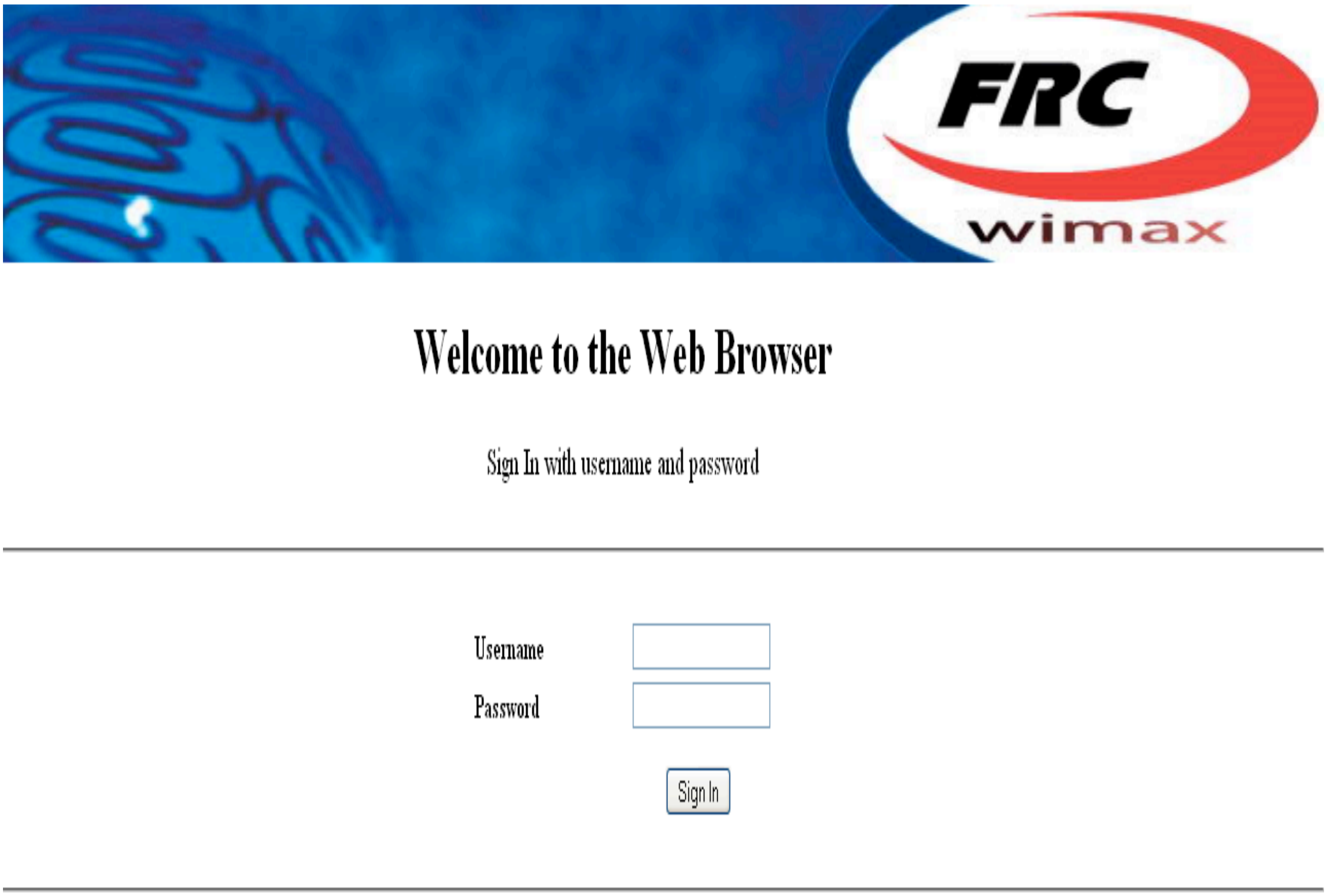
3.1 LOGGING IN

To log in to the GUI, perform the following steps:

1. Ensure the installation described in Chapter 2 is complete. Check that the CPE has power and that the signal strength is good.

2. Launch an Internet browser on the administrator's PC.

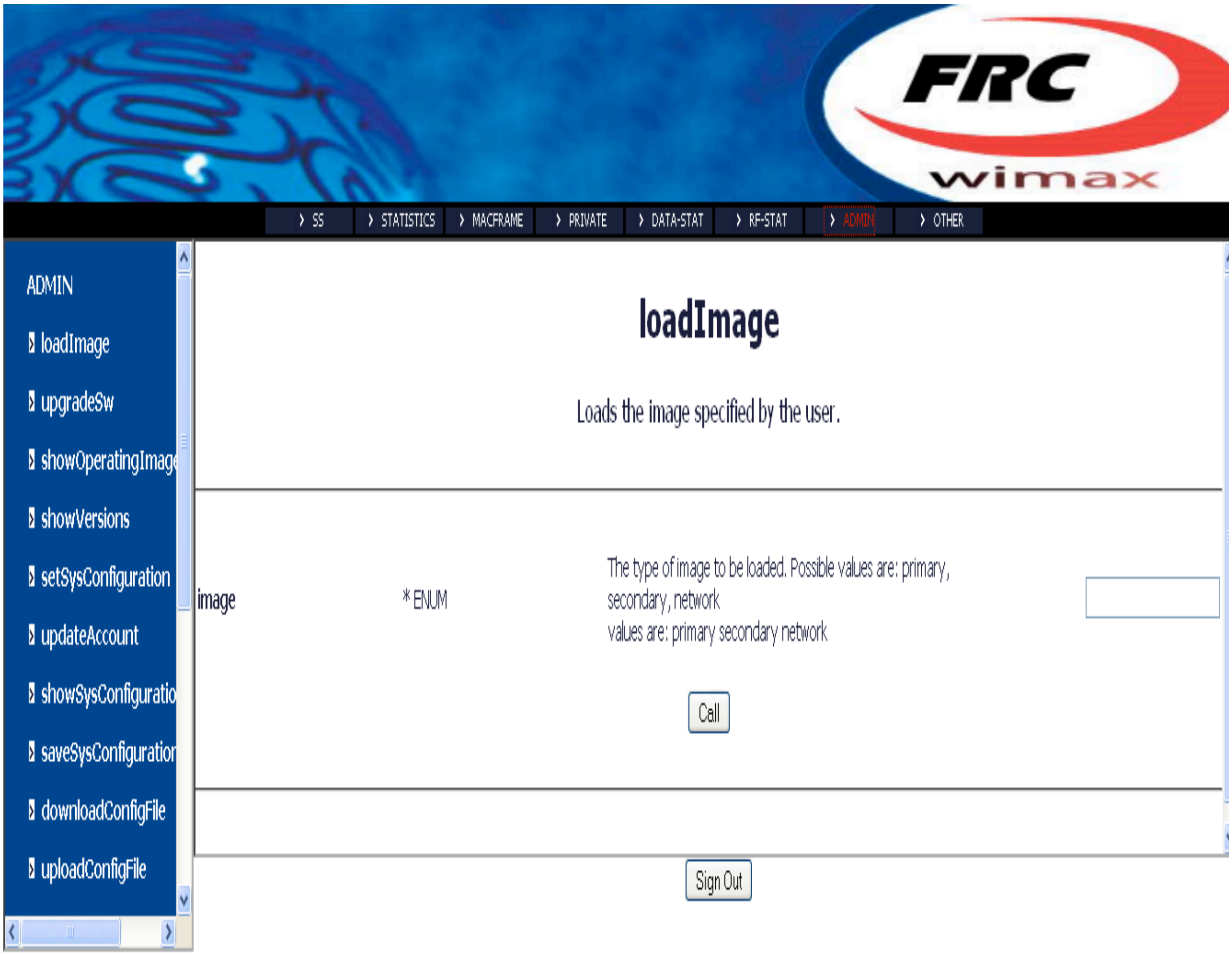
3. Enter the default IP address 192.168.0.21 in the browser address field and press Enter. The Login screen displays:



Welcome to the Web Browser

Sign In with username and password

4. Enter user name <frcweb> and password <frcadmin> and click OK. Then CPE configuration homepage appears:



loadImage

Loads the image specified by the user.

image *ENUM The type of image to be loaded. Possible values are: primary, secondary, network
values are: primary secondary network

NOTE: The CPE functions in Router or Bridge mode.

