 RF card statistics
localhost-RBM(config)# radio rf <TAB>
Possible completions:
  RF card identifier 0 range
localhost-RBM(config)# radio rf 0
localhost-RBM(config-rf-0)# <TAB>
Possible completions:
  antenna-method      Radio antenna method disabled/enabled
  frequency           Center frequency
  rate-adaptation     Rate Adaptation (RA) algorithm settings
  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-RBM(config-rf-0)#
```

10.8.2 User CONFIG Mode

To access User CONFIG mode:

1. Type **admin** while in Global CONFIG level, then **users**, then **user** with your [user name] (Example 1 shows **admin**, as the user name and Example 2 as **roy**). At the terminal, the screen displays:

Example 1

```
localhost(config)# admin <TAB>
Possible completions:
  aaa
  cli      Command-line Interface settings
  snmp     SNMP agent settings
  users    CLI/web user settings
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 (access level)
  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)#
```

Example 2

```

localhost(config)#
localhost(config)# admin users user roy <TAB>
Possible completions:
  group      Group the user belongs to
  password   User password
  <cr>
localhost(config)# admin users user roy password
(<MD5 digest string>): *****
Reconfirm (<MD5 digest string>): *****
Value for 'group' [read-only,read-write]: read-write
localhost(config-user-roy)# ?
Possible completions:
  group      Group the user belongs to (access level)
  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)#

```

10.8.3 RBM CONFIG Mode (Hub Modules Only)

To access the RBM CONFIG mode:

```

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 Historical event list
  mgmt       Management interface settings
  pm         Performance measurements
  ptp        PTP settings
  radio      Radio Interface Settings
  rbm-general-config RBM provisioning settings
  rbm-table  RBM configuration table
  session    Global default CLI session parameters
  system     System settings
  user
  webui     Web UI specific configuration
  ---
  abort     Abort configuration session
  clear     Remove all configuration changes
  commit    Commit current set of changes
  compare   Compare configuration

```

```

copy          Copy a list entry
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
  ---
  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)# ?
Possible completions:
  direction          Service flow direction
  flow-classification Service flow packet classifiers
  priority            Service flow priority
  qos                 QoS settings
  ---
  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-service-flow-1)# flow-classification ?
Possible completions:
  rule      Flow classification rule
HUB_traffic(config-service-flow-1)# flow-classification rule
Possible completions:
  <index:unsignedInt> 1 range
HUB_traffic(config-service-flow-1)# flow-classification rule 0
HUB_traffic(config-rule-0)# show full
rbm-table rbm 0c:a1:38:00:00:81
  service-flows service-flow 1
    flow-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 maximum value
  min-tos            Type of service minimum value
  priority           Rule priority
  protocol           Classification 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
  vlan-id            VLAN ID (non-stacking)
  vlan-priority      VLAN (non-stacking) priority bit
  ---
  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

```

10.9 Saving Configuration Changes Made Via X-1200 CLI

When using the X-1200 CLI to change parameters on the X-1200 system configuration, the changes do not take effect immediately. This example shows the process to follow to make system configuration changes, via the X-1200 CLI, that take effect on the X-1200 system and have them saved across system restarts.

For example, to change the radio frequency on the X-1200 system, you run the **radio** Global CONFIG command:

```
localhost#  
localhost# config terminal  
localhost(config)# radio rf 0  
localhost(config-rf-0)# frequency 2310000  
localhost(config-rf-0)#
```

While you have entered a new value for the radio frequency, for instance: 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-rf-0)# commit  
#commit complete  
localhost(config-rf-0)#
```

Now your change takes effect and the radio frequency is actually operating at the 2310000 frequency on the X-1200 system.

However, this has only makes a change to the current running configuration of the X-1200 system—not the startup configuration (the startup configuration is loaded upon booting the system). This means that if the system restarts, the running configuration changes are lost unless they are saved to the startup configuration. To do this, copy the running configuration to the startup configuration on the X-1200 system by using the **copy** Privileged EXEC command:

```
localhost(config-rf-0)# exit  
localhost(config)# exit  
localhost# copy running-configuration startup-configuration  
localhost#
```

Through the X-1200 CLI, by way of this example, you have successfully:

- made a change to the X-1200 system configuration
- committed this change to the running configuration
- copied the running configuration to the startup configuration
- saved the configuration change across system restarts

10.10 Writing and Running X-1200 CLI Scripts

To simplify the loading of common or repetitive configuration setups, the X-1200 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-1200 system:

1. Save the script as text.
2. Then perform a copy and paste function directly into the X-1200 CLI at the Global CONFIG level.

The script then runs on the X-1200 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 remaining 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-1200 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.

10.11 Using Help

The X-1200 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 QUESTION MARK (?) gives different results. Table 7, *Help Commands* summarizes the help system.

Table 7 Help Commands

Command	Description
?, help, TAB	Lists all commands or command options available in the current CLI level.
partial-commandTAB	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.

10.11.1 ? (QUESTION MARK Key)

You can input the QUESTION MARK (?) key whenever you need additional information. When you enter ?, the CLI displays all available choices for that level. When you enter ? on a line by itself or when it is preceded by one or more spaces, a list displaying all of the next available choices appears. Refer to Example 1.

EXAMPLE 1:

Privileged EXEC Level

From the localhost# 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:
  admin          Administrative settings and commands
  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 Historical event list
  exit       Exit the management session
  export-logs Export debug logs to the specified FTP server for
               offline analysis.
  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
  license-key Download a software license key and apply it to the
               module.
  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
  ping    Debug network connectivity using ping
  pm     Performance measurements
  prompt1 Set operational mode prompt
  prompt2 Set configure mode prompt
  radio  Radio interface settings
  quit   Exit the management session
  screen-length Configure screen length
  screen-width Configure screen width
  script Script actions
  send   Send message to terminal of one or all users
  shell  Debug shell.
  show   Show information about the system
  show-defaults Show default values when showing the configuration

```

source	File to source
system	System commands
terminal	Set terminal type
timestamp	Enable/disable the display of timestamp
who	Display currently logged on users
write	Write configuration

Global CONFIG Level (HM)

localhost# **config terminal**

Entering configuration mode terminal

localhost(config)# ?

Possible completions:

admin	Administrative settings and commands
alias	Create command alias.
bridge	L2 bridge settings
ethernet	Ethernet port settings
event-history	Historical event list
mgmt	Management interface settings
pm	Performance measurements
ptp	PTP settings
radio	Radio interface settings
rbm-general-config	RBM provisioning settings
rbm-table	RBM configuration table
session	Global default CLI session parameters
system	System settings
user	
webui	Web UI specific configuration

abort	Abort configuration session
clear	Remove all configuration changes
commit	Commit current set of changes
compare	Compare configuration
copy	Copy a list entry
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

Global CONFIG Level (RBM)

localhost-RBM# config terminal

Entering configuration mode terminal

localhost-RBM(config)# ?

Possible completions:

admin	Administrative settings and commands
alias	Create command alias.
ethernet	Ethernet port settings
event-history	Historical event list
mgmt	Management interface settings
pm	Performance measurements
ptp	PTP settings
radio	Radio interface settings
session	Global default CLI session parameters
system	System settings
user	
webui	Web UI specific configuration

abort	Abort configuration session
clear	Remove all configuration changes
commit	Commit current set of changes
compare	Compare configuration
copy	Copy a list entry
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 user knows the command keyword, but the list and format of parameters is not. Refer to Example 2.

Example 2

You can terminate an X-1200 CLI command with a `?` to display the complete help on that command:

