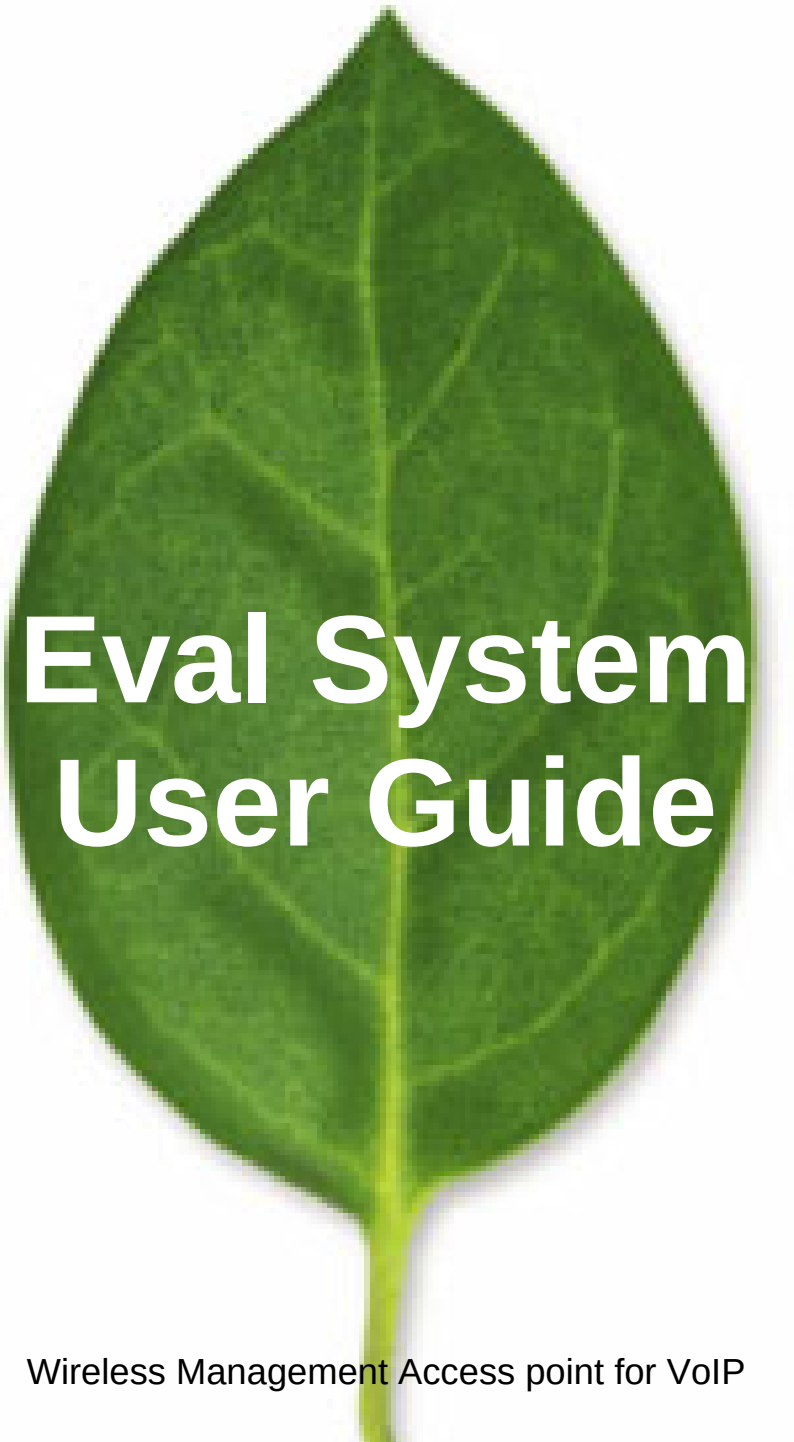


Eval System User Guide

Wireless Management Access point for VoIP

CQW-BS1000

PLANEX COMMUNICATIONS INC.

Table of Contents

1.0 Scope

This User guide is the primary document for installation and operation of the Evaluation System. It provides basic information and product background for system integrators and designers evaluating one or more of Planex's technologies related to the CQW-BS1000 Spatial Division Multiple Access (SDMA).

1.1 Guide Content

This guide contains tabletop installation instructions including:

- Selecting a site
- Connecting to power and the network
- Installing software and powering up the unit
- Changing the factory default MAC address
- Configuration
- Focusing on the web interface, including a summary of Command Line Interface (CLI) commands
- Managing the CQW-BS1000 Evaluation System via the web interface and the CLI
- Troubleshooting
- Specifications
- Glossary of important terms

2.0 Introduction

The CQW-BS1000 Evaluation System is designed to help in the testing and evaluation of the Planex CQW-BS1000, a tri-channel IEEE 802.11 MAC/BaseBand processor. The system is a complete operating three channel Access Point that can be configured as a three sector SDMA AP or a dual-band (2.4 and 5GHz) AP with a monitoring channel.

2.1 CQW-BS1000 Evaluation System Features

The CQW-BS1000 Evaluation System can operate three concurrent channels of IEEE 802.11b, g or a (or any combination) using the three sector SDMA antenna provided. Alternately, omni-directional antennas can be used for a dual-band AP with continuous monitoring. In either mode, the CQW-BS1000 Listen+Learn protocol simplifies the installation and management of one or more CQW-BS1000

Evaluation System access points by automatically configuring the channel and transmit power settings for the AP. When enabled, the CQW-BS1000 Listen+Learn protocol monitors RF activity in the environment when the access point is powered on. This monitoring process discovers other access points (both CQW-BS1000 and non-CQW-BS1000 access points) in the vicinity of the CQW-BS1000 Evaluation System. The data gathered during the monitoring process is then used to select channel and transmit-power settings that minimize interference between the CQW-BS1000 Evaluation System and other access points, resulting in increased performance of wireless data transfer through the CQW-BS1000 Evaluation System. When multiple CQW-BS1000 Evaluation Systems are connected to the same wired network, the CQW-BS1000 Evaluation Systems work cooperatively to determine the channel and transmit-power settings that provide optimal wireless data transfer performance for the wireless network.

3.0 Installation

This section contains information about proper installation of the system to maximize performance. Following these guidelines will enable the best possible results for the evaluation.

3.1 Finding the Correct Site

One of the major advantages of the CQW-BS1000 Evaluation System is that it greatly simplifies the site selection process. However, there are some guidelines that should be followed to optimize performance.

3.1.1 SDMA Capacity vs Range Mode

Although the simultaneous use of three channels is the main benefit of the sectorized antenna SDMA, it is also possible to increase range by setting all three sectors on the same channel. For maximum capacity the three sectors must be set to channel 1, channel 6 and channel 11.

3.1.2 User Distribution

As a general rule, it is a good idea to locate the CQW-BS1000 Evaluation System in the center of the distribution of users, but this assumes a fairly even distribution.

Because configuration (and reconfiguration) of the sectors is so simple, and Planex's Listen+Learn software can help with interference mitigation and load balancing, this consideration for site selection is not very critical.

3.1.3 Avoiding Reflective Surfaces

The most important concern in the selection of a mounting site is the avoidance of walls, ceilings, floors and metal surfaces close to the CQW-BS1000 Evaluation

System. These surfaces tend to reflect radio frequency (RF) signals and, if they are close, reflect strong signals. This results in a reduction of SDMA effectiveness, which means more interference and therefore poorer signal quality.

Wherever possible, keep the CQW-BS1000 Evaluation System 10-20 feet from walls. Ideally, it should be placed at a height that is equidistant from the ceiling and the floor (tabletop mount). It will work well where these goals can't be met, but where they can, performance will be better.

3.1.4 Minimizing Interference

The Planex Listen+Learn software enables the CQW-BS1000 Evaluation System to operate efficiently even in the presence of interfering signals, but when looking for the ideal site, you should avoid certain things, including:

- 802.11b, 802.11g and Bluetooth Access Points
- 2.4GHz cordless telephones
- 2.4GHz wireless cameras, area monitors, etc.
- Microwave ovens in regular use

3.1.5 Obstacles

RF signals at 2.4GHz do not easily pass through obstacles. Depending on the construction material used, walls between the CQW-BS1000 Evaluation System and the intended station(s) attenuate the signal, thereby reducing the effective range. It is always best to avoid as many walls as possible, especially if the walls have significant metal content or foil-backed insulating materials.

Signals will traverse floors or ceilings, so it is possible to cover more than one floor with a single CQW-BS1000 Evaluation System, but they do tend to be severe attenuators, and you should expect reduced range on the other side.

3.1.6 Power and Network Connections

The ideal location must also provide for power and network connections for the CQW-BS1000 Evaluation System. Because it is 802.3af compliant, a single Power over Ethernet cable will provide both. If PoE hubs are not in use, the CQW-BS1000 Evaluation System must be located where a source of AC power (for the external power supply) is available.

3.1.7 Serial Port

The serial port is RS-232C compliant. We recommend that this port be used for initial configuration and testing. Once the settings for the wired Ethernet port and

the wireless interfaces are set to work with your network, any one of them (serial port, Ethernet port, or wireless) may be used for configuration changes or AP management. Be sure that the serial port settings of the attached terminal device are the same as those of the CQW-BS1000 Evaluation System.

Table 3.1 Serial Port Settings

Item	Setting
Bit Rate	115200bps
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

3.1.8 Power-over-Ethernet Connection

When connected to an IEEE 802.3af compliant powered hub, the CQW-BS1000 Evaluation System receives all of its required power from the hub. No external power supply is required. Once the PoE cable is plugged into the CQW-BS1000 Evaluation System, the unit begins its initialization. This will take approximately one minute.

3.1.9 Using the External Power Supply

If you are not using powered Ethernet, the CQW-BS1000 Evaluation System is powered by the included external power supply. Plug the external supply into an AC source (100–250V, 50–60Hz) and plug the DC side into the CQW-BS1000 Evaluation System External Power Supply connector. The unit will begin its initialization. This will take approximately one minute.

3.1.10 Changing the Factory Default MAC Address

The CQW-BS1000's Ethernet MAC address is programmed at the factory and should not require user modification. If the user wishes to change the factory default MAC address to a user-specific MAC address, the serial interface must be used. After setting up the serial interface as specified in Serial Port above, follow the procedure given below to change the MAC address.

1. Power cycle the AP.
2. When it begins to boot, press <Ctrl><C> simultaneously (bootloader prompt appears).
3. Execute the following command to set the MAC Address of the Ethernet port.

set_npe_mac -p 0 xx:xx:xx:xx:xx:xx<Enter> (xx:xx:xx:xx:xx:xx is the MAC address)

4. Power cycle the AP. The new MAC address should take effect.
5. The wireless interface MAC addresses should also be updated.

4.0 Configuration and Operation

This section discusses the configuration and operation of the CQW-BS1000 Evaluation System.

4.1 Default Settings

The table below displays the settings contained in the **defaults** configuration file, and therefore represents the state of the system at initial startup.

Table 4.1 CQW-BS1000 Evaluation System Default Configuration Settings

AP	
Parameter	**Setting**
Boot Configuration File	defaults
Country Code	Off

AP Security Mode	Legacy-clear
VLAN ID	1
VLAN Priority	0
Open System Authentication	On
Open System 802.1X Authentication	Off
Shared Key Authentication	Off
Shared Key 802.1X Authentication	Off
802.1X Authentication	Off
WPA Authentication	Off
WEP Key Length	64
WEP Key Select	1
WEP Key #1	31:32:33:34:35
WEP Key #2	31:32:33:34:35
WEP Key #3	31:32:33:34:35
WEP Key #4	31:32:33:34:35
WPA Cipher Suites	tkip
WPA Key Management Suite	dot1x
WPA Shared Key	wpa-passkey
Allow Wireless AP Management	On
MAC Filter Status	Off
MAC Filter Default Access	Allowed
Telnet	Off

Wireless Sectors			
Parameter	**Sector 1 Setting**	**Sector 2 Setting**	**Sector 3 Setting**
Sector Status	Started	Started	Started
SSID	BEK	BEK	BEK
Channel	1	6	11
RX Sensitivity (NIC Dependent)	High	High	High
Maxrate	54	54	54
Automatic Rate Adjustment	On	On	On
Basic Rates	1,2,5.5,11	1,2,5.5,11	1,2,5.5,11
RTS	Off	Off	Off
RTS Threshold	2346	2346	2346
Self CTS	Off	Off	Off
Fragmentation	Off	Off	Off
Fragmentation Threshold	2346	2346	2346
Txpower	7	7	7
Auto Transmit Power Adjustment	Off	Off	Off
Beacon Interval	100	100	100
Header Type	Long	Long	Long
Auto Transmit Power Adjustment	Off	Off	Off
Backhaul	Off	Off	Off
Backhaul VLAN Dot1Q Tagging	Off	Off	Off
Broadcast Public SSID	On	On	On
Allow only 802.11g Clients	Off	Off	Off
Allow All-OFDM Basic Rate	Off	Off	Off

TCPIP	
Parameter	**Setting**
Subsystem Status	Started
IP Address	192.168.1.1
Net Mask	255.255.255.0
Gateway Address	0.0.0.0
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0
DHCP Client	Off
Ethernet	
Parameter	**Setting**
Port Status	Started
Speed	Auto
Auto-Negotiation	On
Full Duplex Mode	Auto
Flow Control	On
VLAN 802.1Q Tagged	Off
DHCP	
Parameter	**Setting**
Subsystem Status	Stopped
Leasetime	86400
DNS	192.168.1.242
Domain	bandspeed.com
Subnet Mask	255.255.255.0
Broadcast Address	192.168.1.255
Router	192.168.1.241
Address Start	192.168.1.100
Address End	192.168.1.110
IP Range Comment	The Main IP Range.

RADIUS	
Parameter	**Setting**
Subsystem Status	Stopped
IP Address	192.168.1.250
Port	1812
Reauthentication Timeout	3600
Reauthentication Status	Disabled
Authentication Retries	2
Authentication Retry Interval	60
Key Cache Time	
Secret Key	
HTTP Server	
Parameter	**Setting**
HTTP Server	Enabled
WLAN Access	Enabled
Ethernet Access	Enabled
Port Number	80
Listen And Learn	
Parameter	**Setting**
Auto Configuration/LnL	Off
Auto Configuration Status	Stopped
Mode	Sector
Monitor NIC	2
2Ghz_NIC	1
5Ghz_NIC	3

4.2 Command Line Interface

This section explains the Command Line Interface (CLI) used with the CQW-BS1000 Evaluation System.

Note: Although the CLI can be used to change settings while the CQW-BS1000 Evaluation System is running, we recommend that it be stopped before making changes and restarted once the changes have been made. Changes

do not take affect until the system is restarted. The system uses NICs that require significant processor power while running, which limits the time available to the CLI and causes it to miss occasional characters.

4.2.1 Command Conventions

The commands are shown using the following conventions:

- Triangular brackets (< >) indicate a required choice.
- Square brackets ([ ]) indicate optional items.
- Vertical bars (|) separate mutually exclusive choices.
- **Boldface** indicates commands and keywords that are entered exactly as shown.
- *Italics* indicate values that must be supplied by you.

Examples:

- Examples show screen displays and the command line in the screen font.
- Information you need to enter in examples are shown in **boldface** font.
- Variables that you must supply are shown in *italic* font.

Selecting a menu item (or screen) is indicated by the following convention:

- Click Start>Settings>Control Panel.

4.2.2 Getting Started

When the CQW-BS1000 Evaluation System completes its initialization following power up, the terminal equipment attached to the serial port will display a login prompt. Type **admin** and press Enter, then enter **Bandspeed** for the password and press Enter again. This will bring the prompt **BEK>**. The system can now be configured, operated, and managed using the CLI.

4.2.3 Commands

This section describes the commands provided by the CQW-BS1000 Evaluation System Command Line Interface (CLI). These commands can be used to modify the CQW-BS1000 Evaluation system configuration.

Configuration changes made to the CQW-BS1000 Evaluation System can be saved to a configuration using the **save** command described in section 4.2.3.2. The configuration file used to boot the can be selected using the **bootconfig** command described in section 4.2.3.7.

IMPORTANT NOTE: To keep the system configuration persistent between power reset cycles, the **save** command described in section 4.2.3.2 must be used before doing a power cycle reset otherwise the configuration will be lost.

4.2.3.1 Help

help delete

help get [bootconfig | ethernet | tcpip | ap | sector | stations | stats | radius | switch | http | snmp | version | log | autoconfig | dfs | tpc | rrm]

help list

help load

help reset

help save

help set [bootconfig | ethernet | tcpip | ap | sector | radius | switch | http | snmp | autoconfig | dfs | tpc |rrm]

help start

help stop

4.2.3.2 Password

passwd – Change the administrator password.

4.2.3.3 Save

save <*cfg_filename*> – Create and save a configuration file containing the currently active configuration.

4.2.3.4 Delete

delete <*cfg_filename*> – Delete a configuration file.

4.2.3.5 List

list – List all configuration files.

4.2.3.6 Load

load <*cfg_filename*> – Load a configuration file that was previously created using the **save** command. The AP must be stopped using the **stop ap** command prior to using the **load** command. After the **load** command has been issued, the **start ap** command must be issued to restart the AP.

4.2.3.7 Bootconfig

get bootconfig – Display the boot configuration file for next boot.

set bootconfig <*cfg_filename*> - Select the configuration file used to boot the CQW-BS1000 Evaluation system. The change takes effect on the next system boot.

4.2.3.8 Start

start [ap | eth | sector<1|2|3|*> | tcpip | dhcp | http | autoconfig | radius | snmp | dfs]

4.2.3.8 Stop

stop [ap | eth | sector<1|2|3|*> | tcpip | dhcp | http | autoconfig | radius | snmp | dfs]

4.2.3.9 Reset

reset - this command resets the AP system.

4.2.3.9 Sector

get sector* - Get all sectors status.

get sector<1|2|3> ssid - Get sector ssid.

get sector<1|2|3> bssid – Get per-sector broadcast ssid status.

get sector<1|2|3> channel - Get channel number.

get sector<1|2|3> maxrate - Get sector max rate.

get sector<1|2|3> basicrate – Get sector basic rate setting.

get sector<1|2|3> sensitivity – get sector RX sensitivity.

get sector<1|2|3> rts – Get RTS setting (enabled/disabled).

get sector<1|2|3> cts – Get self-CTS setting (enabled/disabled)

get sector<1|2|3> frag - Get frag

get sector<1|2|3> txpower – Get Tx power.

get sector<1|2|3> beacon - Get beacon interval.

get sector<1|2|3> header - Get header type.

get sector<1|2|3> mode – displays operating mode 11G, 11A, 11BG or 11B.

get sector<1|2|3> diversity – displays antenna diversity.

get sector<1|2|3> dpd – displays Digital Pre-Distortion configuration of sector baseband.

Set Sector*X* sets the specified parameter for the sector number used for *X*, where *X* is 1-3. The selected parameter is set for all sectors if sector* is used with this command.

There are no commands specifically to set 802.11g mode or 802.11a mode. To set a sector to 802.11g mode, the sector maxrate is set to an 802.11g data rate (6, 9, 12, 18, 24, 36, 48 or 54) with the sector channel set to a 2.4GHz channel (1 – 11). To set 802.11a mode, the sector channel must be set to a standard 802.11a channel (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157 or 161). An attempt to set an illegal

combination, i.e., 802.11a maxrate with 802.11b channel, will result in an error message.

set sector<1|2|3|*> ssid <ssid_name> - Set sector ssid.

set sector<1|2|3|*> mode [11B|11BG|11G|11A] - Set the sector's radio band. For 2.4Ghz band, select the type(s) of stations allowed to associate.

set sector<1|2|3|*> channel <channel_number> - Set channel number.

For 802.11b and 802.11g the channel_number selections are 1 – 11.

For 802.11a the channel_numbers selections are 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157 or 161.

set sector[X] bssid [enable|disable] – Turn per-sector broadcast ssid on or off

set sector<1|2|3|*> maxrate <rate_value> [auto | fixed] - Set max rate.

For 802.11b the maxrate rate_values are 1, 2, 5.5 or 11

For 802.11g and 802.11a the maxrate rate_values are 6, 9, 12, 18, 24, 36, 48 or 54

set sector<1|2|3|*> basicrate <rate_value1> <rate_value2>… - set basic rate.

For 802.11b the basicrate rate_values are 1, 2, 5.5, 11.

For 802.11g and 802.11a the basicrate rate_values are 6, 9, 12, 18, 24, 36, 48, 54.

set sector<1|2|3|*> sensitivity [high | medium | low] - set RX sensitivity

set sector<1|2|3|*> rts [*rts_value*] [enable | disable] – Set RTS; usable values are 256 - 2346.

set sector<1|2|3|*> frag [*frag_value*] [on | off] – Set frag; usable values are 256 – 2346.

set sector<1|2|3|*> txpower [<*tx_power_value*>] | [auto] | [fixed] | [max54]] – Set Tx power in dbm unit; usable values are 0 – 20. The max54 sets the transmit power to the maximum level that can achieve a 54Mbps datarate.

set sector<1|2|3|*> beacon <*beacon_interval*> - Set beacon interval; usable values are 20 - 1000.

set sector<1|2|3|*> header [short | long | both] – Set header.

set sector<1|2|3|*> allofdmbasic [enable | disable] – enable or disable all OFDM rates as basic rate.

set sector<1|2|3|*> diversity [antenna1 | antenna2 | both] – Set antenna diversity per-sector basis.

set sector<1|2|3|*> dpd [enable | disable] – Enable or disable Digital Pre-Distortion per sector basis.

set sector<1|2|3|*> radiomeasure [enable | disable] – Enable or disable radio measurement feature.

start sector<1|2|3|*> - starts the selected sector.

stop sector<1|2|3|*> - stops the selected sector.

4.2.3.10 AP

get ap macaddr – Get AP MAC address

get ap filter – Get the MAC address filter settings

set ap filter enable – Enable MACaddress filtering

set ap filter Disable – Disable MAC address filtering

set ap filter allow – Set default to allow listed MAC addresses

set ap filter disallow – Set default to disallow listed MAC addresses

set ap filter xx:xx:xx:xx:xx:xx [allow | disallow | clear] – Add/delete MAC address lists

allow: Add the MAC address to the allowed list

disallow: Add the MAC address to the disallowed list

clean: Delete the MAC address from the lists

set ap sessiontimeout <timeoutvalue> – Set login session timeout

get ap sessiontimeout – Get login session timeout

4.2.3.11 TCPIP

get tcpip – Get current settings for the TCP/IP stack.

Example:

```
TCPIP Subsystem Configuration and Status
=======================================
Subsystem Status ................... : Started
IP Address ......................... : 10.1.4.85
Subnet Mask ........................ : 255.255.255.0
Gateway Address .................... : 10.1.4.1
Primary DNS Address ................ : 10.1.1.1
Secondary DNS Address .............. : 10.1.1.2
DHCP Client ........................ : On
```

get tcpip ipaddr - Get IP address for the AP. *Ex. 10.1.4.85.*

get tcpip netmask - Get the subnet mask for the AP. *Ex. 255.255.255.0.*

get tcpip gateway - Get gateway router address used by AP. *Ex. 10.1.4.1.*

get tcpip dns - Get address(es) of DNS servers to be used by AP.

get tcpip dhcp - Get DHCP client setting for AP.

set tcpip ipaddr <ip_address> - Statically assign IP address for the AP.

set tcpip netmask <net_mask> - Set the subnet mask for the AP.

set tcpip gateway <gateway_address> - Set the gateway router address to be used for forwarding packets not on the subnet.

set tcpip dns <pri_dns_address> [<sec_dns_address>] – Set DNS server address(es) to be used by the AP.

set tcpip dhcp [enable | disable] – Set DHCP to enable/disable. If set to *enable* the AP will use a DHCP client to obtain its IP address. If set to *disable* the AP will use the statically assigned IP address you specify.

4.2.3.12 Ethernet

get ethernet – Get Ethernet configuration parameters.

Example:

```
Ethernet Port Configuration and Status
======================================
Port Status ....................... : Started
Auto Negotiation .................. : On
Speed ............................. : Auto
Full Duplex Mode .................. : Auto
Flow Control ...................... : On
VLAN 802.1Q Tagged ................ : Off

Link Status:
Link .............................. : Up
Linked Speed ...................... : 100
Linked Duplex ..................... : Half
```

get ethernet link – Get Ethernet link status. Includes up/down status, link speed in Mbps, and duplexing status.

Example:

```
Link Status:
Link ............................... : Up
Linked Speed ....................... : 100
Linked Duplex ...................... : Half
```

get ethernet stats – Get Ethernet statistics.

Example:

```
Ethernet Statistics:
====================================
Tx Packet Count .................... : 88
Rx Packet Count .................... : 4639417
Tx Error Packet Count .............. : 0
Rx Error Packet Count .............. : 0
Missing Packet Count ............... : 0
Frame Aligment Error Count ......... : 3
Tx Collision Count ................. : 2
Tx Multiple Collision Count ........ : 0
PHY Rx Packet Count ................ : 4636508
PHY Rx Broadcast Packet Count ...... : 1166
PHY Rx Multicast Packet Count ...... : 2909
Tx Abort Packet Count .............. : 0
Tx Underrun Packet Count ........... : 0
```

get ethernet speed - Get Ethernet data rate in Mbps.

get ethernet duplex - Get Ethernet duplexing status, i.e. half or full.

get ethernet auto - Get Ethernet auto-negotiation setting.

set ethernet speed [10 | 100 | 1000] – Set Ethernet data rate to 10Mbps/100Mbps/1000Mbps.

set ethernet duplex [enable | disable] – Set Ethernet duplexing to full/half. This is dependant on the type of Ethernet network you will be connecting to.

set ethernet auto [enable | disable] – Set Ethernet auto-negotiation enable/disable. Autonegotiation determines duplex/data rate settings automatically so you don’t have to specify them.

set eth dot1q [enable | disable] - enable/disable 802.1Q VLAN tagging on Ethernet port.

