

QorIQ LS1024A Reference Design Board User Guide

1 Introduction

This document describes the Multifunction Reference Design Board from Freescale Semiconductor. This document is a startup user guide for operating and upgrading the following LS1024A Reference Design Boards:

This document is organized as follows:

2, “[Reference Design Boards](#)”—This section gives an overview of LS1024A Reference Design boards.

3, “[Getting Started](#)”—This section describes how to setup and operate the LS1024A Reference Design Board under different scenarios.

4, “[Reference Design Board Operation](#)”—This section describes the Board operations.

5, “[Configuration Through Web User Interface](#)”—This section describes the Reference Design board GUI configuration through Web User interface.

6, “[Flashing or upgrading software](#)”—This section describes the configurations and steps to upgrade the file system and flash memory.

Contents

1. Introduction	1
2. Reference Design Boards	4
3. Getting Started	8
4. Reference Design Board Operation	13
5. Configuration Through Web User Interface	16
6. Flashing or upgrading software	67
7. Appendix	79
8. Revision History	94

7, “Appendix” —This section explains the Fax testing setup and Inter-asterisk setup.

1.1 Acronyms in this Document

The following table gives a summary of acronyms appearing in this document.

Table 1. Acronyms in this Document

Acronyms	Description
B2BUA	Back to Back User Agent
CO	Central Office
DFEC	Dual Filter Echo Cancellor
DDR	Dial-on-Demand Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DSP	Digital Signal Processing
ESD	Electrostatic Sensitivity Discharge
GUI	Graphical User Interface
FXS	Foreign Exchange Subscriber
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
LAN	Local Area Network
NAT	Network Address Translation
PBX	Private Branch Exchange
PCI	Peripheral Component Interconnect
PHY	Ethernet Physical Interface device
PLL	Phase-Locked Loop
POTS	Plain Old Telephone Service
PPPoE	Point-to-Point Protocol Over Ethernet
RVDS	Real Veiw Developer Suite
SIP	Session Initiation Protocol
SLIC	Subscriber Line Interface Circuit
SNAT	Secure Network Address Translation
SoC	System-on-Chip
SOHO	Small Office/Home Office
SPI	Serial Peripheral Interface
TDM	Time-Division Multiplexing
TFTP	Trivial File Transfer Protocol

Table 1. Acronyms in this Document (continued)

Acronyms	Description
USB	Universal Serial Bus
VLC	Video LAN Client
WAN	Wide Area Network

1.2 Board Package Contents

Freescall delivers Reference Design Board in a box with Electrostatic Sensitivity Discharge (ESD) warning labels. The package contains the following components:

- Freescale Reference Design Boards provided for evaluation of the LS1024A device
- Power supply
- LS1024A Reference Design Board User Guide

Other components may be present in the delivery. Always check the packing list of your delivery for complete contents description.

1.3 Design Kit Summary

A design kit is available supporting the board package, and includes the following materials:

- Documents, such as software manuals, application notes, training slides and so on.
- OpenWrt Software Development Kit (SDK).
- Source Code for Drivers.
- Media Stream Binary Firmware.
- Hardware Reference Design Materials.

1.4 Precautions

Observe the following precautions when handling the board:

- Connect all cables to the board before switching the power.
- Be cautious when updating bootloader (microloader and Barebox/U-Boot). If the procedure fails, then the board will not boot anymore.

1.5 Electrostatic Discharge

When handling any electronic component or assembly, observe the following minimum electrostatic discharge abatement precautions to prevent damage:

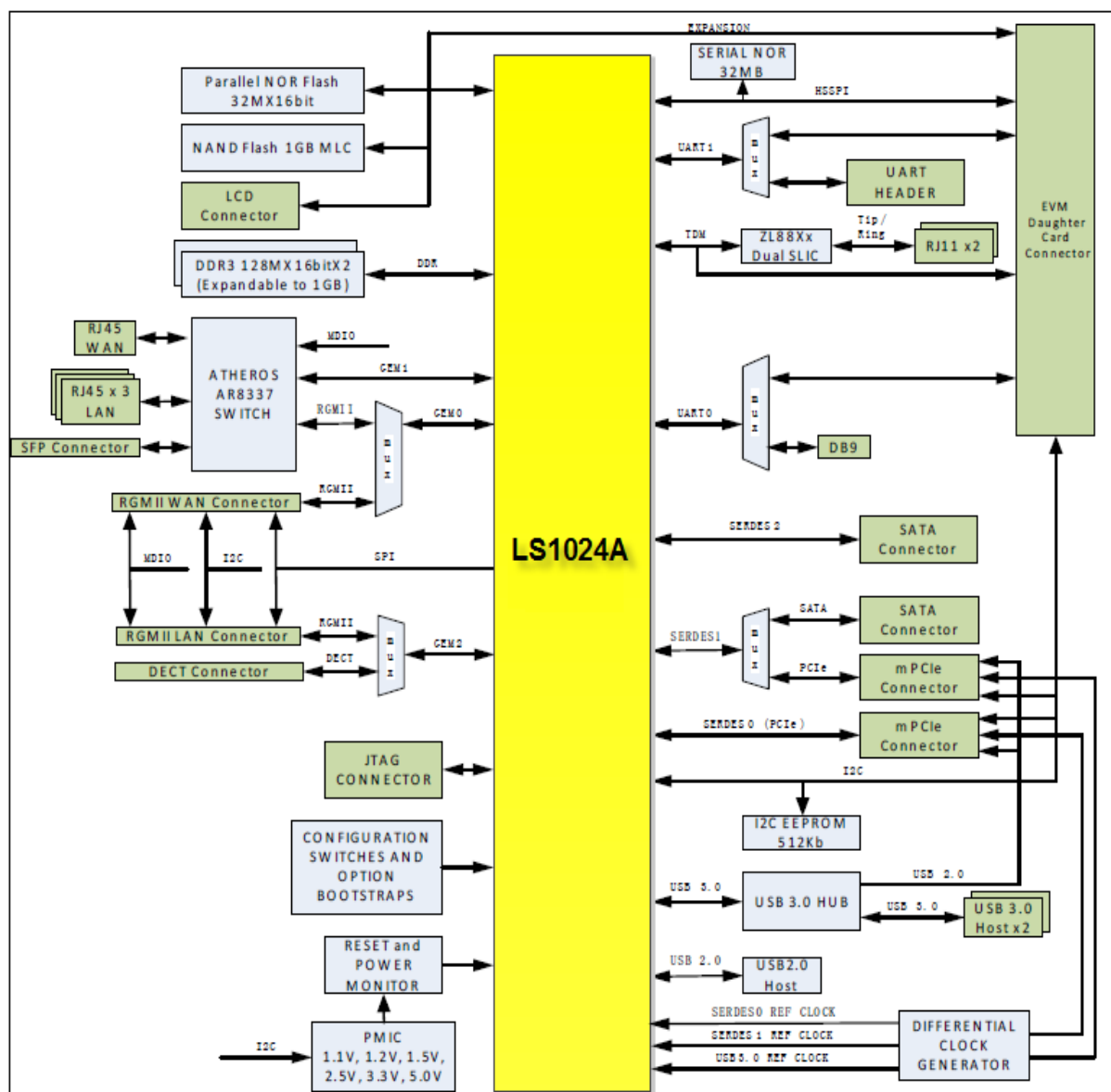
- Treat all assemblies, components, and interface connections as static-sensitive.
- Avoid working in carpeted areas, and keep body movement to a minimum while removing or installing boards, to minimize buildup of static charge.
- To help reduce ESD, remove all jewelry.
- Use ESD preventing accessories, such as wrist straps or heel straps.

2 Reference Design Boards

2.1 Features

This section describes the features of LS1024A Reference Design Board.

Figure 1. LS1024A RDB Top Level block diagram



2.2 Feature Overview

The Reference Design Board provides the following hardware interfaces:

- MEMORY
 - Default 256MB (2x128Mx16). Supports 512MB (2X256MX16) DDR3
 - 64MB (32Mx16) NOR FLASH
 - 2 GB NAND Flash
 - 64MB SPI Nor FLASH
 - 64KB I²C EEPROM
- ETHERNET
 - The switch AR8337 should be set to Mode 5: MAC0-RGMII, MAC6-SGMII, PHY4-RGMII.
- MAC0 (RGMII)
 - Atheros Gigabit Ethernet Switch PHY4 or PHY4-MAC5-MAC6. This interface is muxed with RGMII0 Connector
- MAC1 (RGMII)
 - Atheros Gigabit Ethernet Switch MAC0
- MAC2 (RGMII)
 - RGMII1 Connector
- USB 4 PORT SMSC USB3.0 HUB
 - 2*USB TYPE 3.0A Connectors
 - 2 Mini PCI EXPRESS Connectors
- 1 PORT USB2.0 Controller
 - 1*USB Type 2.0A Connector
- SERDES
 - PCI EXPRESS—Two Mini PCI Express Connectors and PCIE1 is muxed with SATA0
 - SATA—Two SATA Connectors.
- DECT
 - One Adaptor Socket on board
- VOICE
 - 2 FXS Ports (ZL88601 Dual Wide Band SLIC)
- UART
 - UART0 is connected to on board DB9 connector
 - UART1 is brought to 5 pin connector
 - V-Cut Board provides RS232 Cabled Interface
 - EXPANSION 128 Pin High Density Connector
 - Expansion Bus
 - SPI Bus
 - TDM Bus
 - I²C Bus
 - UART Busses

- GPIO
- System and External Reset
- Power (PMIC) (12V, 5V, 3.3V)
- LCD Connector
 - Expansion Bus
 - SPI Bus
- Mechanical Form Factor Allows Mounting into an Enclosure

2.3 Software Overview

The software delivered with the Reference Design Board is programmed in the flash device on the board, and is ready to use. Newer software release when available can be downloaded from Freescale Web.

The files provided with the Linux Reference Application Development Kit (ADK) based on OpenWrt have been programmed into the flash. The [“Section 6, “Flashing or upgrading software”](#) section describes how to upgrade image to a newer code release. [Table 2](#) gives the binary image and file system image names.

Table 2. Binary Image Names

Design Board	JFFS2 File System	Bootloader	Kernel Binary	UBI
LS1024A Reference Design Board	For glibc build <ul style="list-style-type: none"> – jffs2-128k-c2000-openwrt-c2k_X.Y.Z c2kmfcnevm (NOR) – jffs2-nand-1024k-c2000-openwrt-c2k_X.Y.Z c2kmfcnevm For uclibc build <ul style="list-style-type: none"> – jffs2-128k-c2000-openwrt-c2k_X.Y.Z c2kmfcnevm-uclibc (NOR) – jffs2-nand-1024k-c2000-openwrt-c2k_X.Y.Z c2kmfcnevm--uclibc 	We have primary and secondary boot loader For glibc build <ul style="list-style-type: none"> – u-boot-2013.01-X.Y.Z-c2kmfcnevm.bin – barebox-c2kmfcnevm-2011.06.0-X.Y.Z.bin – barebox-diags-c2kmfcnevm-2011.06.0-X.Y.Z.bin – microloader-{nor/nand}-M862{a b}-c2kmfcnevm-2011.06.0-X.Y.Z.bin here ab can be: 01,02,03,04,06,07,08,60,61,61_NAS*, 62,91-98. For uclibc build <ul style="list-style-type: none"> – u-boot-2013.01-X.Y.Z-c2kmfcnevm-uclibc.bin – barebox-c2kmfcnevm-uclibc-2011.06.0-X.Y.Z.bin – barebox-diags-c2kmfcnevm-uclibc-2011.06.0-X.Y.Z.bin – microloader-{nor/nand}-M862{a b}-c2kmfcnevm-uclibc-2011.06.0-X.Y.Z.bin here ab can be: 01,02,03,04,06,07,08,60,61,62,91-98.	For glibc build <ul style="list-style-type: none"> – ulmage-c2000-openwrt-c2k_X.Y.Zc2kmfcnevm For uclibc build <ul style="list-style-type: none"> – ulmage-c2000-openwrt-c2k_X.Y.Zc2kmfcnevm-uclibc 	For glibc build <ul style="list-style-type: none"> – ubi-nor-c2000-openwrt-c2k_X.Y.Zc2kmfcnevm – ubi-nand-c2000-openwrt-c2k_X.Y.Zc2kmfcnevm For uclibc build <ul style="list-style-type: none"> – ubi-nor-c2000-openwrt-c2k_X.Y.Zc2kmfcnevm-uclibc – ubi-nand-c2000-openwrt-c2k_X.Y.Zc2kmfcnevm-uclibc

Note:

- LS1024A has NAS and HGW variants. In this table, image names of HGW variants are provided. 61_NAS µloader is present only in NAS variants Use _nas along with the board name in case of NAS variants. For example, the JFFS2 file system image name for LS1024A EVM for NAS variant would be: jffs2-128k-c2000-openwrt-c2k_X.Y.Z c2kevm_nas
- For NAS variant, only glibc build µloader is supported, uclibc is not supported.
- The version for U-Boot and that for barebox may be different

NOTE

The version numbers shown above (X.Y.Z) change with new releases. Contact the Freescale sales representative to receive the most recent system and binary images.