3.2 SYSTEM SETTINGS

The System Settings is used to review, change and save all CPE system settings. Only the administrator can make changes to this screen.

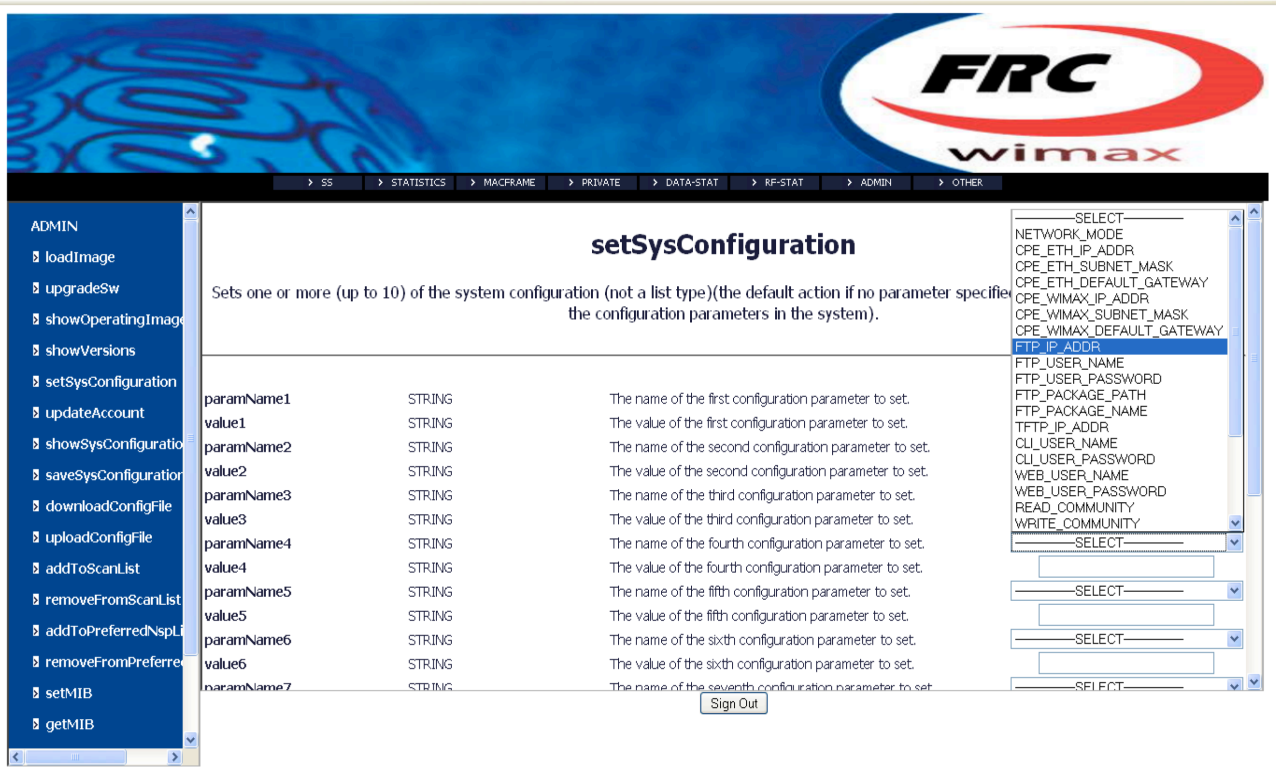
3.2.1 CHANGING SYSTEM CONFIGURATION

To change the CPE system configuration setting, perform the following steps:

1. Enter into the **Admin** Tab field.

2. Enter into **setSystemConfiguration*** field in the left side of Browser.

3. Click **Apply Changes** as shown in the screen below**.



setSysConfiguration

Sets one or more (up to 10) of the system configuration (not a list type)(the default action if no parameter specifie[d] the configuration parameters in the system).

paramName1	STRING	The name of the first configuration parameter to set.
value1	STRING	The value of the first configuration parameter to set.
paramName2	STRING	The name of the second configuration parameter to set.
value2	STRING	The value of the second configuration parameter to set.
paramName3	STRING	The name of the third configuration parameter to set.
value3	STRING	The value of the third configuration parameter to set.
paramName4	STRING	The name of the fourth configuration parameter to set.
value4	STRING	The value of the fourth configuration parameter to set.
paramName5	STRING	The name of the fifth configuration parameter to set.
value5	STRING	The value of the fifth configuration parameter to set.
paramName6	STRING	The name of the sixth configuration parameter to set.
value6	STRING	The value of the sixth configuration parameter to set.
paramName7	STRING	The name of the seventh configuration parameter to set.

* False CPE-Wimax setting could damage the access to CPE or damage CPE itself.

** Changing system Configuration need to be saved by “SysSavedConfigutation” to keep the updated configuration parameters permanent on flash.