4.2.3.13 DHCP

get dhcp – Get current parameters for the DHCP server.

Example:

```
DHCP Server Configuration and Status
=====================================
Subsystem Status ..... : Stopped
Lease Time ........... : 86400
DNS .................. : 10.1.2.1 10.1.2.2
Domain ............... : bandspeed.com
Subnet Mask .......... : 255.255.255.0
Broadcast Address .... : 192.168.1.255
Router ............... : 192.168.1.1
Start IP Address ..... : 192.168.1.10
End IP Address ....... : 192.168.1.254
Range Comment......... : The Main IP Range.
```

get dhcp leasetime – Get current DHCP lease time in seconds.

get dhcp dns – Get addresses of current DNS servers to be used by DHCP.

get dhcp domain – Get the domain currently associated with DHCP.

get dhcp netmask – Get the subnet mask associated with the DHCP address space.

get dhcp broadcast – Get the broadcast address for DHCP.

get dhcp router – Get the address of the default gateway (router) to be used by DHCP clients.

get dhcp range – Get the IP range to be used for DHCP-assigned addresses.

set dhcp - Display DHCP parameters that can be set.

set dhcp leasetime <int> - Set the DHCP lease time in seconds.

set dhcp dns <dns ip addr1> [dns ip addr2] – Set DNS server IP addresses to be used by DHCP (maximum two, minimum one). When specifying two addresses, the addresses must be separated by a space.

set dhcp domain <domain name or ip> – Set domain for DHCP. The domain name can be a conventional domain name such as “bandspeed.com” or an IP address such as “12.23.34.100”.

set dhcp netmask <IP addr> – Set the subnet mask for DHCP.

set dhcp broadcast <IP address> – set the broadcast address for DHCP.

set dhcp router <string, "12.23.34.45 12.23.34.200"> – Set the gateway router to be used by DHCP clients.

set dhcp range <IP addr start> <IP addr end> - Set the IP address range for assignment to DHCP clients.

set dhcp range comment <string> – Set comments for DHCP IP address range.

4.2.3.14 Listen and Learn (LnL)

By default, AutoConfig/LnL is disabled on the system. In this default condition the basic AP functionality will be exactly the same as a standard AP. AutoConfig/LnL must be enabled by the user for it to be operational. This is set as the default to simplify certification testing.

set <autoconfig|lnl> <enable | disable> – enable or disable the AutoConfig/LnL on the wireless access point. Enable AutoConfig/LnL is only the initial step before starting the AutoConfig/LnL. LnL is still not running, it is only enabled. Note: if AutoConfig/LnL is running, ‘stop <autoconfig|lnl>’ must be executed before ‘set <autoconfig|lnl> off ‘ can be run. Otherwise, an error message will be returned.

set <autoconfig|lnl> mode <sector|omni> – set the operational mode of AutoConfig/LnL on the wireless access point (sector – AutoConfig/LnL will be running in SDMA mode, omni – AutoConfig/LnL will be running in omni-directional access point mode).

set <autoconfig|lnl> monitor_nic <nic_number> – configure the NIC on the wireless access point will be the monitoring NIC when AutoConfig/LnL is running on omni-directional access point.

set <autoconfig|lnl> 2ghz_nic <nic_number> – configure the NIC on the wireless access point will be the access NIC in 2 GHz band when AutoConfig/LnL is running on omni-directional access point.

set <autoconfig|lnl> 5ghz_nic <nic_number> – configure the NIC on the wireless access point will be the access NIC in 5GHz band when AutoConfig/LnL is running on omni-directional access point.

set <autoconfig|lnl> metric <1> – configure channel selection metric policy setting. 1) Sum RSSI-based.

set <autoconfig|lnl> config <1> – configure channel configuration policy setting. 1) Pre-defined sequence/rotation-based channel configuration.

set <autoconfig|lnl> smooth <1|2> – configure channel adaptation smoothing algorism policysetting. 1) No channel adaptation with any station associated. 2) No channel adaptation if number of stations associated is greater than threshold.

set <autoconfig|lnl> sta_thresh <1:100> – configure channel adaptation smoothing algorism threshold.
set <autoconfig|lnl> feedback <1> – configure dynamic transmit power control feedback policy setting. 1) Transmit power control closed-loop feedback.

set <autoconfig|lnl> coop <1|2> – configure interference mitigation policy setting. 1) Minimize interference with only L&L capable APs 2) Minimize interference with all APs in vicinity.

set <autoconfig|lnl> sdma <1> – configure channel scanning policy setting in SDMA mode. 1) Initial full all-sector scan only.

get <autoconfig|lnl> - get the summary of all the configuration of AutoConfig/LnL.

get <autoconfig|lnl> mode – get the current mode of AutoConfig/LnL. It is either ‘sector’ or ‘omni’ (sector – AutoConfig/LnL will be running in SDMA mode, omni – AutoConfig/LnL will be running in omni-directional access point mode).

get <autoconfig|lnl> monitor_nic – get the NIC will be monitoring NIC when AutoConfig/LnL runs in omni-directional access point mode.

get <autoconfig|lnl> 2ghz_nic – get the NIC will be access NIC in 2 GHz band when AutoConfig/LnL runs in omni-directional access point mode.

get <autoconfig|lnl> 5ghz_nic – get the NIC will be access NIC in 5 GHz band when AutoConfig/LnL runs in omni-directional access point mode.

get <autoconfig|lnl> metric – get the channel selection metric policy setting.

get <autoconfig|lnl> config – get the channel configuration policy setting.

get <autoconfig|lnl> smooth – get the channel adaptation smoothing algorism policysetting.

get <autoconfig|lnl> sta_thresh – get the channel adaptation smoothing algorism threshold.

get <autoconfig|lnl> feedback – get the dynamic transmit power control feedback policy setting.

get <autoconfig|lnl> coop – get the interference mitigation policy setting.

get <autoconfig|lnl> sdma – get the channel scanning policy setting in SDMA mode.

start <autoconfig|lnl> - start AutoConfig/LnL on the access point. Note: 'set <autoconfig|lnl> on' must be executed before this command can be run, otherwise, an error message will be returned.

stop <autoconfig|lnl> - stop AutoConfig/LnL on the access point.

Note: When AutoConfig/LnL is running, the following wireless command will return error messages. The reason is the system design doesn't allow user intervention in setting wireless RF parameters when AutoConfig/LnL is running.

Examples

To start AutoConfig/LnL in SDMA mode from a default system configuration

set autoconfig enable
set autoconfig mode sector
start autoconfig

To start AutoConfig/LnL in OMNI mode from a default system configuration

set autoconfig enable
set autoconfig mode omni
start autoconfig

To stop and disable AutoConfig/LnL when AutoConfig/LnL is running

stop autoconfig

set autoconfig disable

4.2.3.15 HTTP Server

get http – get all HTTP parameters

get http wlanaccess – display Ethernet access

get http ethaccess – display Ethernet access

get http port – display port number

set http [enable | disable] – set HTTP state

set http port <int> - set port number

Note: WEP is enabled when either **open enencryp** or **share enencryp** is set; disabled when both **open disencryp** and **share disencryp** are set.

4.2.3.16 Security

This section lists CLI commands used to display and configure the CQW-BS1000 Evaluation System security features.

The following commands display and modify the global security settings for the AP.

set ap security [legacy-clear|legacy-encrypt|wpa|wpa2|wpa+wpa2|tsn]

Sets the global security mode for the AP. The following table shows the type of wireless stations allowed to associate for each security mode.

Security Mode	No Security	WEP STA	WPA STA	WPA2 STA
legacy-clear	Y	N	N	N
legacy-encrypt	N	Y	N	N
wpa	N	N	Y	N
wpa2	N	N	N	Y
wpa+wpa2	N	N	Y	Y
tsn	N	Y	Y	Y

get ap security - Displays the selected security mode.

The following commands are used to display and modify security settings when the CQW-BS1000 Evaluation System is configured for legacy-encrypt mode.

set ap keylength [64|128] – Sets static WEP key length (64-bit or 128-bit).

set ap wepkey<1|2|3|4> ascii <string> - Sets the static WEP key(1-4) value with an ASCII string.

set ap wepkey<1|2|3|4> hex <hex_string> - Set the static WEP key(1-4) value with a hex string.

set ap keyselect <1|2|3|4> - Selects the static WEP key to be used for packet transmission.

get ap keylength - Displays the static WEP key length.

get ap keyselect - Displays the static WEP key index used for encrypting packets prior to transmission.

The following commands are used to display and modify security settings when the CQW-BS1000 Evaluation System is configured for the wpa, wpa2, wpa+wpa2, or tsn security modes.

set ap wpa cipher [wep64 | wep128 | tkip | ccmp] – Set the type of cipher to be used to encrypt unicast cipher suite supported by the AP.

set ap wpa keymanagement [dot1x | psk] - set key management suite support by the AP.

set ap wpa-psk ascii <string> - set WPA PSK with an ASCII string.

set ap wpa-psk hex <hex_string> - set WPA PSK with a hex string.

get ap wpa - display the WPA security configuration.

4.2.3.17 Stations

get stations – Get current associated client stations and statistics for each station.

4.2.3.18 Authentication (RADIUS) Server

get radius - get all parameters for RADIUS server configuration
get radius ip - get RADIUS IP address
get radius port - get RADIUS port number
get radius key - get RADIUS secret key. The key is displayed as *****
get radius keycachetime - get RADIUS key cache time
get radius timeout - get RADIUS re-authentication time
get radius retries - get RADIUS authentication retries
get radius interval - get RADIUS authentication retry interval
get radius reauthentication - get re-authentication enable

Encryption setting for Open System authentication and Shared Key authentication should be both either enabled or disabled. Otherwise undefined behaviors could happen and cause problems for the association of wireless client to the Gypsy AP. The problem is caused by the inability of wireless client to choose the authentication method to associate.

set radius ip <IP address "12.23.34.45"> - set RADIUS ip address
set radius port <int> - set RADIUS port
set radius key - set RADIUS secret key. CLI prompts user for the key. The key is displayed as *****
set radius keycachetime - set RADIUS key cache time.
set radius timeout <int> - set RADIUS re-authentication timeout

set radius retries <int> - set RADIUS authentication retries

set radius interval <int> - set RADIUS authentication retry interval

set radius reauthentication [enable | disable] - set re-authentication enable

4.2.3.19 Wireless Backhaul

The CQW-BS1000 Evaluation System supports point to point wireless backhaul between one CQW-BS1000 Evaluation System root device and one CQW-BS1000 Evaluation System repeater device. The root device is the system will be connected to the Ethernet wired network. The repeater device is the system that the wireless station will associate to. This network configuration allows extending the range of signal coverage without the cost of deploying wired connection to the repeater device.

IMPORANT NOTE: The **secure** option for wireless backhaul connection is not very stable for this release, the **nosecure** option is recommended to be used for evaluating this feature.

set sectorX backhaul [enable | disable] – enable/disable wireless backhaul on sector X.

set sectorX backhaul [root | repeater] - set sector X to “root” mode or “repeater” mode. Root mode is for the central distribution system; repeater for the remote system.

set sectorX backhaul ssid <string> - set SSID used to setup wireless backhaul link.

set sectorX backhaul passphrase <string> - set passphrase to encrypt the wireless backhaul link, this has to be the same on both repeater and root.

set sectorX dot1q [enable | disable] – enable/disable 802.1Q VLAN tagging on the wireless backhaul on the sector X.

set sectorX backhaul [secure | nosecure] – set sector X backhaul connection to use encryption or not to use encryption.

get sectorX backhaul - display configurations of wireless backhaul on the sector X.

get sectorX dot1q – diplay configuration of 802.1Q VLAN tagging on the wireless backhaul on the sector X.

get sectorX bhstats – display status of wireless backhaul on sector X

Example:

To setup a wireless backhaul connection, connect the root device to the Ethernet network with a CAT5 cable. Leave the repeater device disconnected from the Ethernet network.

On the root device, enter the following commands:

set sector3 channel 64
set sector3 backhaul enable
set sector3 backhaul root
set sector3 backhaul ssid backhaultest
set sector3 backhaul passphrase secret

set sector3 dot1q disable
set sector3 backhaul nosecure

On the repeater device, enter the following commands:

stop eth
set sector1 channel 64
set sector1 backhaul enable
set sector1 backhaul repeater
set sector1 backhaul ssid backhaultest
set sector1 backhaul passphrase secret
set sector1 dot1q disable
set sector1 backhaul nosecure

Use the following command to check the backhaul status on the root device:

get sector3 bhstats

4.2.3.20 SSID and VLAN

The CQW-BS1000 Evaluation System supports multiple SSIDs. For each SSID, the BSP maintains a separate SSID configuration. Each SSID configuration contains one or more SSID name(s), the SSID security settings, and the SSID VLAN settings for the SSID. There are two types of SSIDs: a Public SSID and a Private SSIDs.
A Public SSID is an SSID that is advertised in each sector's beacon frames. The CQW-BS1000 Evaluation System supports one Public SSID configuration. The Public SSID cannot be deleted. With the Public SSID, a unique SSID name can be assigned to each sector. The Public SSID VLAN and security settings, however, are the same for all sectors.
The CQW-BS1000 Evaluation System supports zero or more Private SSIDs to be configured. Private SSIDs are not advertised in beacon frames. Private SSIDs use the same SSID name on all sectors. Private SSID VLAN and security settings are the same for all sectors.

The following commands are used to modify the Public SSID settings.

set ap sectorssid vlan <vlan_id> - Assigns a VLAN_ID to the Public SSID. Any station associated with the Public SSID will be on the VLAN with vlan_id.

set ap sectorssid vlan_priority <int> - Set VLAN priority for the Public SSID VLAN. The default VLAN is used for stations associated to the SSID broadcast by a sector.

set ap sectorssid wpa [enable | disable] - Enable/disable WPA authentication and key management with the Public SSID.

set ap sectorssid open [enable | disable] [en-dot1x|dis-dot1x] - Enable/disable Open System authentication with Public SSID; Enable/disable 802.1X authentication requirement with Public SSID.

set ap sectorssid shared [enable | disable] [en-dot1x|dis-dot1x] - Enable/disable Shared Key authentication with the Public SSID; Enable/disable 802.1X authentication requirement with Public SSID.

set ap sectorssid dot1x [enable | disable] - Enable/disable 802.1X authentication with the Public SSID.

get ap sectorssid – Display the Public SSID configuration settings.

The following commands are used to create and configure Private SSIDs.

set ap ssid <ssid_name> [enable | disable] - Add/delete a new Private SSID on the AP.

set ap ssid <ssid_name> vlan <vlan_id> - Assigns a VLAN_ID to a Private SSID. Any station that associates with a Private SSID will be on the VLAN with vlan_id.

set ap ssid <ssid_name> vlan_priority <priority> - Set VLAN packet priority on the selected VLAN. Valid priorities are

0-7.

set ap ssid <ssid_name> open [enable | disable] [en-dot1x | dis-dot1x] - Enable/disable Open System authentication with a Private SSID; Enable/disable 802.1X authentication requirement with a Private SSID.

set ap ssid <ssid_name> shared [enable | disable] [en-dot1x|dis-dot1x] - Enable/disable Shared Key authentication with a Private SSID; Enable/disable 802.1X authentication requirement with a Private SSID.

set ap ssid <ssid_name> dot1x [enable | disable] - Enable/disable 802.1X authentication with a Private SSID.

set ap ssid <ssid_name> wpa [enable | disable] - Enable/disable WPA authentication and key management with a Private SSID.

get ap ssid – Display the list of Private SSIDs defined.

get ap ssid <ssid_name> - Display configuration settings for a Private SSID.

4.2.3.21 SNMP Server

get snmp – display SNMP configuration settings
get snmp wlanaccess – display wlan access
get snmp ethaccess – display Ethernet access
get snmp name - display system name string
get snmp location - display system location string
get snmp admin - display admin contact info string
get snmp rwstring - display read-write community string
get snmp rostring - display read-only community string
get snmp trapip - display trap IP address

set snmp [**enable|disable**] – set SNMP state
set snmp wlanaccess [**enable|disable**] – set wlan access
set snmp ethnaccess [**enable|disable**] – set Ethernet access
set snmp name <**string**> - set system name string
set snmp location <**string**> - set system location string

set snmp admin <**string**> - set admin contact info string
set snmp rwstring <**string**> - set read-write community string
set snmp rostring <**string**> - set read-only community string
set snmp trapip <**x.x.x.x**> - set trap IP address

4.2.3.22 Country Code

set ap country [off|US (USA)|CN (China)|FR (France)

|AU (Australia)|KR (Korea)|JP (Japan)|CA (Canada)|BR (Brazil)

|MX (Mexico)|AT (Austria)|BE (Belgium)|HK (Hong Kong)

|NZ (New England)|TW (Taiwan)|GB (UK)|DE (Germany)|IE (Ireland)

|IT (Italy)|NL (Netherlands)|PT (Portugal)|DK (Denmark)

|FI (Finland)|NO (Norway)|SE (Sweden)|SG (Singapore)|CH (Switzerland)]

[I(Indoor) O(Outdoor) otherwise (Indoor/Outdoor)]

System has to be power reset after changing country code.

Examples

set ap country CH - set China Indoor/Outdoor

set ap country USI - set US Indoor

set ap country GBO - set UK Outdoor

get ap country – displays the selected country code

4.2.3.23 Spectrum Management

set sector<1|2|3|*> specmgmt <enable | disable> – make spectrum management enable or disable on a per-sector basis

set sector<1|2|3> chansw <channel> <count> - causes a sector to switch channels and the count is the number of **T**arget **B**eacon **T**ransmission **T**imes until the channel switch is to take place.

set sector<1|2|3> quiet <count> <duration> - causes a sector to stop transmitting, including beacons and count is the number of **T**arget **B**eacon **T**ransmission **T**imes until the quiet interval is to take place. The duration is the number of **T**ime **U**nits that the quiet interval is to last. A TU is 1024 microseconds. Note that the sector will continue to receive traffic, especially in the case where promiscuous mode is enabled on the sector. Neither the host driver nor the MAC firmware will transmit anything during this period.

set sector<1|2|3> quiet <count> <duration> <STA MAC address> – same as the command above except that this is for remote measurement.

Notes:

channel (required)is the channel to perform the measurement on

delay (required) is the time until the start of the measurement interval (TUs)

duration (required)is the length of the measurement interval(TUs)

MACAddress (optional)is the MAC address of the STA that will perform the measurement. It is local measurement if no MACAddress is set

4.2.3.24 DYNAMIC FREQUENCY SELECTION (DFS)

start dfs – start the dfs periodic measurement

stop dfs – stop the dfs periodic measurement

set sector<1|2|3|*> dfs localmeasure <enable | disable> – enable/disable the promiscuous mode in the sector so as to accept/reject the abort frames.

set sector<1|2|3|*> dfs remote measure <enable | disable> – enable/disable internal sending of the measurement request to remote associated stations.

set dfs measurement remote period <period> – set the time interval between the end and start of DFS measurement procedure in seconds.

set dfs measurement remote interval <interval> – set the time interval between each successive measurement request sent to the stations in seconds.

set dfs measurement remote duration <duration> – set the duration for which the measurement should be carried out by the station in seconds.

set dfs measurement remote starttime <start time> – set the time to start the measurement after the station receives the measurement request.

set dfs channelswitch count <count> - sets the value after which the channelswitch is to take place in TBTTs.

set dfs default - load all the default values for the DFS parameters

get dfs – get the current values of all the DFS parameters

get dfs measurement local – get the status of DFS local measurement

get dfs measurement Remote – get the status of DFS remote measurement

get dfs measurement remote period – get the value of DFS measurement remote period

get dfs measurement remote interval – get the value of DFS measurement remote interval

get dfs measurement remote duration – get the value of DFS measurement remote duration

get dfs measurement remote starttime – get the value of DFS measurement remote start time

get dfs channelswitch count - get the value DFS channelswitch count

get dfs default - get the default values of DFS parameters

4.2.3.25 TRANSMIT POWER CONTROL (TPC)

set tpc localmaxtxpower <channel> <maxpower> – set the local maximum power for a particular channel permitted in the regulatory domain.

get tpc – get the local maximum power set for the all the channels in the current regulatory domain.

get tpc <channel> – get the local maximum power set for the specified channel in the current regulatory domain.

4.2.3.26 RADIO RESOURCE MEASUREMENT (RRM)

get sector<1|2|3> rrmreport channelload <channel> [STA MAC address] - issue channel load measurement request and retrieves report. Station Address is optional, It can be Unicast/broadcast/multicast address. If station address is not given, then it is considered to be a local measurement.

get sector<1|2|3> rrmreport noisehistogram <channel> [STA MAC Address] - issue noise histogram measurement request and retrieves

report. Station Address is optional, It can be Unicast/broadcast/multicast address. If station address is not given, then it is considered to be a local measurement.

get sector<1|2|3> rrmreport frame <channel> [STA MAC Address] - issue frame measurement request and retrieves report. Station Address is optional, It can be Unicast/broadcast/multicast address. If station address is not given, then it is considered to be a local measurement.

get sector<1|2|3> rrmreport hiddennode <channel> [STA MAC Address] – issue hidden node measurement request and retrieves report. Station Address is optional, It can be Unicast/broadcast/multicast address. If station address is not given, then it is considered to be a local measurement.

get sector<1|2|3> rrmreport statistics <channel> [STA MAC Address] – issue Station statistics measurement request and retrieves report. Station Address is optional, It can be Unicast/broadcast/multicast address. If station address is not given, then it is considered to be a local measurement.

get sector<1|2|3> rrmreport beacon <**active|passive|table**> **<channel> [STA MAC Address]** – issue Beacon measurement request and retrieves report. Station Address is optional, It can be Unicast/broadcast/multicast address. If station address is not given, then it is considered to be a local measurement.

get sector<1|2|3> rrmreport mediumsensing <ccaidle|ccabusy|navbusy> <channel> [STA MAC Address] – issue Medium Sensing measurement request and retrieves report. Station Address is optional, It can be Unicast/broadcast/multicast address. If station address is not given, then it is considered to be a local measurement.

get sector<1|2|3> rrmreport neighbor – retrieve neighbor report locally.

get rrm report <tokennumber> – retrieve the received report for the given token number.

get rrm tokens - retrieve all the tokens for the transmitted but not timedout measurement request.

set rrm beacon interval <interval> - set the Randomization Interval.

set rrm beacon duration <duration> - set the measuremet duration.

set rrm beacon period <period>[m|s|t] - set the measurement period, m – msec. s-seconds t – TU, Default is TU.

set rrm beacon measurement_interval <interval>[m|s|t] - set the measurement Interval m – msec. s-seconds t - TU, Default is TU.

set rrm beacon condition <condn> - set the condition.

set rrm beacon threshold <threshold> - set threshold.

set rrm beacon hystersis <hystersis> - set hystersis.

set rrm beacon bssid <BSSID> - set BSSID.

get rrm beacon - get the current values.

set rrm mediumsensing interval <interval> - set the Randomization Interval.

set rrm mediumsensing duration <duration> - set the measuremet duration.

set rrm mediumsensing rpithreshold <threshold> - set RPI threshold.

set rrm mediumsensing binoffset <bin offset> - set Bin Offset.

set rrm mediumsensing binduration <bin duration> - set bin duration.

set rrm mediumsensing bins <bins> - set the number of bins.

get rrm mediumsensing – get the current values.

set rrm frame interval <interval> - set the Randomization Interval.

set rrm frame duration <duration> - set the measuremet duration.

get rrm frame – get the current values.

set rrm noisehistogram interval <interval> - set the Randomization Interval.

set rrm noisehistogram duration <duration> - set the measuremet duration.

get rrm noisehistogram – get the current values.

set rrm channelload interval <interval> - set the Randomization Interval.

set rrm channelload duration <duration> - set the measuremet duration.

get rrm channelload – get the current values.

set rrm hiddennode interval <interval> - set the Randomization Interval.

set rrm hiddennode duration <duration> - set the measuremet duration.

get rrm hiddennode – get the current values.

set rrm statistics interval <interval> - set the Randomization Interval.

set rrm statistics duration <duration> - set the measuremet duration.

get rrm statistics
abstract – get the current values

set rrm threshold <threshold> – set the threshold for the request to be blocking or non-blocking in seconds.

set rrm reportttl <expiration time> - report time to live in the list, ie. the expiry time after the measurement timeout in seconds.

4.2.3.27 Quality of Service (QoS)

Qos control

set qos [enable|disable] – enable/disable 802.11e QOS on Access Point.

set qos qbssload [enable|disable] – enable/disable QBSS Load IE.

get qos qbssload – display qbssload.

get qos – display 802.11e QOS configuration.

EDCA parameters for class of service

set qos be ecwmin <0-15> - set minimum contention window for best effort class of service.

set qos be ecwmax <0-15> - set maximum contention window for best effort class of service.

set qos be aifsn <0-15> - set number of defer slots for best effort class of service.

Set qos be txop [11b|11ag] <range> -set txop limit for different mode for best effort class of service.

set qos be default – set all parameters for best effort class of service to default settings.

get qos be – displays all parameters for best effort class of service.

set qos bk ecwmin <0-15> - set minimum contention window for background class of service.

set qos bk ecwmax <0-15> - set maximum contention window for background class of service.

set qos bk aifsn <0-15> - set number of defer slots for background class of service.

Set qos bk txop [11b|11ag] <range> -set txop limit for different mode for background class of service.

set qos bk default – set all parameters for background class of service to default settings.

get qos bk – displays all parameters for background class of service.

set qos vi ecwmin <0-15> - set minimum contention window for video class of service.

set qos vi ecwmax <0-15> - set maximum contention window for video class of service.

set qos vi aifsn <0-15> - set number of defer slots for video class of service.