```
localhost(config)# mgmt ?
Possible completions:
  default-gateway  IP default gateway
  interfaces       Management interfaces control
  ip               Management IP address and netmask
  ip-config-mode   Management IP mode
  syslog           Syslog server settings
  traffic-tunneling Traffic tunneling enable/disable [HM only]
```

10.11.2 help Command

From the prompt, you can enter the **help** command when you want to display a brief description of the X-1200 CLI help system.

In Privileged EXEC mode:

```
localhost# help ?
Possible completions:
  admin           Administrative settings and commands
  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   Historical event list
  exit            Exit the management session
  export-logs     Export debug logs to the specified FTP server for
                  offline analysis.
  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
  license-key     Download a software license key and apply it to the
                  module.
  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
  ping            Debug network connectivity using ping
  pm              Performance measurements
  prompt1        Set operational mode prompt
```

prompt2	Set configure mode prompt
quit	Exit the management session
radio	Radio interface settings
screen-length	Configure screen length
screen-width	Configure screen width
script	Script actions
send	Send message to terminal of one or all users
shell	Debug shell.
show	Show information about the system
show-defaults	Show default values when showing the configuration
source	File to source
system	System commands
terminal	Set terminal type
timestamp	Enable/disable the display of timestamp
who	Display currently logged on users
write	Write configuration

In Global CONFIG mode:

Localhost-RBM(config)# **help ?**

Possible completions:

abort	Abort configuration session
admin	Administrative settings and commands
alias	Create command alias.
bridge	L2 bridge settings [<i>HM only</i>]
clear	Remove all configuration changes
commit	Commit current set of changes
compare	Compare configuration
copy	Copy a list entry
do	Run an operational-mode command
end	Terminate configuration session
ethernet	Ethernet port settings
event-history	Historical event list
exit	Exit from current mode
help	Provide help information
insert	Insert a parameter
load	Load configuration from an ASCII file
mgmt	Management interface settings
move	Move a parameter
no	Negate a command or set its defaults
pm	Performance measurements
ptp	PTP settings
pwd	Display current mode path
radio	Radio interface settings
rbm-general-config	RBM provisioning settings [<i>HM only</i>]
rbm-table	RBM configuration table [<i>HM only</i>]
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

session	Global default CLI session parameters
show	Show a parameter
system	System settings
top	Exit to top level and optionally run command
user	
validate	Validate current configuration
webui	Web UI specific configuration
<cr>	

10.11.3 Partial-keyword - TAB

At any point in the command line, the user can press the **TAB** key to display the valid inputs from that point on in the CLI command.

When you cannot recall a complete command name or keyword, type in the first few letters, press the **TAB** key, 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.
bridge	L2 bridge settings
ethernet	Ethernet port settings
mgmt	Management interface settings
pm	Performance measurements
ptp	PTP settings
radio	Radio interface settings
rbm-general-config	RBM provisioning settings
rbm-table	RBM configuration table
session	Global default CLI session parameters
system	System settings
user	
webui	Web UI specific configuration
	Output modifiers
<cr>	ssho

10.12 Upgrading System Software through the X-1200 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
system software upgrade-status not started
localhost#
```

To upgrade the software through the X-1200 CLI:

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-1200 CLI. Log in again once the X-1200 system is back up and running.

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

10.13 Show Command Options

The following **show** command options are available in both the Privileged EXEC and Global CONFIG command levels:

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

Example 1 — show active-alarms

To display a list of active alarms on the module, enter **show active-alarms**:

```
localhost# show active-alarms
active-alarms alarm 0c:a1:38:00:00:6a SYNC 7001
  type          equipment
  probable-cause loss-of-signal
  severity      major
  timestamp     2013-02-25T11:24:55-05:00
  notification-id 114
  comment-data  "System lost synchronization with timing source"
```

Example 2 — show mgmt

To display the current management IP address for the module, enter **show mgmt**:

```
localhost# show mgmt
mgmt current-ip 192.168.5.30/24
```

Example 3 — show pm

To display a list of current performance measurements for the module, enter **show pm**:

```
localhost# show pm
pm ethernet if in-octets 77801855
pm ethernet if in-octets-per-second 164
pm ethernet if in-pkts 183023
pm ethernet if out-octets 15148474
pm ethernet if out-octets-per-second 0
pm ethernet if out-pkts 25021
pm ethernet if in-discards 101243
pm ethernet if in-errors 0
pm ethernet data in-octets 5003726
pm ethernet data in-octets-per-second 25
pm ethernet data in-pkts 64547
pm ethernet data out-octets 259533
pm ethernet data out-octets-per-second 0
pm ethernet data out-pkts 935
pm ethernet mgmt in-octets 6736704
pm ethernet mgmt in-octets-per-second 0
pm ethernet mgmt in-pkts 17233
pm ethernet mgmt out-octets 14888941
pm ethernet mgmt out-octets-per-second 0
pm ethernet mgmt out-pkts 24086
pm rf-stats interference -104
pm rbm 0c:a1:38:00:00:4f
  ip-address 192.168.5.32
  up-time 247734
  ethernet if in-octets 5184025
  ethernet if in-octets-per-second 13
  ethernet if in-pkts 63944
  ethernet if out-octets 0
  ethernet if out-octets-per-second 0
  ethernet if out-pkts 0
  ethernet if in-discards 0
  ethernet if in-errors 0
  ethernet data in-octets 5184025
  ethernet data in-octets-per-second 13
  ethernet data in-pkts 63944
  ethernet data out-octets 0
  ethernet data out-octets-per-second 0
  ethernet data out-pkts 0
  ethernet mgmt in-octets 0
  ethernet mgmt in-octets-per-second 0
  ethernet mgmt in-pkts 0
  ethernet mgmt out-octets 0
  ethernet mgmt out-octets-per-second 0
  ethernet mgmt out-pkts 0
  rf-stats dl-cinr-ant0 29
  rf-stats dl-cinr-ant1 29
  rf-stats dl-rssi-ant0 -65
  rf-stats dl-rssi-ant1 -67
  rf-stats dl-mcs qam256-6by8
  rf-stats dl-antenna-method mimo
```

```

rf-stats ul-cinr-ant0 28
rf-stats ul-cinr-ant1 28
rf-stats ul-rssi-ant0 -66
rf-stats ul-rssi-ant1 -65
rf-stats ul-mcs qam256-6by8
rf-stats ul-antenna-method mimo
rf-stats coupling 39
rf-stats tx-bytes 110667541
rf-stats rx-bytes 21179235
rf-stats ul-crc-errors 0
rf-stats dl-crc-errors 0
rf-stats hcs-errors 0
rf-stats rx-gain-ant0 45
rf-stats rx-gain-ant1 45
rf-stats tx-power 10
rf-stats interference -104

