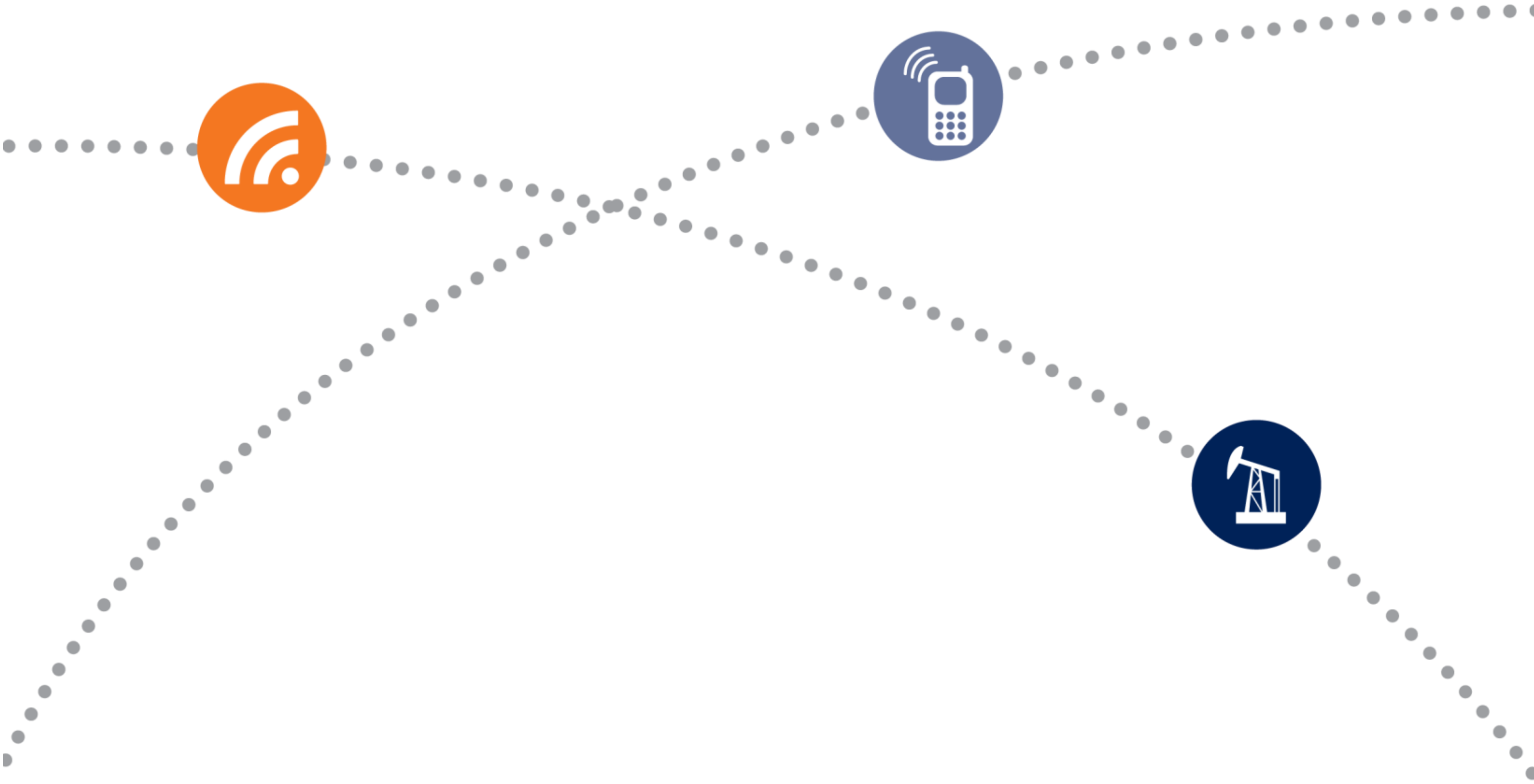


WBSn Family

Release Notes

WBSn-2400 and WBSn-2450
Software Version: 1.3.2
Doc version: v14
Jan 2013

FCC Statement

Federal Communication Commission Interference Statement

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 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operated in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Limitation of Liability:

(a) Alvarion shall not be liable to the purchaser or to any third party, for any loss of profits, loss of use, interruption of business or for any indirect, special, incidental, punitive or consequential damages of any kind, whether arising under breach of contract, tort (including negligence), strict liability or otherwise and whether based on this agreement or otherwise, even if advised of the possibility of such damages.