Set qos vi txop [11b|11ag] <range> -set txop limit for different mode for video class of service.

set qos vi default – set all parameters for video class of service to default settings.

get qos vi – displays all parameters for video class of service.

set qos vo ecwmin <0-15> - set minimum contention window for voice class of service.

set qos vo ecwmax <0-15> - set maximum contention window for voice class of service.

set qos vo aifsn <0-15> - set number of defer slots for voice class of service.

Set qos vo txop [11b|11ag] <range> -set txop limit for different mode for voice class of service.

set qos vo default – set all parameters for voice class of service to default settings.

get qos vo – displays all parameters for voice class of service.

Admission Control

set qos acm [enable|disable] – enable/disable Admission Control for 802.11 Qos.

get qos acm – displays Admission Control setting.

Frame classification

set qos ip_protocol <int> [be|bk|vi|vo|disable] – set a frame classification based on IP protocol field in the IP header to a class of service (be – best effort, bk – background, vi – video, vo – voice,

disable - clear a frame classification based on IP protocol field in the IP header).

get qos ip_protocol - Displays the configured values for different types of data streams.

set qos ip_dscp <0-63> [be|bk|vi|vo|disable] – set a frame classification based on IP DSPC value in TOS field of IP header to a class of service (be – best effort, bk – background, vi – video, vo – voice, disable - clear a frame classification based on IP DSCP value in TOS field of IP header).

get qos ip_dscp - Displays the configured values for different types of data streams.

set qos ip_precedence <0-7> [be|bk|vi|vo|disable] – set a frame classification based on IP precedence value in TOS field of IP header to a class of service (be – best effort, bk – background, vi – video, vo – voice, disable - clear a frame classification based on IP precedence value in TOS field of IP header).

get qos ip_precedence - Displays the configured values for different types of data streams.

set qos mapping [vlan | ip_dscp | both] – Apply QoS based on vlan id`s or ip_dscp values or via both.

get qos mapping – Displays whether the current mapping is done based on vlan id`s or ip_dscp values or both.

Action Frames

set qos blockack immediate [enable|disable] – set/reset Immediate Block Ack.

get qos blockack immediate - Displays whether immediate Blockack is enabled or not.

set qos blockack delayed [enable|disable] – set/reset Delayed Block Ack.

get qos blockack delayed – Displays whether Delayed Blockack is enabled or not.

set qos blockack timeout <int> – sets the block ack timeout.

get qos blockack timeout – Displays Blockack Timeout.

set qos addba_timeout <int> – set the AddBA Response Timeout.

get qos addba_timeout - Displays AddBA response timeout

set qos addts_timeout <int>– set the AddTS Response Timeout.

get qos addts_timeout – Displays AddTS Response timeout.

set qos qap_retrylimit <int> - set the Missing Ack Retry limit.

set qos dls [enable|disable] – Allow/Disallow DLS in QBSS.

get qos dls – Displays whether Dls is enabled or disabled.

Operations

set qos chan_util_bcn_interval <int> - set the Channel Utilization Beacon Interval.

**get qos chan_util_bcn_interval - ** displays the Channel Utilization Beacon Interval.

4.2.4 Firmware Update

The CQW-BS1000 Evaluation System includes a utility to manage the firmware update process, which uses the Trivial File Transport Protocol (TFTP) to upload the revised firmware. The following describes the procedure for performing the update:

The flash update uses a TFTP client on the AP to download the new firmware image from a TFTP server on the network.

4.2.4.1 Update from the Command Line

1. Setup a TFTP server on either a Linux or Windows system and connect it to the network.
2. Copy three image files (XXX_ixp425-le-gnu_waps.jffs2, XXX_ixp425-le-gnu_rootfs.jffs2, and XXX_ixp425-le-gnu_kernel.bin, where XXX is the build number) to the TFTP server directory (/tftpboot on Linux).
3. Start the AP and configure its IP address so it can reach the TFTP server.
4. Type **flash** at the AP command line prompt (**IXP425**>).
5. Type **y** when asked to confirm the flash update.
6. Enter the TFTP server's IP address followed by **enter** when asked.
7. Enter XXX (where XXX is the build number) followed by **enter** when asked for the version number.
8. **Programming Firmware. This will take about 1 minutes. Please wait** will be displayed. Wait for it to finish.
9. If the update failed, an error message will be display. Please check the TFTP server's IP address, build number, and network connection before trying it again.
10. If the update is successful, please power the CQW-BS1000 Evaluation System off and then on. The next boot will use the newly installed image.

4.2.4.2 Update from the Web Interface

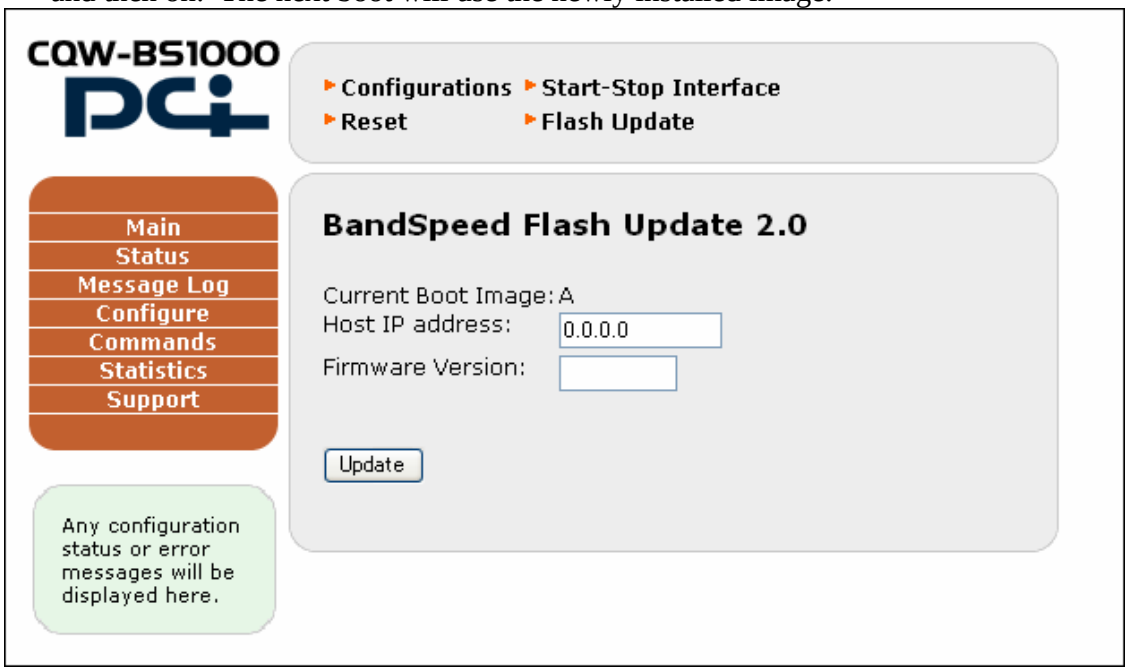
1. Setup a TFTP server on either a Linux or Windows system and connect it to the network.

2. Copy three image files (XXX_ixp425-le-gnu_waps.jffs2, XXX_ixp425-le-gnu_rootfs.jffs2, and XXX_ixp425-le-gnu_kernel.bin, where XXX is the build number) to the TFTP server directory (/tftpboot on Linux).
3. Start the AP and configure its IP address so it can reach the TFTP server.
4. Launch the web brower
5. Connect to the AP by typing in the IP address of the AP in the browser
6. Log into the Ap via web interface when prompted. (NOTE: password is case-sensitive)

   Login: admin

   Password: Bandspeed

7. Navigate and select Commands->Flash Update
8. Type TFTP server IP address into the **Host IP address** slot
9. Type XXX build number into the **Firmware Version** slot
10. Click on the **Update** button
11. If the update is successful, please power the CQW-BS1000 Evaluation System off and then on. The next boot will use the newly installed image.



4.2.4.3 Update from via RedBoot

At time if the previous flash image is damage, it may be necessary to flash back to the last known image via RedBoot

1. Setup a TFTP server on either a Linux or Windows system and connect it to the network.
2. Copy three image files (XXX_ixp425-le-gnu_waps.jffs2, XXX_ixp425-le-gnu_rootfs.jffs2, and XXX_ixp425-le-gnu_kernel.bin, where XXX is the build number) to the TFTP server directory (/tftpboot on Linux).
3. Reboot the AP and press Control-C immediately to get in the RedBoot screen

4. **Type flash –l <*local IP address*> –h <*TFTP server IP address*> -t XXX** (at the **RedBoot**> prompt) where local IP address is any static IP address available on the same subnet with the TFTP server.
5. Once the firmware update is completed, the AP should automatically reboot itself.
6. The AP is now operational.

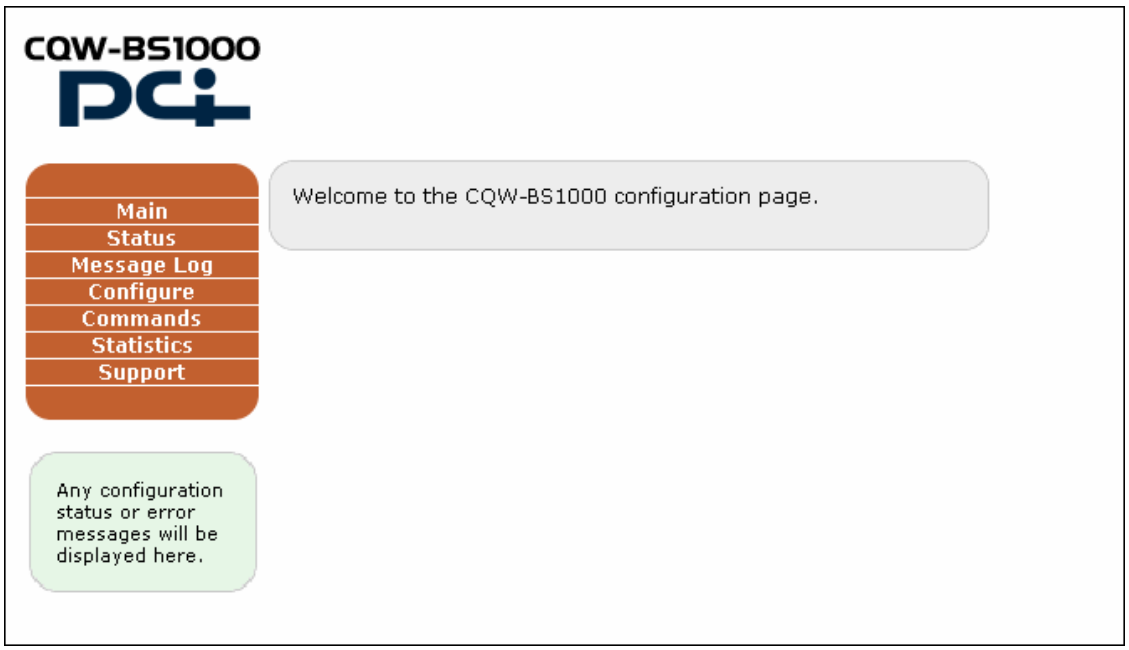
4.3 Web Interface

The Web interface provides the simplest means for configuring and managing the CQW-BS1000 Evaluation System. You can access it through the wired Ethernet connection or the wireless interface. The IP address of the client device (Ethernet NIC or wireless NIC) should be set to an address in the same subnet as the CQW-BS1000 Evaluation System, (e.g., if the CQW-BS1000 Evaluation System is set to IP address 192.168.1.1, the NIC should be set to 192.168.1.x, where x is a number between 2 and 255, so that the full IP address does not conflict with another device in the subnet).

Open a Web browser and enter the address of the CQW-BS1000 Evaluation System (e.g., http://192.168.1.1). A login and password are required to access the system, as shown in Figure 4.1. The defaults are login: admin and password: Bandspeed.(password is case-sensitive) This connects to the CQW-BS1000 Evaluation System Web interface, and the main screen displays, as shown in

Figure 4.1 Login Window

Figure 4.2 CQW-BS1000 Evaluation System Main Window



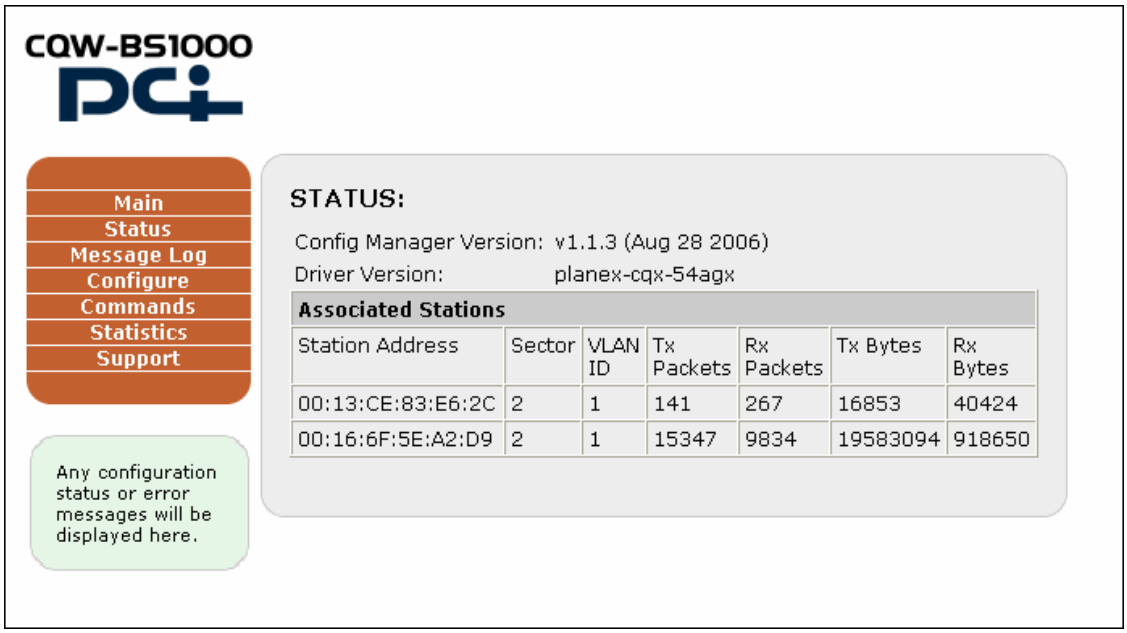
The box on the left side of the screen is the main menu. The **Status** window provides information about the current system version numbers, and about the associated stations and sector-by-sector throughput information. Access basic system configuration via **Configure**. The **Commands** option allows you to set and change the configuration files, and contains controls for starting and stopping all system interfaces as well as a system reset button. While the CQW-BS1000 Evaluation System is in operation, statistics are being captured and can be accessed from the **Statistics** window. The **Support** page provides links to the online Help files and the Bandspeed Web site, and contains the link for updating system firmware.

The Web interface is designed for easy customization, enabling OEMs to change the look and feel to match their own equipment interfaces.

4.3.1 The Status Page

The Status page displays the current system status.

Figure 4.4 Status Page



The **Status** page displays software and firmware versions, and the status of the stations associated with the CQW-BS1000 Evaluation System.

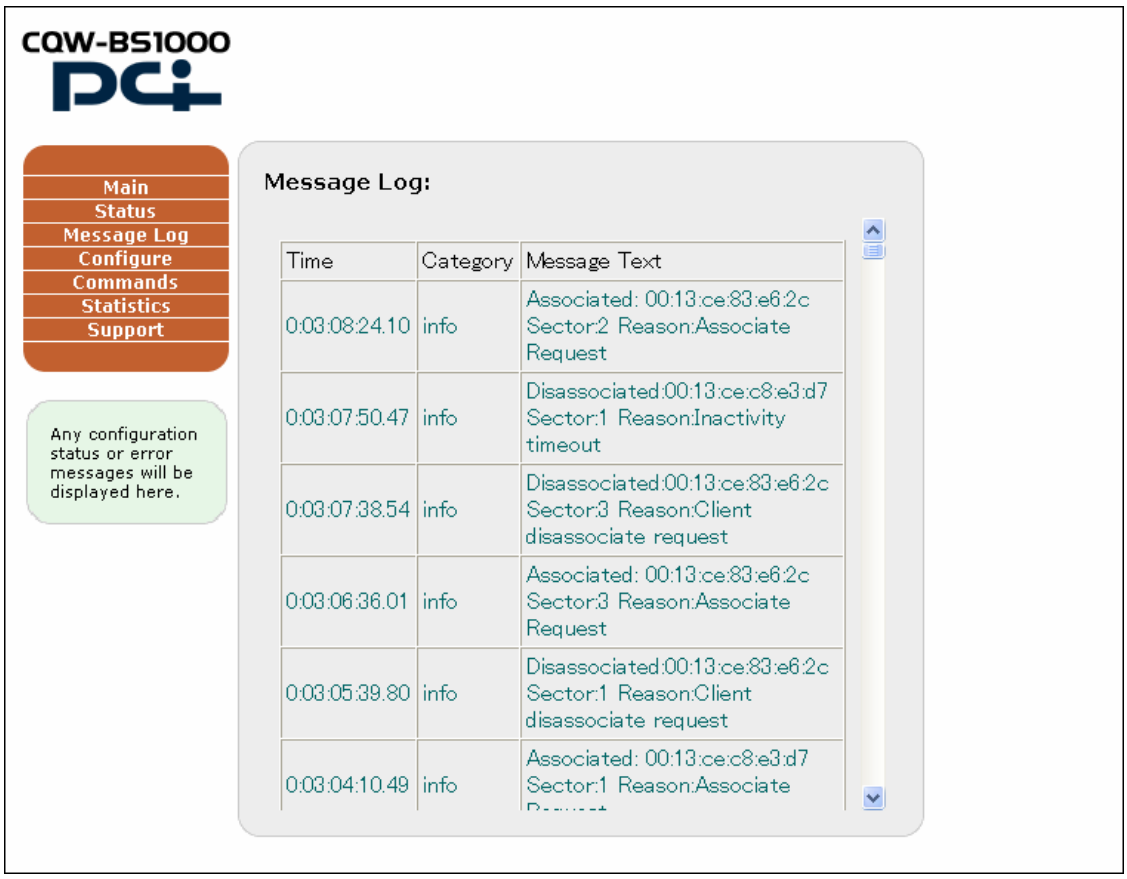
4.3.2 The Message Log

The message log page displays events that are captured during the startup and operation of the CQW-BS1000 Evaluation System. Table 4.1 lists all of the possible messages with the message category. The time shown in the log represents the time since the last power-on, in *days:hours:minutes:seconds.hundredths.* Figure 4.4 shows a typical message log shortly after system startup.

Table 4.1 Message Log Information

Category	Message
information	Station "MAC" associated with sector "X".
information	Station "MAC" disassociated with sector "X" due to: "Y".
information	Station "MAC" denied authentication on sector "X" due to: "Z"
information	Station "MAC" denied association on sector "X" due to: "Z"
information	Backhaul link established between "MAC" on channel X
warning	Backhaul link disconnected.
information	Access point running firmware version "VERSION"
information	HTTP server started.
warning	HTTP server failed to start.
information	SNMP server started.
warning	SNMP server failed to start.
information	TCP/IP stack started with address "X"
warning	Failed to connect with DHCP server.
warning	TCP/IP stack failed to start due to IP address conflict.
information	DHCP server started.
warning	DHCP server failed to start due to: "Y"
warning	Sector "X" failed to start due to: "Y".
information	RADIUS server started.
warning	RADIUS server failed to start due to: "Y"
error	Failed to conect to radius server "IP Address"
information	Link established on ethernet port at "X speed"
warning	Link lost on ethernet port.
information	Access point started.
warning	Access point failed to start due to: "Y"
information	Auto configuration started.
information	Auto configuration completed.
error	Auto configuration failed to complete due to "Y"
error	"Error X occurred that should never occur."
information	Station "MAC" reassociated with sector "X".
information	Sector "X" started.
information	Sector "X" stopped.
information	Link established on ethernet port.
information	Ethernet auto negotiated "X" speed" and "Y" duplex mode.
information	Ethernet forced to "X" speed and "Y" duplex mode
warning	TKIP MIC error in packet received from station "X"

Figure 4.5 Message Log Display



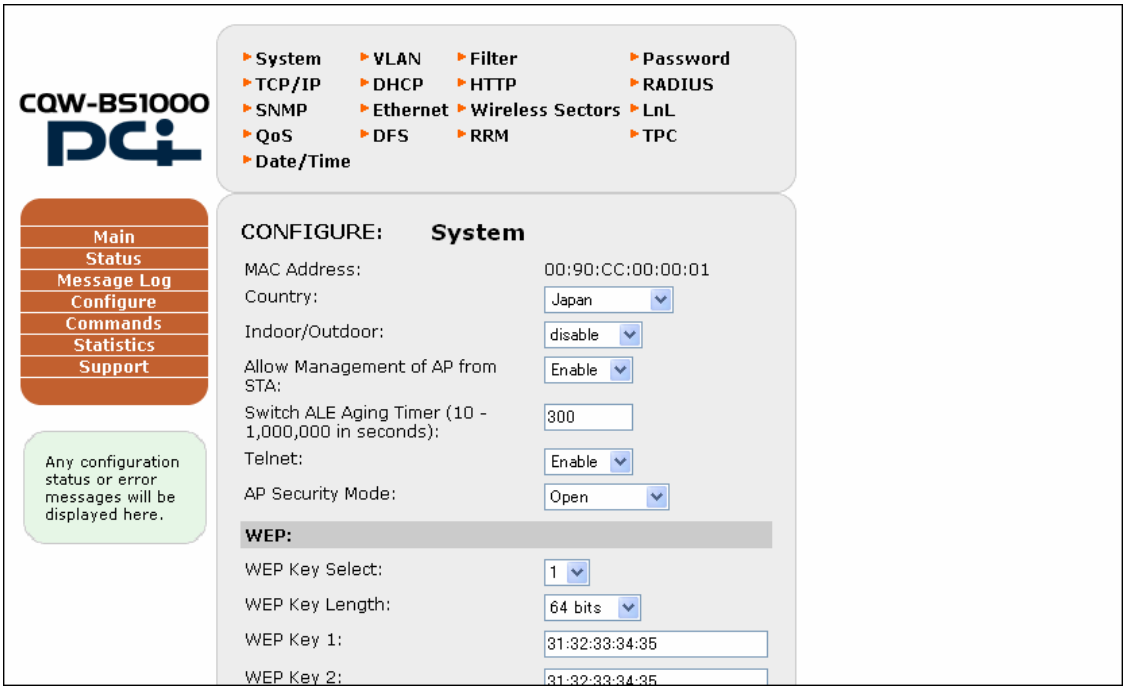
4.3.3 Configure Menu

The **Configure** menu has fourteen submenus that group system configuration into logical categories:

- System
- SSID/Security/VLAN
- Filter
- Password
- TCP/IP
- DHCP
- HTTP
- RADIUS
- SNMP
- Ethernet
- Wireless Sectors
- Listen and Learn
- QoS
- DFS
- RRM
- TPC
- Date and Time.

Configure - System :

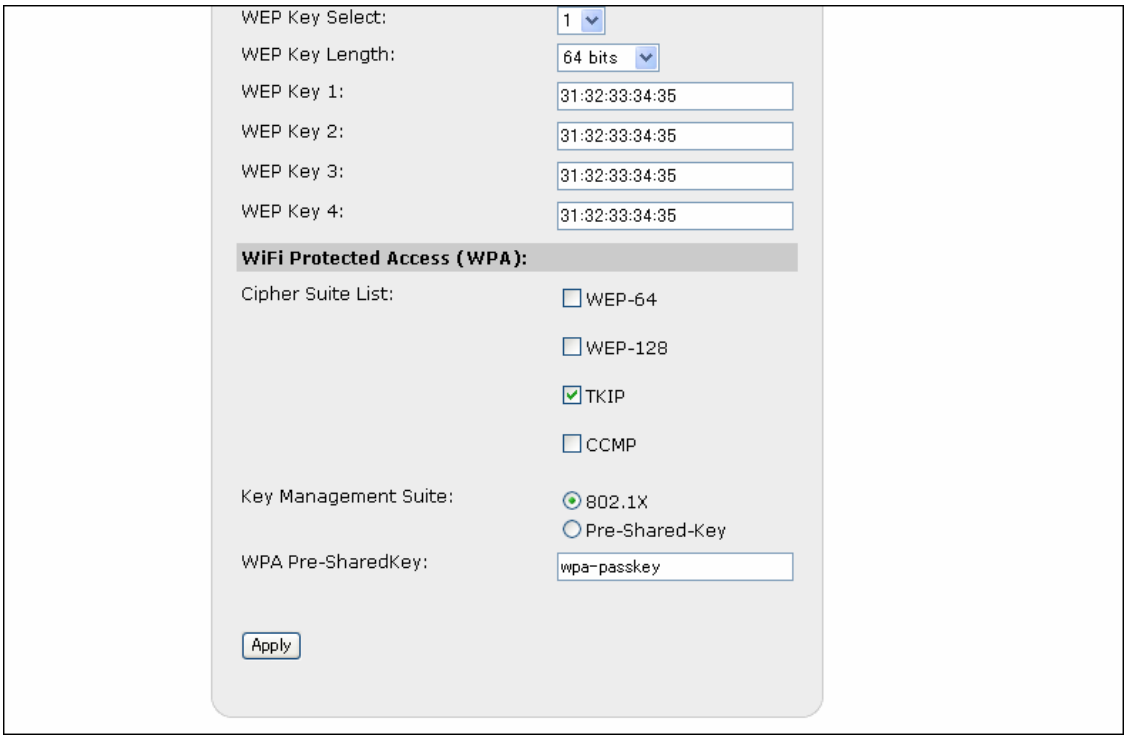
Figure 4.6a Configure System Window (Top Portion)



The **Configure>System** menu includes the auto-configuration setting, and all of the authentication and security settings. The **Mode** menu includes selections for **Range** or **Capacity**. This determines the sector preferences during auto-configuration, for support for either range mode (3-channel mode) or capacity mode (6-channel mode).