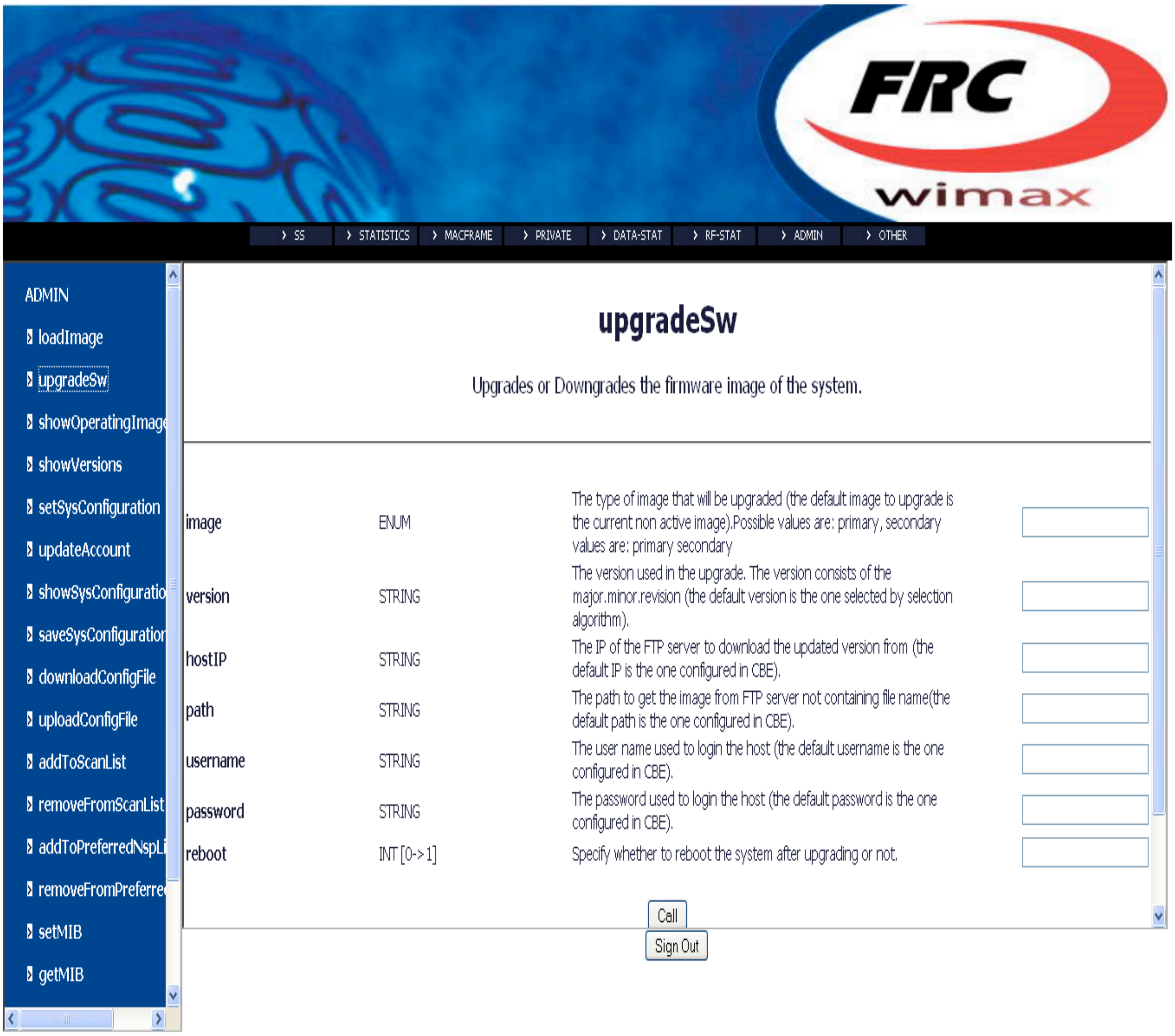
3.2.2 UPGRADE SYSTEM FIRMWARE

To Upgrade the CPE Wimax firmware system, perform the following steps:

1. Enter into the **Admin** Tab field.

2. Enter into **upgradeSw** field in the left side of Browser.

3. Choose the **Upgrade Changes** as shown in the screen below.



upgradeSw

Upgrades or Downgrades the firmware image of the system.

image	ENUM	The type of image that will be upgraded (the default image to upgrade is the current non active image).Possible values are: primary, secondary values are: primary secondary	
version	STRING	The version used in the upgrade. The version consists of the major.minor.revision (the default version is the one selected by selection algorithm).	
hostIP	STRING	The IP of the FTP server to download the updated version from (the default IP is the one configured in CBE).	
path	STRING	The path to get the image from FTP server not containing file name(the default path is the one configured in CBE).	
username	STRING	The user name used to login the host (the default username is the one configured in CBE).	
password	STRING	The password used to login the host (the default password is the one configured in CBE).	
reboot	INT [0->1]	Specify whether to reboot the system after upgrading or not.	

NOTE: Upgrade firmware need permission of system administrator to have successful upgrade. False Upgrade could damage the CPE.

The following parameters should be set correctly in the CPE configurations for SW Upgrade:

FTP Server IP address

FTP user name

FTP password

File path

File name

If any of the configuration parameters are not correct, the system will use the default values for configurations. If the system can't find a newer version or fails to find the specified version the system will keep running with the old SW version.

Other functionalities you can do with **Admin** Tab of the CPE Wimax are the following:

1. Web Configuration for Bridge.
2. Web Configuration for Router.
3. Web Configuration for Vlan.
4. Web Configuration for Operational Frequencies.
5. Web Configuration for SNMP.
6. Web Configuration security setup.
7. Web Configuration for CLI security setup.
8. security setup
9. Default settings reset.

NOTE: Special Tutorial session needed for the web user, moreover, fully awareness of Wimax functionalities are required.

3.2.3 CPE CONFIGURATION PARAMETERS

Configuration Parameter name	Description	Default Value
CPE_ETH_IP_ADDR	The CPE Ethernet IP address	192.168.0.21
CPE_ETH_SUBNET_MASK	The CPE Ethernet subnet mask	255.255.255.0
CPE_ETH_DEFULT_GATEWAY	The CPE Ethernet default gateway	192.168.0.1
CPE_WIMAX_IP_ADDR	The CPE WiMAX IP address (used as static IP if the CPE fails to acquire IP using DHCP)	172.25.25.30
CPE_WIMAX_SUBNET_MASK	The CPE WiMX subnet mask	255.255.255.0
CPE_WIMAX_DEFULT_GATEWAY	The CPE WiMAX default gateway	172.25.25.1
FTP_IP_ADDR	The IP address of the FTP server	192.168.0.220
FTP_USER_NAME	The user name of the FTP server	frcwimax
FTP_USER_PASSWORD	The password of the FTP user	frcwimax
FTP_PACKAGE_PATH	The path of the upgrade packages	/cpe_upgrade
FTP_PACKAGE_NAME	The base name of the upgrade packages	FRC_WIMAX_CPE_.z
TFTP_IP_ADDR	The IP address of the TFTP server	192.168.0.10
CLI_USER_NAME	The user name of the CLI	frccli
CLI_USER_PASSWORD	The password of the CLI user	frcadmin
WEB_USER_NAME	The user name of the web	frcwb
WEB_USER_PASSWORD	the web user password	frcadmin
Configuration Parameter name	**Description**	**Default Value**
READ_COMMUNITY	The read community for the	public

	default SNMP manager	
WRITE_COMMUNITY	The read community for the default SNMP manager	private
TRAP_SERVER_ADDR	The address of the trap server	192.168.0.10
IS_AUTO_UPGRADE_ENABLED	If true automatic upgrade is enabled	False
AUTO_UPGRADE_TIME	The interval between auto-upgrades	1 (days)
CUSTOMER_NAME	The name of the customer	CUSTOMER_NAME
CONFIGURATION_FILE_NAME	The configuration file name	config.xml
SYSTEM_LOCATION	The location of the CPE	SYSTEM_LOCATION
IS_WRITING_LOGS_ON_FTP_ENABLED	Enables and disables transferring logs to the FTP server	FALSE
NETWORK_DEPLOYMENT	A bitmap containing the current enabled network protocols. The bitmap contains the ORing of the different values.	BRIDGE_ENBLED 1 ROUTER_ENBLED 2 DHCP_CLIENT_ENBLED 4 DHCP_SERVER_ENBLED 8 DHCP_RELAY_ENBLED 16 PPPOE_CLIENT_ENBLED 32 PPPOE_PROXY_ENBLED 64 VLAN_ENBLED 128
Configuration Parameter name	**Description**	**Default Value**
EAP_TTLS_USERNAME	The full username required for TTLS inner authentication.	cpe@thebluzone.com
EAP_TTLS_PASSWORD	The password required for TTLS inner authentication	tbzuser

EAP_MODE	Defines which EAP is used TLS or TTLS	1 -> TTLS
DEVICE_CERTIFICATE_FILE_PATH	The full path on the FTP server on which to upload/download	-> FTP root folder
SUPP_WORKAROUND	Enables and disables the supplicant workaround on the CPE	False