```

ID	DIRECTION	QOS TYPE	IN OCTETS	IN		OUT		OUT PKTS
				PER SECOND	PKTS	PER SECOND	PKTS	
1	downlink	be	4929028	44	63954	4928613	12	63949
2	uplink	be	0	0	0	0	0	0

DIRECTION	MCS VALUE	USAGE	
		PER SECOND	COUNT
uplink	qam256-6by8-iso	4	4
uplink	qam256-5by8-mimo	179	179
uplink	qam256-6by8-mimo	49550926	49550926
downlink	qpsk-3by4-iso	4	4
downlink	qam256-5by8-mimo	288	288
downlink	qam256-6by8-mimo	49550817	49550817

DIRECTION	CINR VALUE	MEASUREMENT	
		PER SECOND	COUNT
uplink	24db-mimo	88	88
uplink	25db-mimo	176	176
uplink	26db-mimo	148	148
uplink	27db-mimo	118	118
uplink	28db-mimo	2851859	2851859
uplink	28db-iso	5	5
uplink	29db-mimo	46698645	46698645
downlink	23db-mimo	24	24
downlink	24db-mimo	184	184
downlink	25db-mimo	152	152
downlink	26db-mimo	80	80
downlink	27db-mimo	144	144
downlink	28db-mimo	47065345	47065345
downlink	29db-mimo	2485168	2485168
downlink	29db-iso	5	5

```

pm rbm 0c:a1:38:00:00:5b
ip-address 192.168.5.31
up-time 247792
ethernet if in-octets 5183936
ethernet if in-octets-per-second 13
ethernet if in-pkts 63940
ethernet if out-octets 495
ethernet if out-octets-per-second 0
ethernet if out-pkts 5
ethernet if in-discards 0
ethernet if in-errors 0
ethernet data in-octets 5183936
ethernet data in-octets-per-second 13
ethernet data in-pkts 63940
ethernet data out-octets 0
ethernet data out-octets-per-second 0
ethernet data out-pkts 0
ethernet mgmt in-octets 0
ethernet mgmt in-octets-per-second 0
ethernet mgmt in-pkts 0
ethernet mgmt out-octets 0
ethernet mgmt out-octets-per-second 0
ethernet mgmt out-pkts 0
rf-stats dl-cinr-ant0 30
rf-stats dl-cinr-ant1 28
rf-stats dl-rssi-ant0 -62
rf-stats dl-rssi-ant1 -65
rf-stats dl-mcs qam256-6by8
rf-stats dl-antenna-method mimo
rf-stats ul-cinr-ant0 29
rf-stats ul-cinr-ant1 28
rf-stats ul-rssi-ant0 -65
rf-stats ul-rssi-ant1 -68
rf-stats ul-mcs qam256-6by8
rf-stats ul-antenna-method mimo
rf-stats coupling 40
rf-stats tx-bytes 110804768
rf-stats rx-bytes 21206579
rf-stats ul-crc-errors 0
rf-stats dl-crc-errors 28
rf-stats hcs-errors 0
rf-stats rx-gain-ant0 39
rf-stats rx-gain-ant1 45
rf-stats tx-power 7
rf-stats interference -66
    
```

ID	DIRECTION	QOS TYPE	IN OCTETS	IN	IN PKTS	OUT	OUT	OUT PKTS
				PER SECOND		PER SECOND	PER SECOND	
1	downlink	be	4929648	12	63963	4928176	12	63940
2	uplink	be	0	0	0	0	0	0

```

          USAGE
DIRECTION  MCS VALUE  COUNT
-----
    
```

```

uplink      qam256-6by8-iso  3
uplink      qam256-5by8-mimo 370
uplink      qam256-6by8-mimo 49557916
downlink    qpsk-3by4-iso    3
downlink    qam256-5by8-mimo 53864
downlink    qam256-6by8-mimo 49504422

```

DIRECTION	CINR VALUE	MEASUREMENT COUNT
uplink	22db-mimo	55
uplink	23db-mimo	130
uplink	24db-mimo	130
uplink	25db-mimo	93
uplink	26db-mimo	89
uplink	27db-mimo	1089238
uplink	28db-mimo	48468482
uplink	29db-mimo	5
uplink	29db-iso	3
downlink	22db-mimo	5504
downlink	23db-mimo	43976
downlink	24db-mimo	4304
downlink	25db-mimo	55
downlink	26db-mimo	16050
downlink	27db-mimo	41495
downlink	28db-mimo	5412495
downlink	29db-mimo	43998495
downlink	29db-iso	3
downlink	30db-mimo	35784

Example 4 — show radio

To display the radio interface settings, such as the link and operational states, enter **show radio**:

```

localhost# show radio
      OPERATIONAL LINK
ID  STATE          STATE
-----
0   operational    link-up

```

Example 5 — show system

To display system information for the module such as up-time, system identification details, software versions, and timing information, enter **show system**:

```
localhost# show system
system up-time "2 days, 22 hours, 6 minutes, 23 seconds"
system id model X-1200
system id serial-number A130919004
system id module-type hm
system id mac-address 0c:a1:38:00:00:29
system id radio-0 3.3-GHz
system id cpld-revision 0x0002
system id order-code xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
system id bootloader-ver 1.2.3.9858
system time sync-state synchronized
system time gps-state synchronized
system time local-time 2013-11-12T11:23:33-00:00
system software running-version 1956.1.1_12
system software restart-version 1956.1.1_12
system software available-version 1956.1.1_11
system software upgrade-status switchover-succeeded
```

11 System Provisioning

This chapter describes the tasks associated with preparing an X-1200 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

11.1 Initial System Setup and IP Configurations

When you receive a new X-1200 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, then check your connectivity by pinging the HM using **169.254.1.1/24**—the Craft IP address that is always accessible (as it cannot be changed by the user).
2. After successfully pinging the Craft IP address, either:
 - a. Open a web browser and navigate to the IP address that you pinged to bring up the X-1200 WebUI, or
 - b. Use a Secure Shell (SSH) client to log on to the X-1200 CLI using a 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).
3. 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
- use the Dynamic Host Configuration Protocol (DHCP) to configure this IP address.