The **AP Security Mode** drop-down menu includes settings for Open (authenticate only stations with no security enabled), WEP (authenticate only stations with WEP enabled), **WPA-Only** (authenticate only stations with WPA enabled), WPA2, WPA+WPA2 (authenticate only stations with WPA or WPA2 enabled) or **TSN** (Transition Security Network – authenticates stations regardless of security mechanism used).

Figure 4.6b Configure System Window (bottom section)



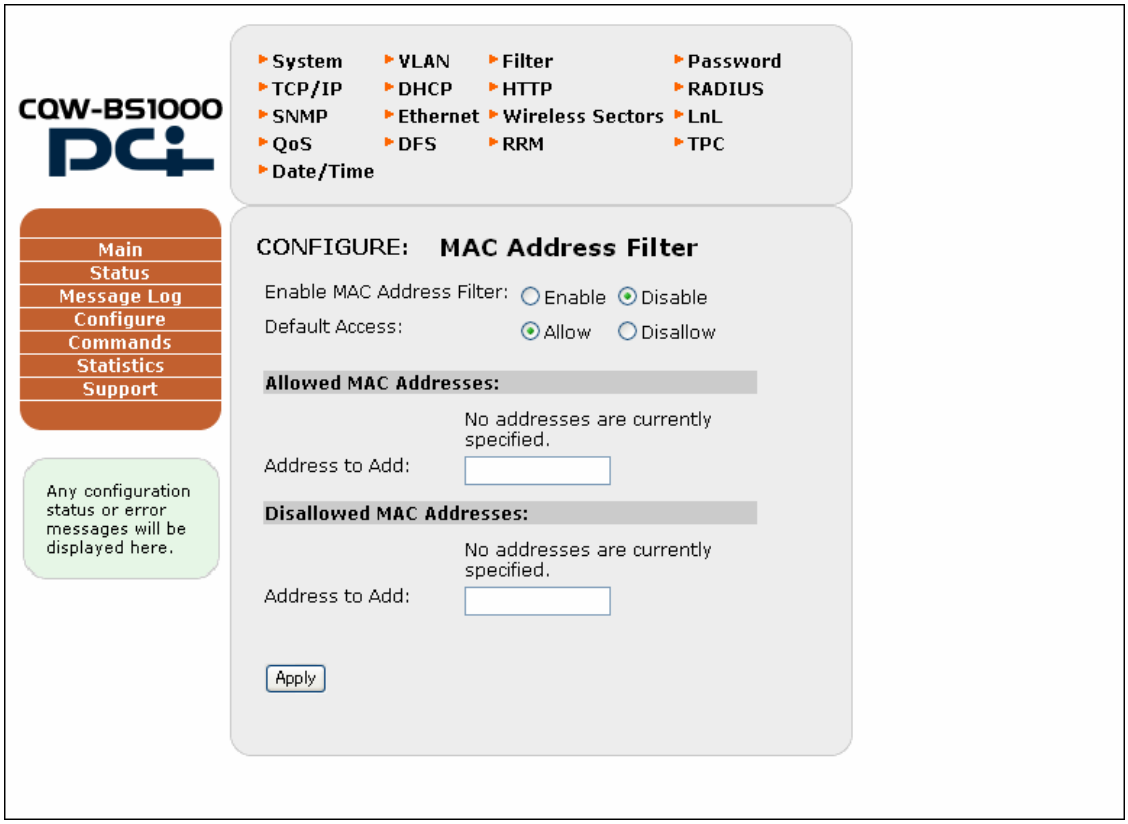
Configure - SSID/Security/VLAN :

Figure 4.7 Configure SSID/Security/VLAN Window

The **Configure>SSID/Security/VLAN** window includes all of the settings used for setting VLAN configuration.

Configure - Filter :

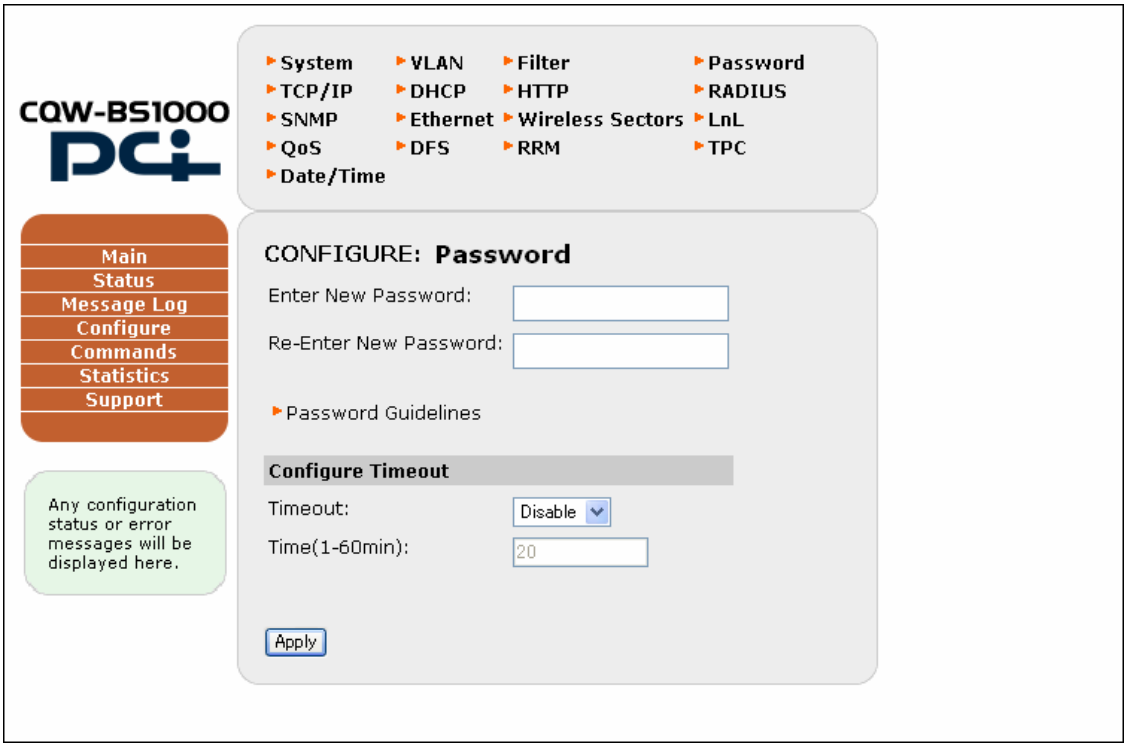
Figure 4.8 Configure Filter Window



The **Configure>Filter** window allows you to select MAC addresses to allow or to block (disallow).

Configure - Password :

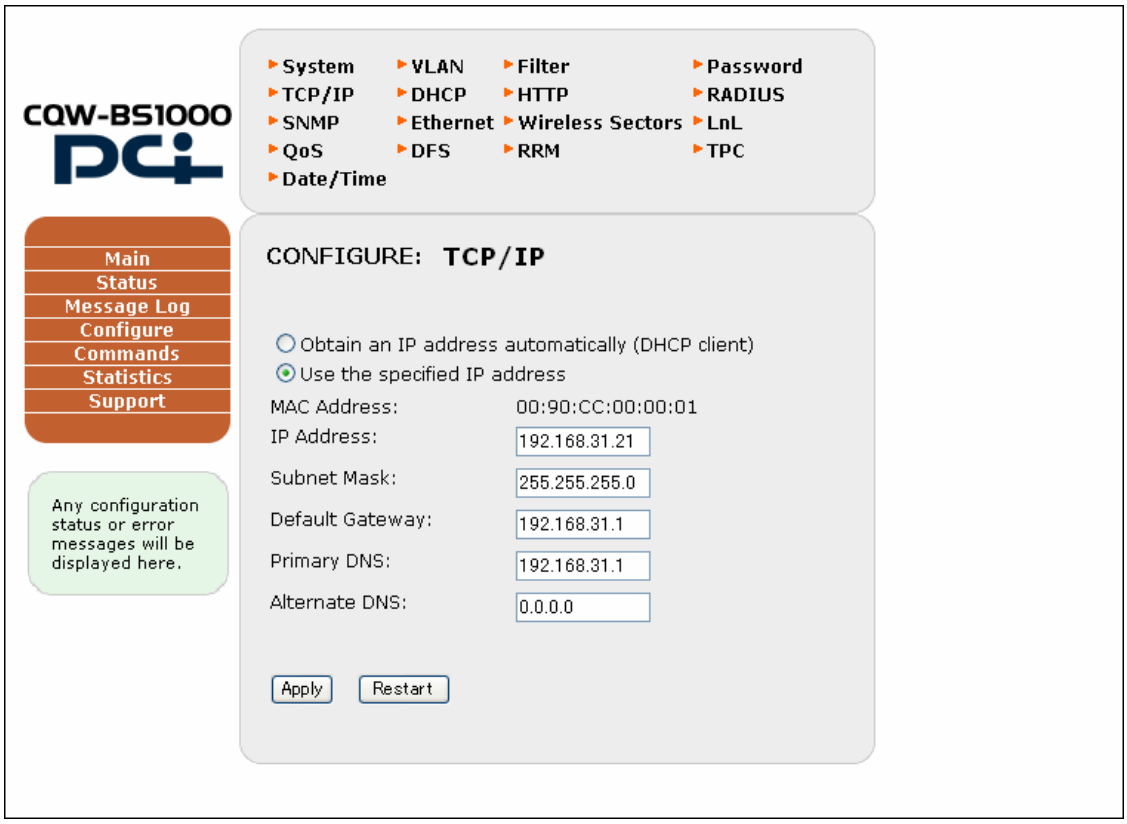
Figure 4.9 Configure Password Window



The Configure>Password window allows you to change the default password.

Configure - TCP/IP :

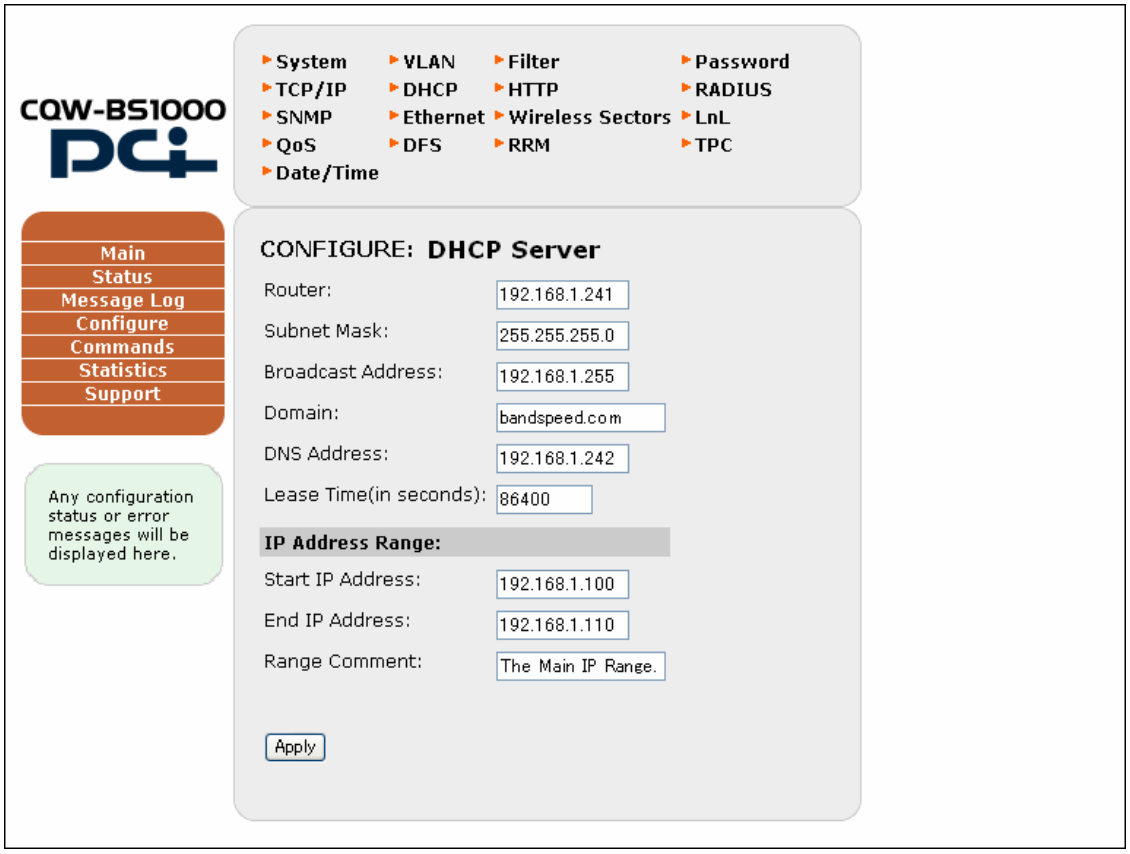
Figure 4.10 Configure - TCP/IP Window



The **Configure>TCP/IP** window contains the settings for the system IP addresses, and the option to have it obtain its IP address automatically (DHCP client).

Configure – DHCP :

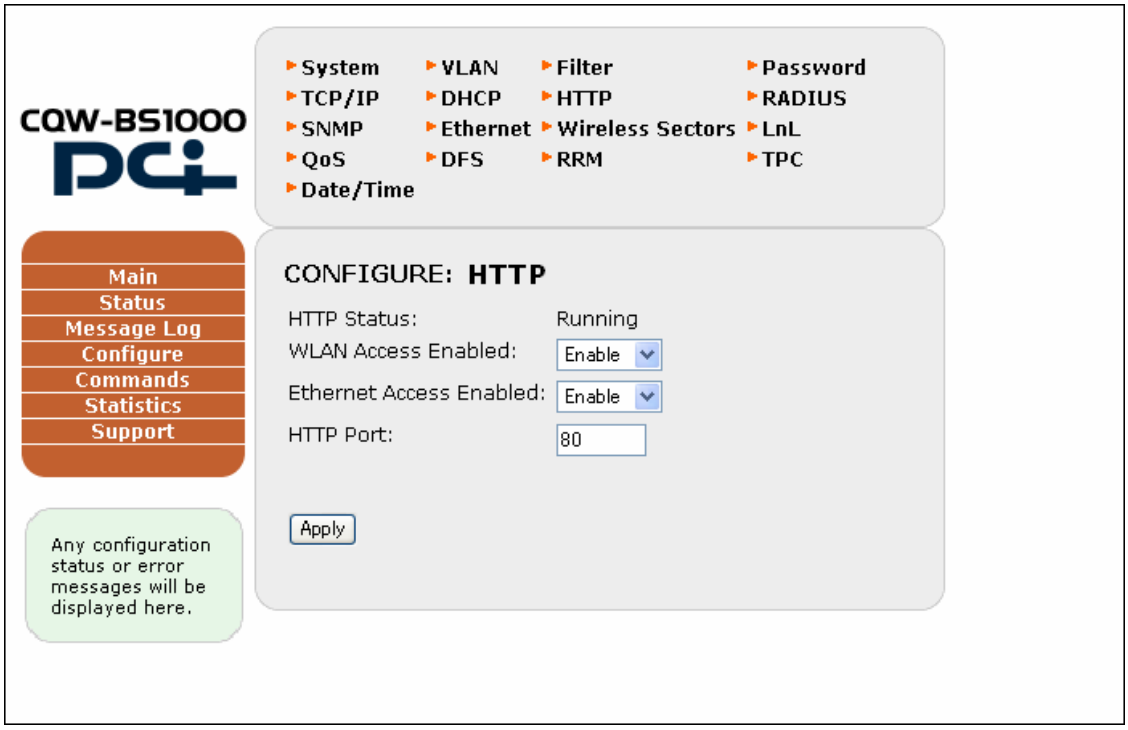
Figure 4.11 Configure – DHCP Window



The **Configure>DHCP** window includes all of the settings for DHCP hosting.

Configure – HTTP :

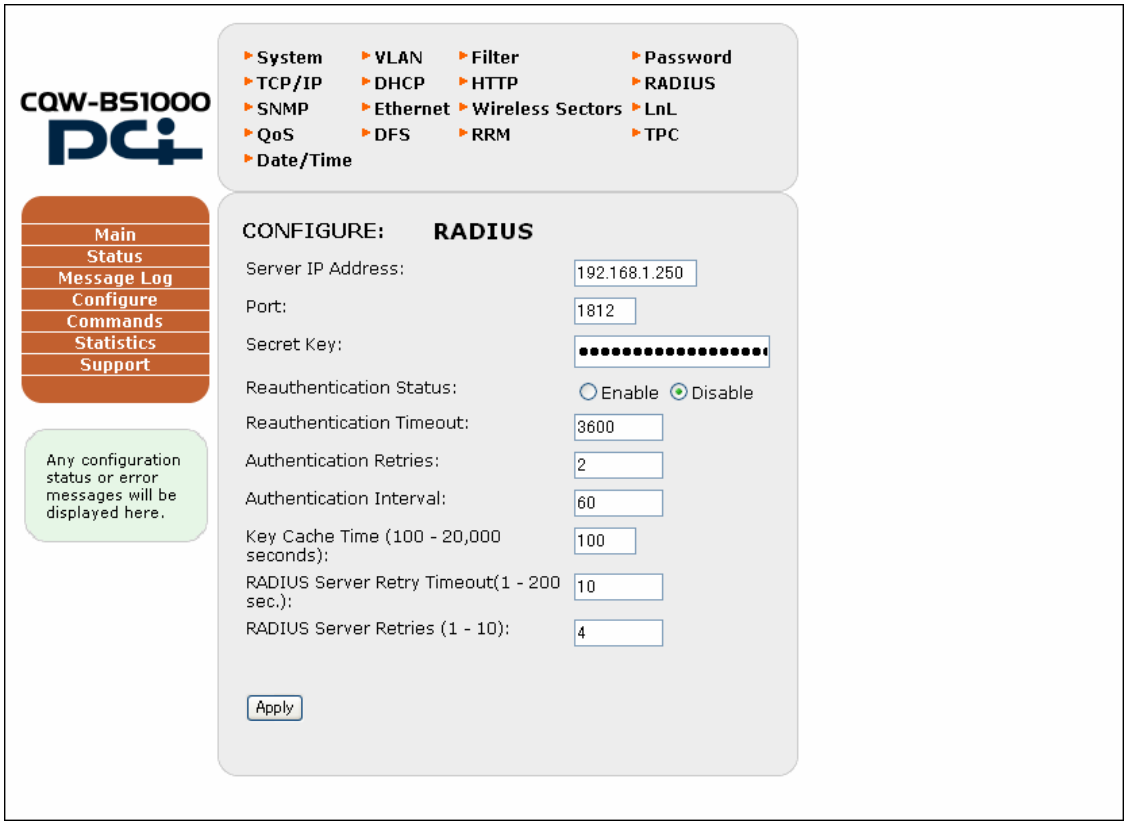
Figure 4.12 Configure HTTP Window



The **Configure>HTTP** window displays the status of HTTP Interface, allows you to configure WLAN Access Enable, Ethernet Access Enable, and also to change the HTTP port.

Configure – RADIUS :

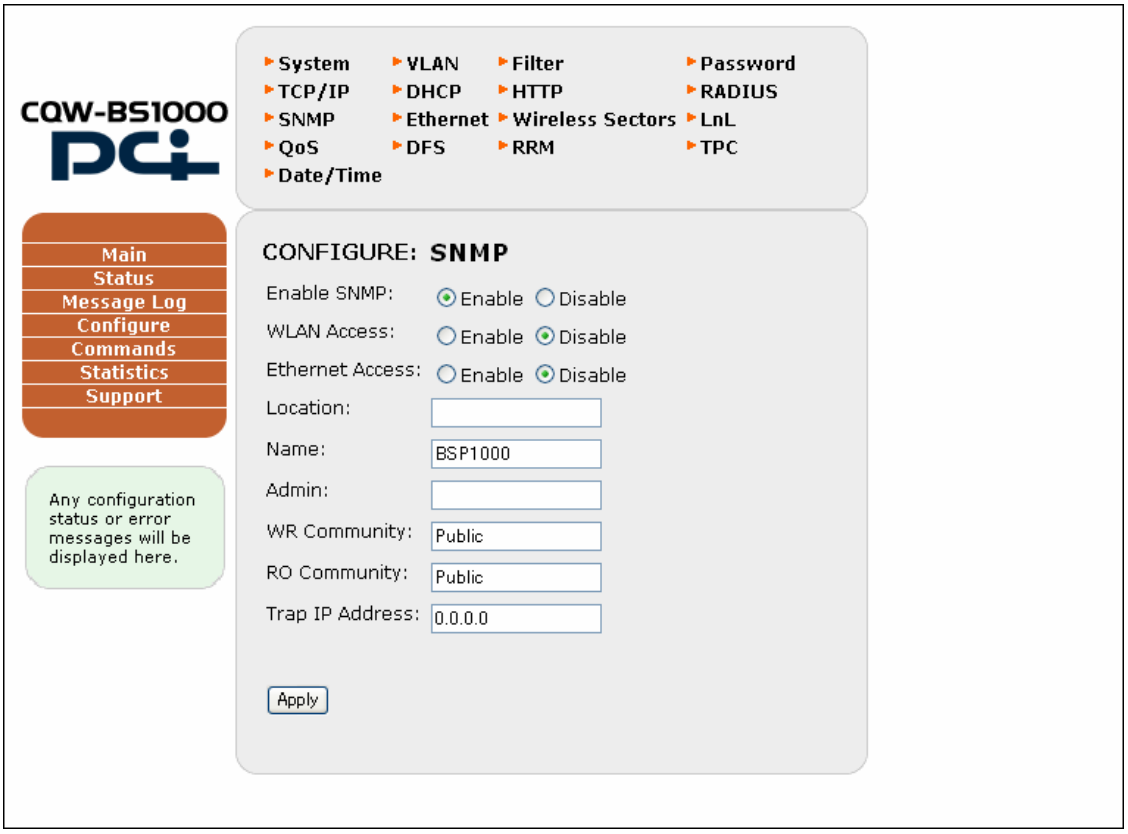
Figure 4.13 Configure RADIUS Window



The **Configure>RADIUS** window includes all of the settings used for the RADIUS server, and sets the reauthentication parameters.

Configure - SNMP :

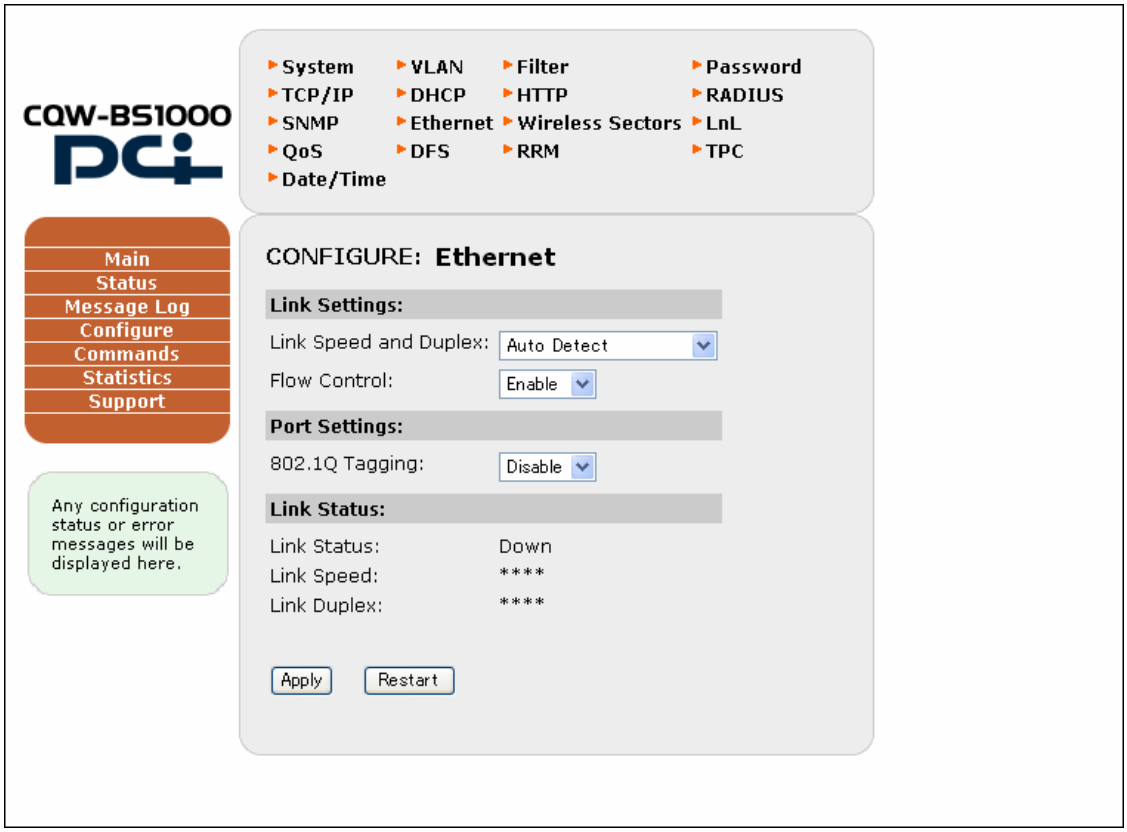
Figure 4.14 Configure SNMP Parameteres.



The **Configure > SNMP** Interface contains the Access Points` SNMP Server Parameters.