(b) To the extent permitted by applicable law, in no event shall the liability for damages hereunder of Alvarion or its employees or agents exceed the purchase price paid for the product by purchaser, nor shall the aggregate liability for damages to all parties regarding any product exceed the purchase price paid for that product by that party (except in the case of a breach of a party’s confidentiality obligations).

Contents

1 Overview

Alvarion Wi-Fi base station with 802.11n support (WBSn) is a family of advanced Gigabit outdoor Wi-Fi base stations operating in the 2.4 and 5 GHz unlicensed bands. WBSn base stations use spatially adaptive Beamforming 802.11n and powerful interference immunity suite to deliver best range and capacity, addressing the rapidly growing needs for operators to deliver new content-rich services, while maintaining quality of service and profitability. WBSn base stations enable service providers, governments and enterprises to deliver high quality Wi-Fi services in metro and rural areas, with significantly fewer base stations, and at much lower cost.

1.1 Two-way Spatially Adaptive 802.11n Beamforming

WBSn base stations combine Alvarion's true two-way Beamforming with 802.11n 3x3:3 MIMO, delivering best capacity and coverage, with speeds of up to 450 Mbps per band.

1.2 Interference Immunity Suite

Leveraging a decade of outdoor Wi-Fi experience, Alvarion's Interference Immunity Suite includes:

- Beamforming, with its inherent ability to suppress interference
- The Dynamic Interference Handling (DIH) algorithm, that continuously optimizes receiver's parameters according to varying noise levels
- The Automatic Channel Selection (ACS) algorithm, that automatically identifies, selects and utilizes the best operating channel
- The Alvarion Rate Adaptation algorithm (WARA), which enables optimal rate selection in outdoor environments with high interference
- Down Tilted Antenna (DTA) and sector antenna abilities to reject noise out of their fields-of-view

1.3 Carrier Grade Design

WBSn base stations are designed for high reliability and manageability, including a robust IP-68 certified enclosure for harsh environments, security and QoS features, FCAPS management suite, and simple and easy installation.

Sector	Omni	Sector plus Omni
■ WBSn-2400-S ■ WBSn-2450-S	■ WBSn-2400-O ■ WBSn-2450-O	■ WBSn-2450-SO ■ WBSn-2450-OS

2 Hardware and Software Features

This section describes all hardware and software features that were introduced in earlier versions of WBSn products, as well as in version 1.3.1.

2.1 Supported Hardware

Version 1.3.2 supports all WBSn base station models:

- WBSn-2450-S – outdoor 802.11n 3x3:3 MIMO base station, operating in 2.4 GHz with 120 degree antenna field-of-view
- WBSn-2400-O – outdoor 802.11n 3x3:3 MIMO base station, operating in 2.4 GHz with Omni directional field-of-view
- WBSn-2450-S – outdoor 802.11n 3x3:3 MIMO base station, operating in 2.4 GHz and 5 GHz, with 120 degree dual-band antenna field-of-view
- WBSn-2450-O – outdoor 802.11n 3x3:3 MIMO base station, operating in 2.4 GHz and 5 GHz, with Omni directional dual-band antenna field-of-view
- WBSn-2450-SO – outdoor 802.11n 3x3:3 MIMO base station, operating in 2.4 GHz and 5 GHz, with 120 degree antenna in 2.4 GHz and Omni directional field-of-view in 5 GHz
- WBSn-2450-OS – outdoor 802.11n 3x3:3 MIMO base station, operating in 2.4 GHz and 5 GHz, with 120 degree antenna in 5 GHz and Omni directional field-of-view in 2.4 GHz

WBSn base stations are powered by dedicated Power over Ethernet (PoE) injectors. Three types of PoEs are available and can be ordered separately: 90 – 264V AC PoE, -48V DC PoE and rack-mount -48V DC PoE. All PoEs use power over GbE. The rack-mount PoE can power up to three WBSn units.