Configuration Structure	**Configuration Parameter name**	**Description**	**Default Value**
BRIDGE_CONFIG_STRUCT		Contains the different configuration parameters related to the Bridge.	
	basicIngressFilterEnabled	Enables/Disables the Basic Ingress Filter. When enabled all packets coming from the WiMAX destined to a MAC address in the authenticated list will not pass through the bridge except the DHCP and ARP.	0
	egressBroadcastFilterEnabled	Enables/Disables the Egress Broadcast Filter. When enabled the bridge will not pass through any broadcast or multicast packets coming from the Ethernet.	0
	ingressBroadcastFilterEnabled	Enables/Disables the Egress Broadcast Filter. When enabled the bridge will not pass through any broadcast or multicast packets coming from the WiMAX.	0

Configuration Structure	Configuration Parameter name	Description	Default Value
ROUTER_CONFIG_STRUCT		Contains the NAT related configurations. The structure is formed of an argument which enables/ disables NAT support and a list of NAT mapping rules.	
VLAN_CONFIG_STRUCT	natEnabled	Enables/Disables NAT support. When disabled the CPE is acting as a router between the two interfaces	0
	routerCmd	A NAT mapping rule. The default NAT rule, maps all subnets on the Ethernet interface to the IP address of the WiMAX interface.	map wmxEnd1 0/0 - 0/32
		Contains a list of VLANs configuration parameters. Eac entry contains the following parameters	
	vlanInterface	The interface on which to create the VLAN.	0-> Ethernet 1-> WiMAX
	vlanName	The name of the VLAN which must begin with the prefix “vlan”	
	vlanId	The ID of the VLAN to be placed in the VLAN tag	
	netAddr	The IP address of the VLAN interface	
	netMask	The netmask of the VLAN interface	

3.2.4 IP ADDRESS ASSIGNMENT AND CONFIGURATION FILE RETRIEVAL

The system configuration parameters are maintained in the configuration file saved on flash.

The configuration file saved on flash can exist because of any of the following events:

System finds no configuration file on flash and automatically retrieves a configuration file from a TFTP server. This depends on whether the CPE is offered a configuration file in the DHCP OFFER message or not.

- In case no configuration file is offered by DHCP or the CPE fails to acquire an IP using DHCP, the CPE retrieves either the MAC address configuration file or the default configuration file.
- In case a configuration file is specified in the DHCP, the CPE retrieves either the configuration file specified in the DHCP offer message or the MAC address configuration file or the default configuration file.
- User manually downloads a configuration file using the downloadConfigFile command and reboots.
- User issues a saveSysConfiguration command which saves the current runtime configurations to flash.

As soon as the CPE connects to the BS and is in the OPERATIONAL state, the CPE will start acquiring an IP address using DHCP.

If the CPE successfully acquires an IP address using DHCP, and the DHCP server is configured to offer a configuration file, then the CPE will attempt to retrieve the specified configuration file whether or not a file exists on flash.

If the system successfully retrieves the DHCP configuration file, it will compare its timestamp with the timestamp of the configuration file saved on flash, if newer it will overwrite the file on flash, else it will ignore the retrieved file and continue operation with the one on flash.

If the system fails to acquire an IP using DHCP (four retries performed) then the system will use the IP address specified in the configuration file as the CPE_WIMAX_IP_ADDR.

If the system fails to retrieve the specified file or the file is corrupted and no file exists on flash, the CPE will attempt to retrieve a configuration file from TFTP server baed on its MAC address. If it fails to find the file or the file is corrupted (wrong CRC or mal formatted XML) the CPE will attempt to retrieve the default configuration file. If it fails to retrieve the default configuration file or the file is corrupted (wrong CRC or mal formatted XML), the CPE will use the default configurations saved as macros.

For each TFTP connection, the system will attempt three times with two minutes gap between each retry.

3.2.5 CHANGING CONFIGURATION FILE AFTER INITIALIZATION

To trigger the CPE to use a different configuration file other than the one retrieved in its initialization; the downloadConfigFile command must be used.

Please refer to downloadConfigFile command for more information about changing the configuration file after initialization.

3.2.6 SNMP CONFIGURATION TOOL

MG-SOFT MIB Browser is one of the SNMP Browser tools. Also MG-soft is a flexible, technically superb, powerful and user-friendly SNMP Browser. MIB Browser allows you to perform SNMP Get, SNMP GetNext, SNMP GetBulk and SNMP Set operations. To obtain MG-SOFT MIB Browser software you can refer to http://www.mg-soft.com/download.html.

3.2.7 FACTORY RESET PROCEDURE

The factory reset procedure is used to restore the system configurations to their defaults. For this purpose a configuration file containing the default factory settings should be maintained on flash. The factory reset can be triggered by either pushing a HW push button or from the CLI/Web interfaces.

To handle wrongful presses on the push button, it must be pressed for at least 5 seconds.

3.2.8 STATUS LED

The CPE is equipped with a green LED that indicates the status of the CPE software. The LED flashes with different speeds thus indicating three modes:

1. Before firmware loading -> Off
1. During Firmware loading -> Rapid flashing
2. Scanning for BS -> Slow flashing
3. Connected to a BS (Operational) -> On

3.2.9 AUTHENTICATION SUPPORT

The CPE supports three modes of authentication:

1. Null authentication: This can be enforced by setting the PKM version to none on the BS.
2. Supplicant workaround flag: In which case the CPE is only involved in the authentication using dummy keys. It is not recommended to use this mode.
3. EAP Authentication using either TLS or TTLS.

In order to switch between the workaround and supplicant modes, the SUPP_WORKAROUND configuration parameter must be set and saved.

1. If the supplicant is enabled then SUPP_WORKAROUND flag is set to True, the CPE will work with the supplicant workaround mode with the next authentication procedure, however it is recommended to stop and start the CPE.
2. To switch from the workaround mode to the Supplicant mode, a reboot is needed since the supplicant needs to be initialized in the BSP.

CHAPTER FOUR: CLI COMMANDS

4.1 LOADIMAGE

loadImage		
Arguments	image (M)	Represents which image will be loaded. Possible values are: primary : loads the primary image secondary: loads the secondary image network: loads image from network
Description	Load the firmware.	
Examples	loadImage primary loadImage secondary loadImage network	

4.2 UPGRADESW

upgradeSw		
Arguments	image (O)	Represents which image will be upgraded. Possible values are: primary: upgrades the primary image secondary : upgrades the secondary image If not specified, system upgrades the non-
	version (O)	String representing the version which is used in the upgrade. The version consists of the major.minor.revision If the version is not specified, the Version
	hostIP (O)	The IP address of the FTP server on which upgraded software is placed. If hostIP is not specified, the default host IP configured in
	path (O)	The full path to the software image on the FTP server. If path is not specified, the default path configured in the CPE is used.
	username (O)	The user name to login to the FTP server to get the software image. If the user name is not specified the username configured in
	password (O)	The password to login to the FTP server to get the software image. If the user name is not specified the password configured in
	reboot (O)	Specify whether to make reboot for system after upgrade is completed.
Description	Upgrades/Downgrades the firmware on the CPE.	
Examples	upgradeSw upgradeSw primary upgradeSw secondary reboot=1 upgradeSw secondary v0.0.1	