Configure – Ethernet :

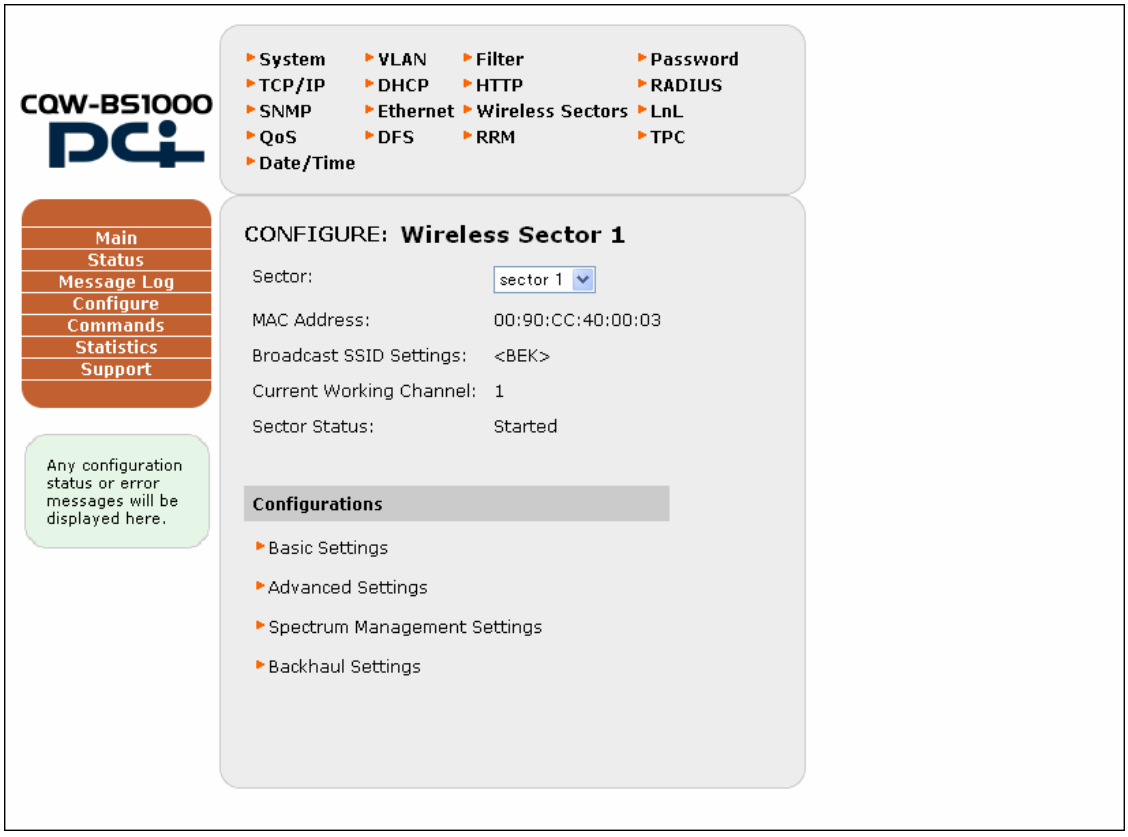
Figure 4.15 Configure Ethernet Window



The **Configure>Ethernet** menu includes the link speed with duplex and flow control settings, and displays the current Ethernet port status.

Configure - Wireless Sectors :

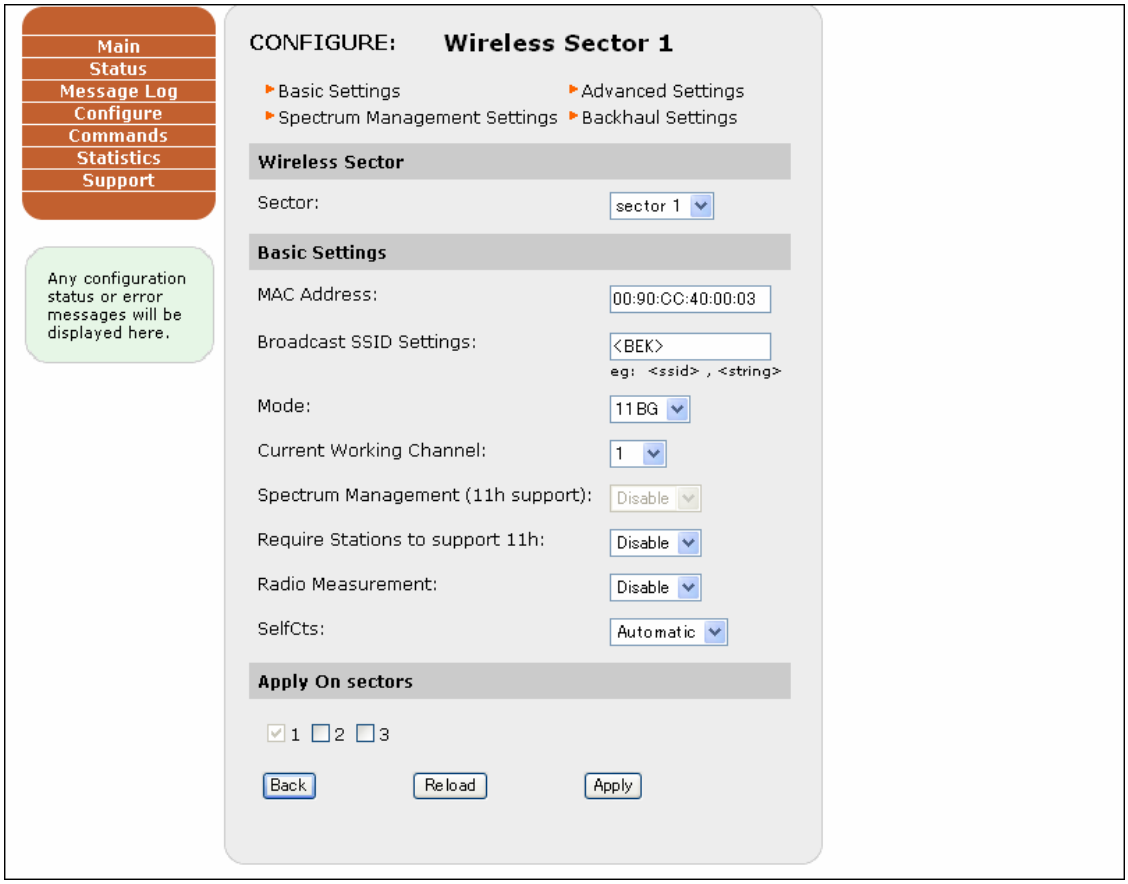
Figure 4.16 Configure Wireless Sectors Window .



The Configure>WirelessSector menu has submenus for the individual ssector.These menus contain all of the AP settings for the selected sector.

Configure – Basic Settings :

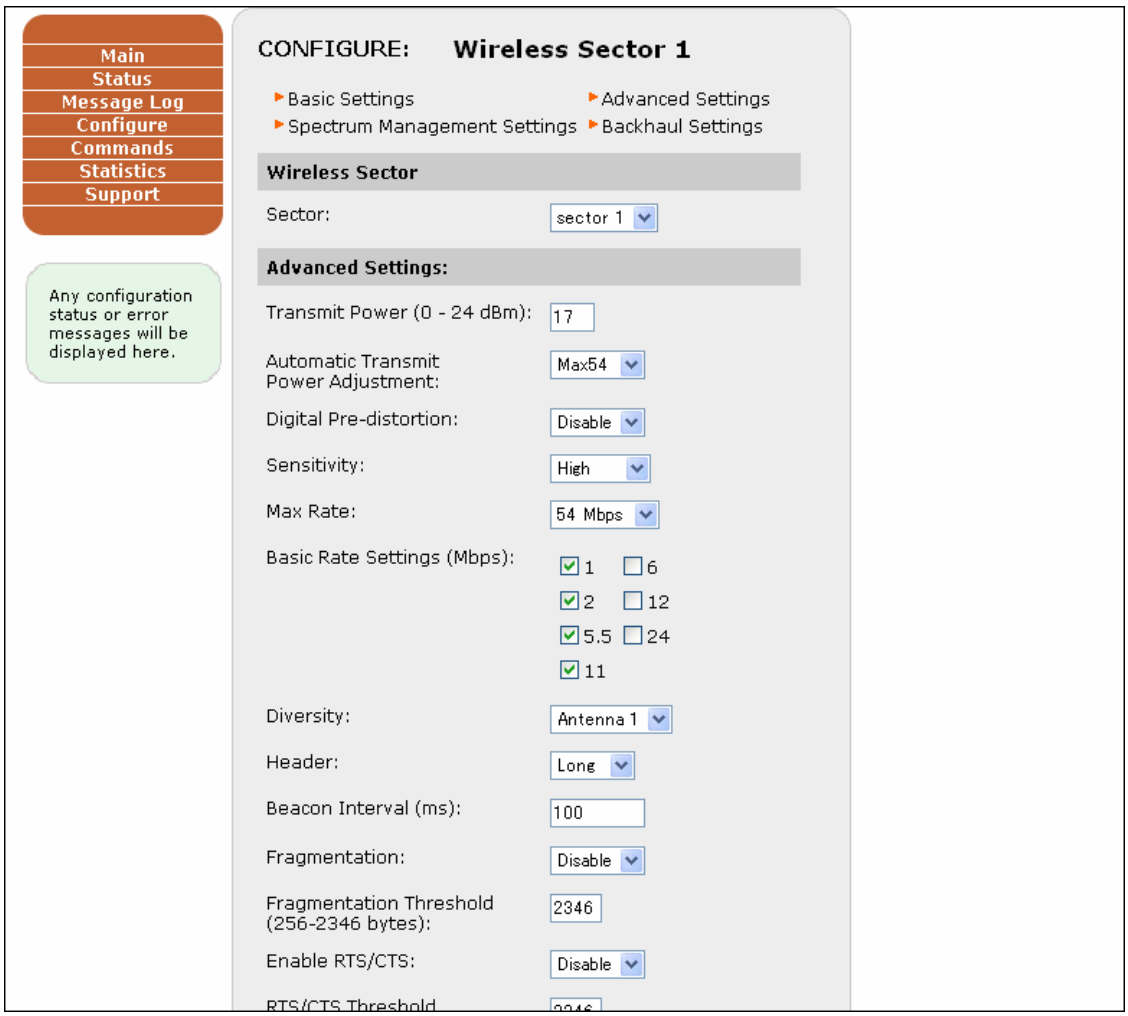
Figure 4.17 Configure Wireless Sectors – Basic Settings.



The **Configure>BasicSettings** includes the Basic parameters like MAC Address of the sector, Broadcast SSID also Enable or Disable Spectrum Management and Radio Measurement.

Configure – Advance Settings :

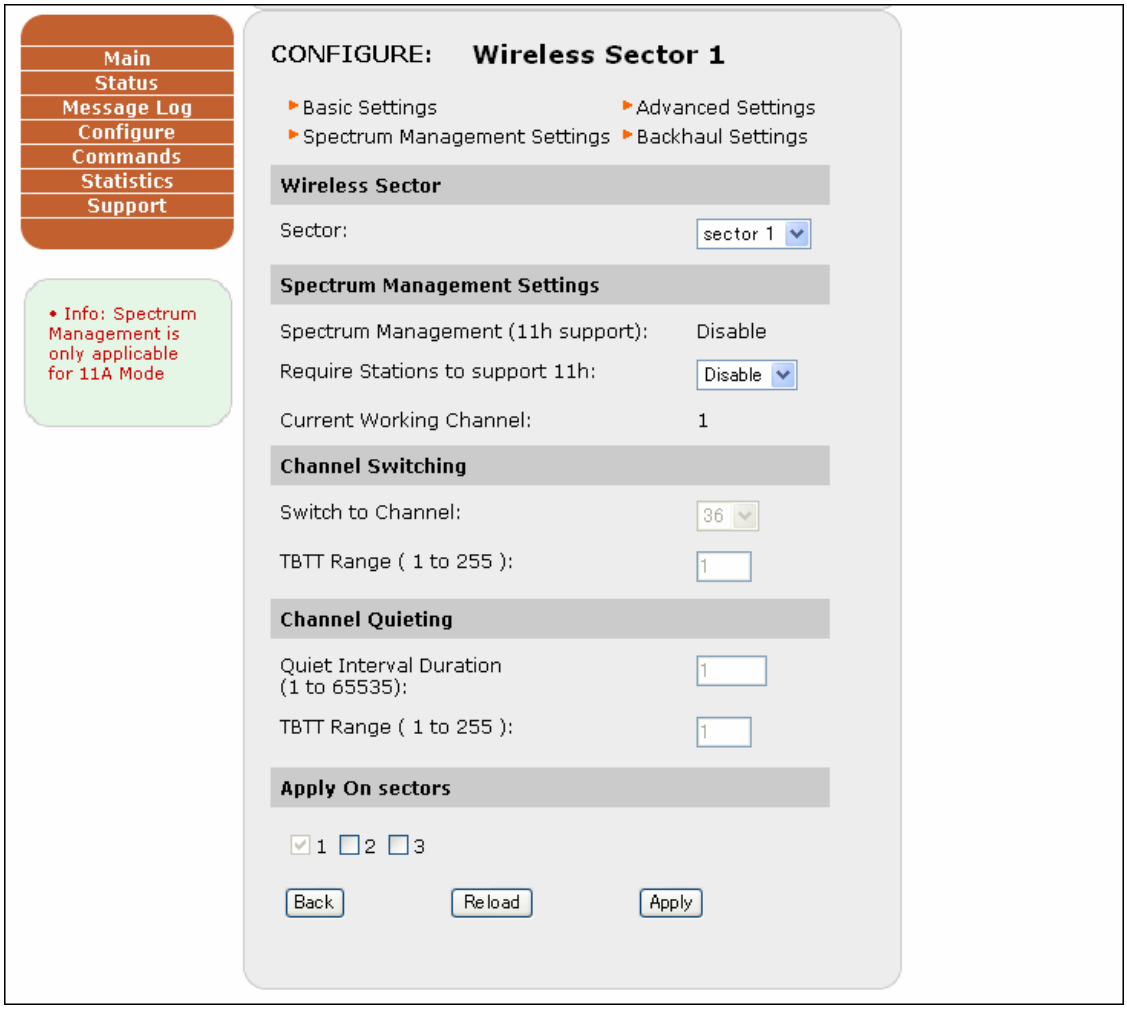
Figure 4.18 Configure Wireless Sectors – Advance Settings



The **Configure>AdvanceSettings** include the advanced parameters that can be configured on the sector.

Configure- Spectrum Management :

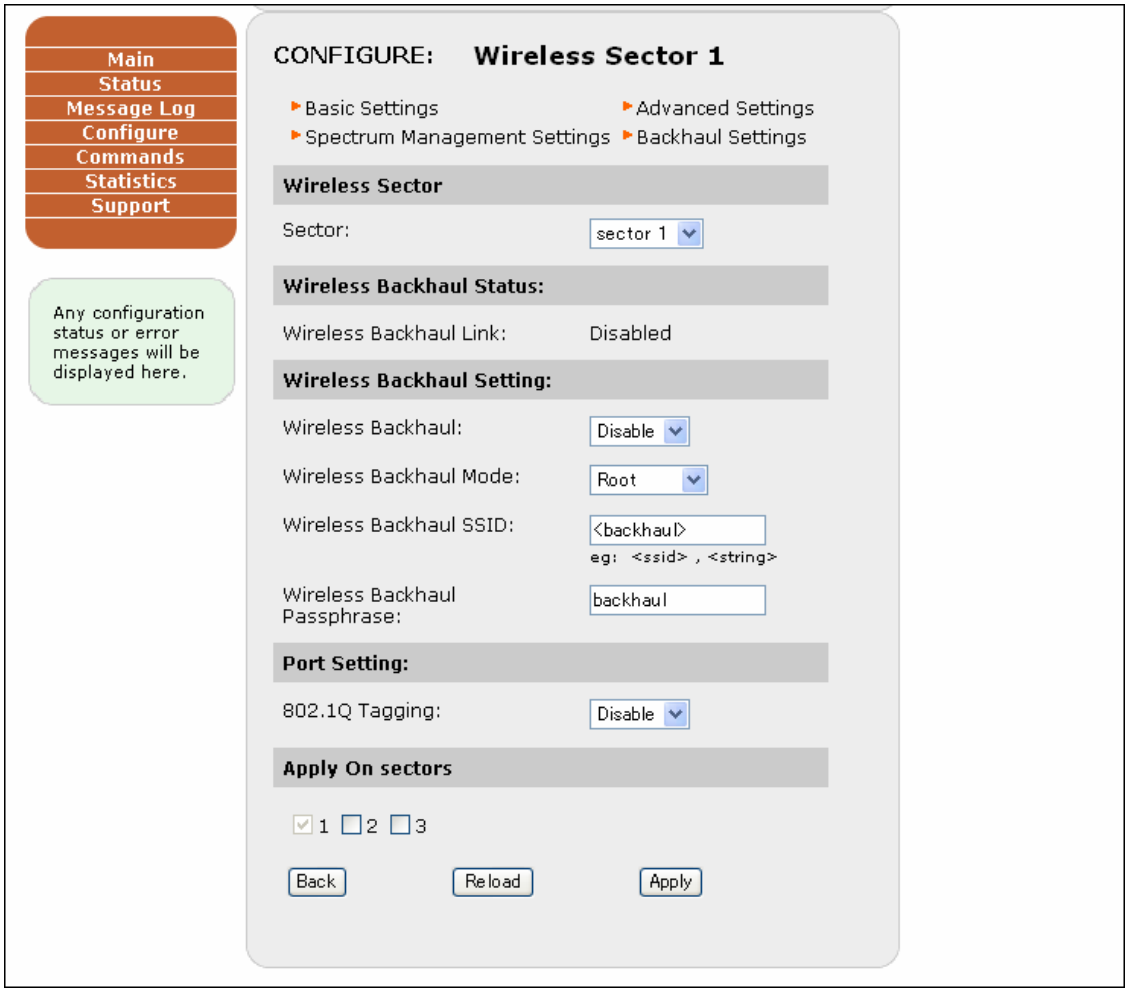
Figure 4.19 Configure Wireless Sectors – Spectrum Management Settings.



The **Configure >SpectrumManagement** contains the parameters to be set for Spectrum Management.

Configure – Backhaul Settings :

Figure 4.20 Configure Wireless Sectors – Backhaul Settings.



The Configure > BackhaulSettings is used to configure the Backhaul settings on a particular sector.

Configure Listen and Learn :

Figure 4.21a Configure Listen and Learn Features (Top Portion)

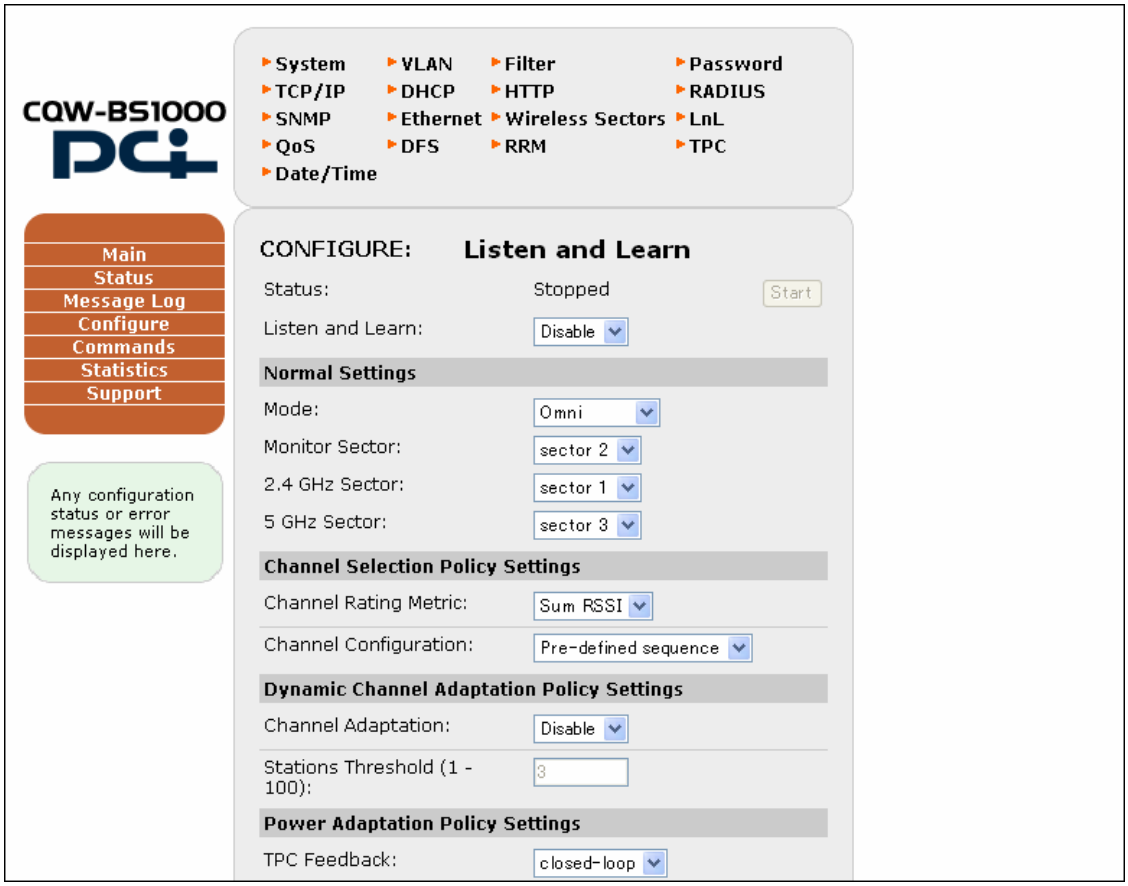
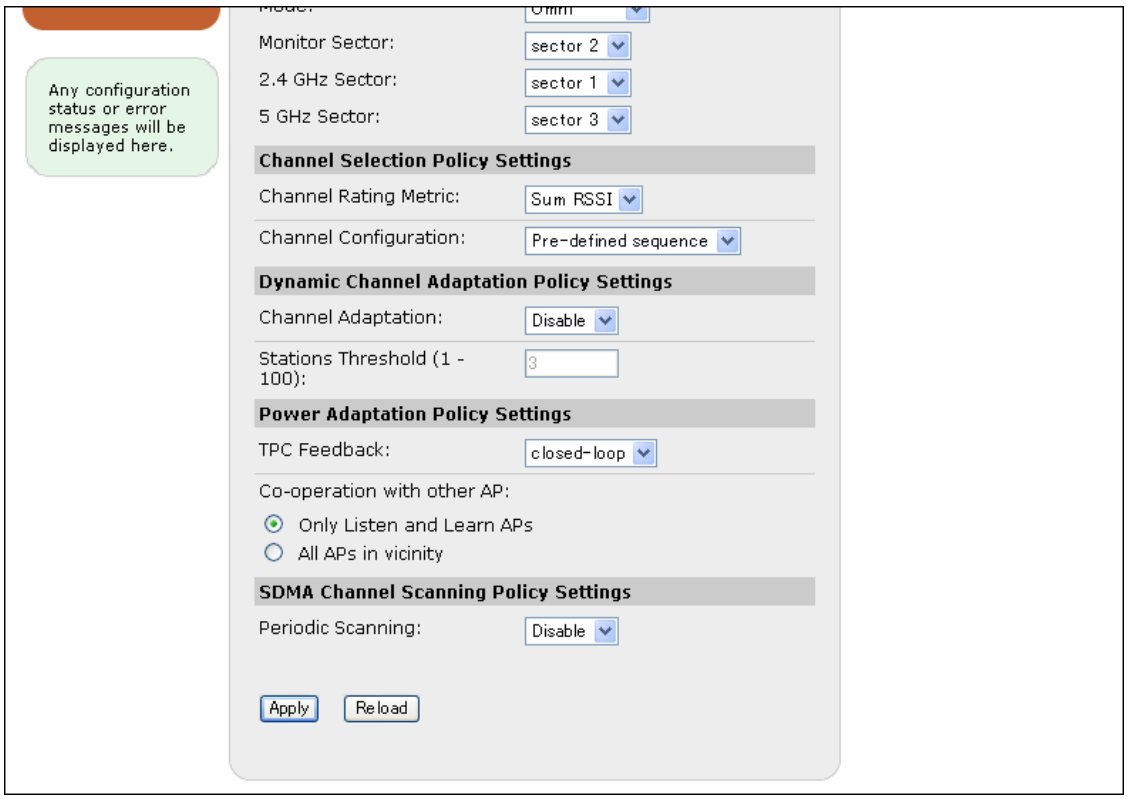


Figure 4.21b Configure Listen and Learn Features (Bottom Portion)



The **Configure>Listen and Learn** menu provides a convenient interface to all Listen and Learn features. These features apply to the AP as a whole and allow automatic configuration and adaptation to the wireless environment.