2.2 Frequency Bands and Regulatory Domains

Version 1.3.2 supports 2.4 GHz band (2.400-2.483 GHz, with 13 channels) and 5 GHz band (4.900-5.900 GHz). The products can be configured to operate in either 20MHz or 40MHz channel bandwidths.

Four regulatory domains are supported:

- US country code (FCC certified at 2.4 GHz and 5.8 GHz)
- EU country code (ETSI certified at 2.4 GHz, 5.4 GHz and 5.8 GHz)
- JP country code (TELEC certified at 2.4 GHz, 4.9 GHz and 5.4 GHz)
- UN country code (universal - unregulated)

2.3 Interference Immunity Algorithms

WBSn supports enhanced algorithms for dealing with outdoor Wi-Fi interference. The DIH, ACS and WARA algorithms are powered by Alvarion technology, utilizing the experience garnered by Alvarion over more than a decade in outdoor large scale Wi-Fi deployments.

The algorithms are optimized to provide maximum capacity at maximum range in challenging outdoor environments, leveraging the two-way Beamforming 802.11n, 3x3:3 MIMO, WARA and Dynamic Interference Handling (DIH) mechanisms.

Version 1.3 supports offline ACS, optimized for selecting the best channel to reach maximum range, with maximum capacity to associated clients in the covered area.

3 New Features introduced in v1.3.2

The following sections describe the new features introduced in this version.

3.1 Router Mode

Router mode offers several capabilities, including Network Address Translation (NAT) and DHCP Server. In Router mode, one or more LANs (groups of wireless clients) are mapped to a WAN (backhauling interface towards the Internet). Router mode forwards traffic between a LAN and a designated WAN, while keeping NAT rules of translating the IP addresses.

For additional information on Router Mode please refer to the User Manual.

3.2 Web Redirection and Walled Garden

Web Portal Redirection (a.k.a. ”Captive Portal”) capability is useful for authenticating non-EAP capable clients. Associated (non-authenticated) clients are redirected to a Captive Portal in which they are requested to insert their username and password which WBSn then validates with a RADIUS server.

The Walled Garden is a “White List” of URLs which users can access with no need for authentication. One of the URLs in this list can be a server through which users may purchase access to the network, and obtain their username and password. For URLs that are not included in the White List, the integral Access Controller presents a Captive-Portal to the user.

With an internal Access Controller license installed, a WBSn provides Web Portal Redirection and Walled Garden without the need for any additional external hardware.

For a limited time period, this feature is available without the Access Controller license. In future releases it will be blocked and enabled only to customers who purchase the Access Controller license (to be detailed in future releases).

3.3 Accounting for Wireless Clients

Accounting is required for billing and statistical purposes. With an internal Access Controller license installed, a WBSn provides per-user time and throughput RADIUS accounting messages, without the need for any additional external hardware. This feature is currently available for all wireless clients whether associated to secured (e.g. WPA2-RADIUS) or non-secured (i.e. Open) VAPs. In future versions Accounting will also be available for users authenticated using Web-Authentication portal, and the Accounting will start after the clients are authenticated. The Accounting Start and Interim messages include information about the connected wireless client, including its IP address, if known to the base station (base on DHCP messages exchanged with the client).

For a limited time period, this feature is available without the Access Controller license. In future releases it will be blocked and enabled only to customers who purchase the Access Controller license (to be detailed in future releases).

Note: This feature is disabled by default.

3.4 Unique Enhancements for Open Security Sessions

WBSn have always supported Open, WEP, WPA and WPA2 security mechanisms. This release provides enhancement to the authentication mechanism for open (non-encrypted) sessions. The enhancement is achieved by RADIUS-based MAC authentication which is now available when configured to “Open (802.1x + MAC Auth)”.

Moreover, in this latest release the authentication mechanisms were enhanced to support EAP-based 802.1x Authentication also for the open session mode (by setting “Open (802.1x Auth)”). When such non-standard authentication is in use a special supplicant SW on the client device is required to handle EAP (Extended Authentication Protocol) over the open session.

3.5 Wireless System Modes

WBSn can be operated in two wireless system modes: Capacity and Coverage modes. Capacity mode is the default system mode, as most customers expect to provide maximum capacity to the maximum number of users. Alternatively, the user can change this setting to Coverage mode, where maximum coverage can be achieved with some degradation in the overall system capacity. In Coverage mode, the user can set the Basic Rate Set to include 802.11b clients. Otherwise, the system is set by default to only allow connections of 802.11g/n clients (relevant to 2.4GHz band radio only).