3 Getting Started

This section describes how to setup and operate the LS1024A Reference Design Boards under different scenarios.

3.1 Equipment Needed for Operation

The configuration setup requires the following materials:

- One Reference Design Board package, which includes:
 - One Reference Design Board.
 - +12 V power supply for Reference Design Board.
- One Serial cable for Reference Design Board serial console.
- One Local Area Network (LAN) PC with—P4 processor (recommended); No firewall enabled; Serial port and HyperTerminal; Ethernet port with IP on LAN subnet; Video LAN Client (VLC) application; and X-lite soft SIP application.
- Optional wireless adapter for wireless operation.
- One Wide Area Network (WAN) PC with—P4 processor (recommended); No firewall enabled; Ethernet port with IP on WAN subnet; VLC application; A DVD movie data file stored on hard drive.
- Two Plain Old Telephone Service (POTS) telephone sets with telephone cords.
- Two IP telephone sets, which support Session Initiation Protocol (SIP)—One configured for LAN, the other one for WAN.
- One AC Power Strip with six outlets.
- Five Ethernet cables for:
 - LAN IP telephone set to Reference Design Board LAN port.
 - LAN PC to Reference Design Board LAN port.
 - WAN IP telephone set to Ethernet Switch connected to Reference Design Board WAN port.
 - WAN PC to Ethernet Switch connected to Reference Design Board WAN port.
 - Ethernet Switch to Reference Design Board WAN port.

NOTE

To set up a minimum configuration for operation, use two POTS telephone sets and two IP telephone sets for the voice and two PCs for the data routing.

3.2 Connections for Voice Operation

3.2.1 LS1024A Connection

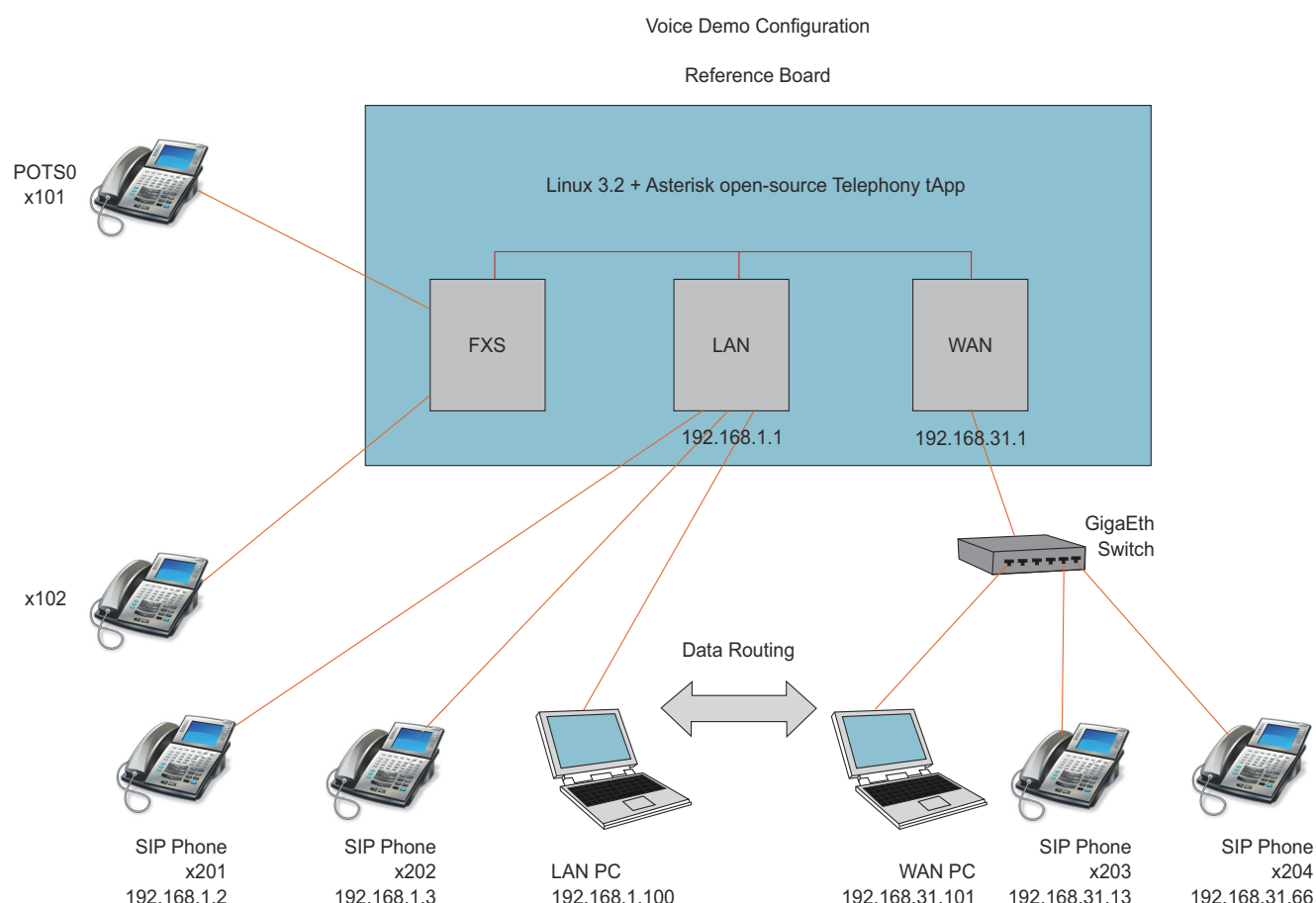
The following list describes the components connecting to the LS1024A Reference Design Board:

1. Two POTS telephone sets numbered 101 through 102, connected through RJ45.

2. The LAN IP telephone sets and the LAN PC or notebook, connected to any of the four LAN Ethernet ports using Ethernet cables.
3. The WAN IP telephone sets and a WAN PC notebook, connected to an external GigaEth switch. The external Ethernet switch is connected to the WAN Ethernet port on the Reference Design Board WAN daughter card through an Ethernet serial cable.
4. The serial port J_SER1 is connected to LAN PC serial port through a serial cable.
5. The +12 V DC power supply is connected to the power terminal of the Reference Design Board.

The following figure illustrates the connection details of the Reference Design Board voice demo configuration.

Figure 2. Reference Design Board Voice Demo Configuration

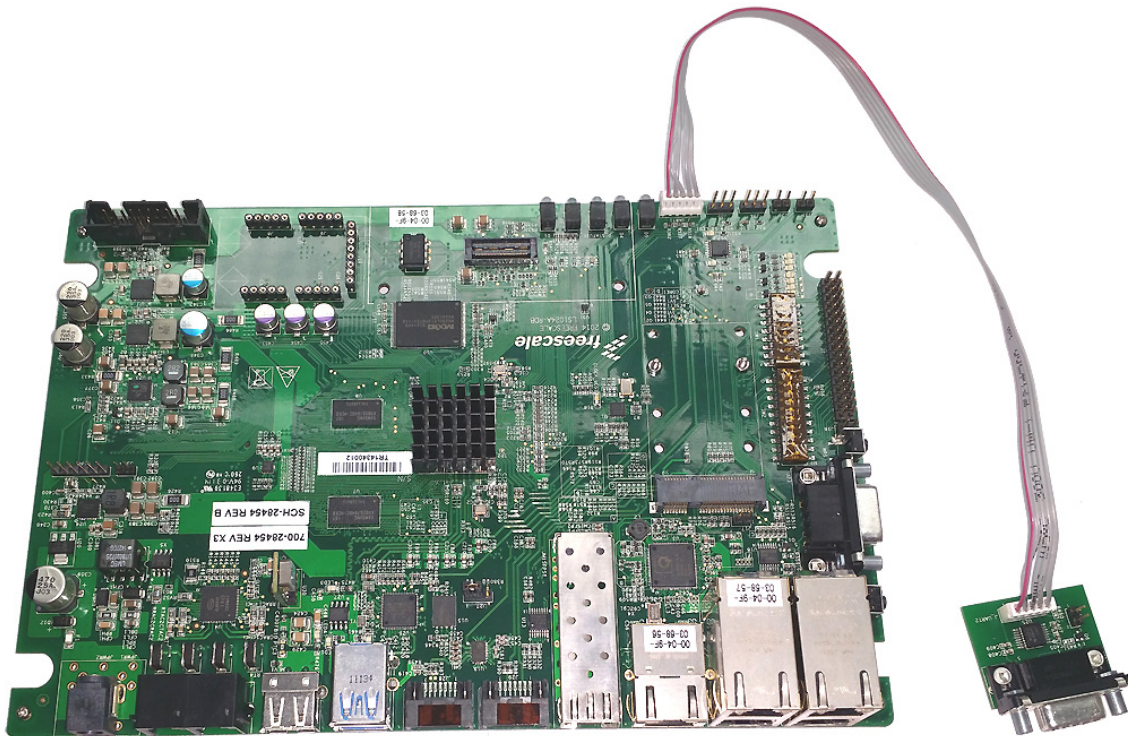


3.3 Reference Design Boards

3.3.1 LS1024A Board

The following figure shows the LS1024ARDB Reference Design Board.