Configure – QoS :

Figure 4.22a Configure QoS Parameters (Top Portion)

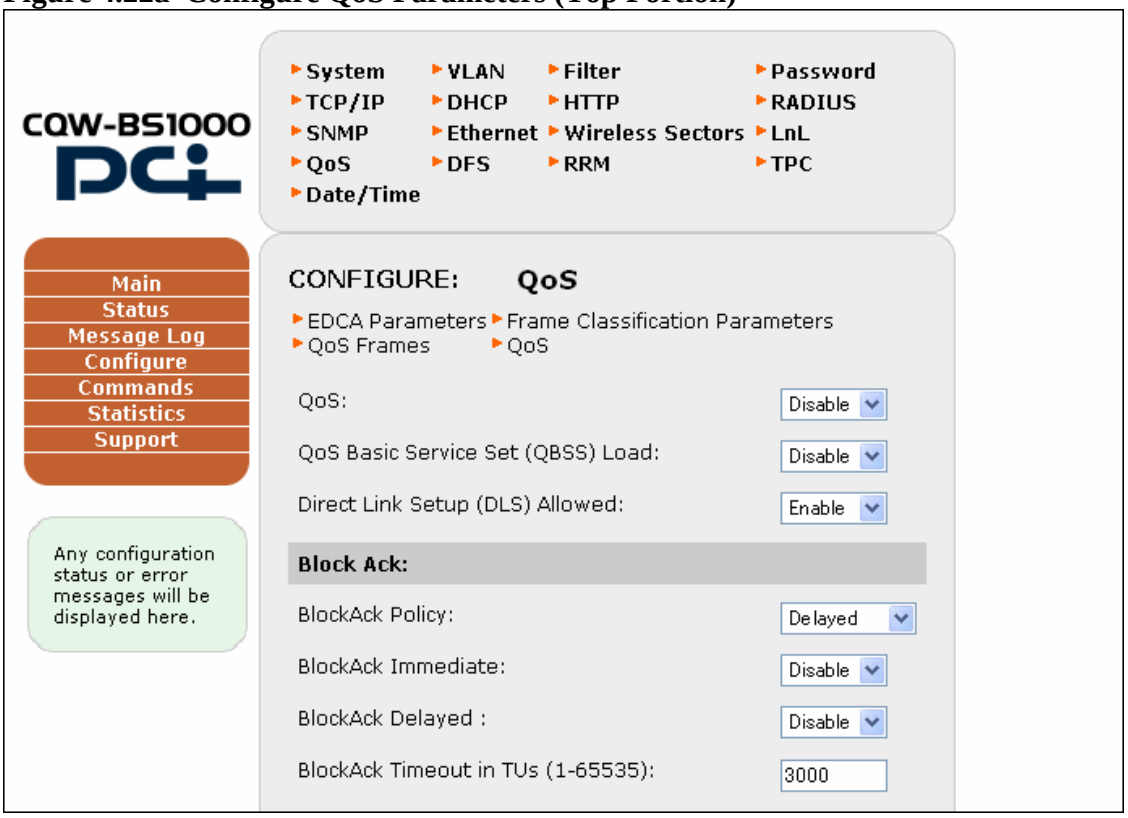
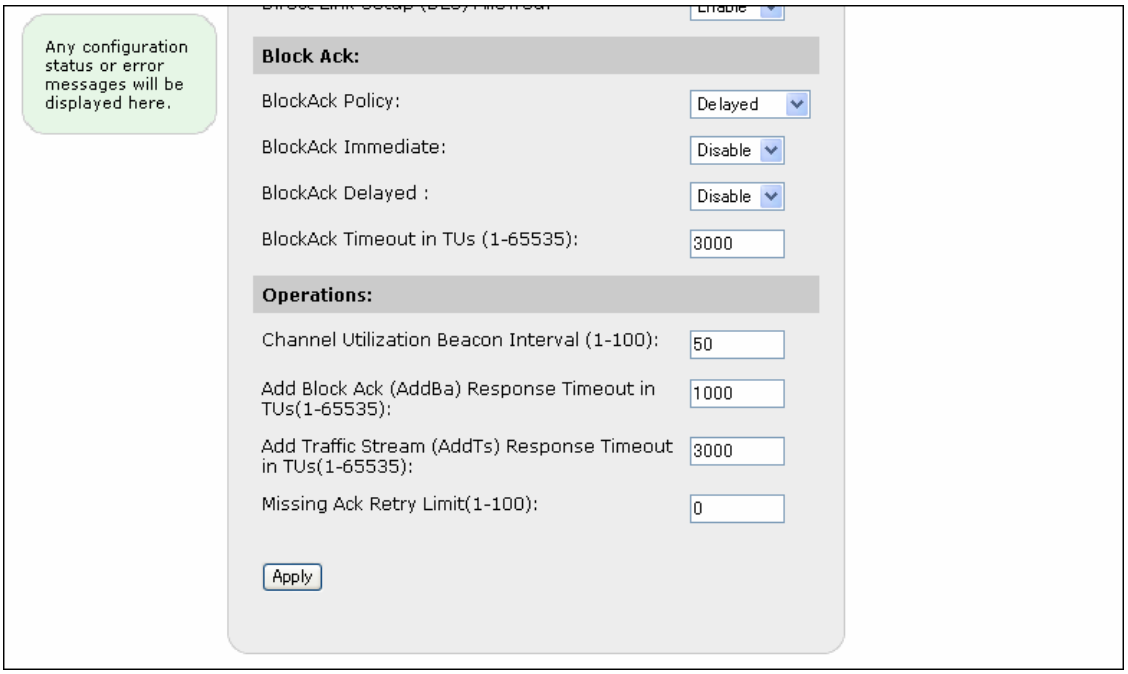


Figure 4.22b Configure QoS Parameters (Bottom Portion)



The **Configure > QoS** contains the standard QoS configurations**.**

Configure QoS – EDCA Parameters :

Figure 4.23a Configure QoS – EDCA Parameters (Top Portion)

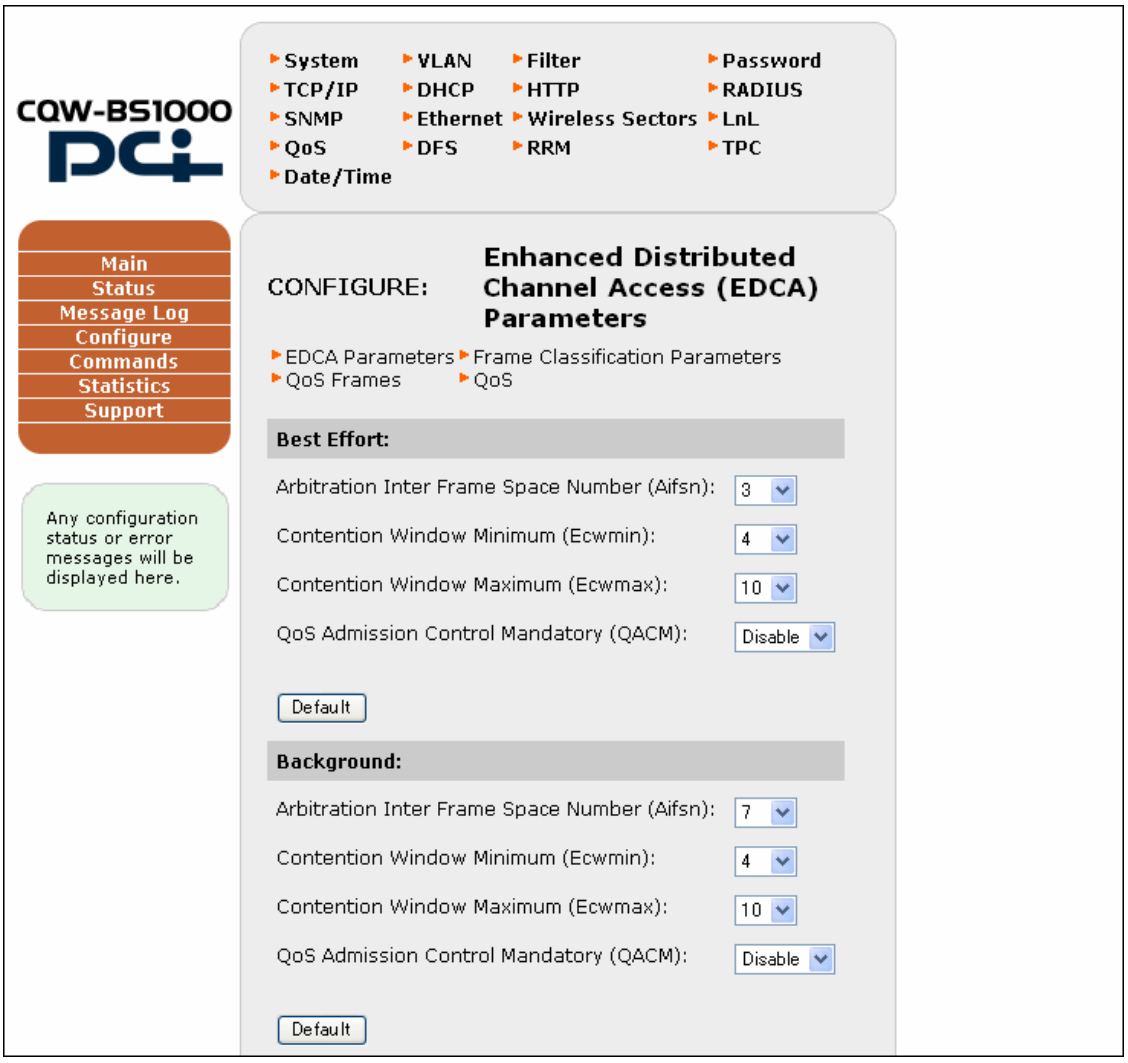
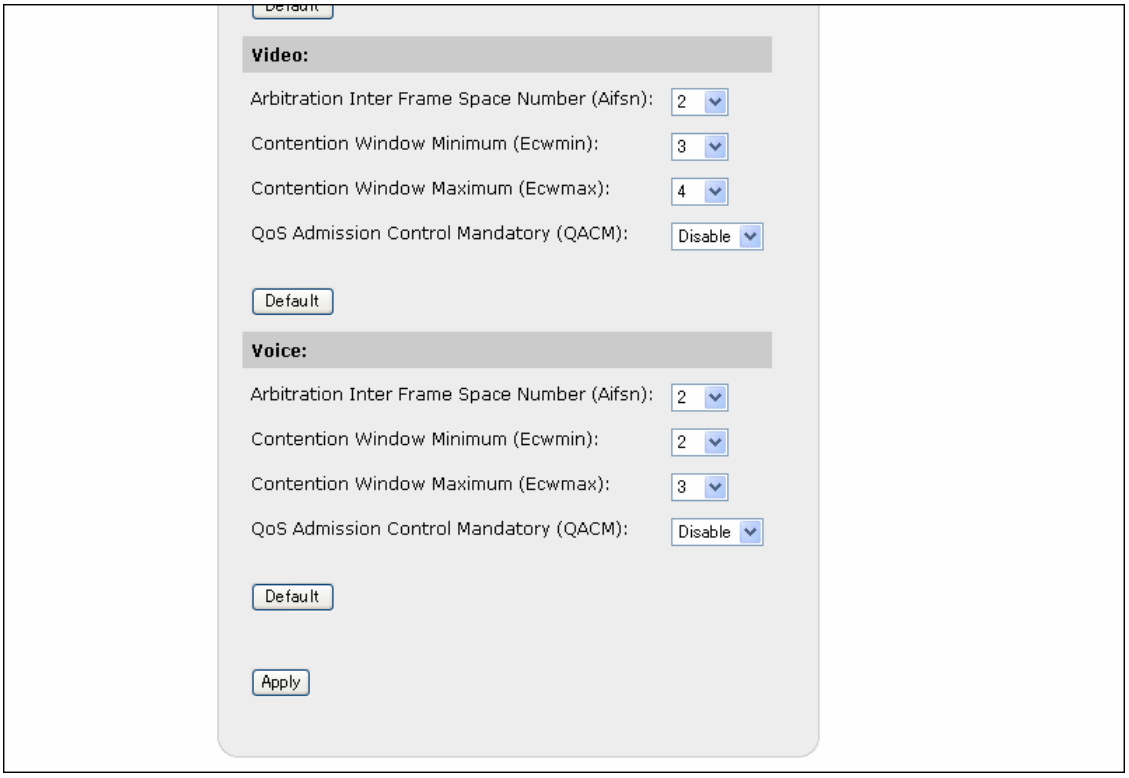


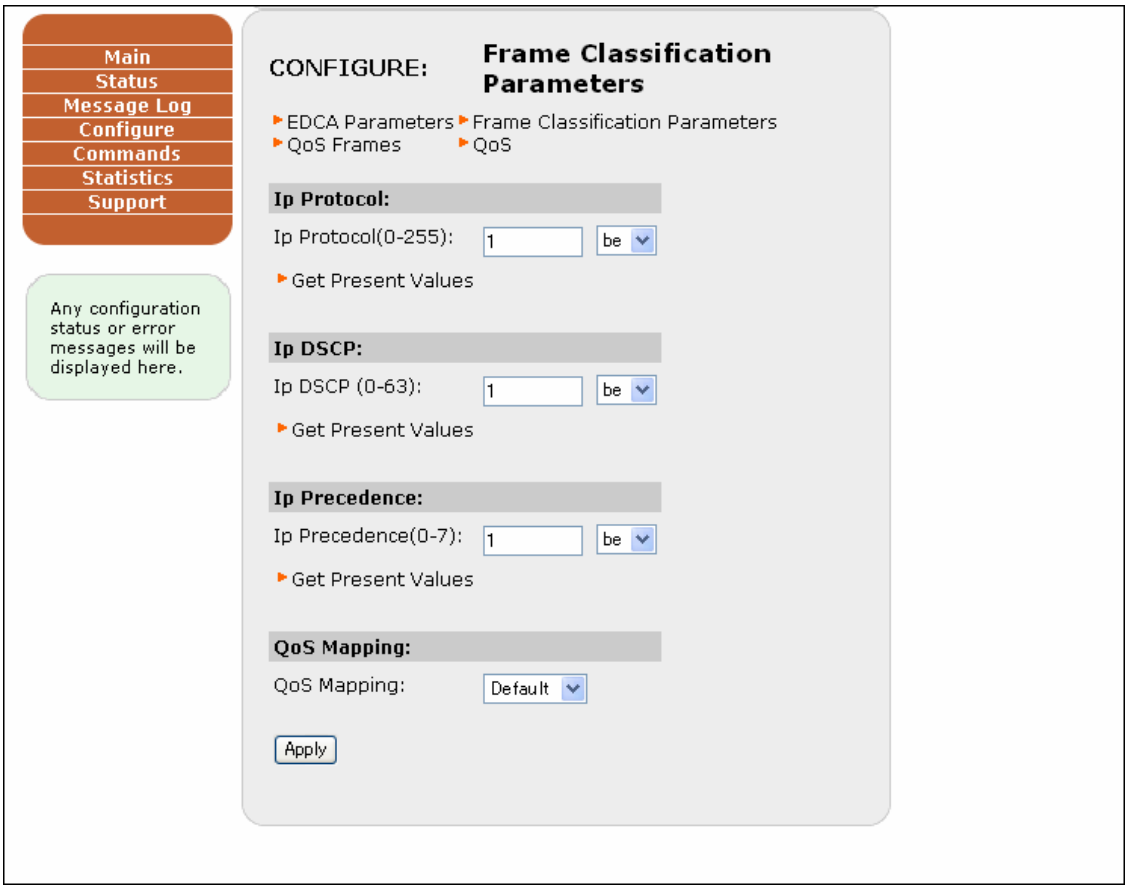
Figure 4.23b Configure QoS – EDCA Parameters (Bottom Portion)



The **Config > EDCA Parameters** configures the QoS parameters for different types of Data streams.

Configure QoS – Frame Classification Parameters :

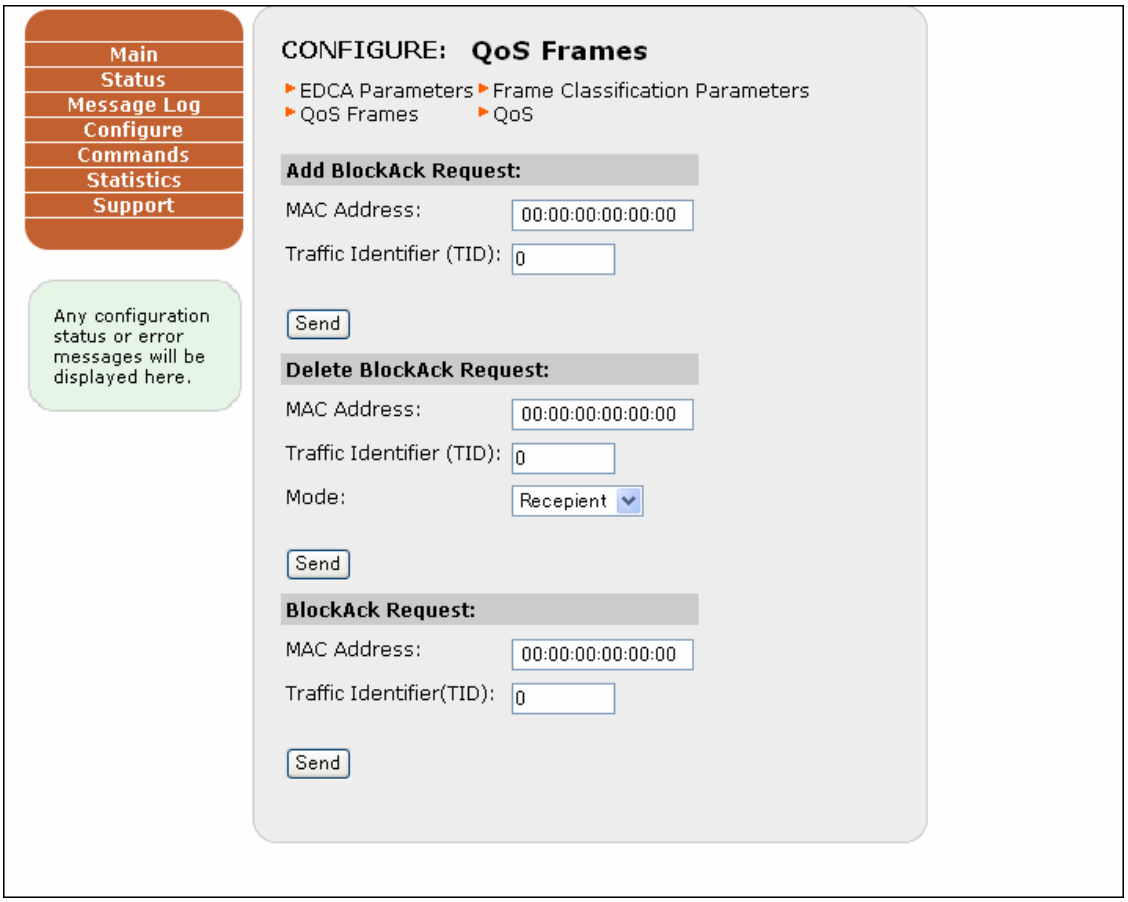
Figure 4.24 Configure QoS – Frame Classification Parameters



The **configure > Frame classification parameters** configures the IP protocol attributes for different types of data streams.

Configure QoS – QoS Frames :

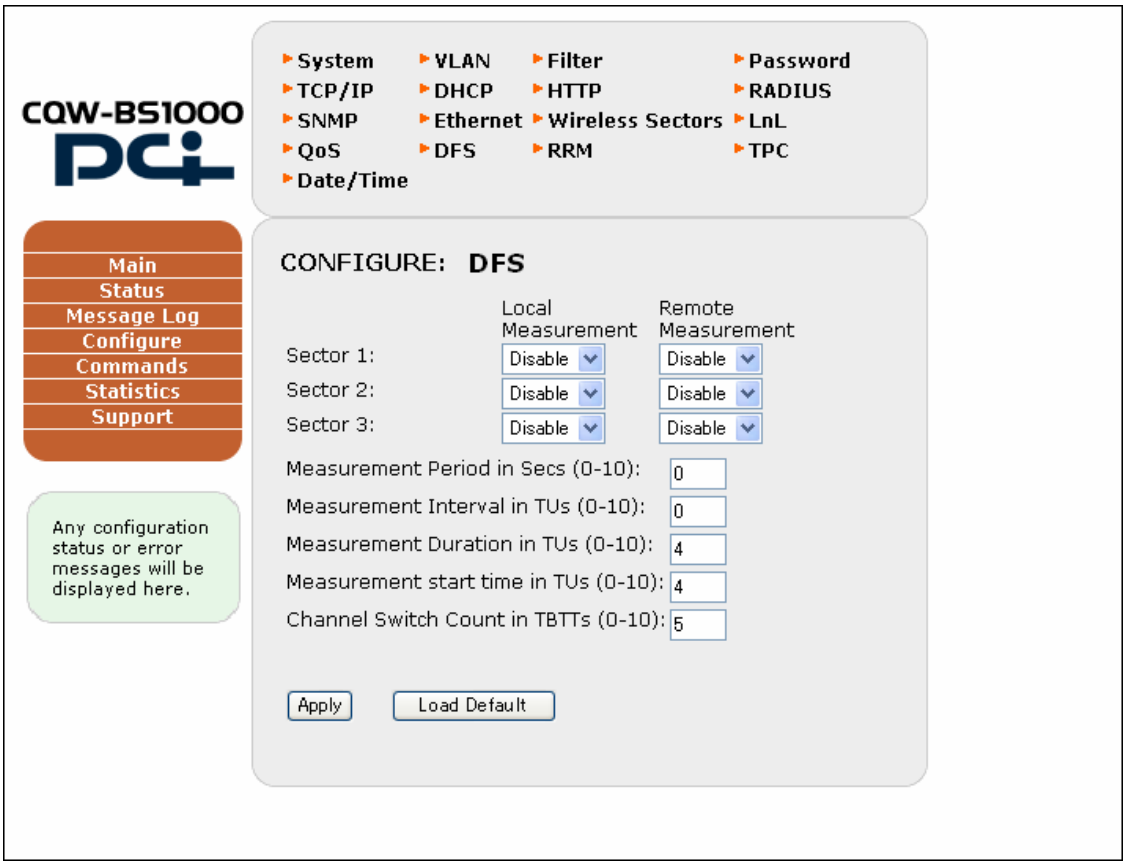
Figure 4.25 Configure QoS – QoS Frames



The **configure > QoS Frames** configures the BlockAck configurations for a MAC Address.

Configure DFS :

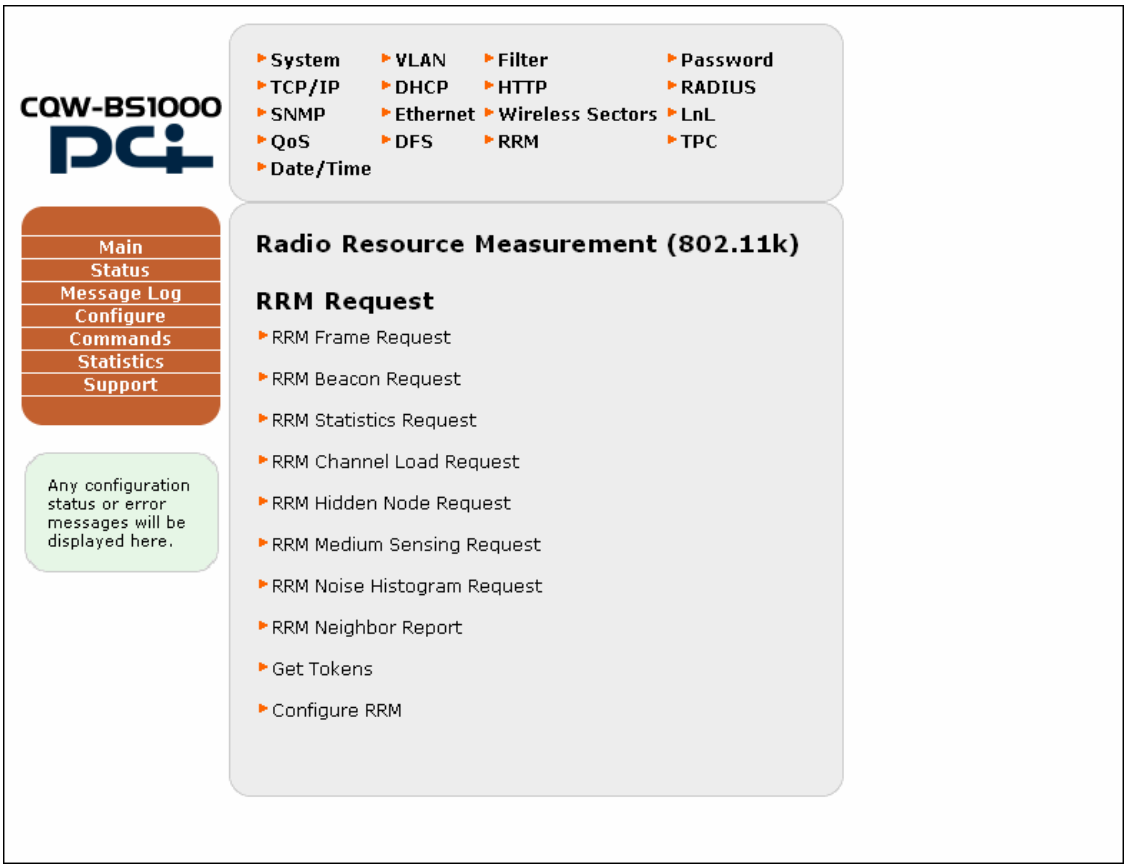
Figure 4.26 Configure DFS Control Parameters



The **Configure>DFS** menu provides a convenient interface to all 802.11h DFS process control parameters. These features apply to each wireless sector.