Note: To have DHCP properly assign an address to your X-1200 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.

11.1.1 Assigning a Management IP Address

By default, the X-1200 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-1200 WebUI, as follows:

1. Navigate to the **Setup > System** page of the X-1200 WebUI.

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

2. Change the **Mgmt IP Address** option 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. Use the **Refresh** button return to the previous settings and to update the information on the screen.

The screenshot shows the X-1200 WebUI configuration page for the System. The 'Management Interface' section is active, showing the following settings:

- Current IP Address: N/A
- Mgmt IP Address: DHCP Static
- IP Address: 192.168.1.238
- Netmask: 255.255.255.0
- Gateway: Gateway: 192.168.1.1
- Mgmt VLAN: Enable Disable

Other sections visible include System Identification (System Name: BLiNQ-module, System Location: Test Site, System Contact: Jen Smith, System Description: Hub pointing MW), System Time Configuration (Sync State: Synchronized, System Date/Time: 2013-02-06T16:18:26, System Time Zone: UTC-12:00, System Clock Source: GPS), and Ethernet Port Configuration (Operational State: Down, Operational Speed/Duplex: NA NA Duplex, Auto-Negotiation: On Off).

Alternately, if you wish to use the X-1200 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 terminal
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.
localhost(config)# end
localhost# copy run start
```


11.1.2 Configuring the Radio Interface

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-1200 system:

1. Navigate to the **Setup > Radio Interface** page of the X-1200 WebUI.
2. Set the **Radio Administrative State** to **Enabled**.
3. Ensure that both the HM and RBM have their radio frequencies set to matching values that are within the range of usable frequency for the X-1200 system.

Note: The radio frequency tuning granularity is 1 kHz.

4. Click **Apply** in the bottom right corner for the changes to take effect or select the **Refresh** button to cancel and return to the previous settings.

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 12, *Preambles, Flows, and Network Provisioning*)
- Since the RBM factory default value for the preamble index is **All**, it automatically accepts preambles from any HM. Other preamble index values are configurable, 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
 - Max/Min DL MCS
 - Max/Min UL MCS

System Overview	Setup	Bridge	RBM	Performance	PM History	Events	Admin
System	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <h4>Radio Settings</h4> <p>Operational Status: Operational</p> <p>Radio Administrative State: Enabled ▼</p> <p>Radio Interface Type: 3.5</p> <p>RF Frequency (kHz): <input type="text" value="3500000"/></p> <p>Channel Bandwidth (MHz): 10MHz ▼</p> <p>Max Transmit Power (dBm): <input type="text" value="10"/></p> <p>Frame Duration (ms): 5ms ▼</p> <p>TDD DL/UL Ratio: 50:50 ▼</p> <p>Preamble Index: <input type="text" value="0"/></p> </div> <div style="width: 45%;"> <h4>Rate Adaptation</h4> <p>Min DL MCS: QPSK 3/4 ▼</p> <p>Max DL MCS: 256QAM 6/8 ▼</p> <p>Min UL MCS: QPSK 3/4 ▼</p> <p>Max UL MCS: 256QAM 6/8 ▼</p> </div> </div>						
Radio Interface							

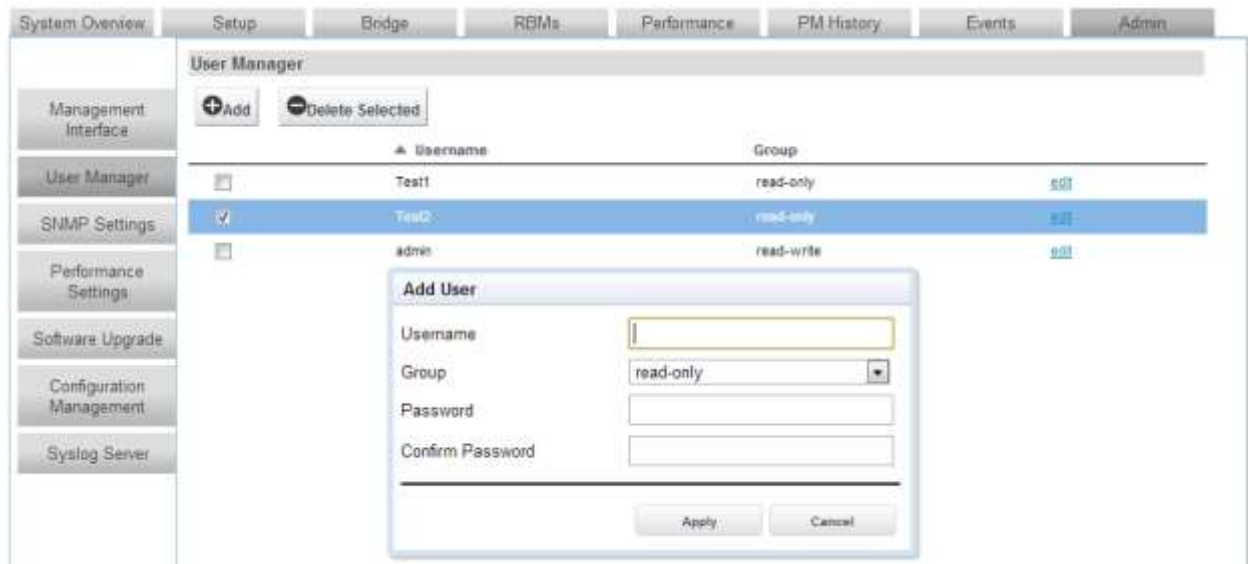
11.2 Adding Users

You can add users to the X-1200 system through either the X-1200 WebUI or the X-1200 CLI.

11.2.1 Add Users using X-1200 WebUI

To add users to the X-1200 system using the X-1200 WebUI:

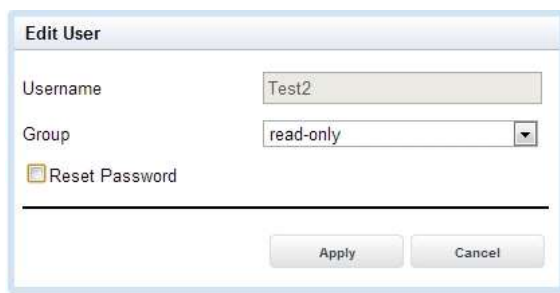
1. Navigate to the **Admin > User Manager** page of the X-1200 WebUI.
2. Click **Add** to add a user. An **Add User** dialog box appears.



3. From the **Add User** dialog box, you can now enter a username, password, and choose the access level of that user (**Group**) (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-1200 system.
4. You can also edit existing users to the X-1200 by selecting **edit** on the same line as the user you want to modify. The **Edit User** dialog box appears. Adjust the settings as required.



To change the user name, delete this user and re-input under a new name.

- 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.

To reset a password, select the **Reset Password** check box. The **New Password** and **Confirm Password** fields appear. Type in the new password and confirm it. Inform the user of the new password.

- For any of the actions, select **Apply** for the changes to take effect or **Cancel** to abandon this action.

11.2.2 Add Users using the X-1200 CLI

To add users to the X-1200 system using the X-1200 CLI, enter these commands:

```
localhost#
localhost# config terminal
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.
localhost(config)# end
localhost# copy run start
```

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

11.3 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 **RBM's > RBM General** X-1200 WebUI 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 **RBM's > Default Service** page. All RBMs connecting to this HM are then assigned this service flow definition profile. 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 **RBM**s > **RBM List** 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.

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 11.4, “Configuring and Adding Individual RBMs”.

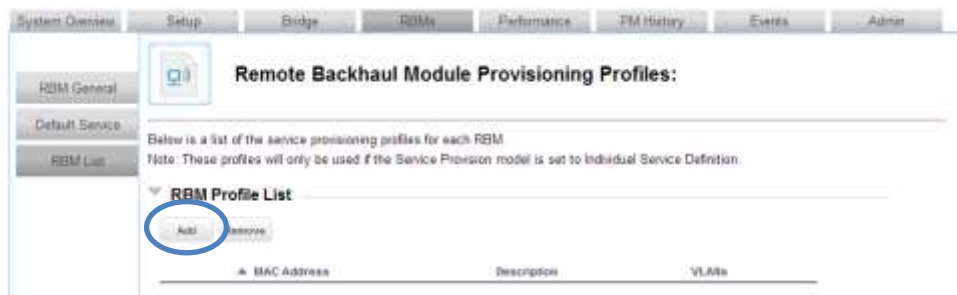
11.4 Configuring and Adding Individual RBMs

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-1200 system on an RBM-by-RBM basis. This can be done through either the X-1200 WebUI or the X-1200 CLI.

11.4.1 Using the X-1200 WebUI

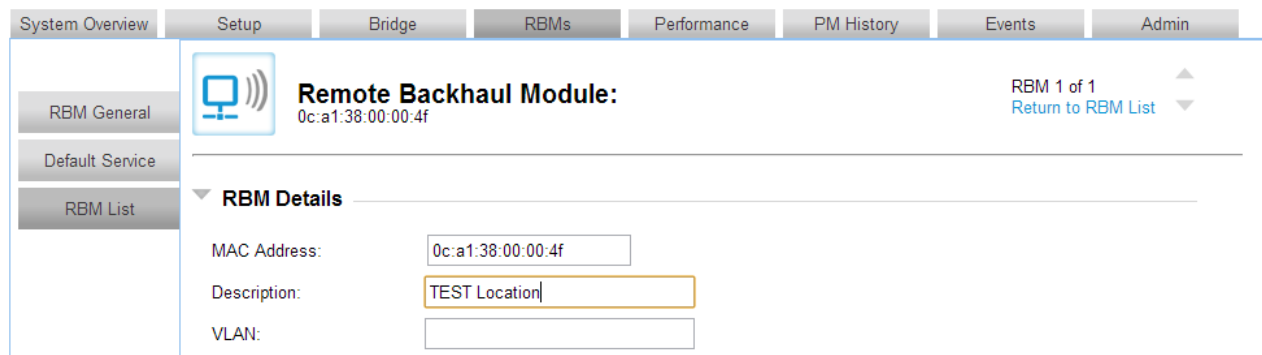
For example, to configure a default, pass-all, bidirectional service flow on the HM for one RBM on the X-1200 system using the X-1200 WebUI:

1. Navigate to the **RBM**s > **RBM List** page of the X-1200 WebUI.
2. Click the **Add** button to add an RBM.



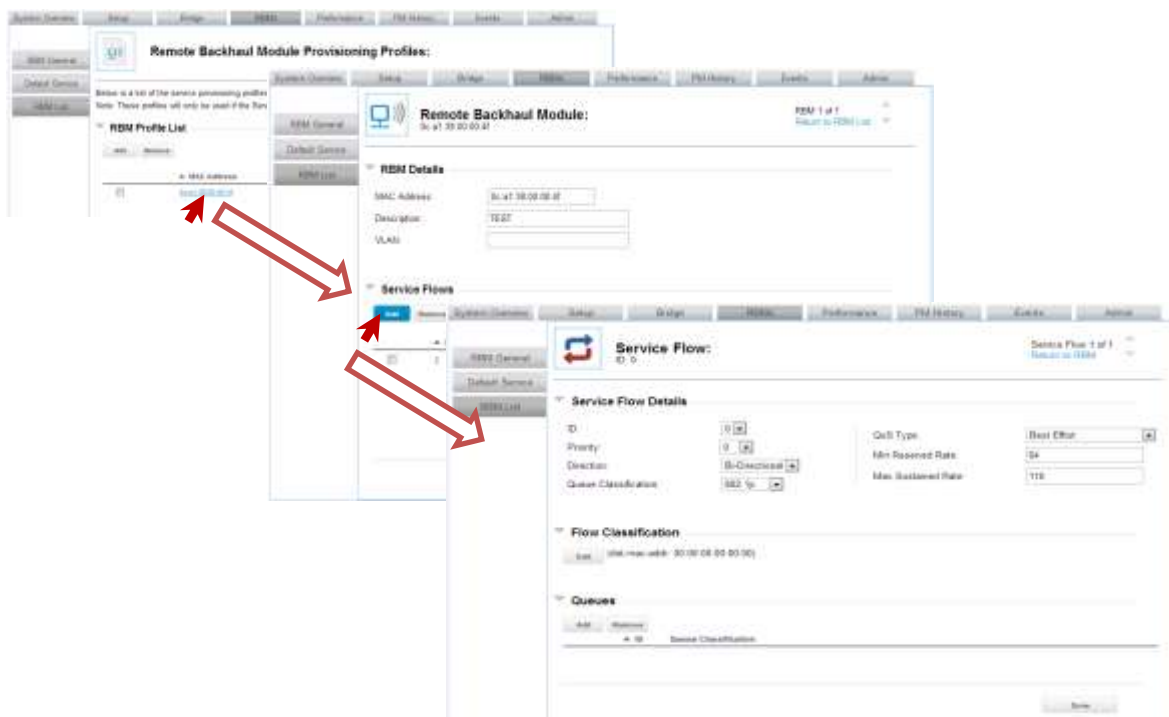
A **Remote Backhaul Module:** page appears.

3. In the **Remote Backhaul Module:** page, under the **RBM Details** area, enter the MAC address for your RBM along with a description (for instance, a location) and the VLAN, if desired, in the appropriate boxes.

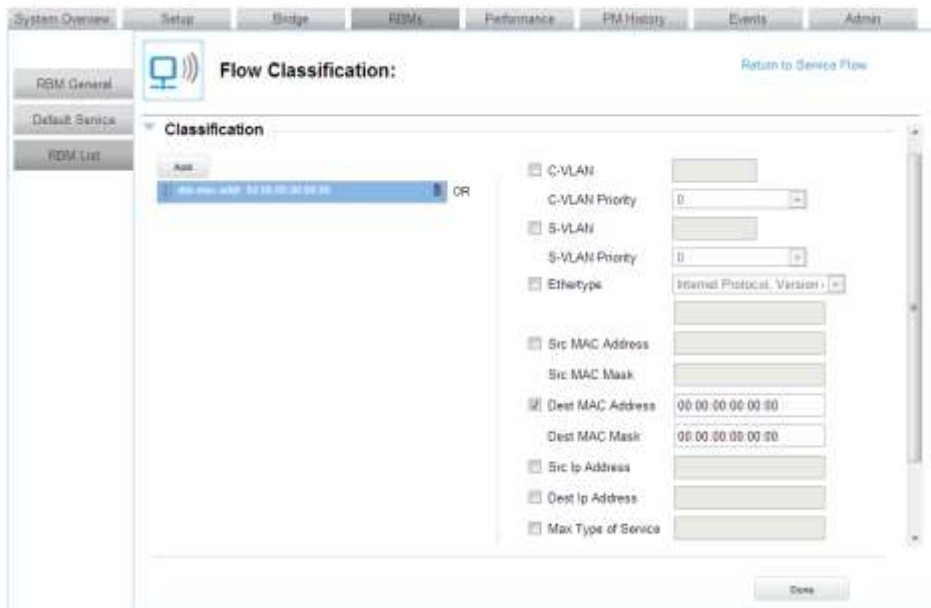


When you enter a MAC address, the MAC address displays below the **Remote Backhaul Module:** title (for instance, Remote Backhaul Module: xx:xx:xx:xx:xx:xx).

4. If you need to edit a RBM, select the MAC address of the desired RBM under the **MAC Address** heading on the default **RBMs > RBM List** page. The **Remote Backhaul Module: xx:xx:xx:xx:xx:xx** for the selected RBM appears. From the **Service Flows** area of the page, click the **Add** button to add a service flow. The **Service Flow:** page appears.



5. In the **Service Flow Details** area: Leave the **Direction** and **QoS Type** as their defaults. Set the desired priority for this RBM with the **Priority** option. In the **Flow Classification** area, click **Add** to add a classification rule(s). A **Flow Classification:** page appears. Under **Classification**, select **Add** to create an empty flow classification. Create the flow classification, by selecting the options from the list on the right hand side.



Tip: If you want all traffic to pass -- Select the **Dest MAC Address** check box and set both values to 00:00:00:00:00:00 to allow for any destination MAC Address.