3.6 Improved Performance

Alvarion is constantly working on improving performance of the product. As with earlier versions, this version brings improvements of radio performances and stability including extended capacity, improved operation in multiple clients’ scenarios, and operation in high interfered environments.

3.7 Improved Network Security

Alvarion is constantly working on improving the security of the network. This version brings an option to block DHCP server traffic coming from Wireless clients. With this capability, the operator can protect the network from malicious DHCP servers installed on end-users devices.

4 Known Issues

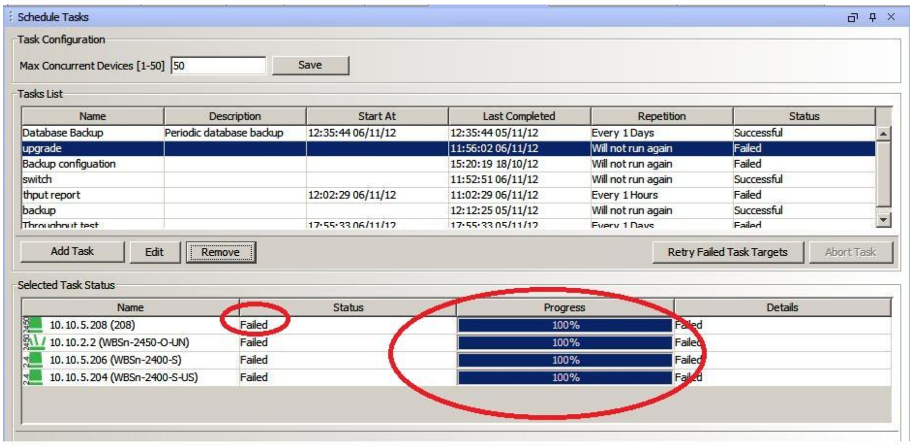
The following table describes the known issues and workarounds for WBSn V1.3.2.

Known Issue	Description
HTTP Management Interface – Java application	WBSn HTTP management interface provides a Graphical User Interface (GUI) that is basically a JAVA Application. Users of iPads, or iPhones (or other devices incompatible with Java applications), who wish to manage the Alvarion base stations need to remotely connect to a host using a remote connection application. From the remote host they can log-in and manage the base stations. The following web browsers work correctly with WBSn GUI interface: ■ Internet Explorer v8 or later ■ FireFox v12 or later ■ Chrome v19 or later Java version 1.6 or later shall be used.
IEEE 802.11n supports only AES Encryption Keys (#200)	The 802.11n standard only permits the use of AES keys when operating within a secured network. Therefore, it is strongly recommended that VAPs will be either Open or WPA2 AES secured. In case TKIP or WEP clients are expected to connect, they must connect using 802.11g interface. Additionally, a WEP-secured VAP can only be configured for first VAP (i.e. VAP-1).
Missing Notifications of starting Firmware Upgrade / Rollback and SW switch banks (#498, #504, #509)	The HTTP GUI notifications indicating the beginning of firmware-related operations (e.g. firmware upgrades, switching banks, and rollbacks) are missing. Please refer to the section entitled Firmware in the User Guide for a comprehensive description of the WBSn firmware upgrade process.

Known Issue	Description
Association Table may hold stale information (#472)	On rare cases, the Association Table may contain outdated information of Wi-Fi clients that are no longer connected to the system. **Workaround**: Refresh the Association Table, and identify the active clients by looking at clients' traffic (TX[Byte] and RX[Bytes]).
Default VAP parameters are not consistent (#555)	Sometimes, when initiating the settings of a new VAP wrong default values may appear. **Workaround**: Overwrite the wrong default values with the desired values. Or alternatively, try to repeat the operation.
VAP editing window resets pre-configure values (#529)	When editing an existing VAP, some of the parameters (e.g. PSK type) are reset to default values and must be re-entered.
Issues with Auto-negotiation of Ethernet speed (#1699, #1758)	Auto-negotiation of the Ethernet port may fail with some Ethernet switches (e.g. Huawei model S2309) and may cause duplex-mismatch on the Ethernet link. As a result, backhaul throughput will degrade, and spontaneous reboots of the base station may happen. Manual setting of the Ethernet speed takes effect but is not seen on the GUI. **Workaround**: Set manually the Ethernet speed (recommended to 1000Mbps or 100Mbps Full Duplex) at both the backhaul switch and WBSn.
Downgrading to versions earlier than 1.3.2rev8 – should be done using 'Rollback'	Rollback from v1.3.2 to earlier versions (e.g. 1.0.1 or 1.1.1) should be performed using the GUI Rollback mechanism.
SNMP access to WBSn doesn't work to wireless clients (#1844)	SNMP Access is not available for wireless clients. **Workaround**: Remote log-in to a host on the backhaul interface and perform the SNMP access from that host.