Configure RRM :

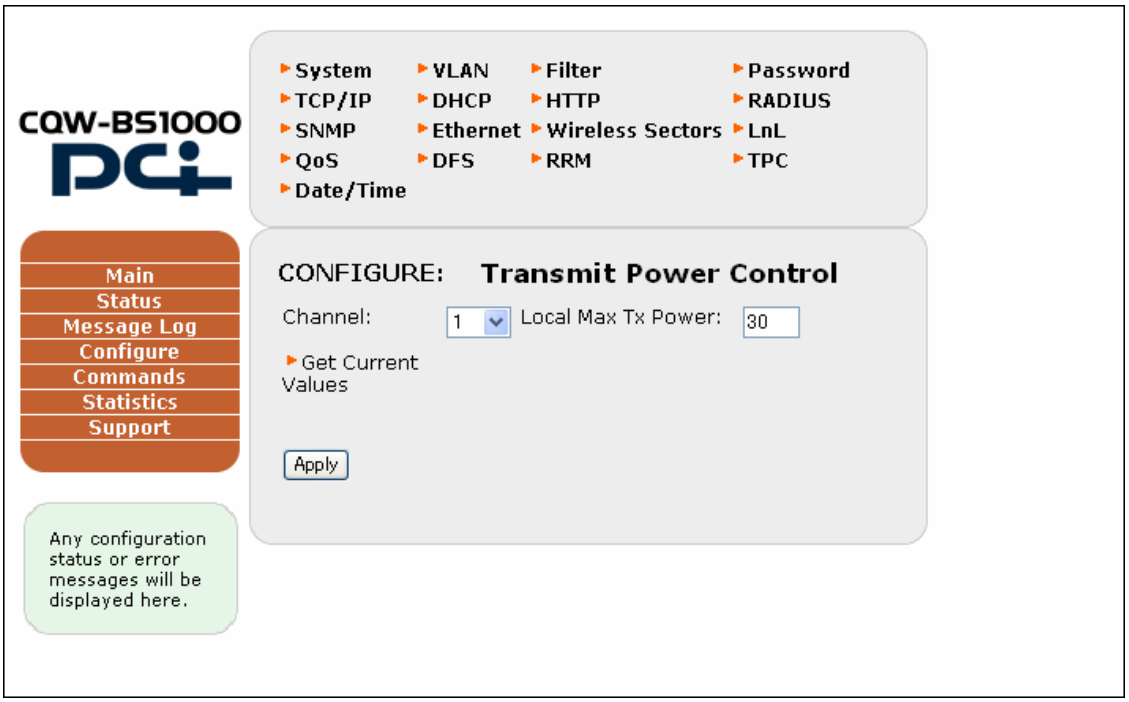
Figure 4.26 Configure RRM Measurement Requests



The **Configure>RRM** menu provides a convenient interface to all 802.11k Remote Radio Measurement requests. Measurement requests may be issued on any wireless sector.

Configure TPC :

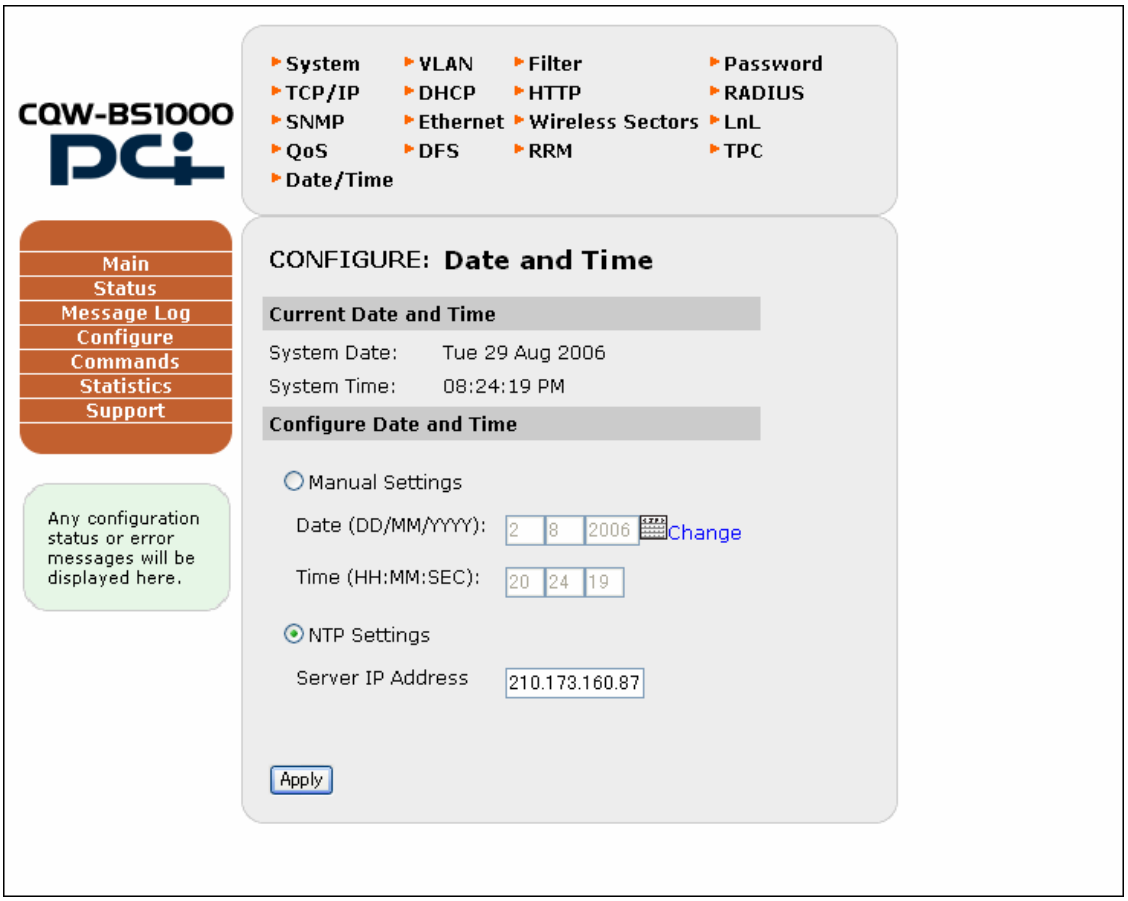
Figure 4.27 Configure TPC Process Parameters



The **Configure>TPC** menu provides an interface to Transmit Power Capabilities. These capabilities apply to the AP as a whole, on a per-channel basis.

Configure Date and Time :

Figure 4.28 Configure Date and Time



The **Configure>Date and Time** can be used to configure the system Date and Time

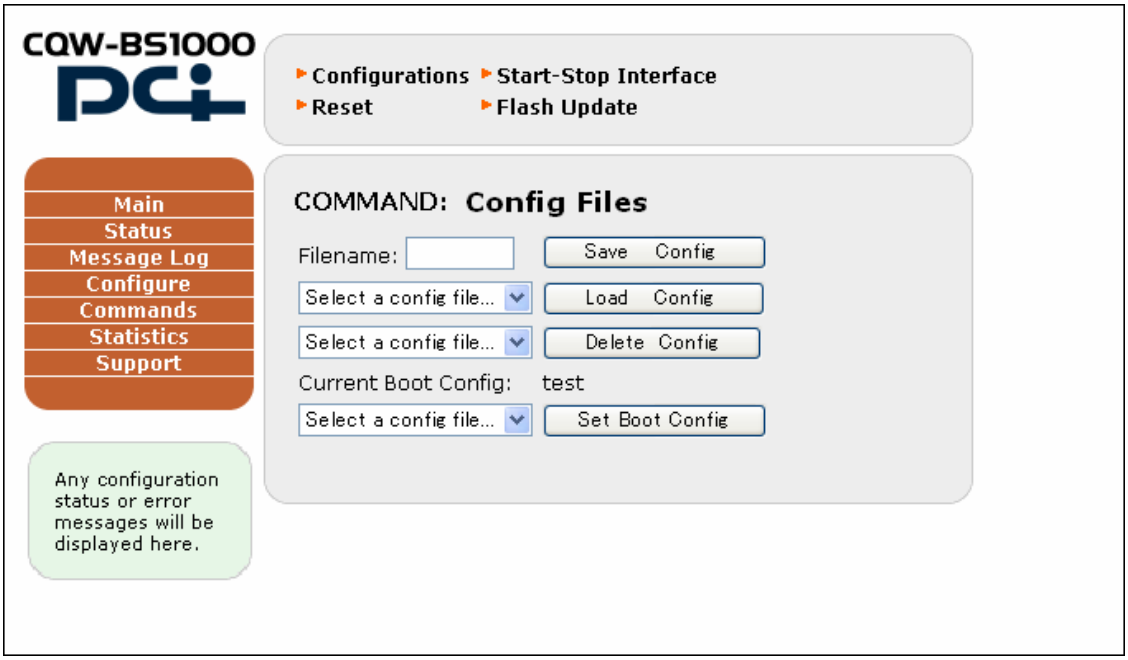
Commands Menu

The Commands menu includes three submenus:

- Configurations
- Start/Stop Interface
- Reset
- Flash Update

Commands - Configurations :

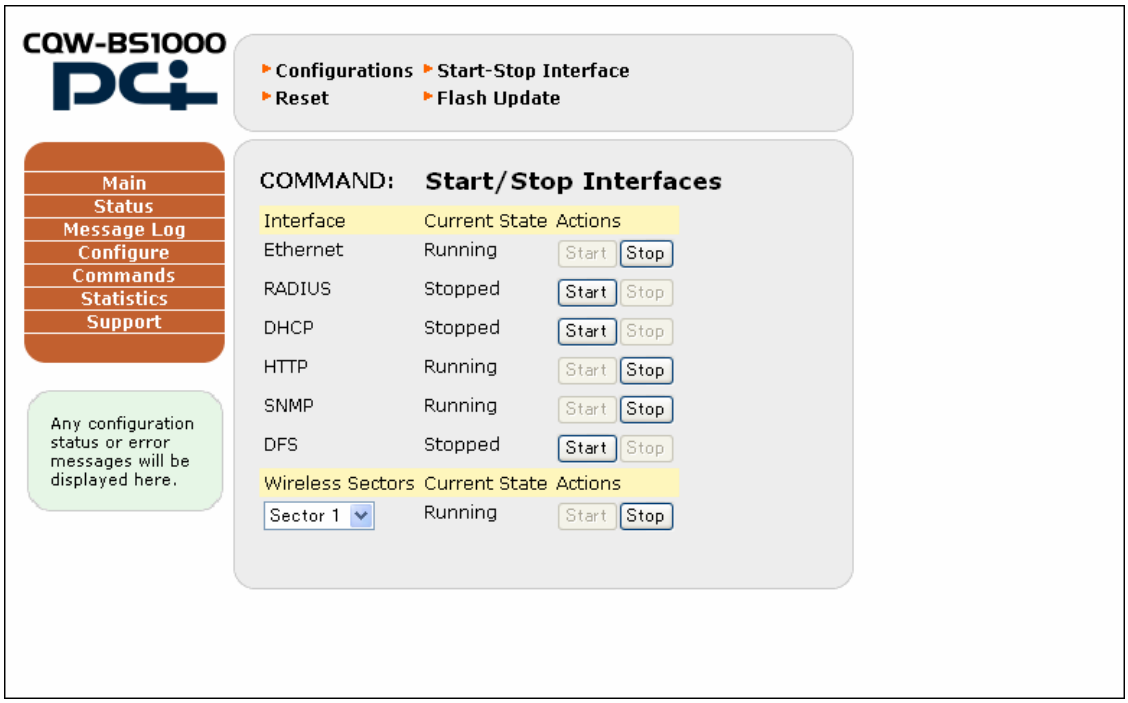
Figure 4. 29 Command Configuration Window



Use the **Commands>Configurations** menu to manage the configuration files., such as, creating a new configuration file, displaying the contents of current configuration file and displaying the differences of two configuration files..

Commands - Start/Stop Interface :

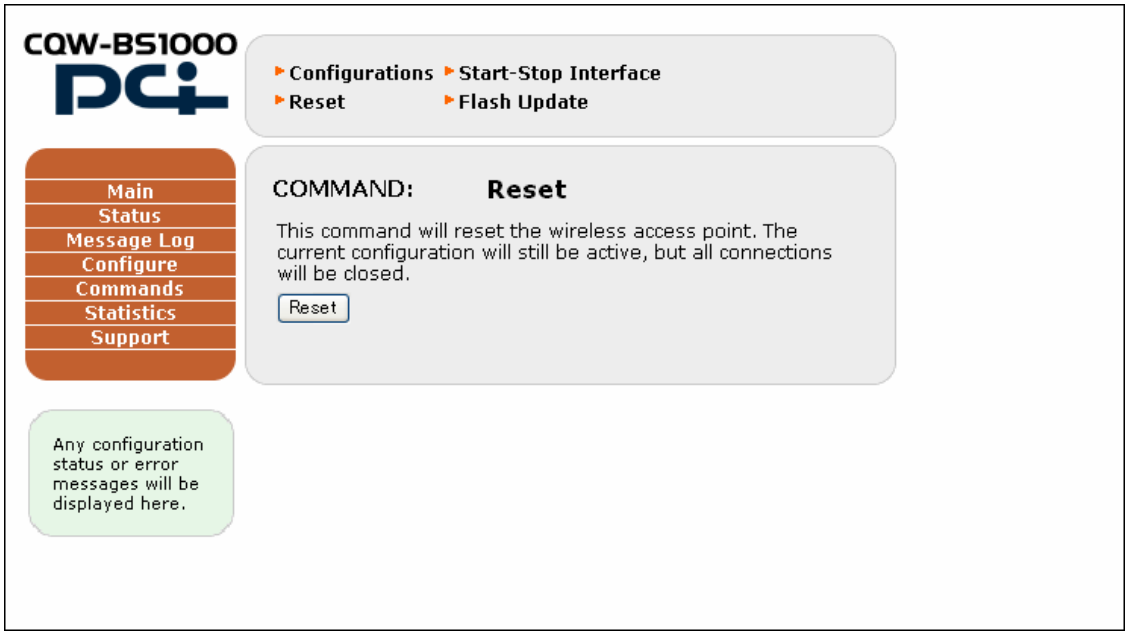
sFigure 4.30 Command Start/Stop Interface Window



The **Commands>Start/Stop Interface** window allows you to directly start and stop all of the system interfaces and shows the current status for each.

Commands – Reset :

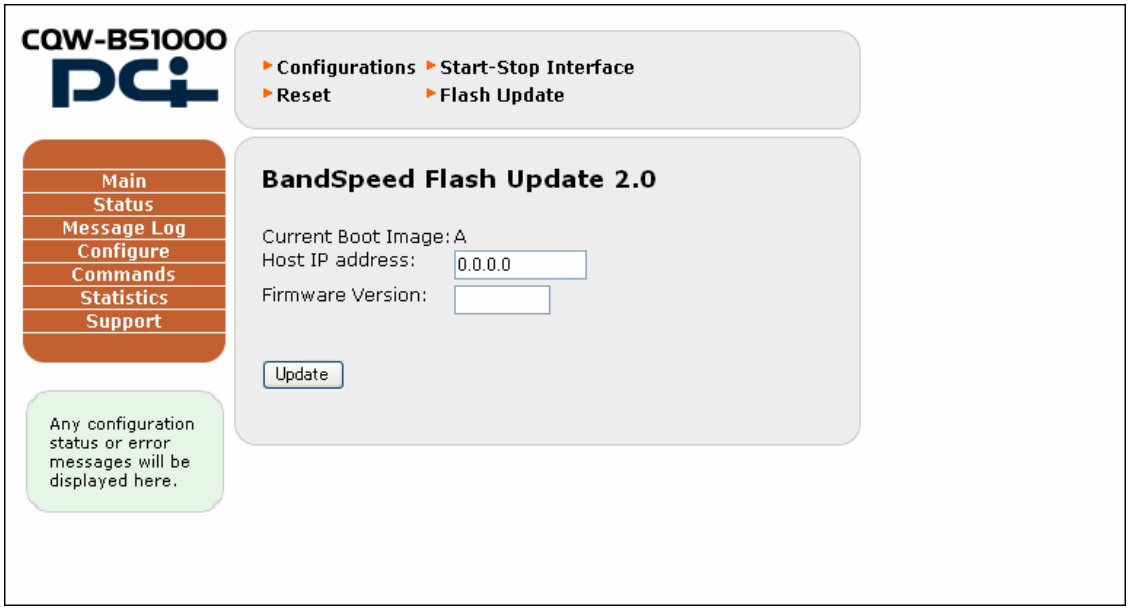
Figure 4. 31 Command Reset Window



The **Commands>Reset** window allows you to perform a system reset. It does not change the configuration but does close all of the connections.

Commands – FlashUpdate :

Figure 4. 32 Bandspeed Flash Update.



The **Command > FlashUpdate** is used to update the Firmware Image on the Access Point.

4.3.4 Statistics Window

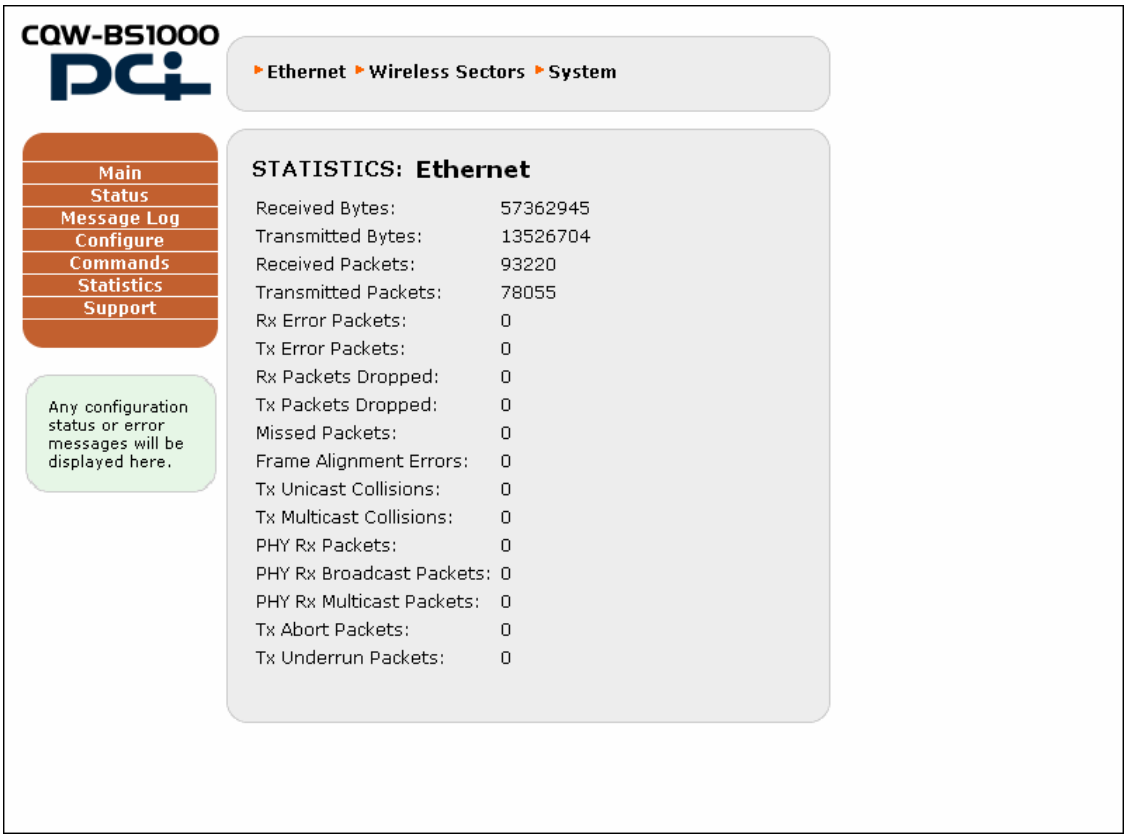
The Statistics window includes five submenus:

- Ethernet
- Wireless Sectors
- System

Each of these windows displays the statistics compiled since the last Reset, off-on power cycle, or Stop/Start cycle of individual interfaces.

Statistics – Ethernet :

Figure 4. 33 Ethernet Statistics Window



Statistics – Wireless Sector :

Figure 4.34a Sector 1 (of 3) Statistics Window (Top Portion)

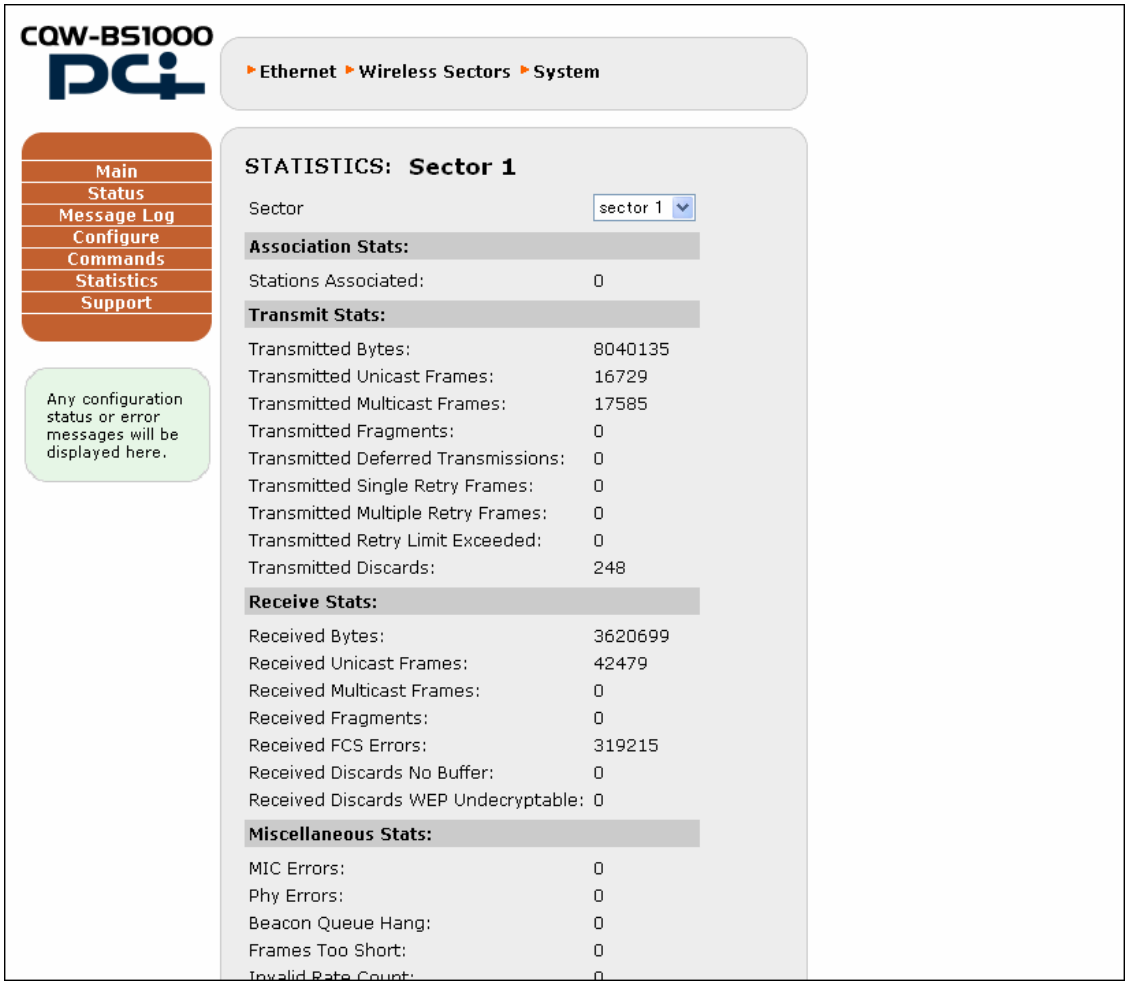
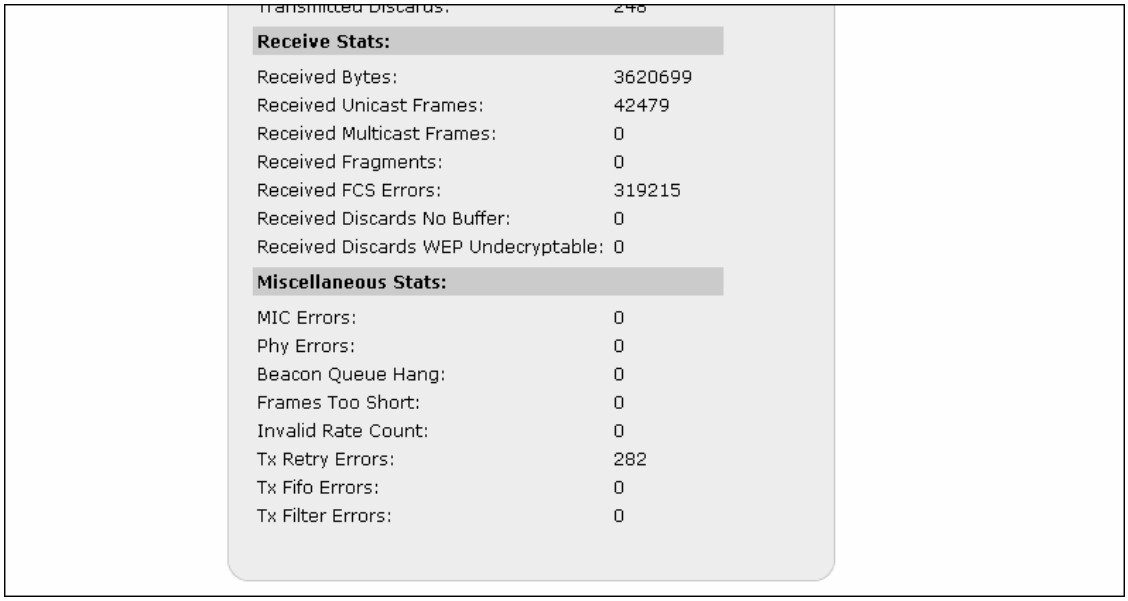
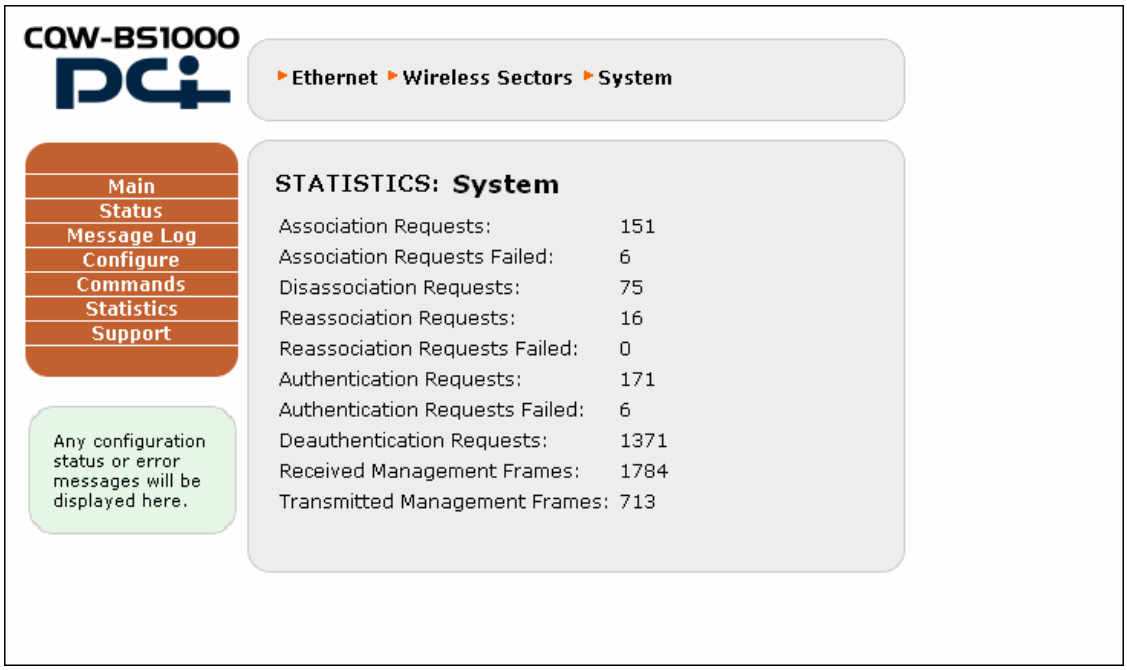


Figure 4.35b Sector 1 (of 3) Statistics Window (Bottom Portion)



Statistics – System :

Figure 4.36 System Statistics Window



4.3.5 The Support Page

The support page provides important links to the Planex Web site, online Help files, and to the firmware update site to get the latest firmware for the CQW-BS1000 Evaluation System.