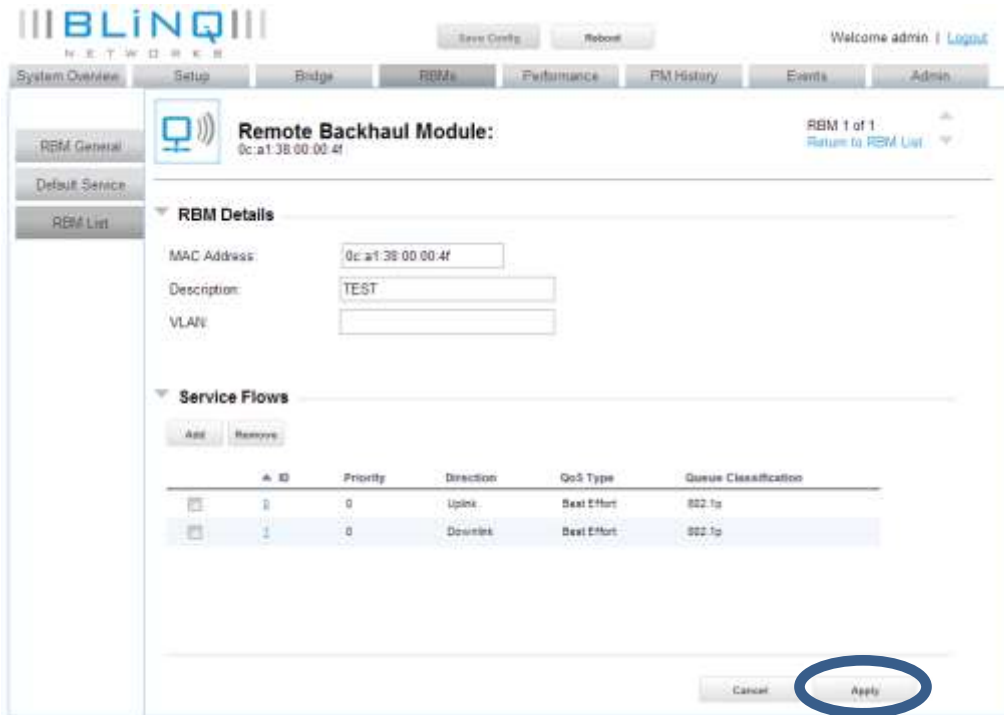
6. Use the hyperlinks in the top right hand corner to return to the **Remote Backhaul Module: xx:xx:xx:xx:xx:xx**. Under the **Service Flows list** area; click **Add** to add another service flow for the other direction, if using an Uplink/Downlink flow.
7. Under the **Service Flow Details** area; use the **Direction** option to change the direction of this service flow to **Uplink** or **Downlink**, as needed.



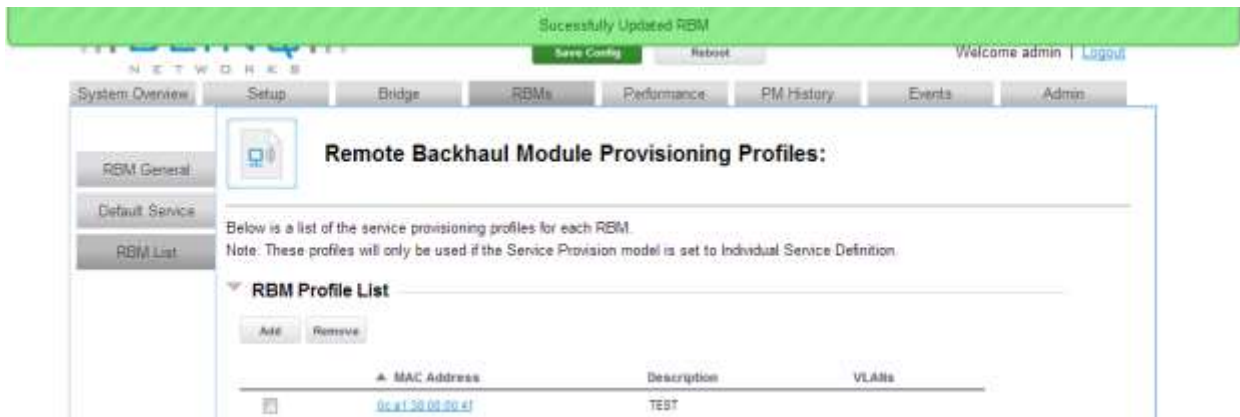
8. Under **Flow Classification**, select **Edit** to add a classification, the **Flow Classification** page appears. Under **Classification**, click **Add**, an empty classification appears; select the options from the right hand side to add a classification rule for this service flow.

Tip: If you want all traffic to pass: Select the **Dest MAC Address** check box and set both values to 00:00:00:00:00:00 to allow for any destination MAC Address.

9. Click **Apply** for the changes to take effect or **Cancel** to abandon this action.



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



10. To save your changes, select the **Save Config** button at the top of the main screen.

The system notifies you that the running configuration has been successfully copied to the startup configuration.

11.4.2 Using the X-1200 CLI

Alternately, you can use the X-1200 CLI to configure individual RBMs; for example, to configure a default pass-all, bidirectional service flow on the HM for one RBM using the X-1200 CLI, enter these commands:

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

localhost(config-rbm-0c:a1:38:00:00:4f)# service-flows //Create the first service flow
service-flow 1 for one direction
Value for 'direction' [downlink,uplink]: downlink
Value for 'priority' (<unsignedByte>): 0
Value for 'qos service-type' [best-effort,guaranteed-bit-
rate]: best-effort
localhost(config-service-flow-1)# flow-classification rule 1 //Add the classification rule
that allows for any
destination MAC address

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
localhost(config-rbm-0c:a1:38:00:00:4f)# service-flows //Create the second service
service-flow 2 flow for the other direction
Value for 'direction' [downlink,uplink]: uplink
Value for 'priority' (<unsignedByte>): 0
Value for 'qos service-type' [best-effort,guaranteed-bit-
rate]: best-effort
localhost(config-service-flow-2)# flow-classification rule 1 //Add the classification rule
that allows for any
destination mac address

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)# commit //Commit the commands so
Commit complete. that they take effect
localhost(config-rule-1)# end
localhost# copy run start //Copy the running
configuration to the startup-
configuration so that upon
reboot this configuration will
be loaded
```