Known Issue	Description
Wireless Client Isolation mode setting (#1829, #2271)	Setting parameters of the Wireless Client Isolation mode requires the parameters to be set one at a time. First enable the mode then set the backhaul interface to which the wireless clients' traffic will be forwarded. Moreover, by default and in most cases, the Ethernet interface is the backhaul interface. Set a specific VAP to be the backhaul interface only if you are absolutely sure a CPE connected on that VAP provides the backhaul.
Web Authentication Profile update (#1810)	Not all parameters from the Web-Authentication profile can be removed. **Workaround**: Remove the entire profile and create a new one.
Missing IP Address field in Association Table (#1651)	The Association table includes the IP Address field for clients that are connected with DHCP-assigned address. However, after clients disconnect and reconnect, the IP Address may be missing from the Association Table.
Blocking DHCP Server traffic (#1617)	Blocking DHCP Server traffic is possible to configure only if Wireless client isolation is enabled.
Upgrade success notification may be wrong (#1718)	On rare cases, the Upgrade process ends with 'Success' indication while the actual new firmware was not loaded. **Workaround**: Check that the desired firmware is loaded to the other bank. If not, reboot the system and repeat the Upgrade procedure

<table>
<tr><th>Known Issue</th><th>Description</th></tr>
<tr><td rowspan="2">Upgrade procedure using WavioNet</td><td>WavioNet task for firmware upgrade is efficient and useful. However, upgrading from firmware 1.3.1 to 1.3.2 may be indicated as ‘failed’, although the upgrade passed successfully.



Schedule Tasks

Task Configuration

Max Concurrent Devices [1-50]: 50

Tasks List

<table>
<tr><th>Name</th><th>Description</th><th>Start At</th><th>Last Completed</th><th>Repetition</th><th>Status</th></tr>
<tr><td>Database Backup</td><td>Periodic database backup</td><td>12:35:44 06/11/12</td><td>12:35:44 05/11/12</td><td>Every 1 Days</td><td>Successful</td></tr>
<tr><td>upgrade</td><td></td><td></td><td>11:56:02 06/11/12</td><td>Will not run again</td><td>Failed</td></tr>
<tr><td>Backup configuation</td><td></td><td></td><td>15:20:19 18/10/12</td><td>Will not run again</td><td>Failed</td></tr>
<tr><td>switch</td><td></td><td></td><td>11:52:51 06/11/12</td><td>Will not run again</td><td>Successful</td></tr>
<tr><td>thput report</td><td></td><td>12:02:29 06/11/12</td><td>11:02:29 06/11/12</td><td>Every 1 Hours</td><td>Failed</td></tr>
<tr><td>backup</td><td></td><td></td><td>12:12:25 05/11/12</td><td>Will not run again</td><td>Successful</td></tr>
<tr><td>Throughput test</td><td></td><td>17:55:33 06/11/12</td><td>17:55:33 05/11/12</td><td>Every 1 Days</td><td>Failed</td></tr>
</table>

Selected Task Status

<table>
<tr><th>Name</th><th>Status</th><th>Progress</th><th>Details</th></tr>
<tr><td>10.10.5.208 (208)</td><td>Failed</td><td>100%</td><td>Failed</td></tr>
<tr><td>10.10.2.2 (WBSn-2450-O-UN)</td><td>Failed</td><td>100%</td><td>Failed</td></tr>
<tr><td>10.10.5.206 (WBSn-2400-S)</td><td>Failed</td><td>100%</td><td>Failed</td></tr>
<tr><td>10.10.5.204 (WBSn-2400-S-US)</td><td>Failed</td><td>100%</td><td>Failed</td></tr>
</table>