Figure 4.32 Support Window

5.0 Trouble Reporting

Trouble reporting is done via the Planex Web site. At http://www.planex.co.jp/support/techform/, click **Technical Support**. After supplying your username and password, click **Ticket** to fill out a trouble ticket, or the email address (support@bandspeed.com) to send the report in an email.

6.0 Specifications

This section provides technical specifications for the Planex CQW-BS1000 Evaluation System.

6.1 Antenna

Figure 6.1 shows the azimuth and elevation beam patterns for each sector of the Planex CQW-BS1000 Evaluation System. Table 6.1 provides the electrical and mechanical specifications.

Figure 6.1 Beam Pattern (Each Sector)

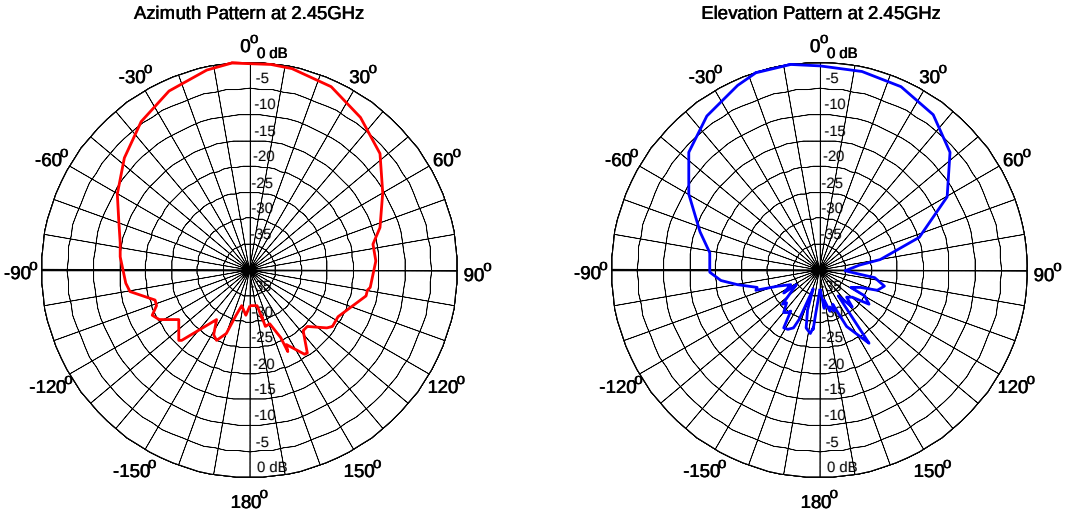


Table 6.1 Electrical and Mechanical Specifications

Electrical	
Coverage	Three 60° beams covering 360°
Frequency Range	ISM-band (extended), 2.39 GHz to 2.5 GHz
Gain	7dBi
VSWR	<2.5:1 over the entire band
Halfpower Beamwidth (±4°)	Horizontal: 60° Vertical: 70°
Side Lobe Level	>20dB below main lobe
Front-to-Back Ratio	>25dB
Port-to-Port Isolation	>50dB
Polarization	Linear vertical
Diversity	Dual, vertical spatial
Maximum Input Power	10 watts
Mechanical	

Connectors	SMB Female (12)
Material	Reflector: Aluminum Radome: n/a
Overall Dimensions	10.33” H × 16.0” Diameter (26cm × 40.6cm)
Weight (Indoor Version)	4.55 lbs (2.1 kg)

6.2 Reference Design

The Planex CQW-BS1000 Evaluation System is compliant with all applicable standards including 802.11b, 802.11g, 802.11a, 802.3 PHY (10/100Mbit/s), 802.3af, JTAG, and mini-PCI v1.0.

- Power Supply Interface includes:
- Power Over Ethernet (POE) using 10/100 FE Interface, or
- Optional—AC Power Supply Interface
  - Supports +3.3V Power requirements for SOC-RDP system
  - Supports +1.5V for low power devices.

AMD Au1500 High Performance Processor includes:

- MIPS32 CPU core running at 400 or 500MHz
- 16KB Cache Instruction and 16KB Cache Data
- Integrated PCI Bus Controller—32 Bit PCI 2.2 Compliant
- Integrated SDRAM Controller—Support SDRAM Memory
- Integrated SRAM Controller—Support Flash and SRAM Memory
- Integrated Dual UART Serial Ports—Support 2 UARTs Port
- Integrated DMA Controller and EJTAG

Au1500 Processor Memory Interface supports:

- 1MB of High Performance SRAM Memory, 32-bit Interface
- 16 MB of Flash Memory, 32-bit Interface
- 64MB of SDRAM Memory, 32-bit Interface

PCI Bus Interface supports:

- 8 Mini PCI V1.0 Slots at 33MHz
- 1 PCI 10/100 FE Controller
- A single PCI clock for each PCI Bus load

Serial I/O Interface includes:

- UART Core with external RS-232 Transceiver Interface
- Support for standard DB9 Connector as DTE Interface

EJTAG Interface:

- Follows the MIPS EJTAG 2.5 Specification
- Supports Extended Instructions and Registers
- Provides Debug Exceptions
- Supports breakpoints from the processor bus, along with data/instruction breakpoints

10/100 Fast Ethernet Controller (MAC/PHY) Interface supports:

- External 10/100 signaling
- Single integrated MAC/PHY device in a single package
- Auto-negotiation and parallel detection
- 10/100 BaseT Transformer with POE hooks
- Standard RJ45 Modular Jack

LED Interface supports:

- SOC-RDP Function Block Status using GPIO signals
- WLAN NIC Status, 3 Status LEDs per port using GPIO signals

7.0 Glossary

802.11: 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The original specification provides for an Ethernet Media Access Controller (MAC) and several physical layer (PHY) options, the most popular of which uses GFSK modulation at 2.4GHz, enabling data rates of 1 or 2Mbps. Since its inception, two major PHY enhancements have been adopted and become “industry standards”. 802.11b adds CCK modulation enabling data rates of up to 11Mbps, and 802.11a specifies OFDM modulation in frequency bands in the 5 to 6GHz range, and enables data rates up to 54Mbps.

Authentication: The process of establishing the identity of another unit (client, user, device) prior to exchanging sensitive information.

Bluetooth: An open specification for short-range wireless voice and data communication. Bluetooth is a trademark owned by Telefonaktibolaget L M Ericsson, Sweden, and licensed to promoters and adopters of the Bluetooth Special Interest Group (SIG).

DFS: Dynamic frequency selection refers to the radar avoidance algorithm referred by 802.11h amendment.

DHCP: Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DNS: Domain Name Service. An Internet service that translates a domain name such as gemtek-systems.com to an IP address, in the form xx.xx.xx.xx, where xx is an 8 bit hex number.

EIRP: The Effective Isotropic Radiated Power of a transmitter is the power that the transmitter appears to have if the transmitter was an isotropic radiator, i.e., if it radiated equally in all directions. By virtue of the gain of a radio antenna, dish, radio telescope or optical telescope, a beam is formed that preferentially transmits the energy in one direction. The EIRP is given by the product of the gain and the transmitter power.

Ethernet: Ethernet is the most widely installed local area network (LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coaxial cable or special grades of twisted-pair wires. Ethernet is also used in wireless LANs. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10Mbps. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.

Fast Ethernet or 100BASE-T provides transmission speeds up to 100Mbps and is typically used for LAN backbone systems, supporting workstations with 10BASE-T cards. Gigabit Ethernet provides an even higher level of backbone support at 1000Mbps (1 gigabit or 1 billion bits per second). 10-Gigabit Ethernet provides up to 10 billion bits per second.

HTTP: The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

Hub: In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. A hub usually includes a switch of some kind. (And a product that is called a "switch" could usually be considered a hub as well.) The distinction seems to be that the hub is the place where data comes together and the switch is what determines how and where data is forwarded from the place where data comes together. Regarded in its switching aspects, a hub can also include a router.

IEEE: Institute of Electrical and Electronics Engineers. The IEEE describes itself as the world’s largest professional society. The IEEE fosters the development of standards that often become national and international standards, such as 802.11.

IP: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

ISP: An ISP (Internet Service Provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

LAN: A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or as many as thousands of users (for example, in an FDDI network).

MAC: Medium Access Control. In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packet formatting and addressing, and error detection.

OFDM: Orthogonal frequency-division multiplexing (OFDM) is a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. The technology was first conceived in the 1960s and 1970s during research into minimizing interference among channels near each other in frequency.

In some respects, OFDM is similar to conventional frequency-division multiplexing (FDM). The difference lies in the way in which the signals are modulated and demodulated. Priority is given to minimizing the interference, or crosstalk, among the channels and symbols comprising the data stream. Less importance is placed on perfecting individual channels.

RADIUS: RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

Router: On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each Internet point-of-presence. A router is often included as part of a network switch.

Routing is a function associated with the Network layer (layer 3) in the standard model of network programming, the Open Systems Interconnection (OSI) model. A layer-3 switch is a switch that can perform routing functions.

RRM: Radio Resource measurement refers to 802.11k amendment.

SDMA: SDMA, or spatial division multiple access, is a communications mode that optimizes the use of the radio spectrum and minimizes the system cost by taking advantage of methods to segment geographic areas.

SNMP: Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMP is described formally in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157 and in a number of other related RFCs.

Switch: In telecommunications, a switch is a network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.

Relative to the layered Open Systems Interconnection (OSI) communication model, a switch is usually associated with layer 2, the Data-Link layer. However, some newer switches also perform the routing functions of layer 3, the Network layer. Layer 3 switches are also sometimes called *IP switches*.

TCP: TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP handles the actual delivery of the data, TCP keeps track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

Telnet: Telnet is the way to access someone else's computer, assuming they have given permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to be actually logged on as a user of that computer.

TKIP: The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalent Privacy, which is used to secure 802.11 WLANs. TKIP provides per-packet key mixing, a message integrity check, and a rekeying mechanism, thus fixing the flaws of WEP.

WEP: Wired Equivalent Privacy is the built-in baseline security protocol that is rolled into the 802.11b protocol. WEP is disabled by default in most shipping WLAN hardware, showing that vendors have never particularly had confidence in WEP and have assumed security would be deployed as a basic WLAN functionality by customers. WEP inhibits raw throughput at a ratio of about 50%.

Wi-Fi: Wi-Fi is short for ***wi****reless* ***fi****delity* and is another name for IEEE 802.11b. It is a trade term promulgated by the Wireless Ethernet Compatibility Alliance (WECA). "Wi-Fi" is used in place of 802.11b in the same way that "Ethernet" is used in place of IEEE 802.3. Products certified as Wi-Fi by WECA are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

WLAN: A WLAN (wireless local area network) is one in which a mobile user can connect to a LAN through a wireless (radio) connection. A standard, IEEE 802.11,

specifies the technologies for WLANs. The standard includes an encryption method, the WEP algorithm.

8.0 Configurable Parameters

This section provides details of the configurable parameters that are accessible through either the CLI or HTTP user interfaces. It focuses on the effects of the parameters and why one would want to change them.

Each configurable parameter has an associated API function that provides access to modify it. Both the CLI and HTTP methods of changing a particular parameter access the same API function. The user interfaces are different (see preceding sections on CLI and HTTP) but the underlying mechanisms are the same.

8.1 Wireless Sectors (interfaces)

The term sector in the CQW-BS1000 product represents a wireless interface consisting of radio, base-band and MAC components. Wireless sector and wireless interface are used interchangeably to describe the same thing.

The CQW-BS1000 production product has three wireless interfaces, each of which can function as a physical AP.

Each of the three interfaces has a number of configurable parameters that can impact operation of the radio, base-band or MAC components. The use of each parameter is discussed below. See the CLI or HTTP sections for information on setting parameters.

8.1.1 MAC Address

The MAC address for each wireless interface can be changed to suit the needs of a particular user and/or site. Although the CQW-BS1000 factory default configuration provides unique MAC addresses for the Ethernet interface and all wireless interfaces, the user may override these with locally-administered MAC addresses or with MAC addresses prefixed with a user-specific OUI.

There is no need for a user to change the MAC address. It is entirely optional.

8.1.2 Mode

Each wireless interface may be set to operate in one of four 802.11 modes, 11A, 11B, 11BG and 11G. Switching modes may have side-effects that must be anticipated. For example, switching from 11A to 11B causes the selection of a new default channel appropriate to that mode. More on this under each mode discussed below.

8.1.2.1 11A Mode

11A mode selects the 5 GHz band (channels 36, 40, 44, 48 etc). The 5 GHz band has the advantages of less interference than the 2.4 GHz band, more channels to choose from and data rates up to 54 Mbps. Setting the mode of a wireless interface to 11A restricts associations on that interface to stations operating in 11A mode.

One disadvantage of 11A mode is the regulatory domain specific restrictions on operating in the presence of radar signaling. In the US, Europe and Australia, it is a requirement to immediately vacate certain channels where known radar signatures are detected. The sets of channels to be concerned about are 52 – 64 (US and Europe) and 100 – 140 (Australia, parts of Europe and soon to be US).

The CQW-BS1000 will automatically monitor for known radar signatures when Spectrum Management is enabled (see discussion of this parameter below). If radar signatures are detected, the CQW-BS1000 will switch to a radar-free channel. The process of switching channels may disrupt the quality of time-sensitive services like voice. Since radar avoidance is required by law (see the 802.11h standard and associated FCC and ETSI documents), this potential disruption is unavoidable when operating in affected channels.

8.1.2.2 11B Mode

11B mode selects the 2.4 GHz band (channels 1 through 11). The 2.4 GHz band is considerably more congested than the 5 GHz band and is limited to data rates up to 11 Mbps. Setting the mode of a wireless interface to 11B restricts associations on that interface to stations operating in 11B mode.

Select 11B mode when the BSS needs to support only 11B stations and not 11G stations.

8.1.2.3 11BG Mode

11BG mode selects the 2.4 GHz band (channels 1 through 11) in “mixed” mode. The 2.4 GHz band is considerably more congested than the 5 GHz band and is limited to data rates up to 11 Mbps for 11B stations and 54 Mbps for 11G stations.

Note that the overall throughput for a station operating in mixed mode may be significantly lower, due to 11G protection mode (self-CTS). 11G protection mode adds some overhead to 11G transmissions to prevent them from impacting legacy 11B traffic. The CQW-BS1000 (and participating 11G stations) automatically engage this mode when required. The result of engaging protection mode is that the performance of 11G stations is substantially reduced. See the discussion of self-CTS for more information.

Select 11BG mode when the BSS needs to support both 11B and 11G stations.

8.1.2.4 11G Mode

11G mode selects the 2.4 GHz band (channels 1 through 11) in “pure G” mode. The 2.4 GHz band is considerably more congested than the 5 GHz band and is limited to data rates up to 54 Mbps.

Note that “pure G” mode assumes there are no 11B stations operating in the BSS and that protection mode (self-CTS) is not required. This allows the interface to operate at optimal efficiency, achieving throughput similar to 11A mode in the 5 GHz band. This of course will depend on local interference in the selected channel.

Select 11G when the BSS needs to support only 11G stations and not 11B stations.

8.1.3 Channel

Selection of a particular mode results in selection of a default channel for that mode. Depending on interference and congestion in that default channel, it may or may not yield optimal performance. Manually selecting a new channel is experimental at best. You can simply try another channel and see if your throughput improves. Avoiding channel 6 in the 2.4 GHz band is a good idea, since many APs default to that channel and it tends to be congested.

If the Listen + Learn feature is enabled, the process of channel selection is continuous and fully automatic. The CQW-BS1000 monitors for interference in all channels and either stays on the current channel or switches channels if overall performance would benefit from the switch. Needless to say, enabling Listen + Learn is recommended over manual channel selection.

8.1.4 Self-CTS (11G Protection Mode)

11G Protection Mode is automatically enabled whenever both 11G and 11B stations interoperate within a BSS. The 802.11g standard requires that this be fully automatic.

Turning 11G Protection Mode off is an option for 11G (“pure G”) mode if the user wishes to completely eliminate the possibility that use of self-CTS is adversely affecting 11G throughput (for benchmarking, etc).

There is no need for a user to change this parameter. It is entirely optional and probably better avoided.

8.1.5 Transmit Power

The Transmit Power setting determines the power level in dBm that frames will be transmitted at. The Transmit Power level must be carefully balanced with the Maximum Data Rate to avoid distortion. For example, setting the Transmit Power to 25 dBm with the Maximum Data Rate at 54 Mbps will likely result is distortion and therefore failed attempts to transmit. Lowering either the Transmit Power or the Maximum Data Rate will eliminate the distortion, thus a Transmit Power of 25 dBm will work much better with a Maximum Data Rate of 48 Mbps or 36 Mbps.

If the user wishes to elevate the Transmit Power in order to reach a distant station, it is likely that the Maximum Data Rate will need to be lowered to avoid distortion.

Normally, this parameter should not be adjusted by the user as it is overridden by the default Automatic Transmit Power Adjustment setting. See the section on Automatic Transmit Power Adjustment for more information.

8.1.6 Automatic Transmit Power Adjustment

The Automatic Transmit Power Adjustment parameter determines behavior of the CQW-BS1000 device driver with respect to transmit power limitation. It defaults to a setting of Max54, which ensures that the device driver will never transmit a frame with a transmit power level too high for the data rate. This setting overrides the Transmit Power value in dBm.

It is recommended that this parameter be set to Max54 and not modified by the user, as doing so guarantees the CQW-BS1000 will never transmit a distorted frame due to an excessive transmit power level (optimizes range and throughput together).

If the Listen + Learn feature is enabled, the process of transmit power adjustment is continuous and fully automatic. The CQW-BS1000 monitors all channels and adjusts its transmit power to accommodate nearby CQW-BS1000 access points. Needless to say, enabling Listen + Learn is recommended over manual Transmit Power selection.

8.1.7 Digital Pre-distortion

Digital Pre-distortion is a Planex-proprietary feature that improves transmit efficiency when used with certain radios. For the Maxim radio in the CQW-BS1000 production hardware, this parameter has no effect. Future versions of the CQW-BS1000 hardware may use radios where this parameter does have effect and this document will be updated to advise its use.

8.1.8 Sensitivity

The receive sensitivity parameter determines how sensitive a wireless interface radio is to low-energy signals. A low-energy signal could be a distant station that is legitimately trying to associate with the CQW-BS1000 AP or it could be cross-interface interference from another wireless interface on the same CQW-BS1000 mini-PCI board.

The sensitivity parameter is set to “high” by default, to ensure that distant stations are “heard” by the CQW-BS1000. If it is known that all stations needing network access through the CQW-BS1000 are relatively close (like, in the same room), the receive sensitivity can be set to “medium” or “low”.

The only reason to set sensitivity to anything but “high” is to avoid cross-interface interference between wireless interfaces on the same CQW-BS1000 mini-PCI board. This might occur if you are running two or three interfaces in the same mode (e.g. 11G) and on adjacent channels.

Sensitivity is an advanced tuning parameter that normally does not need to be changed from its default “high” setting. Avoid changing it unless you suspect cross-interface interference between two or more interfaces on your CQW-BS1000 board.

8.1.9 Maximum Data Rate

The maximum data rate parameter limits the data rate used on a CQW-BS1000 interface. It defaults to the maximum rate allowed for an operating mode (e.g. 54 Mbps for 11A and 11G, 11 Mbps for 11B). The maximum data rate is used in the CQW-BS1000 software’s auto-rate-adjusting algorithm and is the maximum rate that the software will adjust to when up-rating.

There is typically no need to modify the maximum data rate, except for a situation where high transmit power levels are required to reach distant stations. In this case, a data rate of 54 Mbps might not be achievable at a high power level like 20 dBm (due to distortion) and the maximum data rate should be set to something lower like 48 Mbps or 36 Mbps.

Note that the CQW-BS1000 software’s auto-rate-adjusting algorithm will work around a problem with high transmit power by retransmitting at a lower data rate when a higher data rate fails. Although this works, it is not as efficient as avoiding the failing data rate altogether. In cases where the transmit power needs to be set higher than normal to reach distant stations, it may be necessary and will be more efficient to reduce the maximum date rate to account for the potential distortion at the default maximum data rate.

See the discussion of transmit power for more information.

8.1.10 Diversity

Diversity controls the use of antennas on the CQW-BS1000. Each wireless interface has a primary antenna (Antenna 1, default) and a secondary antenna (Antenna 2). Either of these antennas can be selected manually for an interface. The setting applies to both receive and transmit operations.

Setting Diversity to Both causes the device driver to alternately try each antenna, eventually settling on the antenna that yields the best performance.

For transmit (using Both), the preferred antenna setting is maintained on a per-station basis and attempts to transmit to a station are tried first using the preferred antenna from the last transmission.

For receive (using Both), the antenna setting is mostly driven by the transmit diversity algorithm (transmit diversity trumps receive diversity). When there is little transmit activity to drive diversity, the receive diversity algorithm selects an antenna that has the highest RSSI for all stations combined. Typically, it is not the case that traffic will be mostly receive traffic and most of the time, diversity will be driven by the transmit algorithm.

The need to modify this parameter is site-dependent. Some users may find that setting Diversity to Both yields better overall performance for all stations. Other users may find that best performance is achieved by selecting a particular antenna. The best way to establish this is to experiment with the three settings, measure the performance yield of each setting and make a decision based on those results.

8.1.11 Header (preamble)

The Header parameter determines the default preamble type that the CQW-BS1000 MAC will use to transmit in 11B mode. It has no meaning in OFDM modes (11G or 11A).

In 11B mode, a longer preamble allows the receiving side greater time to synch-up on the incoming frame (144 microseconds for long, 72 microseconds for short). The CQW-BS1000 will receive 11B frames that are transmitted by a station with *either* long or short preamble and will respond to (acknowledge) received frames using the same preamble length as the received frame. To summarize:

- The header parameter is specific to 11B mode
- It determines only how the CQW-BS1000 will transmit 11B frames
- It takes 72 microseconds longer to transmit a 11B frame with a long preamble
- Using long preamble may achieve greater interoperability with legacy 11B stations

8.1.12 Beacon Interval

The Beacon Interval is the period in milliseconds between beacon transmissions in a BSS. This parameter can be adjusted higher or lower as a user requires, however adjusting it to too high a value may cause stations to disassociate (station-dependent).

This is set to 100 milliseconds by default and the user should not need to modify it.

8.1.13 Fragmentation

The Fragmentation parameter determines whether or not the CQW-BS1000 MAC will fragment frames into smaller pieces, as indicated by the Fragmentation Threshold parameter. Typically, fragmentation is done to ensure that frames are transmitted cleanly on the first try, by reducing the number of continuous bits transmitted and thereby the likelihood of a transmission error.

Fragmentation overhead is significant, due to the acknowledgement required for every fragment (as opposed to a single acknowledgement for the complete frame). Typically, modern auto-rating algorithms obviate fragmentation . . . although there may be extreme cases where better throughput could be achieved using fragmentation. Users in this situation probably have a serious problem in their network that needs correcting first.

Normally, this parameter should not be modified by the user and should only be modified either as an experiment or by a wireless expert who has determined that fragmentation will solve a specific problem he’s experiencing.

8.1.14 RTS/CTS

The RTS/CTS parameter determines whether or not the CQW-BS1000 MAC will initiate an RTS/CTS sequence preceding transmission of certain data frames, as indicated by the RTS/CTS Threshold parameter. Typically, RTS/CTS exchanges are done to ensure the medium is clear prior to transmitting data. Often, this is done to avoid the so-called “hidden node problem”.

RTS/CTS overhead is significant, due to the RTS and CTS transmission times and the SIFS times between them.

Normally, this parameter should not be modified by the user and should only be modified either as an experiment or by a wireless expert who has determined that use of RTS/CTS will solve a specific problem he’s experiencing (such as the hidden node problem).

8.1.15 Sector (interface) Operating Mode

This parameter should be left at the “Normal” setting, unless there is a specific need to use the interface for spectrum analysis. Note that setting this parameter to Basic Spectrum Analyzer disables all access point functionality previously running on that interface.