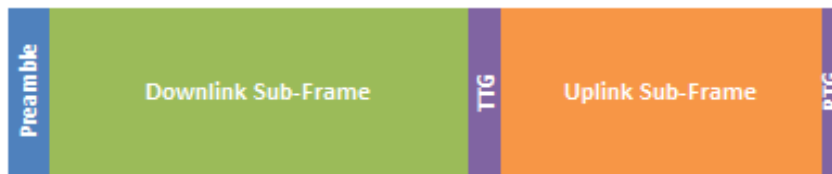

12 Preambles, Flows, and Network Provisioning

This chapter describes the role and use of preamble series indices and service flows in provisioning multiple X-1200 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). This chapter also covers 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

12.1 Preamble Functional Description

The X-1200 system uses Time Division Duplex (TDD) to transport wireless traffic data. TDD divides the data stream into frames. There are two frame_size options: 3.125¹ 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 optional¹). 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-1200 system.

Preamble indices identify and separate clusters of X-1200 modules from each other, and enhance the receive operation performance of the X-1200 system when different clusters are deployed in close geographical or Radio Frequency (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 in the other cluster).

¹ Not available in the current release.

Note: BLiNQ Networks recommends that clusters in close geographic or RF proximity be assigned unique preamble indices. It is also recommended that RBMs in these clusters be pre-configured to connect to only one HM by matching this HMs preamble configuration. This ensures accurate operation of the RBM pointing system during installation.

12.2 Preamble Operational Description

A Hub and RBM only register and communicate 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:

- An HM can have up to four RBMs registered at any one time.
- There are 32 possible X-1200 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).
- RBMs can be configured to either use a specific preamble index value or a list of preamble index values. In this latter case, the RBM attempts to use each of the values in the list when initiating communication with an HM.

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 1:4 cluster, preamble series index value 1 for the second 1:4 cluster, preamble series index value 2 for the third 1:4 cluster, and so forth, all the way up to preamble series index value 31 for the 32nd 1:4 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 8.4.4, "*Setup - Radio Interface Page*" 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 first 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.

12.3 Provisioning Preambles

The default Preamble Series index settings can be seen in the **Setup > Radio Interface** page of the X-1200 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:

System Overview	Setup	Bridge	RBM	Performance
System	Radio Settings Operational Status: Operational Radio Administrative State: Enabled Radio Interface Type: 3.5 RF Frequency (kHz): 3500000 Channel Bandwidth (MHz): 10MHz Max Transmit Power (dBm): 10 Frame Duration (ms): 5ms TDD DL/UL Ratio: 50:50 Preamble Index: 0			
Radio Interface				

RBM Radio Settings show the factory default of **All** for **Preamble Series**, but the box below the **All** check box can be set to use any single unique preamble index value from 0 to 31 (Uncheck the **All** check box and the field becomes available):

System Overview	Setup	Performance	Events	Admin
System	Radio Settings Operational Status: Operational Radio Administrative State: Enabled Radio Interface Type: 3.5 RF Frequency (Hz): 3500000 Channel Bandwidth (MHz): 10MHz Frame Duration (ms): 5ms Preamble Series: <input checked="" type="checkbox"/> All <input type="text"/> Pointing Mode (BSI): <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled			
Radio Interface				

RBM can also be set to two different preamble operating modes through the **Setup > Radio Interface** X-1200 WebUI page for RBMs:

- **Defined Preamble Mode**—When the RBM preamble series index is set to a value between 0 to 31, it only connects and registers to a serving HM pointed in its direction that matches its preamble value setting. This is the recommended operating mode for live networks.
- **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 and automatically determines the proper preamble index to use with a potential serving HM.

You typically use the **Defined Preamble Mode** 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**. This ensures that all new RBM installations are consistent with the network planning and that RBMs are pointed in the best direction for their designated serving HM.