Figure 3. LS1024A Reference Design

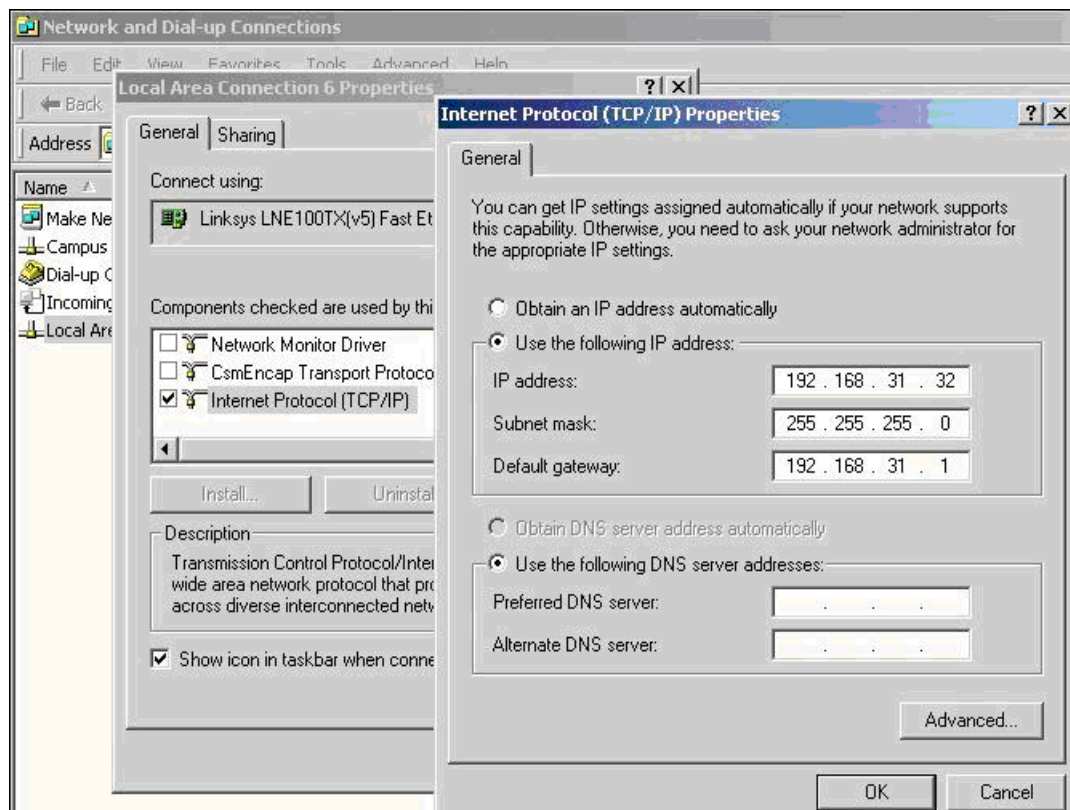


3.4 Configuration for the Voice Operation

The following steps illustrate the configuration for LS1024A Reference Design Board:

1. Configure the Default Gateway on the PC, IP telephone set, and other LAN devices to match the IP address of the Reference Design Board—192.168.1.1.
2. Configure the Default Gateway for all WAN devices to—192.168.31.1. The following figure illustrates the IP address configuration details.

Figure 4. Default IP Address Configuration



3. Configure the IP address of the IP telephone set to any IP address within the sub-network (LAN or WAN).
4. The SIP account is “sip0” for extension 201, “sip1” for extension 202, “sip2” for extension 203, and “sip3” for extension 204. Predefine a total of four SIP accounts. Leave the secret code for the telephone set as blank. The following figure shows the SIP account screen.

Figure 5. SIP Account Screen

5. If the Reference Design Board was ever reset, some IP telephone sets may require a reboot to register to the SIP server on the board.
6. Set the configuration parameters on the serial console of the LAN PC as follows:
 - Bit per Second: 115200
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
7. Verify the code revision.
 - The following message is shown when `μloader` boots


```
barebox 2011.06.0 (Mar 1 2013 - 02:55:28)
Board: Mindspeed C2000
c2k_spi_probe
```
 - The following message is shown when barebox boots after `μloader`

```
## Starting Barebox at 0x01000000 ...
barebox 2011.06.0 (Mar 1 2013 - 02:53:42)
Board: Mindspeed C2000
```
 - The U-Boot version appears on the top boot log, after power or reset of the board

The code build version appears after entering a key to activate the console:



— Check the Linux version by using the `uname` command at the OpenWrt prompt:

```
root@OpenWrt:/# uname -a
Linux OpenWrt 3.2.54 #16 SMP Tue Nov 11 10:44:47 IST 2014 armv7l GNU/Linux
```

4 Reference Design Board Operation

This section describes the LS1024A board operations. To operate the Board, follow the steps listed below:

Power cycle the LS1024A Board. Wait for few seconds for the system initiation. After the booting completes, press ENTER to activate the port. The `OpenWRT~#` prompt appears on the console.



4.1 Network Video Stream Transfer

The data routing functionality is accomplished by reading a video stream from one of the network interfaces (LAN, WAN, Wireless), sent by a video server located on another network interface (WAN to LAN video stream transfer). Perform the following steps to enable data routing functionality:

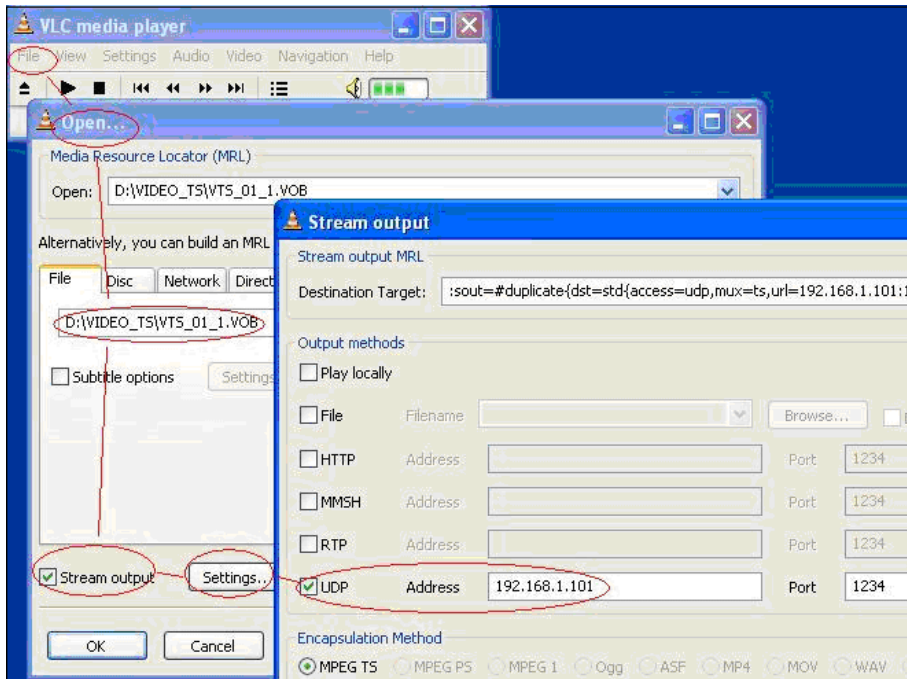
1. Install the VLC application on both LAN and WAN PCs in the system setup.
2. On the LAN PC, open the VLC program and select Open Network Stream under the File menu. Select UDP protocol, Port 1234. This configures the PC to be a media client to play the video received from the network.
3. To start sending the video stream onto the network, open the VLC program on WAN PCs; select File, Open File, Browse, and select the movie data file (with extension name *.VOB* and file size over 1 Gigabytes).

NOTE

On some DVD disks, the movie data is encrypted so that it is not suitable for the data streaming process. Before starting this operation, verify the VLC application's ability to play the movie on the local PC.

The following figure shows the VLC screen.

Figure 6. VLC Screen



4. Enable the Stream output box and click **Settings** tab. In the Stream output window, enable UDP protocol, Port 1234 and enter the IP address of the second PC (192.168.1.101 for LAN PC). The video should start playing on the media client LAN PC.
5. Unplugging the network cable stops the video and plugging the cable back resumes the video.

NOTE

- The POTS numbers, Conference number, IP telephone numbers, and IP addresses can be modified using the Web User Interface on the Reference Design Board.
- VLC is a free multimedia player for various audio and video formats. It can also be used as a server for unicast or multicast streams in IPv4 or IPv6 on a high-bandwidth network.
- The WAN PC acts as a media server that streams video to the IP network. The LAN PC acts as media client that captures video from the IP network.

4.2 Operate POTS-to-POTS Calls

To run the video process described above, perform the following operation:

1. Pick one of the POTS telephone sets and dial the number to a different POTS telephone set. The POTS telephone sets can be dialed as: POTS-0 number is 101; POTS-1 number is 102, and so on.
2. When the called POTS telephone set rings, select the phone. The telephone sets are now connected in G.711 mode.

3. To test all POTS telephone sets, repeat steps 1 to 2. Hang all POTS telephone sets to finish the POTS-to-POTS connection process.

4.3 Operate POTS-to-IP Calls

Pick one of the POTS telephone sets and dial the number for one of the IP telephone sets. The default numbers for the IP telephone sets are 201 to 204. If you hear a busy tone or a “not available” prompt, reboot the IP telephone set to re-register it to the SIP server running on the Reference Design Board.

Pick the IP telephone set when it rings to verify the connection. Hang to finish the POTS-to-IP connection process.

NOTE

It is possible to establish a call from a IP telephone set to one of the POTS telephone sets connected to the Reference Design Board. Some IP telephone sets may require pressing the SEND key after dialing to initiate the call.

4.4 WiFi Operation

This WiFi operation requires a separate PC running Windows with a wireless 802.11N adapter and a driver installed.

The operation code pre-loaded on the LS1024A Reference Design Board has the WiFi driver for the Atheros chipset installed. The configuration for the WiFi interface is handled in the code and ready for the WiFi operation.

4.5 Configuring the Wireless PC for Operation

The example configuration in this section assumes a notebook computer with an embedded 802.11N wireless card.

When booting the Boards with a mini-PC wireless card installed, the code detects the card and configures it as a Wireless Access Point. The default SSID for the Reference Design Board is OpenWrt-mspd-vap0. By default all VAPs are disabled and the user should enable it. The IP address of the wireless interface on the Reference Design Board is 192.168.3.1. DHCP is disabled on the Access Point (AP). Configure the wireless PC adapter as follows:

1. Disable DHCP and configure with static IP address 192.168.3.5.
2. Disable the security setting (set WEP to none).
3. Save the settings.
4. Search the available wireless networks and ensure that “OpenWrt-mspd-vap0” appears in the list. Select the “OpenWrt-mspd-vap0” network and press Connect.
5. The wireless PC now connects to the AP on the Reference Design Board.
6. From the PC, ping the IP address 192.168.3.1, to verify the communication between the PC and wireless adapter in the Reference Design Board. A successful ping indicates an established connection between the PC with the wireless adapter in the Reference Design Board.

4.6 Wireless Operation

After a successful connection, a new sub-network 192.168.3.x is established. The Linux system running on the device performs the data routing for this sub-network the same way as WAN or LAN. The same data routing process described before can be performed using the wireless PC.

The purpose of the WiFi operation is to show the functionality and data routing for the WiFi interface on the LS1024A product. The throughput and compatibility are controlled by the WiFi chip and driver.

5 Configuration Through Web User Interface

This section describes the **LS1024A** Reference Design board GUI configuration through Web User interface.

The LS1024A OpenWrt package can be configured through Web User Interface. This can be done from any computer connected in a local network through Hypertext Transfer Protocol (HTTP). When entering the IP address, 192.168.1.1 in the local network, the system prompts the user to enter the Username and Password. By default there is no password set for the `root/admin` user. If you access the GUI web interface without configuring the password from console, GUI interface asks the user to set the password and the window pops up to set the password. After setting the password, the user needs to access the GUI pages with the `root/admin` username and with this new configured password. [Figure 7](#) show the Set password Screen and Web User Interface Login screen.