</td></tr>
<tr><td><b>Workaround</b>: The following actions are needed in order to verify the status of the firmware bank:

1. Use the Inventory page to verify that version 1.3.2 is loaded on the other bank
2. Perform the ‘Swap bank’ operation
3. Use the Inventory page to verify the new 1.3.2 firmware is loaded on the desired base stations
4. In case a wrong firmware is installed, repeat the upgrade procedure as described above</td></tr>
<tr><td>ACS with automatic switch channel doesn’t keep channel across resets (#1959)</td><td>The channel switch following Automatic Channel Selection (ACS) doesn’t take effect.

<b>Workaround</b>: Run ACS without automatic channel switch. Once the ACS scan is done set manually the recommended channel. Don’t forget to press ‘Apply’ and ‘Save’ so the channel setting will be kept across reboots.</td></tr>
<tr><td>Problems with FTP sessions through WBSn in Router mode (#2241)</td><td>When using Window’s built-in FTP client for FTP sessions through WBSn in NAT-Router mode, the FTP traffic will not pass.

<b>Workaround</b>: use a different FTP client, for example Filezilla FTP client.</td></tr>
</table>

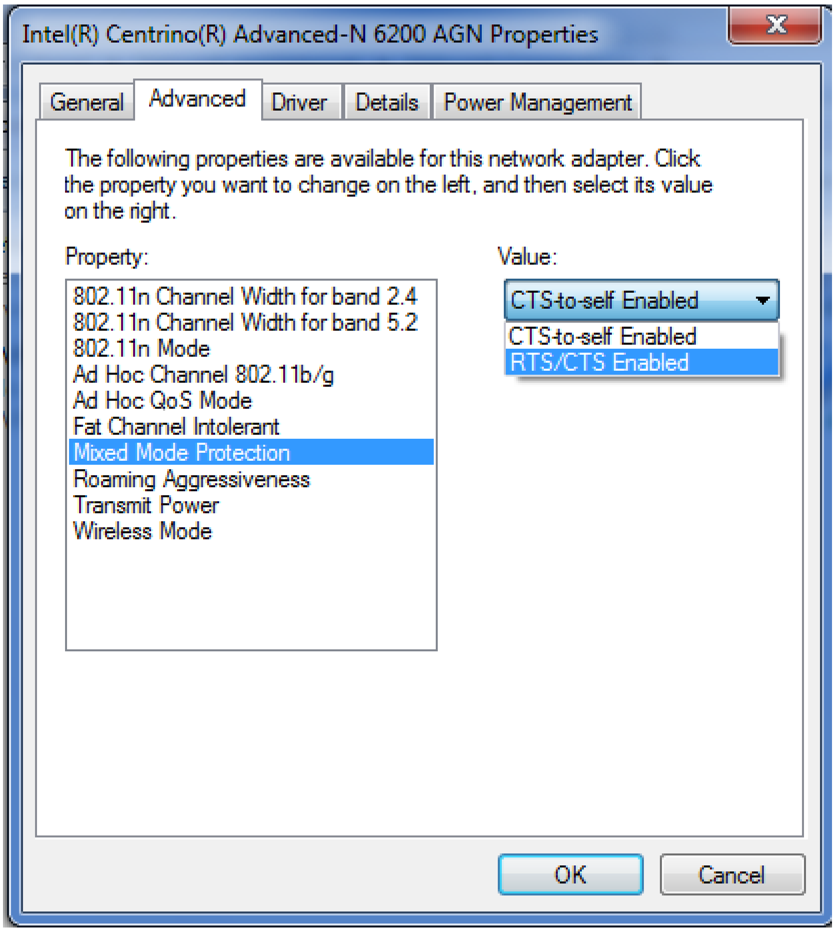
5 Best practices

For installation and configuration instructions, please refer to the WBSn User Guide. For best performances and reliable service operations, it is important to follow these instructions.

5.1 RTS threshold

To better support a CPE-based network and to provide better capacity for such network, it is highly recommended to enable the RTS/CTS option on the CPE side. In scenarios in which CPEs cannot detect each other’s transmission (far away from each other and/or in “hidden node” condition) a lower limit of the RTS Threshold parameter should be used: 256 bytes or lower.