4.3 SHOWVERSIONS

showVersions

Arguments	type (O)	Possible values are: primary : get the version of the primary image secondary: get the version of the secondary image hw: get the HW version If no argument is specified, display the version of images as well as the HW version and the operating image.
Description	Display the versions of the HW and SW versions in the system and state the operating image as well.	
Examples	showVersions showVersions primary showVersions secondary showVersions hw	

4.4 SHOWSYSCONFIGURATION

showSystemConfiguration		
Arguments	paramName(O)	The name of the configuration parameter to show. If no name is given, it displays all the configuration parameters
Description	Retrieves the given configuration parameter or all the system configurations if no argument was given.	
Examples	showSysConfiguration showSysConfiguration CPE_IP_ADDR showSysConfiguration READ_COMMUNITY showSysConfiguration SCAN_LIST	

4.5 SETSYSCONFIGURATION

setSystemConfiguration		
Arguments	paramName 1 (O)	The name of the first parameter to set

	value 1 (O)	The value of the first parameter to set
	paramName 2 (O)	The name of the second parameter to set
	value 2 (O)	The value of the second parameter to set
	…………..	Names and Values of the other parameters
	paramName 10 (O)	The name of the tenth parameter to set
	value 10 (O)	The value of the tenth parameter to set
Description	Set one or more (up to 10) of the system configurations. If no argument is specified the command displays a description of all the configuration parameters in the system.	
Examples	setSysConfiguration setSysConfiguration CUSTOMER_NAME FRC setSysConfiguration IS_AUTO_UPGRADE_ENABLED 1 READ_COMMUNITY public	

4.6 SAVESYSCONFIGURATION

saveSysConfiguration	
Arguments	None
Description	Save permanently on flash the current configuration parameters.
Examples	saveSysConfiguration

4.7 DOWNLOADCONFIGFILE

downloadConfigFile		
Arguments	tftpAddr (O)	The address of the TFTP server in which the configuration file exists. If not given, the default
	filePath (O)	The path and the file name of the configuration file. If not given, the default is used. The specified file path should be on the TFTP root.
	reboot (O)	Reboot option to reboot after getting the file.
Description	Download a new configuration file.	
Examples	downloadConfigFile downloadConfigFile 192.168.0.10 downloadConfigFile reboot=1 downloadConfigFile 192.168.0.10 reboot=1 downloadConfigFile filePath=config.xml downloadConfigFile 192.168.0.10 /downloads/config.xml 1	

4.8 UPLOADCONFIGFILE

uploadConfigFile		
Arguments	tftpAddr (M)	The address of the TFTP server to which the configuration file is uploaded.
	filePath (M)	The path and the file name of the configuration file. The specified file path should be on the TFTP root. Example: /uploads/config.xml
Description	Upload the configuration file stored in flash to the TFTP server	
Examples	uploadConfigFile 192.168.0.10 /uploads/config.xml	

4.9 ADDTOSCANLIST

addToScanList		
Arguments	frequency (M)	The frequency to add.
	duration (M)	The duration.
	bandwidth (M)	The channel bandwidth.
Description	Add new element to the scan list.	
Examples	addToScanList 3650 500 4	

4.10 REMOVEFROMSCANLIST

removeFromScanList		
Arguments	frequency (M)	The frequency to be removed
Description	Remove an element from the scan list.	
Examples	removeFromScanList 3500	

4.11 ADDTOPREFERREDNSPLIST

addToPreferredNspList		
Arguments	nspId (M)	The NSP ID to be added to the preferred to the preferred NSP list
	nspName (M)	The NSP name to be added to the preferred NSP list
	priority (M)	The priority of NSP to be added to the preferred NSP list (0->255). Value can't be 251,252,253,254
Description	Adds new element to the preferred Network Service Provider (NSP) list.	
Examples	addToPreferredNspList AA:BB:CC NSP1 100	

4.12 REMOVEFROMPREFERREDNSPLIST

removeFromPreferredNspList		
Arguments	nspId (M)	The NSP ID to be removed from the preferred to the preferred NSP list
Description	Removes an element to the preferred Network Service Provider (NSP) list.	
Examples	removeFromPreferredNspList AA:BB:CC	

4.13 UPDATEACCOUNT

updateAccount		
Arguments	accountType (M)	The type of account to be updated. Possible values
	userName (M)	The new user names of CLI or WEB account to
	password (M)	The new passwords of CLI or WEB account to update.
Description	Updates the CLI and WEB account user name and password.	
Examples	updateAccount cli cliUser cliFrcPwd updateAccount web webUser webFrcPwd	

4.14 GETMIB

getMIB		
Arguments	module (O)	The module of the MIB variable
	name (O)	The Name of the MIB variable
	index1 (O)	Key to get the specified MIB from a table
	index2 (O)	Key to get the specified MIB from a table
	index3 (O)	Key to get the specified MIB from a table
	index4 (O)	Key to get the specified MIB from a table
	index5 (O)	Key to get the specified MIB from a table
	oid (O)	The object identifier of the MIB variable. The OID value should contain the required indices of the table for accessing a specific entry in a table.
Description	Get the value of the specified MIB. If the MIB module is specified, a MIB name should also be specified; otherwise the MIB OID should be specified. If the index is a MAC address it should be entered in a dotted decimal format.	
Example	getMIB oid = 1.0.8802.16.2.1.3.1.1.3 getMIB module = WMAN-DEV-MIB name = wmanDevBsCurrentSwVersion index1 = 1	

4.15 SETMIB

setMIB		
Arguments	module (O)	The module of the MIB variable
	name (O)	The Name of the MIB variable
	index1 (O)	Key to get the specified MIB from a table
	index2 (O)	Key to get the specified MIB from a table
	index3 (O)	Key to get the specified MIB from a table
	index4 (O)	Key to get the specified MIB from a table
	index5 (O)	Key to get the specified MIB from a table
	oid (O)	The object identifier of the MIB variable
	type (M)	The type of the assigned MIB value. Possible values are: i : integer value c: counter value g: gauge value
	value (M)	The value assigned to the MIB
Description	Set the value of specific MIB. If the MIB module is specified, a MIB name should also be specified; otherwise the MIB full OID should be specified. If the index is a MAC address it should be entered in a dotted decimal format.	
Example	setMIB oid=1.0.8802.16.2.1.3.1.1.1 type=i value=5 setMIB oid=1.0.8802.16.2.1.3.1.1.1 type=h value=192 (Sets the value of a bits MIB to 11000000) setMIB module = WMAN-IF2F-BS-MIB name = wmanIf2fBsSfDirection index1 = 1 index2 = 0.1.2.3.4.5 index3 = 2 type=i value=5	

4.16 GETNEXTMIB

getNextMIB		
Arguments	module (O)	The module of the MIB variable
	name (O)	The Name of the MIB variable
	index1 (O)	Key to get the specified MIB from a table
	index2 (O)	Key to get the specified MIB from a table
	index3 (O)	Key to get the specified MIB from a table
	index4 (O)	Key to get the specified MIB from a table
	index5 (O)	Key to get the specified MIB from a table
	oid (O)	The object identifier of the MIB variable
Description	Get the value of the MIB after the specified one. If the MIB module is specified, a MIB name should also be specified; otherwise the MIB OID should be specified. If the index is a MAC address it should be entered in a dotted decimal format.	
Example	getNextMIB oid=1.0.8802.16.2.1.3.1.1.3 getNextMIB module = WMAN-DEV-MIB name = wmanDevBsCurrentSwVersion index1 = 1	