Figure 7. Set Password Screen

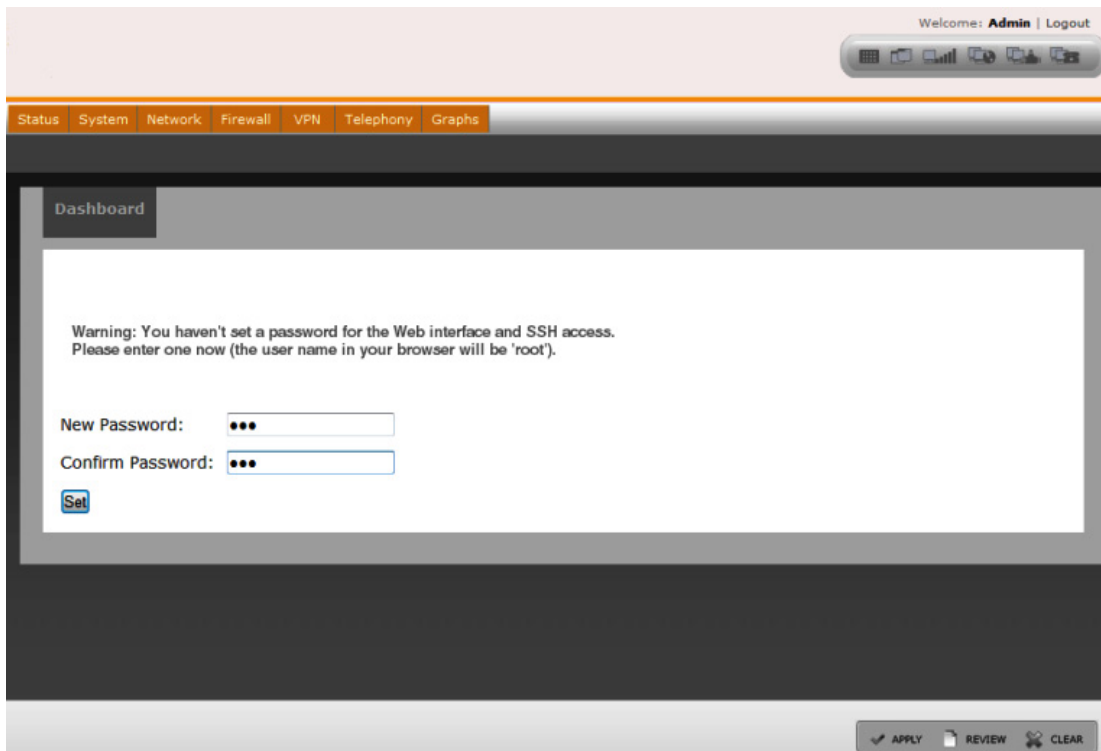
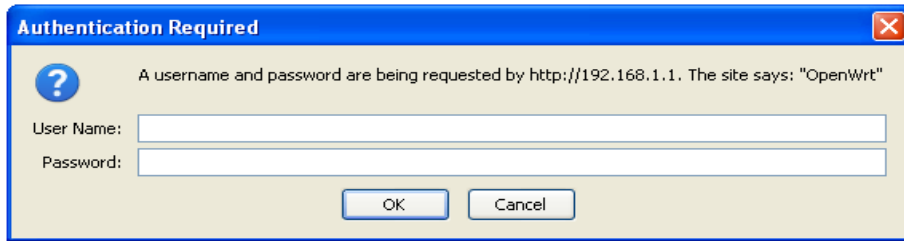


Figure 8. Web User Interface Login Screen

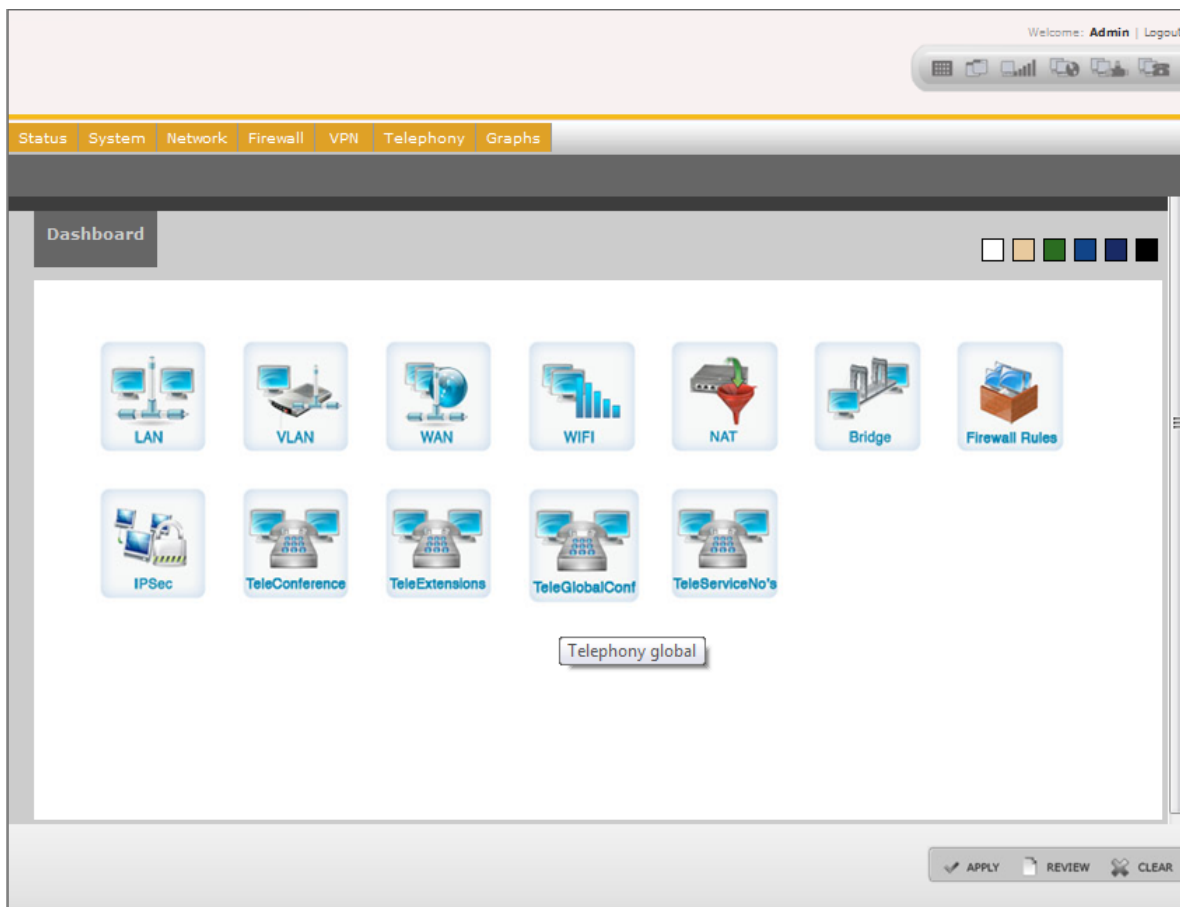


NOTE

To login from CLI, enter the default `username`—`root`. The CLI password can be set from the console using the command—`passwd`.

Dashboard screen gives an overview of the board GUI components. The dashboard screen can be launched from the quick launch option. The quick launch option also helps in launching the Wifi, WAN, LAN, and Voice configuration pages. [Figure 9](#) shows the GUI dashboard screen.

Figure 9. Dashboard



NOTE

- Firewall, VPN, QoS, and Telephony screens are not present for NAS variant of LS1024A device.

5.1 Status

The Status tab shows the LS1024A Reference Design Board status. Click the **Status** tab in the Main menu, and then click the **Connectivity** sub-tab in Status menu to open the system connectivity status screen. Status connectivity page can also be launched from quick launch option.

Figure 10 shows the overview of the Status tab.

Figure 10. Status Connectivity

The screenshot displays the 'Status' tab with the 'Connectivity' sub-tab selected. The interface is divided into three main sections: WAN, LAN, and Wifi, each with a table of configuration parameters. The WAN and LAN sections have orange borders, while the Wifi section has a grey border. At the bottom right, there are buttons for 'APPLY', 'REVIEW', and 'CLEAR'.

WAN:	
MAC Address	00:ED:CD:EF:AA:CC
IP Address	10.1.161.243
Netmask	255.255.254.0
Gateway	10.1.160.9
Connection Type	dhcp
Connected	yes
NAT Enabled	Enabled
DNS Servers	
Bridged	No

LAN:	
MAC Address	00:2A:2B:2C:2D:2E
IP Address	192.168.1.1
Netmask	255.255.255.0
DHCP Server	Enabled
Bridged	No

Wifi:	
MAC Address	
IP Address	
Netmask	
DHCP Server	
Card Type	
Bridged	

APPLY REVIEW CLEAR


Click any of the WAN, LAN, Wifi, or Voice options and navigate to the respective configuration pages from here. Under each option, to configure any specific settings, click the  icon and navigate to the respective configuration pages. Table 3 lists the Status menu sub-tabs.

Table 3. Status Menu Sub-tabs

Sub Tab	Description
Connectivity	Shows the Connectivity status
System	System Status
Interfaces	Available Interfaces
DHCP Clients	DHCP client status
USB	USB device information
PPPoE	PPPoE status
Diagnostics	Diagnostics status

5.2 System

Figure 11 shows the system settings page.

Figure 11. System Settings

The screenshot displays the 'System Settings' page in a web interface. At the top, there's a navigation bar with tabs: Status, System (highlighted), Network, Firewall, VPN, Telephony, and Graphs. Below this is another bar with links: Settings (highlighted), Syslog Settings, Access Control, Password, Backup & Restore, Upgrade, and Reboot. The main content area is titled 'System Settings' and features two sections. The 'System Settings' section includes a 'Host Name' field with the value 'OpenWrt'. The 'Time Settings' section includes a 'Timezone' dropdown menu set to 'User defined (or out of date)', a 'POSIX TZ String' field with 'UTC+0', an 'NTP Server' field, and an 'NTP Server Port' field with '123'. There are also links for 'Remove NTP Server' and 'Add NTP Server'. A help box on the right, titled 'TIMEZONE:', instructs the user to 'Set up your time zone nearest city of your re predefined list.'

Figure 12. System Settings Continued

Configuration Through Web User Interface

The screenshot shows the QorIQ LS1024A Web User Interface. The top navigation bar includes tabs for Status, System (selected), Network, Firewall, VPN, Telephony, and Graphs. Below this, a sub-navigation bar shows Settings, Syslog Settings, Access Control, Password (selected), Backup & Restore, Upgrade, and Reboot. The main content area is divided into three sections: 1. 'rdate Servers' with a text input field and an 'Add' button. 2. 'Webif2 Settings' with a checkbox for 'Enable visual effects', a 'Language' dropdown set to 'English', a 'Theme' dropdown set to 'Original', and a 'Webif2 SSL' section with a red error message: 'uhttpd-mod-tls package is not installed. You need to install it for ssl support:' and an 'Install uhttpd-mod-tls' button. 3. 'Web Configurator Settings' with 'HTTP Port' set to 80 and 'HTTPS Port' set to 443. An 'APPLY' button is located at the bottom right of the interface.

1. Click the **System** tab in the Main menu. Click **Password** sub-tab to change the GUI login password that was configured by the user.

The screenshot shows the 'Password' sub-tab of the QorIQ LS1024A Web User Interface. The top navigation bar is the same as the previous screenshot. The sub-navigation bar shows Settings, Syslog Settings, Password (selected), Samba, Backup & Restore, and Reboot. The main content area is titled 'Password' and contains a 'Password Change:' section with two text input fields: 'New Password:' and 'Confirm Password:'. Below these fields is a 'Save' button. At the bottom right of the interface, there are three buttons: 'APPLY', 'REVIEW', and 'CLEAR'.

2. Change the password and click **Add**.

The following Samba configuration page appears.

NOTE

The Samba subtab shows only if Samba packages are installed.

Figure 13. Samba Configuration

5.3 Network Configuration

5.3.1 WAN Interface Configuration

The WAN Interface can be configured using the WAN configuration screen. The WAN interface is *eth0* in networking subsystem. The WAN interface can be configured in three ways:

- Using a Static IP Address
- Dynamically from the DHCP
- Point-to-Point Protocol Over Ethernet (PPPoE) server

5.3.1.1 Static Configuration

1. Click the **Network** tab in the Main menu, and then click the **WAN** sub-tab in Network menu to open the WAN Configuration screen.

2. Select **Static IPv4** as the Connection Type. Default interface is eth0. Configure the WAN IP address, IPv4 Netmask, and Default Gateway in the IPv4 Settings section as shown in [Figure 14](#).

Figure 14. WAN Static Configuration

[Table 15](#) describes the WAN Static Configuration settings.

Figure 15. WAN Static Configuration Settings

Option	Description	Expected Values
Status	For enabling and disabling the connection	Enable/Disable
Connection Type –Static	To configure the WAN IP address manually.	Static IP
WAN-IP Address	The IP address of the WAN interface. (The eth0 interface is the default WAN)	The IP address is to be entered using a 4-byte address with dot (.) notation.