12.4 Provisioning HM Service Flow Definitions

As explained in Chapter 11, *System Provisioning*, the HM has two service flow definitions for allowing communication to be established with a RBM, set through the **RBM**s > **RBM General** X-1200 WebUI page for HMs:

- **Use Default Service Definition**
- **Use Individual Service Definition**

Refer to section 11.3, “*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**.

12.5 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.

12.5.1 Provisioning Multiple Clusters with the X-1200 WebUI

Using ‘Use Case 2’ from section 12.4, “*Provisioning HM Service Flow Definitions*”, you can, for example, provision three neighboring 1:4 clusters within the same geographic area using the X-1200 WebUI:

First 1:4 Neighbor Cluster:

Using the X-1200 WebUI for the HM:

1. Under **Radio Settings** of the **Setup > Radio Interface** page, enter **0** in the **Preamble Series** box.
2. Click **Apply** for the changes to take effect (or **Cancel** to abandon this action).
3. Select the green **Save Config** button (at the top of the screen) to copy the running configuration to the startup configuraton.

Using the X-1200 WebUI for RBM 1, RBM 2, RBM 3, and RBM 4, respectively:

1. Under **Radio Settings** of the **Setup > Radio Interface** page, enter **0** in the **Preamble Series** box (if required, uncheck the check box beside **All** to make the field available).
2. Click **Apply** for the changes to take effect (or **Refresh** to abandon this action).
3. Select the green **Save Config** button to copy the running configuration to the startup configuration.

Second 1:4 Neighbor Cluster:

Repeat the steps done for the first 1:4 cluster, replacing the **Preamble Series** value 0 with **1**.

Third 1:4 Neighbor Cluster:

Repeat the steps done for the first 1:4 cluster, replacing the **Preamble Series** value 0 with **2**.

12.5.2 Provisioning Multiple Clusters with the X-1200 CLI

Alternately, using ‘Use Case 2’ from section 12.4, “*Provisioning HM Service Flow Definitions*”, you can provision the same three neighboring 1:4 clusters within the same geographic area using the X-1200 CLI:

First 1:4 Neighbor Cluster:

Using the X-1200 CLI for the HM:

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

Using the X-1200 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 1:4 cluster, replacing the **preamble series** value 0 with **1**.

Third 1:4 Neighbor Cluster:

Repeat the steps done for the first 1:4 cluster, replacing the **preamble series** value 0 with **2**.

Further, if applicable for your network, you can repeat this procedure all the way up to preamble series index value 31 for the 32nd 1:4 cluster.

13 Appendices

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

REMARQUE: La traduction française suit le texte anglais.

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

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

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

To prevent unnecessary exposure to RF energy:

- Always install the X-1200 system so as to provide and maintain a minimum separation distance from all persons.
- When the X-1200 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.
- When the X-1200 system is operational, maintain a distance of at least 50 centimeters from the Hub Module (HM) sectored antennas or the Remote Backhaul Modules (RBMs) internal antennas.
- Do not install the X-1200 system in a location where it is possible for people to stand or walk inadvertently in front of an antenna.

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

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

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

Pour éviter toute exposition inutile à l'énergie RF :

- Installer toujours le système X -1200 afin de fournir et de maintenir une distance minimale de séparation avec toutes les personnes.
- Lorsque le système X -1200 est opérationnel, éviter de se tenir directement devant les antennes sectorisées du «Hub Module» (HM) ou devant «Remote Backhaul Module» (RBM) et leurs antennes internes. Les champs d'énergie RF peuvent être présents lorsque l'émetteur est en marche.
- Lorsque le système X -1200 est opérationnel, maintenir une distance d'au moins 50 centimètres à partir des antennes sectorisées du HM ou des antennes internes modules du RBM.
- Ne pas installer le système X -1200 dans un endroit où il est possible pour les gens de se tenir debout ou de marcher en face d'une antenne.

13.2 Equipment Compliance

13.2.1 Federal Communications Commission (FCC) Notices

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

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

13.2.2 Industry Canada Notice

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3 (B)/NMB-3(B)

13.3 List of Acronyms

Table 8 List of Acronyms

ACRONYM	MEANING
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BE	Best Effort
BMC	Best Master Clock
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
Craft IP	IP address typically used by technical personnel to test the equipment
DAN	Design Sharing Networks
DARS	Digital Audio Radio Service
dBi	Decibel isotropic
DBS	Dynamic Bandwidth Sharing
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DN	Directory Number
DNS	Domain Name System
DSCP	Differentiated Services Code Point
ECC	European Communications Committee
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
F/B	Front to Back
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
FTP	File Transfer Protocol
GBR	Guaranteed Bit Rate
GPS	Global Positioning System
HM	Hub Module
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
Kbps	Kilobits per second

L2	Layer 2
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
LPS	Linear Power Supply
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
MPE	Maximum Permissible Exposure
MPLS	Multiprotocol Label Switching
MRC	Maximal Ratio Combining
ms or msec	Millisecond
NLOS	Non Line-of-Sight
NLOS	Non Line-of-Sight
NMS	Network Management System
NOC	Network Operations Center
NTP	Network Time Protocol
OAM	Operations, Administration & Maintenance
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OSS	Operations Support System
PC	Personal Computer
PHY	Physical Layer
PMP	Point-to-Multipoint
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RARP	Reverse Address Resolution Protocol
RBM	Remote Backhaul Module
RF	Radio Frequency
RFEC	Radio Frequency Environment Characterization
RSSI	Received Signal Strength Indicator
RX	Received
s	second

SFP	Small form-factor pluggable
SFTP	Secure File Transfer Protocol
SISO	Single Input Single Output
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSH	Secure Shell protocol
S-VLAN	Stacked VLAN
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Time Division Duplexing
TDM	Time Division Multiplexed
ToS	Type of Service
TX	Transmit
UDP/IP	User Datagram/Internet Protocol
UL	Uplink
URL	Universal Resource Locator
UTC	Coordinated Universal Time
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VSWR	Voltage Standing Wave Ratio
WCS	Wireless Communications Services

© Copyright 2012-2013 BLiNQ Networks Inc. All rights reserved.

CONFIDENTIAL INFORMATION
RESTRICTED USE AND DUPLICATION

The information contained herein is the property of BLiNQ Networks Inc. and is strictly confidential. Except as expressly authorized in writing by BLiNQ Networks Inc., the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care.

Except as expressly authorized in writing by BLiNQ Networks Inc., the holder is granted no rights to use the information contained herein.

BLiNQ and BLiNQ Networks Inc. corporate logo are trademarks of BLiNQ Networks Inc. All other trademarks used in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between BLiNQ and any other company.

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.