4.17 GETBULK

getBulk		
Arguments	module (O)	The module of the MIB variable
	name (O)	The Name of the MIB variable
	index1 (O)	Key to get the specified MIB from a table
	index2 (O)	Key to get the specified MIB from a table
	index3 (O)	Key to get the specified MIB from a table
	index4 (O)	Key to get the specified MIB from a table
	index5 (O)	Key to get the specified MIB from a table
	oid (O)	The object identifier of the MIB variable
	maxRepetitions (M)	The max repetition value in the get bulk request
Description	Gets a bulk of MIBs starting at the specified OID.	
Example	getBulk oid=1.0.8802.16.2.1.3.1.1 maxRepetitions= 15 getBulk module = WMAN-DEV-MIB name = wmanDevBsCurrentSwVersion index1 = 1 maxRepetitions = 10	

Note:

The following is a list of the MIB module names that are used:

- WMAN-DEV-MIB
- WMAN-IF2-SS-MIB
- WMAN-CPE-PRIVATE-MIB

4.18 RESTOREFACTORYSETTINGS

restoreFactorySettings	
Arguments	None
Description	Triggers the factory reset.
Examples	restoreFactorySettings

4.19 DOWNLOADDEVICECERT

downloadDeviceCert		
Arguments	name (M)	A descriptive name of which file to download. This name doesn't match the name of the file on server. It can take one of four values: rootCert: The CA certificate from which the device certificate is generated. deviceCert: The device certificate. deviceKeyFile: The key file
	filePath (O)	The path and the file name of the configuration file. If not given, the default path is used.
	ftpAddr (O)	The address of the FTP server in which the certificate files exist. If not given, the default
	username (O)	The username used in FTP authentication. If not given the default username is used.
	password (O)	The password used in FTP authentication. If not given the default password is used.
Description	Downloads the device certificates one by one. This command should be issued four times in order to download the whole set of files needed for authentication.	
Examples	downloadDeviceCert rootCert	

4.20 UPLOADDEVICECERT

uploadDeviceCert		
Arguments	name (M)	A descriptive name of which file to upload. This name doesn’t match the name of the file on server. It can take one of four values: rootCert: The CA certificate from which the device certificate is generated. deviceCert: The device certificate. deviceKeyFile: The key file
	filePath (M)	The path and the file name of the configuration file. Must be specified
	ftpAddr (O)	The address of the FTP server in which to upload the certificate files. If not given, the default address is used.
	username (O)	The username used in FTP authentication. If not given the default username is used.
	password (O)	The password used in FTP authentication. If not given the default password is used.
Description	Uploads the device certificates one by one. This command should be issued four times in order to upload the whole set of files needed for authentication.	
Examples	uploadDeviceCert rootCert /home/uploads/root.pem uploadDeviceCert deviceCert /home/uploads/deviceCertificate.pem ftpAddr=192.168.0.10 uploadDeviceCert deviceKeyFile filePath=/home/certificates/devkey.pem uploadDeviceCert randomFile /home/uploads/random username=frcwimax password=frcwimax	

4.21 SHOWCURRENTNETWORKDEPLOYMENT

showCurrentNetworkDeployment	
Arguments	None
Description	Show the current network deployment topology working on CPE.
Examples	showCurrentNetworkDeployment

4.22 SETCURRENTNETWORKDEPLOYMENT

setCurrentNetworkDeployment		
Arguments	enableBridge (O)	If true, activate bridge, else disable bridge. If not specified do nothing i.e if enabled leave it enabled.
	enableRouter (O)	If true, activate router, else disable router. If not specified do nothing.
	enableDhcpClient (O)	If true, activate DHCP client, else disable DHCP client. If not specified do nothing.
	enableDhcpServer (O)	If true, activate DHCP server, else disable DHCP server. If not specified do nothing.
	enableDhcpRelay (O)	If true, activate DHCP Relay, else disable DHCP relay. If not specified do nothing.
	enablePPPoEClient (O)	If true, activate PPPoE client, else disable PPPoE client. If not specified do nothing.
	enablePPPoEProxy (O)	If true, activate PPPoE proxy, else disable PPPoE proxy. If not specified do nothing.
	enableVlan(O)	If true, activate VLAN, else disable VLAN. If not specified do nothing.
Description	Configure the current network topology by enabling and disabling the network protocols.	
Examples	SetCurrentNetworkDeployment enableVlan=0 SetCurrentNetworkDeployment enableDhcpClient=1 SetCurrentNetworkDeployment enableBridge=0 enableRouter=1	

4.23 CONFIGUREPPPOE

ConfigurePPPoE		
Arguments	mode (M)	This parameter indicates whether PPP over Ethernet will be configured in client mode or proxy mode. Client: configure PPPoE client
	maxSessionsCount (O)	Maximum total number of PPPoE sessions allowed before incoming PPPoE packets are ignored. (The default is 16).
	authenticationMode (O)	The authentication mode to configure PPPoE to use. It could be: pap: enable using pap protocol chap: enable using chap protocol
	userName (O)	The user name to use to authenticate the
	Password (O)	The password to use to authenticate the peer
Description	Configure PPPoE (client or proxy) on the CPE. This command not making an action for now but it is saving the configuration of PPPoE client in the configurations and proxy is not yet supported.	
Examples	configurePPPoE client 16 pap frcuser frc2009 configurePPPoE client authenticationMode=chap username=frcuser password=frc2009	

4.24 CONFIGUREBRIDGE

configureBridge		
Arguments	broadcastIngressFiltering (O)	Enable broadcast ingress filtering
	broadcastEgressFiltering (O)	Enable broadcast egress filtering
	basicIngressFiltering (O)	Enable basic ingress filtering
Description	Configure Bridge on the CPE.	
Examples	configureBridge 1 1 1 configureBridge broadcastIngressFiltering=0 cconfigureBridge basicIngressFiltering=0 broadcastEgressFiltering=1	

4.25 CONFIGUREROUTER

configureRouter		
Arguments	enableNat (O)	Enable or Disable NAT. The default value is Enable.
Description	Configure Router on the CPE.	
Examples	ConfigureRouter 0 configureRouter enableNat=1 configureRouter	

4.26 CONFIGUREVLAN

configureVlan		
Arguments	vlanName (M)	The name of the VLAN.
	vlanId (M)	The VLAN ID to use in the tags. Valid range is from 1 to 4094.
	netAddr (M)	The vlan network address
	netMask(M)	The vlan sub-net mask
	interface (O)	The interface on which to configure VLAN support. wired: wired interface wireless: wirless interface If not specified, wireless interface is use.
Description	Configure VLAN protocol on the CPE.	
Examples	configureVlan vlan1 10 192.168.0.11 255.255.255.0 wired configureVlan vlan1 11 172.25.25.30 255.255.255.0 wireless configureVlan vlan2 12 172.25.25.30 255.255.255.0	

4.27 REMOVEVLANCONFIGURATION

removeVlanConfiguration		
Arguments	index(O)	This parameter indicates the required index to be removed.
Description	Removes Vlan with specified index. If index is not specified the command will show all name of Vlans available with corresponding index.	
Examples	removeVlanConfiguration removeVlanConfiguration 0 removeVlanConfiguration index=1	

CHAPTER FIVE: TYPICAL USAGE SCENARIOS

Network Deployment Setups as follow:

5.1 BRIDGE SETUP

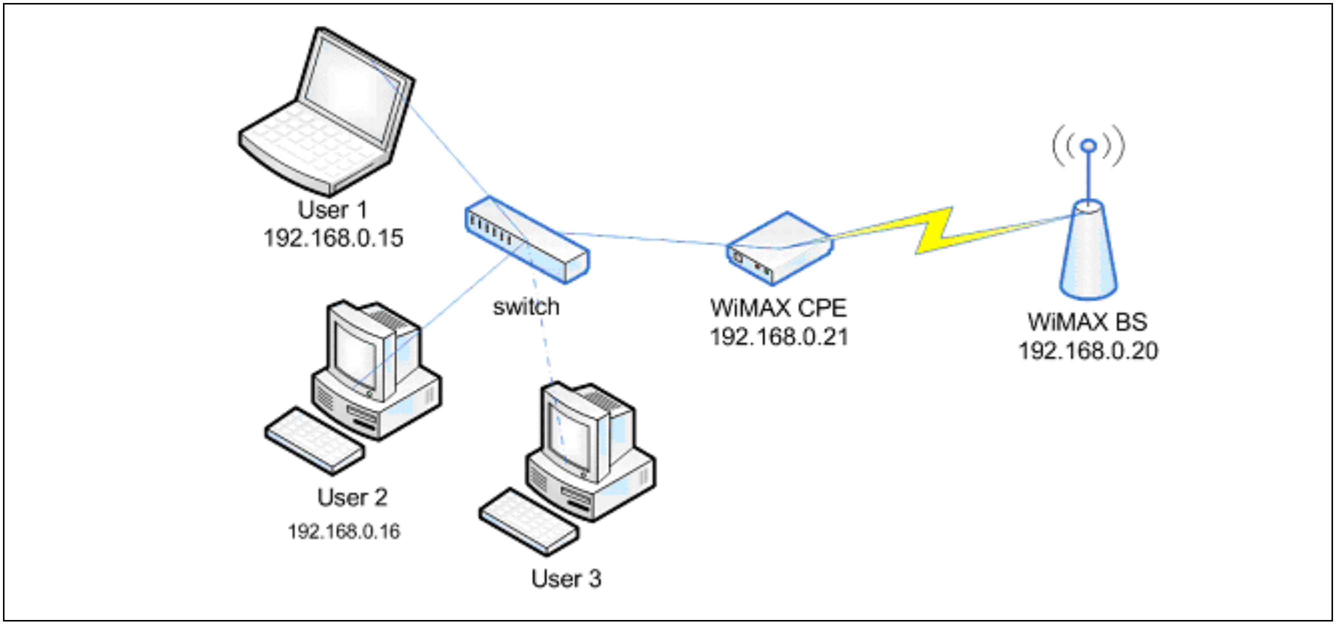


Figure 7: Bridge Setup

5.2 ROUTER SETUP

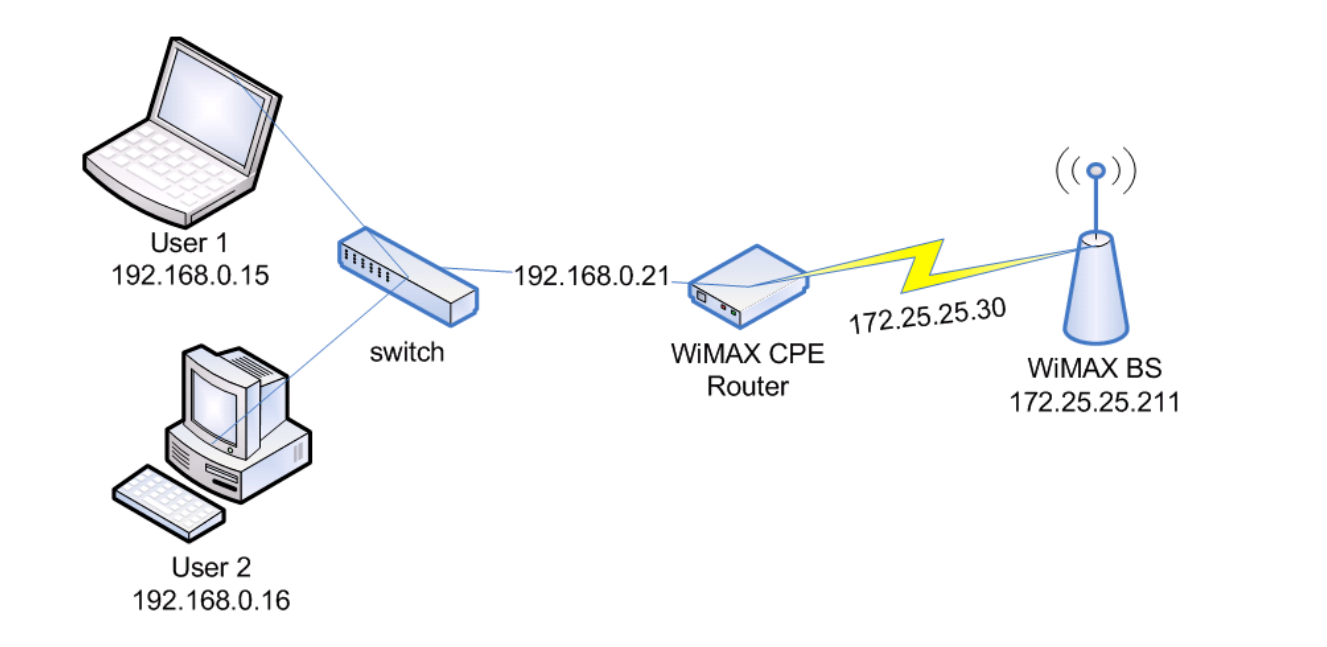


Figure 8: Router Setup

5.3 DHCP SERVER SETUP

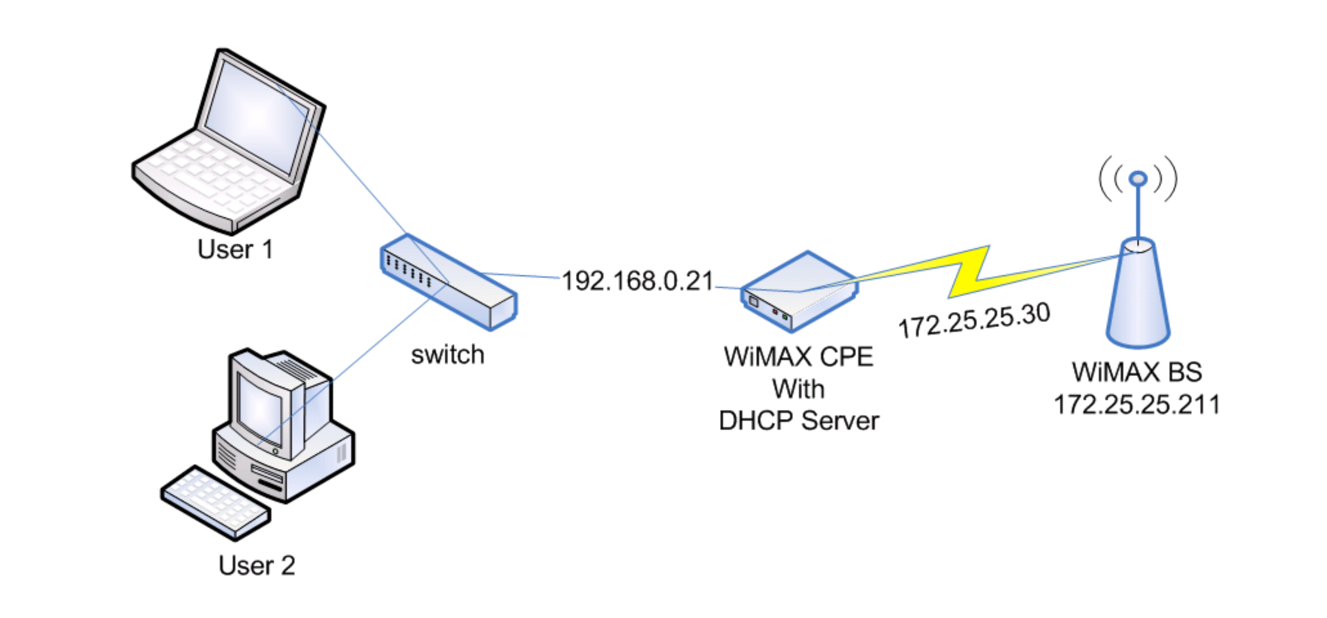


Figure 9: CPE with DHCP server setup

The CPE can be acting in either Bridge or Router modes and will be able to offer DHCP leases to hosts on the Ethernet side such as User1 user 2.

GLOSSARY

This section defines or identifies technical terms, abbreviations, and acronyms used throughout this document.

100BASE-TX IEEE 802.3u specification for 100 Mbps Fast Ethernet over two airs of Category 5 or better UTP cable.

10BASE-T IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3 or better UTP cable.

Administrator An administrator performs the service of maintaining a network. In the case of this Router, the person who sets up the Router and makes changes to the settings.

Advanced Encryption Standard (AES) An strong encryption algorithm that implements symmetric key cryptography.

Authentication The process to verify the identity of a client requesting network access.

Auto-negotiation Signaling method allowing each node to select its optimum operational mode (speed and duplex mode) based on the capabilities of the node to which it is connected.

Base Station A WIMAX service provider's equipment that is installed at a fixed location to provide network connectivity for subscriber stations within a defined service area.

Client A computer on the network that uses the services of the Router, such as the automatic DHCP server and Firewall.

CLI Command Line Interface

Customer Premise Equipment (CPE) Customer Premise Equipment: Communications equipment that resides on the customer's premises.

CS Convergence Sublayer

CSN Connectivity Service Network

Demilitarized Zone (DMZ) A virtual zone in the router that is not protected by The Router's firewall.

One computer can be placed in the DMZ.

Domain Name System (DNS) A system used for translating host names for network nodes into IP

addresses. DNS allows Internet host computers to have a domain name (such as belkin.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and

their respective domain names and IP addresses, so that when a domain name is requested (as in typing **easyDNS.com** into an Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on the home network is the location of the DNS server the ISP has assigned.

Dynamic Host Control Protocol (DHCP) Dynamic Host Configuration Protocol: Provides a framework for passing

configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Dynamic IP An IP address that is automatically obtained from a DHCP server.

Ethernet A popular local area data communications network, which accepts

transmission from computers and terminals. A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 million bits per second (Mbps).

Encryption Data passing between a base station and clients can use encryption to protect from interception and eves-dropping.

Extensible Authentication

Protocol (EAP) An authentication protocol used to authenticate network clients. EAP is

combined with IEEE 802.1X port authentication and a RADIUS authentication server to provide “mutual authentication” between a client, the access point, and the a RADIUS server

File Transfer Protocol (FTP) File Transfer Protocol: A TCP/IP protocol used for file transfer.

Firewall An electronic boundary that prevents unauthorized users from accessing certain files or computers on a network.

Firmware Software stored in memory. Essential programs that remain even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on a disk.

Hypertext Transfer Protocol (HTTP) Hypertext Transfer Protocol: HTTP is a standard used to transmit and receive all data over the World Wide Web.

IEEE 802.16e A standard that provides mobile broadband wireless access using Scalable Orthogonal Frequency Division Multiple Access (SOFDMA).

IP Address IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies an single, unique Internet c computer host. Example: 192.34.45.8.

ISP Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

ISP Gateway Address (see ISP for definition). The ISP Gateway Address is an IP address for t the Internet router located at the IPS's office. This address is required o only when using a cable or DSL modem.