Figure 15. WAN Static Configuration Settings

Option	Description	Expected Values
Netmask	The subnet mask value.	The Netmask is to be entered using a 4-byte address with dot (.) notation.
Default Gateway	The default gateway for this interface.	The default gateway is to be entered using a 4-byte address with dot (.) notation.
Interface	To specify the WAN interface.	It is eth0.

3. Click **Save** to save the configuration information in a temporary file. Review or clear changes from temporary file as needed.
4. Click **Apply** to apply the WAN settings in flash and configure the WAN `eth0` interface in the device.
5. To modify the existing WAN interface configuration, modify the option and click **Save**.
6. The user can also configure Static WAN IPv6 settings from the WAN page main menu. To configure static IPv6 settings, enter the WAN IP Address, Netmask values and IPv6 gateway value.
7. Click **Save** to save the configuration in temporary file.

5.3.1.2 Dynamic Configuration—DHCP

1. Click the **Network** tab in the Main menu, and then click the **WAN** sub-tab in Network menu to open the WAN Configuration screen.
2. In the WAN IPv4 Configuration section, select **DHCP** as the Connection Type.
3. Click **Save** to save the configuration information in a temporary file. Review or clear changes from temporary file as needed.
4. Click **Apply** to apply the WAN settings in flash. [Figure 16](#) shows the Dynamic Configuration-DHCP settings.

Figure 16. WAN Dynamic DHCP Configuration

The screenshot displays the WAN Configuration page in a web interface. At the top, there is a navigation bar with tabs for Status, System, Network (selected), Firewall, VPN, QoS, Telephony, and Graphs. Below this is a sub-menu for Network, with options like WAN, LAN, VLAN, Bridge, Wireless, DHCP, Hosts, UPnP, Nat-Rules, and Route. The main content area is titled 'WAN Configuration: Settings saved'. It contains two main sections: 'WAN IPv4 Configuration' and 'WAN IPv6 Configuration'. In the IPv4 section, 'WAN IPv4 Status' is set to 'Enable' and 'Connection Type' is set to 'DHCP'. The IPv6 section shows 'WAN IPv6 Status' as 'Enable', 'WAN IPv6 Address' as 'fec0::ee01', 'IPv6 Netmask' as '120', and 'Default IPv6 Gateway' as an empty field. A 'Save' button is located at the bottom left of the configuration area. On the right side, there is an 'INTERFACE' section indicating 'Your WAN interface(eth0)'. At the bottom right, there are buttons for 'APPLY', 'REVIEW', and 'CLEAR'.

5.3.1.3 Dynamic Configuration—PPPoE

1. Click the **Network** tab in the Main menu, and then click the **WAN** sub-tab in Network menu to open the WAN Configuration screen.
2. Select **PPPoE** as the Connection Type. Configure PPPoE Username and Password. [Figure 17](#) shows the WAN dynamic PPPoE configuration settings.

Figure 17. WAN Dynamic PPPoE Configuration

3. Click **Save** to save the configuration information in a temporary file.
4. Click **Apply** to save the WAN settings in flash and configure the WAN interface (*eth0*) settings in the device.

Domain Name Service Configuration

WAN-DNS settings are used for relaying the Domain Name Service (DNS) packets from the hosts on the LAN to the DNS server present on the WAN. In this case, the LAN stations configure their DNS server as the LS1024A router platform. The system acts as a proxy for DNS requests. When enabling the DNS relay, the address of the DNS server is specified and DNS requests are relayed to the specified server. [Figure 18](#) shows the WAN-DNS configuration settings.

1. Click the **Network** tab in the Main menu, and then click the **WAN** sub-tab to open the WAN Configuration screen.
2. Configure the WAN-DNS IP address in the WAN Configuration screen. Click **Add** to add the WAN DNS Server IP Address.

Figure 18. WAN DNS Server

The screenshot displays the WAN Configuration page with the following sections:

- WAN IPv4 Configuration:**
 - WAN IPv4 Status: **Enable** (dropdown)
 - Connection Type: **Static IPv4** (dropdown)
 - Interface: (text field)
- IPv4 Settings:**
 - WAN IPv4 Address: **10.1.160.75** (text field)
 - IPv4 Netmask: **255.255.254.0** (text field)
 - Default IPv4 Gateway: (text field)
- WAN DNS Servers:**
 - 192.168.1.1 (text field) with a **Remove** button
 - 192.168.1.1 (text field) with an **Add** button
- WAN IPv6 Configuration:** (Section header, currently empty)

On the right side, there are informational notes:

- INTERFACE:** Your WAN interface(eth0)
- WAN IPV4 SETTINGS:** IPv4 Settings are optional for DHCP and PPTP. They are used as defaults in case the DHCP server is unavailable.
- NOTE:** You should save your settings on this page before adding/removing DNS servers

At the bottom right, there are buttons for **APPLY**, **REVIEW**, and **CLEAR**.

NOTE

WAN-DNS section appears only if the Connection Type is Static IP.

3. Click **Save** to save the configuration information in a temporary file.
4. Click **Apply** to apply the WAN-DNS settings in flash and configure the WAN-DNS settings in the device.
5. To delete the existing WAN-DNS configuration, click **Remove** for the corresponding WAN-DNS IP address and click **Save**.

NOTE

The Remove button is displayed after an address is added.

The user can also configure Static WAN IPv6 settings from the WAN page main menu.

5.3.2 LAN Interface Configuration

The LAN Interface can be configured using the LAN configuration screen. The LAN interface is `eth2` in the networking subsystem.

1. Click the **Network** tab in the Main menu, and then click the **LAN** sub-tab in the Network menu to open the LAN Configuration screen.
2. In the LAN Configuration section, enter the LAN IP address and Netmask details as shown in Figure 19.

Figure 19. LAN Configuration

Table 20 lists the LAN Configuration details.

Figure 20. LAN Configuration

Option	Description	Expected Values
LAN Status	Status of LAN on the interface.	Enable/Disable.
LAN-IP Address	The IP address of the LAN interface. (The <code>eth2</code> interface is the default LAN interface)	The IP address is to be entered using a 4-byte Address with dot (.) notation.
Netmask	The subnet mask value.	The Netmask is to be entered using a 4-byte Address with dot (.) notation.

3. Click **Save** to save the configuration information in a temporary file. Review or clear changes from temporary file as needed.
4. Click **Apply** to apply the LAN settings in flash and configure the LAN interface, that is `eth2`, settings in the device.
5. To modify an existing LAN settings configuration, modify the options and click **Save**.
6. The user can also configure Static LAN IPv6 settings from the LAN page main menu. To configure static IPv6 settings, enter the LAN IP Address, and Netmask values.
7. Click **Save** to save the configuration in temporary file.

5.3.3 VLAN

The user can configure VLAN interface from the VLAN configuration screen.

1. Click the **Network** tab in the Main menu, and then click the **VLAN** sub-tab in the Network menu to open the VLAN Configuration screen.
2. Click **Add New** to add new VLAN interface.
3. Enter the VLAN ID, IP-Address and Netmask ID to create a new VLAN interface. Following figure shows the VLAN configuration page.

Figure 21. VLAN Configuration

The screenshot displays the 'VLAN Configuration' web interface. The top navigation bar includes tabs for Status, System, Network (highlighted), Firewall, VPN, QoS, Telephony, and Graphs. A secondary navigation bar shows options like WAN, LAN, VLAN (highlighted), Bridge, Wireless, DHCP, Hosts, UPnP, Nat-Rules, and Route. The main panel, titled 'VLAN Configuration', features a 'List of created VLAN:' section with a table header (Interface, Network, VLAN ID, IP-address, Netmask, Actions) and a message 'There are no vlans'. Below this is an 'Add New' button and a 'New VLAN:' section with input fields for Network (a dropdown menu showing 'LAN'), VLAN ID, IP-Address, and Netmask. There are also 'Create', 'Reset', and 'Cancel' buttons. At the bottom right, there are 'APPLY', 'REVIEW', and 'CLEAR' buttons.

4. Click **Create** to create VLAN interface.

Table 4 lists the VLAN Configuration details.

Table 4. LAN Configuration

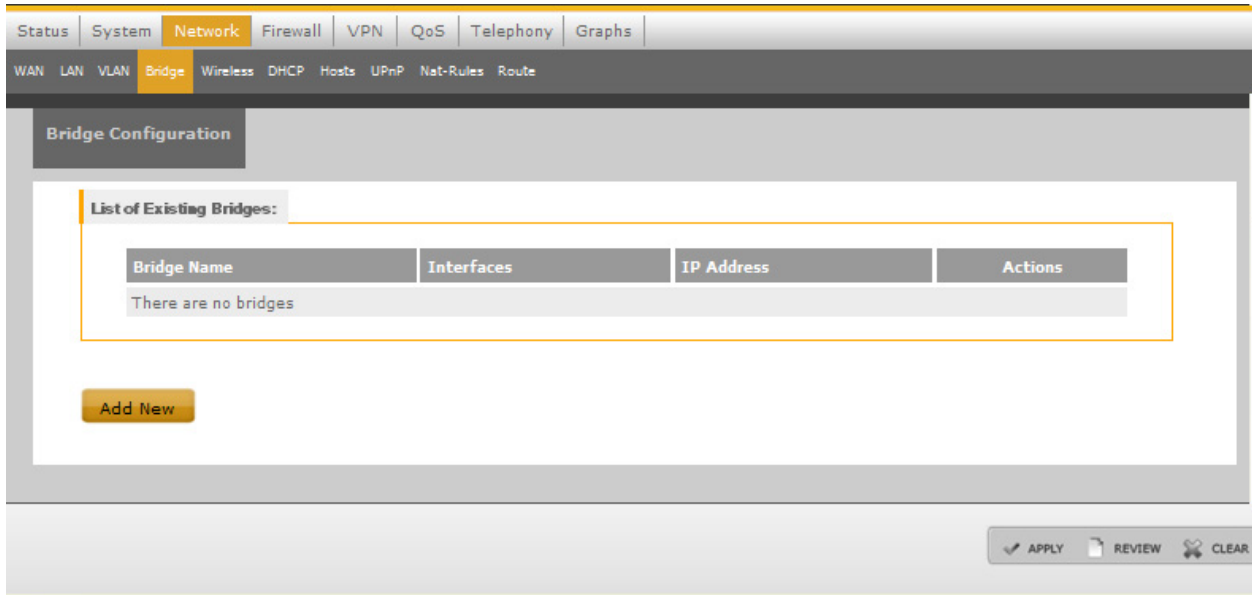
Option	Description	Expected Values
Network	VLAN network	LAN/WAN
VLAN ID	ID of VLAN on the interface.	
VLAN-IP Address	The IP address of the VLAN interface.	The IP address is to be entered using a 4-byte Address with dot (.) notation.
Netmask	The subnet mask value.	The Netmask is to be entered using a 4-byte Address with dot (.) notation.

5.3.4 Bridge Configuration

Bridges with different interfaces can be created using the Bridge Configuration Screen.

1. Click the **Network** tab in the Main menu, and then click the **Bridge** sub-tab to open the Bridge Configuration screen. [Figure 22](#) shows the Bridge Configuration screen.

Figure 22. Bridge Configuration



2. Bridge Configuration screen contains a table of existing bridges, if there are any. It also has a **Add New** link to create new bridges. To create a new bridge, click **Add New** link. [Figure 23](#) shows the Bridge Configuration screen for adding new bridge.
3. Configure the new bridge settings and click **Create** to create a new bridge configuration.

Figure 23. Add New Bridge

Table 5 describes the Bridge Configuration settings.

Table 5. Bridge Configuration Settings

Configuration Settings	Description
Bridge Name	Bridge name, which identifies each bridge.
Bridge Status	Enable/Disable
Bridge Interfaces	Interfaces of the bridge. (LAN, WAN and WiFi)
Bridge IP Address	IP address of the bridge.
Bridge Netmask	Netmask of bridge interface.

5.3.5 Wireless Configuration

The Wireless Interface can be configured using the Wireless Configuration screen.