In Enterprise network, where the network operator has access to the users’ laptops, it is recommended to enable the RTS/CTS protection on the end-user devices.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- 802.11n Channel Width for band 2.4
- 802.11n Channel Width for band 5.2
- 802.11n Mode
- Ad Hoc Channel 802.11b/g
- Ad Hoc QoS Mode
- Fat Channel Intolerant
- Mixed Mode Protection
- Roaming Aggressiveness
- Transmit Power
- Wireless Mode

Value:

CTS-to-self Enabled

- CTS-to-self Enabled
- RTS/CTS Enabled

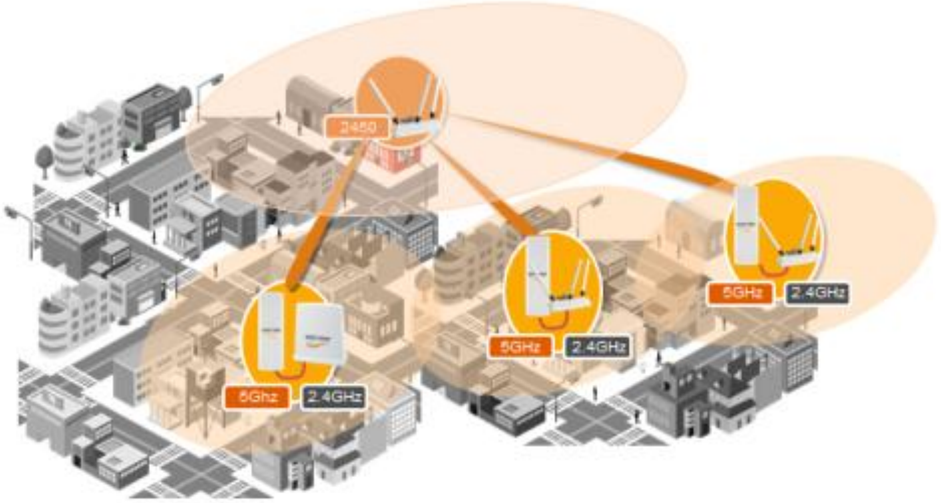
5.2 Recommended CPEs

WBSn supports standard Wi-Fi devices including smart phones, tablets and laptops equipped with Wi-Fi interfaces. When used with Wi-Fi CPEs, it is recommended that Alvarion CPEs be used for maximum performance. These include:

- WCPEn-2400-I – Alvarion indoor 802.11n 2x2 dual-zone CPE with Bridge and Router capabilities
- WCPEn-2400-U22 / WCPEn-2400-U23 – Alvarion indoor 802.11n 1x1 USB adapter for FCC/ETSI respectively.
- WCPEn-2400-O31 / WCPEn-2400-O32 – Alvarion outdoor 802.11n 1x1 CPE for FCC/ETSI regulations respectively
- WCPEn-5000-O – Alvarion outdoor 802.11n 2x2 CPE at 5 GHz.

Further CPEs for both indoor and outdoor use will be added in the coming months.

When WDS mode is required by the customer (refer to the User Manual for more information), it is recommended to use CPEs that were interoperability-tested for such a setup. In this setup, the CPEs provides the backhaul interface to remote base stations. A useful setup would use a central WBSn-2450 while 5G CPEs (such as WCPEn-5000-O) will be used to provide the backhaul.



In case such setup is being used with WCPEn-5000-O, and multiple VLANs are configured to pass through the backhaul interface, the MTU of the WBSn has to be configured to 1470 Bytes.

5.3 Export / Import Configuration

WBSn supports exporting the base station configuration, and importing it to the same or other base stations for configuration distribution. When such an operation is performed, the following procedure should be followed:

1. Export the configuration from WBSn-A and save it to a disk.

2. Import the WBSn-A configuration to WBSn-B.
3. Verify that WBSn-B works properly.
4. At this point you may also import the same WBSn-A configuration file to other base stations.