Local Area Network (LAN) A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). A home network is considered a LAN.

MAC Media Access Control: The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.

MAC Address Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE.

MIB Management Information Base.

Orthogonal Frequency Division Multiplexing (OFDM) Orthogonal Frequency Division Multiplexing: OFDM allows multiple users to transmit in an allocated band by dividing the bandwidth into many narrow bandwidth carriers.

Power Over Ethernet (PoE) Power over Ethernet: A specification for providing both power and data to low-power network devices using a single Category 5 Ethernet cable. PoE provides greater flexibility in locating network devices, and significantly decreased installation costs.

MTU Maximum Transmission Unit. The largest unit of data that can be transmitted on any particular physical medium.

NAT Network Address Translation. This process allows all of the computers on the home network to use one IP address. Using the NAT capability of the Home-Connect home network gateway, access is available to the Internet from any computer on the home network without having to purchase more IP addresses from the ISP.

Port A logical channel that is identified by its unique port number. Applications listen on specific ports for information that may be related to it.

PPPoE Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

PPTP Point-to-Point Tunneling Protocol. A version of PPP (Point-to-Point Protocol) that has the ability to encapsulate packets of data formatted for one network protocol in packets used by another protocol. This tunneling technique allows TCP/IP data to be transmitted over a non-TCP/IP network. PPTP can be used to join different physical networks using the Internet as an intermediary.

SNTP Simple Network Time Protocol. A communication standard that allows for

The transmission of real time information over a network or the Internet.

SPI Stateful Packet Inspection. SPI is the type of corporate-grade Internet s security provided by a HomeConnect home network gateway. Using SPI,

the gateway acts as a firewall, protecting the network from computer hackers.

Static IP An IP address that is manually configured and never changes.

Subnet Mask A subnet mask, which may be a part of the TCP/IP information provided

by the ISP, is a set of four numbers configured like an IP address. It is

used to create IP address numbers used only within a particular network

(as opposed to valid IP address numbers recognized by the Internet, which must assigned by Inter-NIC).

Subscriber Station A general term for a customer's WIMAX terminal equipment that provides connectivity with a base station.

SNMP Simple Network Management Protocol

TCP Transmission Control Protocol. The most common Internet transport layer protocol. TCP is connection-oriented and stream-oriented, and provides for reliable communication over packet-switched networks.

TCP / IP Transmission Control Protocol over Internet Protocol. This is the standard protocol for data transmission over the Internet.

Trivial File Transfer Protocol (TFTP) Trivial File Transfer Protocol: A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. Communications protocol for the Internet Network layer, transport layer, and session layer, which makes it possible to send a datagram message from one computer to an application running in another computer. Unlike TCP, UDP is connectionless and does not guarantee reliable communication; the application itself must process any errors and check for reliable delivery.

UTP Unshielded twisted-pair cable.

WAN Wide Area Network. A network that connects computers located in Geographically separate areas, (i.e., different buildings, cities, countries). The Internet is a wide area network.

VLAN Virtual Local Area Network.

VPN Virtual Private Network.

WAN IP Address The IP address assigned to the router by the ISP.

WLAN Wireless Local Area Network. A local area network that connects Computers close together via radio (such as 802.11b)

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.