1. Click the **Network** tab in the Main menu, and then click the **Wireless** sub-tab to open the Wireless Configuration Screen.

Figure 24. Wireless Configuration

The screenshot displays the 'Wireless Configuration' web page. The top navigation bar includes 'Status', 'System', 'Network', 'Firewall', 'VPN', 'QoS', 'Telephony', and 'Graphs'. The 'Network' tab is active, showing sub-tabs for 'WAN', 'LAN', 'VLAN', 'Bridge', 'Wireless', 'DHCP', 'Hosts', 'UPnP', 'Nat-Rules', 'Route', and 'PPPoE-Relay'. The 'Wireless' sub-tab is selected, leading to the 'Wireless Configuration' page. This page features a 'Radio Configuration' section with a 'Radio0 (PCIe0) Configuration' box. The configuration options are as follows:

- Radio:** Radio0 (PCIe0) (selected), Radio1 (PCIe1), Radio2 (USB)
- Mode:** B+G
- Channel Width:** 20
- Channel:** 1
- Multicast Rate:** 1
- Tx Rate:** 1
- RTS Threshold:** 2347
- CTS Threshold:** 2347

A 'Save' button is located at the bottom of the configuration box. Below this box is a link for 'VAP configuration'. At the bottom right of the interface, there are buttons for 'APPLY', 'REVIEW', and 'CLEAR'.

Table 6 describes the Wireless Configuration settings.

Table 6. Wireless Configuration Settings

Option	Description	Expected Values
Radio	To make WiFi On/Off.	On/Off
Mode	Mode of WiFi card.	Select form dropdown box (depends on card type which is used).
Channel	Number of channels supported.	Select form dropdown box (depends on card type which is used).
Channel Width	The bandwidth to be used. (Only applicable for 11n mode.)	40 MHz/ 20 MHz. Select from the drop down list.
Multicast Rate	Rate supported.	Select form dropdown box. (depends on card type which is used)

Table 6. Wireless Configuration Settings (continued)

Option	Description	Expected Values
Tx Rate	AP Transmit data rate. Used to hardcode AP transmit rate	B Mode – 1, 2, 5.5, 11 A/G Mode – 6, 9, 12, 18, 24, 36, 48, 54 B+ G Mode - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 A+N/G+N Mode - 6, 9, 12, 18, 24, 36, 48, 54, MCS0-MCS15
RTS Threshold	Request-to-send Threshold	Range from 0 to 2347 octets.
CTS Threshold	Clear-to-send Threshold	Range from 0 to 2347 octets.

2. Click **Save** to save the configuration information in a temporary file. Modify, review, or clear changes from temporary file as needed.
3. Click **Apply** to apply the Wireless settings in Flash and configure the interface settings in the device.
4. To modify an existing settings configuration, modify the options and click **Save**.
5. Click the **VAP Configuration** link in the Wireless Configuration screen for Virtual Access Points Configuration. [Figure 25](#) shows the VAP configuration screen.

Figure 25. VAP Configuration Screen

Configuration Through Web User Interface

Navigation: Status | System | **Network** | Firewall | VPN | QoS | Telephony | Graphs

Sub-Menu: WAN | LAN | VLAN | Bridge | **Wireless** | DHCP | Hosts | UPnP | Nat-Rules | Route | PPPoE-Relay

Wireless Advance Configuration

Virtual Access Points:

VAP ID	Radio ID	ESSID	Network	Authentication	Encryption	Status	Actions
vap0	Radio0 (PCIe0)	Openwrt-mspd-vap0	192.168.3.1-255.255.255.0	Open	none	<input type="checkbox"/>	
vap1	Radio1 (PCIe1)	Openwrt-mspd-vap1	192.168.4.1-255.255.255.0	Open	none	<input type="checkbox"/>	
vap2	Radio2 (USB)	Openwrt-mspd-vap2	192.168.5.1-255.255.255.0	Open	none	<input type="checkbox"/>	
vap3		Openwrt-mspd-vap3	192.168.6.1-255.255.255.0	Open	none	<input type="checkbox"/>	
vap4		Openwrt-mspd-vap4	192.168.7.1-255.255.255.0	Open	none	<input type="checkbox"/>	
vap5		Openwrt-mspd-vap5	192.168.8.1-255.255.255.0	Open	none	<input type="checkbox"/>	<input type="button" value="edit"/>
vap6		Openwrt-mspd-vap6	192.168.9.1-255.255.255.0	Open	none	<input type="checkbox"/>	
vap7		Openwrt-mspd-vap7	192.168.10.1-255.255.255.0	Open	none	<input type="checkbox"/>	

Buttons:

- Click the **Action** link to edit the Virtual Access Points.

Wireless Advance Configuration

Edit vap0 Configuration:

Radio: ☒ Radio0 (PCIe0) ☐ Radio1 (PCIe1) ☐ Radio2 (USB)

ESSID:

ESSID Broadcast:

Authentication:

Encryption:

IP Address:

Netmask:

[VAP configuration table](#)

ENCRYPTION TYPE:

WEP key should be alpha-numeric and should not end with "0" and it should be either 10 or 26 characters or you can type something in WEP PASS and generate it through GUI.

WPA-PSK key should be alpha-numeric and minimum 8 to maximum 64 characters.

5.3.6 Dynamic Host Configuration Protocol Server Configuration

The LS1024A platform acts as a DHCP server assigning IP addresses to IP stations on the network. This is typically done on a LAN network. When configuring DHCP, the network ID and the number of host stations to be supported must be specified.

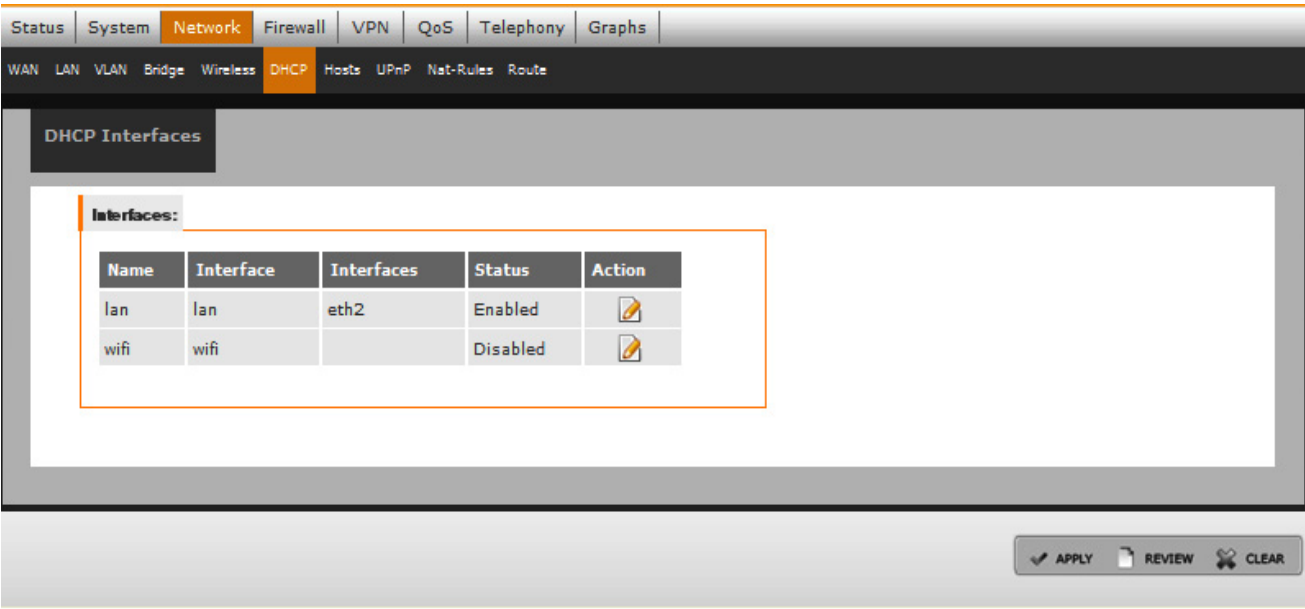
The DHCP server can be enabled on interface (WAN interface-eth0, LAN interface- eth2 or WiFi network). The DHCP subnets can be configured on the required interfaces. The router can be configured for a specific range of DHCP client IP addresses, which can be assigned dynamically by specifying parameters of the start, end, lease time, and interface. The router also facilitates the configuration, modification and deletion of the DHCP server on LAN, WAN, and WiFi interface.

DHCP Configuration Without Bridge Interfaces

The DHCP server can configured without the bridge interfaces.

- 1. Click the **Network** tab in the Main menu, and then click the **DHCP** sub-tab in the Network menu to open the DHCP Configuration screen. [Figure 26](#) shows the DHCP Configuration screen without Bridge Interfaces enabled.

Figure 26. DHCP Configuration Without Bridge Interfaces



- 2. Click **Edit** action tab to edit the DHCP Server. [Figure 27](#) shows the DHCP server modification screen. [Table 7](#) describes the DHCP Configuration settings.

Table 7. DHCP Configuration Settings

Option	Description	Expected Value
DHCP Service	Status of DHCP server on the interface.	Enable/disable
DHCP Start	The starting value among the pool of IP addresses that can be allocated by the server.	IP address
DHCP Num	The ending value among the pool of IP addresses that can be allocated by the server.	Total number of ip address pool.
DHCP Lease Minutes	The time for which the IP addresses are leased by the DHCP server.	The units can be in hours, minutes, or seconds. When entering the value, specify the units. For example, 12h/240m/84000s.

Figure 27. DHCP Interfaces

The screenshot shows the 'DHCP Interfaces' configuration page. At the top, there are tabs for Status, System, Network (selected), Firewall, VPN, QoS, Telephony, and Graphs. Below these are sub-tabs for WAN, LAN, VLAN, Bridge, Wireless, DHCP (selected), Hosts, UPnP, Nat-Rules, and Route. The main content area is titled 'DHCP Interfaces' and contains two sections:

Interfaces:

Name	Interface	Interfaces	Status	Action
lan	lan	eth2	Enabled	
wifi	wifi		Disabled	

DHCP Server For lan:

DHCP Service:

DHCP Start:

DHCP Num:

DHCP Lease Minutes:

At the bottom right, there are buttons for APPLY, REVIEW, and CLEAR.