5.4 Upgrade Procedure

As newer firmware brings new features and improved capabilities, it is always recommended to follow the upgrade procedure described below in order to get up and running with the newer firmware as fast as possible:

1. Prior to performing firmware upgrade, reboot the WBSn unit (the Reboot button appears on the Administration EMS page, or as an NMS scheduled task for multiple devices)
2. Upgrade the WBSn using FTP or HTTP protocol from the EMS, or using an NMS scheduled task for multiple devices
3. Verify the new firmware appears on the Shadow bank
4. Perform ‘Switch Bank’
5. Verify the new firmware is the main firmware
6. Once the new firmware is running successfully, clean browser history (Internet options) and Java temporary files (in Control Panel Java menu), to get all new capabilities on EMS pages

6 Corrected Issues

The following table describes known issues that were corrected in this version.

Issue #	Description
#1759, #1331, #1790	Bad performance in multiple-client environments. Clients are dropped and new connections are impossible in multiple-clients environment
#1615, #1815, #1871	Traffic drop after several working hours. Dynamic Interference Handling mechanism got stuck or degradation of interference handling
#1641	Empty Performance Monitoring files (affecting Real-time and Historical graphs in the NMS)
#1107	Crash when performing ACS on large number of channels
#1431	Wrong values for Tx and Rx rates in GUI and SNMP (NMS Support)

Issue #	Description
#1418	No alarms in alarm table in case system is rebooted with Radio Off
#1396	The switch bank progress bar does not work
#1346	VLAN-interface Default GW does not appear on GUI when IP is assigned automatically
#481, #1315	No Value displayed on HTTP and SNMP interfaces regarding Ethernet speed
#1240	SNMP OID for WiFi Activity had bad value (NMS Support)
#1432	Bad Performance Monitoring (PM) files content (NMS Support)
#1433	Counters of Ethernet PPS had bad values (NMS Support)
#578, #338, #572	No indication when GUI connection to WBSn is lost
#650, #1870	Memory and CPU alarm mechanism has bad notifications. Corrected by improving the memory allocations, improving SNMP access to specific MIB tables and optimizing alarm notifications
#549	Firmware upgrade process cannot be canceled once initiated
#514	Wrong date on ACS results
#667	Mozilla (Firefox) on Win7 is not supported
#904	Proxy ARP configuration doesn’t support DHCP assigned IP Address
#461	Temperature indication on GUI was removed
#503	Firmware ‘Upgrade’ message appears twice
#1085	Upgrade process from NMS failed (on rare cases)
#489	NTP time-zone offset has no effect
#1260	Changing SNMP community by the GUI
#1868	Dual-band ACS scan through Wizard doesn’t work

Issue #	Description
#1881	Limit of maximum users per VAP – increased to maximum possible according to security (up to 256 users for Open VAP)
#1770	Wrong transmit power is set after radio is set off/on
#1409	Wrong internal parameters when range is configured higher than 1km
#2057	In rare cases, upgrade may end up with fallback to firmware on the other bank
#2002	Changing of HTTP GUI username/password access rights may end with inability to access the GUI
#1990	Change of Ethernet speed may end up losing the Management access to the unit
#1942	Change of Ethernet speed while traffic may end up with unit reboot
#1707	Changing Ethernet speed is saved only after 2nd attempt
#1964	Bad user experience even when clients are connected in good SNR (above 10dB)
#1946	Accounting-Start messages should include the IP Address of the connected clients
#1866	Number of Association in the VAP table may be wrong
#1760	System may reset if many clients (above 20) disconnect at the same time
#1731	Adding a new VLAN and a new IP Address may cause GUI freeze
#1729	Deleting WAN interface of a NAT-Router may cause unit reboot
#1626	In WPA-PSK network with many clients connected in TKIP and AES, MIC Failure may happened that causes all clients to disconnect
#1206	Wrong station RSSI may appear in Association table during stress uplink traffic
#1388	Reduced TCP performance due to wrong internal parameters

Issue #	Description
#1781	In rare cases traffic may get stuck to all clients for a period of few minutes
#435	ACS automatically switch to recommended channel
#1933	Upgrade from earlier version required manual setting to Capacity mode
#2296	Upgrade procedure fails
#1660	Small rate of Ping Loss are experienced
#584	Missing per-field check on VAP configuration page
#585	Log-in to HTTP Management Interface – may fail

7 Technical Support

To contact Alvarion's Technical Support, email support@wavionnetworks.com.