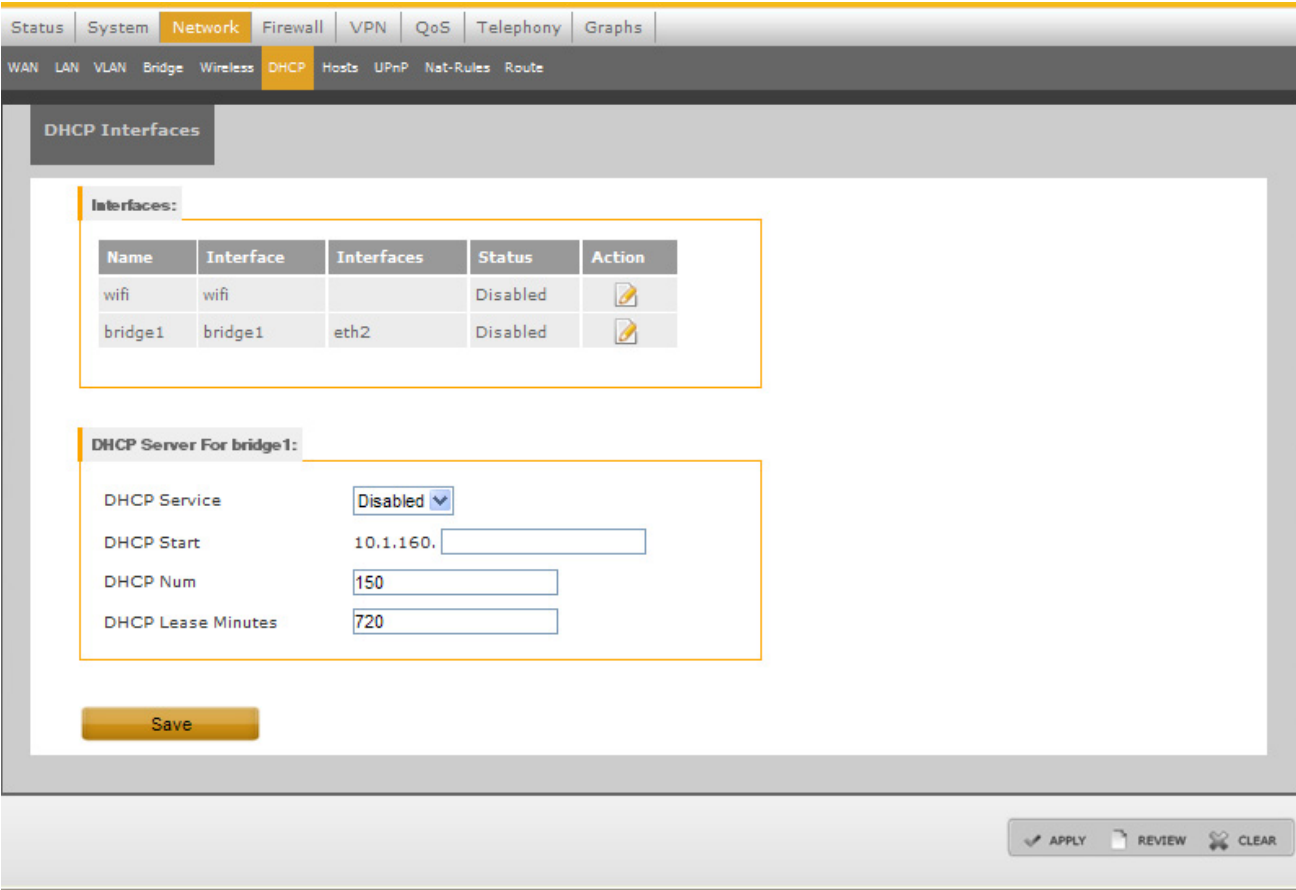
3. Configure the DHCP Service, DHCP Start, DHCP num and DHCP Lease Minutes as shown in [Figure 27](#).
4. Click **Save** to save the configuration information in a temporary file.
5. Click **Apply** to save the DHCP server settings in Flash and configure the DHCP server settings in the device.
6. To modify the existing configuration, modify the options and click **Save**.

DHCP Configuration With Bridge Interfaces

The DHCP server can also be configured with the bridge interfaces.

1. Click the **Network** tab in the Main menu and then click the **DHCP** sub-tab in the Network menu to open the DHCP configuration screen. [Figure 28](#) shows the DHCP Configuration screen with Bridge Interfaces.

Figure 28. DHCP Configuration Screen with Bridge Interfaces



5.3.7 Host

The Static IP address using DHCP server can be configured using the Host Configuration Screen. If a user wants to give any specific IP address to a machine, the user has to configure machine MAC address and the IP address. Host name configures the name for a specific host.

1. Click the **Network** tab in the Main menu, and then click the **Hosts** sub-tab in the Network menu to perform Host Configuration. Configure the Host Name and Static IP Address for DHCP.

Figure 29 shows the Host Configuration Screen.

Figure 29. Hosts Configuration

Host Names:

IP Address	Host Name
127.0.0.1	localhost
	OpenWrt

Static IP addresses (for DHCP):

MAC Address	IP Address

ACTIVE DHCP LEASES

MAC Address	IP Address	Name	Expires in
There are no known DHCP leases.			

APPLY REVIEW CLEAR

5.3.8 UPnP

1. Click the **Network** tab in the Main menu, and then click the **UPnP** sub-tab in the Network menu to configure UPnP.
2. Configure the UPnP as shown in Figure 30. Table 8 gives the UPnP description.

Table 8. UPnP Descriptions

Option	Description
UPnP Daemon	Status of UPnP daemon.
WAN upload	Upload limit in bits/sec.
WAN Download	Download limit in bits/sec.
Log Debug Output	Log Debug options.

Figure 30. UPnP Configuration

The screenshot displays the 'UPnP Configuration' web page. The top navigation bar includes tabs for Status, System, Network (selected), Firewall, VPN, QoS, Telephony, and Graphs. Below this, a sub-menu shows WAN, LAN, VLAN, Bridge, Wireless, DHCP, Hosts, UPnP (selected), Nat-Rules, and Route. The main content area is titled 'UPnP Configuration'. It features a 'UPNP:' section with a yellow border containing four settings: 'UPNP Daemon' set to 'Enabled', 'WAN Upload (bits/sec)' set to '512' kilobits, 'WAN Download (bits/sec)' set to '1024' kilobits, and 'Log Debug Output' set to 'Disabled'. A 'Save' button is located below these settings. To the right, a 'WAN SPEEDS:' section with a question mark icon explains that users should set their WAN speeds in kilobits for reporting to UPnP clients. At the bottom right, there are three buttons: 'APPLY', 'REVIEW', and 'CLEAR'.

To start the miniupnpd, execute the following command:

```
/etc/init.d/miniupnpd start
```

5.3.9 Network Address Translation Configuration

The **LS1024A** Reference Design Board supports the Network Address Translation (NAT) process for additional network security.

Enable NAT enables the concealing properties on the WAN interface, which enables SNAT on all the outgoing packets.

1. Click the **Network** tab in the Main menu, and then click the **NAT-Rules** sub-tab in the Network menu.
2. By default, the NAT is enabled. NAT enable/disable option is set only for outgoing traffic.
3. Create New Rule by entering the Type, Service, WAN IP, and Local IP details.
4. **Select/De-select** Status checkbox to enable or disable NAT. Click **Save** to save this status settings.
5. After configuring new NAT rule, click **Save** to save and **Apply** to apply the changes. [Figure 31](#) shows the NAT Configuration section.


Figure 31. NAT Configuration Section

[Status](#) | [System](#) | [Network](#) | [Firewall](#) | [VPN](#) | [QoS](#) | [Telephony](#) | [Graphs](#)




[WAN](#) | [LAN](#) | [VLAN](#) | [Bridge](#) | [Wireless](#) | [DHCP](#) | [Hosts](#) | [UPnP](#) | [Nat-Rules](#) | [Route](#) | [PPPoE-Relay](#)

Nat Rules

Outbound Rules:

NAT Enabled 

Inbound Rules:

Service	WAN IP	Local IP	Status	Actions
ftp	10.1.161.231	192.168.1.100		 

New Rule:

Type: Inbound

Service:

WAN IP Address:

Local IP:

? **SERVICES LIST:**
 List of services selected from the Firewall->Services list and those services protocol is not ip.

Table 9 describes the NAT Rules.

Table 9. NAT Rules

Option	Description	Expected Vales
Type	Type of traffic.	Inbound option in drop down menu.
Service	Select from drop down. The drop down list is taken from the services created in Services tab, which has a combination of protocol and port number.	Protocol/Port Number
WAN IP address	WAN IP address is generally the board WAN IP address.The packets that come to this IP address are redirected to the Local IP address.	WAN IP Address.
Status	Enable or Disable NAT status	Select/Deselect
Local IP address	IP address of LAN machine for which user is adding NAT rule.	LAN IP Address.

5.3.10 Route

The Route configuration section lists the Route table values assigned to the Reference Design Board.

1. Click the **Network** tab in the Main menu, and then click the **Route** sub-tab in the Network menu.
2. Enter the Route name, Destination IP Address, Netmask, and Gateway values as required.
3. Click **Add** to create a Static Route entry. [Figure 32](#) shows the Route Configuration section.
4. Click **Apply** and the new Route Entry will be shown in the Route table.

Figure 32. Route Configuration

Route Table:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.3.0	0.0.0.0	255.255.255.0	U	0	0	0	ath0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth2
10.1.160.0	0.0.0.0	255.255.254.0	U	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth1
0.0.0.0	10.1.160.9	0.0.0.0	UG	0	0	0	eth0

Static Routes:

Route Name	Dest. IP	Netmask	Gateway	Actions
There are no static routes				

New Route:

Route Name

Dest. IP

Netmask

Gateway

5.3.11 PPPoE Relay

The PPPoE Relay configuration section lists the PPPoE Relay status of the LS1024A Reference Design Board.

1. Click the **Network** tab in the Main menu, and then click the **PPPoE-Relay** sub-tab in the Network menu.
2. Select Server side interface, Client side interface and maximum allowed sessions.
3. Click **Save** to save the settings. [Figure 33](#) shows the PPPoE- Relay configuration section.

Figure 33. PPPoE Relay

5.4 Firewall Configuration

The LS1024A platform provides a security function to control access between Reference Design Board and the LAN or WAN interfaces. [Table 10](#) defines the various security levels.

Table 10. Security Configuration

Traffic Path	High Security	Low Security	No Security
LAN to Reference Design Board	Allowed	Allowed	Allowed
WAN to Reference Design Board	Blocked	Blocked	Allowed
Reference Design Board to LAN	Allowed	Allowed	Allowed

Table 10. Security Configuration (continued)

Traffic Path	High Security	Low Security	No Security
Reference Design Board to WAN	Allowed	Allowed	Allowed
LAN to WAN	Blocked	Allowed	Allowed
WAN to LAN	Blocked	Blocked	Allowed

5.4.1 General—Define the Security Level

1. Click the **Security** tab in the Main menu, and then click the **General** sub-tab in the Firewall menu to open the Firewall Screen.
2. Select the desired Security Level. [Figure 34](#) shows the Firewall General Configuration section.

NOTE

The General Security settings are applicable for both IPv4 and IPv6 traffic. However, the Firewall-Rules are applicable only for IPv4 traffic.

Figure 34. Firewall General Configuration

Firewall General Configuration

Security Level:

☒ No Security

☐ Low Security

☐ High Security

NO SECURITY:
 INBOUND traffic (WAN to LAN) is allowed.
 OUTBOUND traffic (LAN to WAN) is allowed.

LOW SECURITY:
 INBOUND traffic (WAN to LAN) is blocked.
 OUTBOUND traffic (LAN to WAN) is allowed.

HIGH SECURITY:
 INBOUND traffic (WAN to LAN) is blocked.
 OUTBOUND traffic (LAN to WAN) is blocked.

NOTE:
 The General Security settings are applicable for both IPv4 and IPv6 traffic. However, the Firewall-Rules are applicable only for IPv4 traffic.

Save

APPLY REVIEW CLEAR

5.4.2 Services

By default, the well known applications or services are listed in the Services screen. This helps the user to create the security rules by providing the service name rather than the corresponding port number.

1. Click the **Security** tab in the Main menu, and then click **Services** Tab to create New Services.
2. Enter the Service name, Protocol and the Port details. Click **Add**. The list of Services already created will be denoted.
3. From the Action section, delete or edit the existing Services.

Figure 35 shows the Services section.

Figure 35. Services Configuration

List of Services:

Serial No.	Service Name	Protocol	Port Number	Actions
1	telnet	tcp	23	
2	ftp	tcp	21	
3	ping	icmp	8	

New Service:

Service Name:

Protocol:

Port:

5.4.3 Firewall Rules

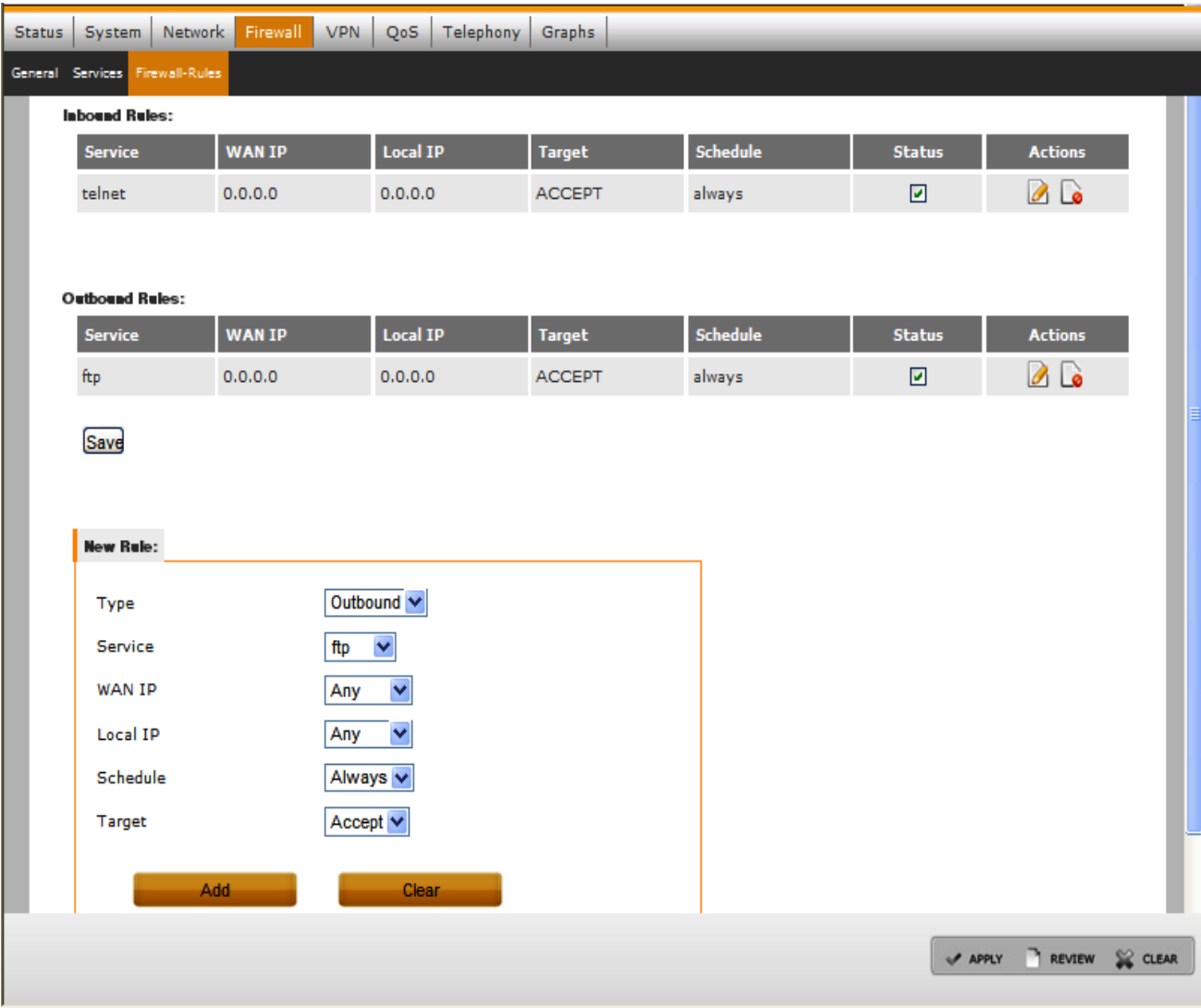
In the Firewall-Rules Configuration screen, the user can add, delete, and edit the rules for both inbound and outbound traffic.

NOTE

The firewall-rules are applicable only for IPv4 traffic.

- 1. Click the **Security** tab in the Main menu, and then click **Firewall-Rules** sub tab.
- 2. Enter Type, Service, WAN IP, Local IP, Schedule, and Target details in the New Rule section.
- 3. From the status checkbox, enable or disable firewall rules. Click **Save** to save this status.
- 4. From the Action section, delete or edit the existing rules.
- 5. Click **Add**. [Figure 36](#) shows the Firewall Rule section.

Figure 36. Firewall Rules Configuration



[Table 11](#) gives the definitions of the Firewall Filter options.

Table 11. Setting the Firewall Filter Rules

Option	Description
Type	Defines Inbound or Outbound traffic
Service	The services listed or configured in the Services Configuration section.
WAN IP	User can give Any or Specific IP address of WAN machine.
Local IP	User can give Any or Specific IP address of LAN machine.
Schedule	The durations and periods are listed in the Schedule Configuration section.
Status	Enable/Disable

- Click **Save** and click **Apply** to apply the changes.

5.5 VPN Configuration

5.5.1 IPSec Policy



- Click the **VPN** tab in the Main menu. The **Ipsec Policy** page opens.
- Click **Add New IPSec Policy** to add new IPSec policy.
- Enter the Policy Name, Remote IP Address, Local IP Address, SPI in, SPI out text box. Select the Protocol Type, Local Network, Remote Network, Encryption Algorithm, and Authentication Algorithm. [Figure 37](#) shows the IPSec Policy Configuration. [Table 12](#) lists the IPSec Policy configuration details.
- Delete or edit the existing policy from the Action section. Enable or disable the existing policy from the Status checkbox. Click **Save** to save the status settings.
- After entering the policy details, click **Add** to add an IPSec policy.

Figure 37. IPSec Policy Configuration

[Status](#) | [System](#) | [Network](#) | [Firewall](#) | **[VPN](#)** | [QoS](#) | [Telephony](#) | [Graphs](#)

IPsec Policy

List of Existing IPsec Policies:

Policy Name	Local Network	Remote Network	Encryption	Authentication	Status	Actions
test	192.168.2.10	192.168.2.10	null	null	<input checked="" type="checkbox"/>	 

[Save](#)

[Add New IPsec policy](#)

New IPsec policy Configuration:

Policy Name:
 Protocol Type:
 WAN IP Address:
 Remote IP Address:
 Local Network:
 IP Address:
 Remote Network:
 IP Address:
 SPI in:
 SPI out:
 Encryption Algorithm:
 Key in:
 Key out:
 Authentication Algorithm:
 Key in:
 Key out:

[Add](#) [Cancel](#)

ENCRYPTION ALGORITHM LENGTHS:
 DES 8bytes, 3DES 24bytes, AES-128 16bytes, AES-192 24bytes, AES-256 32bytes.
AUTHENTICATION ALGORITHM LENGTHS:
 HMAC-MD5 16bytes, HMAC-SHA1 20bytes, HMAC-SHA2-256 32bytes.

[APPLY](#) [REVIEW](#) [CLEAR](#)

- Click **Save** and click **Apply** to apply the changes.

Table 12. IPSec Policy Configuration

Option	Description
Policy Name	Policy name
Policy Type	ESP or AH
Local Network	Single IP or Subnet
Remote Network	Single IP or Subnet
Key In/Key Out	Encryption Algorithm and Authentication Algorithm keys for incoming and outgoing traffic. Keys can either be string or hexadecimal numbers.

Table 12. IPSec Policy Configuration (continued)

Option	Description	
SPI in/SPI Out	Manual keys for incoming and outgoing traffic. The value should be greater than 255 decimal number.	
Encryption Algorithm	Algorithms	Key length in Bytes
	DES-CBC	8
	3DES-CBC	24
	AES-128	16
	AES-192	24
	AES-256	32
Authentication Algorithm	Algorithms	Key length in Bytes
	HMAC-MD5	16
	HMAC-SHA1	20
	HMAC-SHA2-256	32

5.6 QoS Configuration

GUI pages not supported currently.

5.7 Telephony Configuration

The Reference Design Board have the Asterisk PBX software feature for implementing the VoIP service. To create Analog extensions, VoIP extensions, Service numbers (Voice mail main number and call recording number) and to modify Global Configuration use the Web user interface. The user can also perform Conferencing and Unified Diag configuration.

5.7.1 Extensions—Dial Plan Configuration

1. Click **Telephony** tab from the Main menu. The **Extensions** sub-tab opens.

Telephony | Status | System | Network | Firewall | VPN | QoS | **Telephony** | Graphs

Extensions | Service Numbers | Global Config | Conferencing | Unified-Diag | External SIP Proxy

Analog Extensions:

Phone ID	Phone Number	Display Name	Actions
1	101	pots1	
2	102	pots2	

DECT Extensions:

Phone ID	Phone Number	Display Name	Action
1	501	dect1	

FXO Extensions:

Phone ID	Extension Number	Display Name	Action
1	301	FXO	

VoIP Extensions:

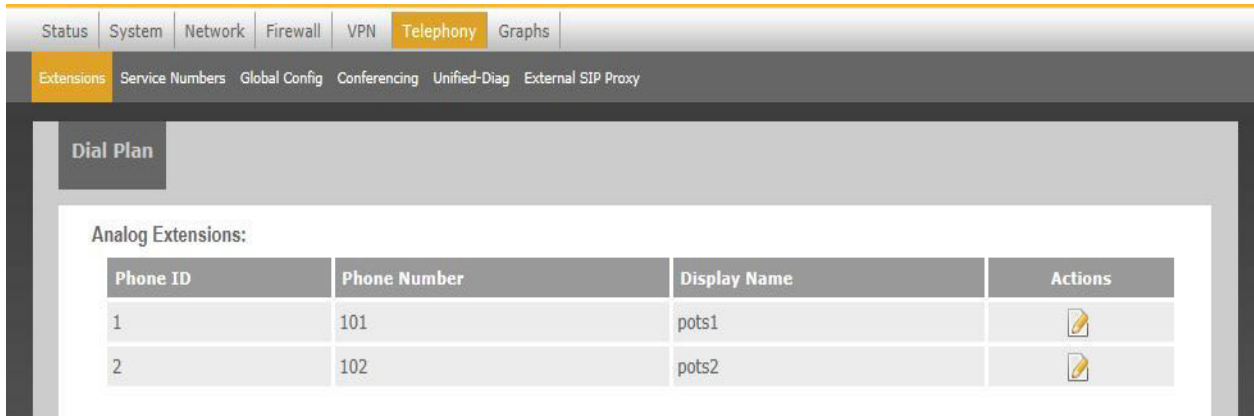
Phone ID	Phone Number	Display Name	Actions
1	201	201	
2	202	202	
3	203	203	
4	204	204	

APPLY REVIEW

5.7.1.1 Analog Extensions

1. Click **Telephony** tab from the Main menu. The **Extensions** sub-tab opens.
2. Two POTS ports are available on the board for connecting two analog telephones. Use the **Edit** function under the Action column to configure the respective telephone. Default analog telephones are 101 and 102 as shown in [Figure 38](#).

Figure 38. Analog Dial Plan Configuration



3. To edit details of analog telephone, click the **edit** link (for example, POTS Phone ID 1).
4. Specify the Name and Number of the telephone and enable the Voicemail check-box to enable voicemail for that phone, and also select the codes allowed for the specific telephone. [Figure 39](#) shows the Analog Configuration section. [Table 13](#) lists the analog extension configuration details.

Figure 39. Edit Analog Extension Configuration

Edit Analog Phone 1

Analog Phone ID	<input type="text" value="1"/>
Name	<input type="text" value="pots1"/>
Number	<input type="text" value="101"/>
Voicemail	<input type="text" value="default"/>
DSP on ACP	<input type="text" value="default"/>
VAD	<input type="text" value="default"/>
BWE Master	<input type="text" value="default"/>
BWE High band	<input type="text" value="4"/> (Default 4)
BWE Low band	<input type="text" value="5"/> (Default 5)

Advanced:

Table 13. Analog Extension Configuration

Option	Description
Analog Phone ID	This is not an editable feature.
Name	Phone ID. This is an editable feature.
Number	Phone number. This is an editable feature.
VoiceMail	Enable/Disable voicemail feature
DSP on ACP	Enable/Disable DSP on ACP
Voice Activity Detection (VAD)	Enable/Disable VAD. VAD detects the presence of speech in an audio signal.

- Click **Save** to save the changes.
- In the Advance Configuration section of the Edit Analog Phone, the user can edit various parameters for echo cancellation. If Echo Canceller type is EC and not Dual Filter Echo Canceller (DFEC), then EC links comes under Advanced section. Click the **Echo-Canceller** link to open the Echo-Cancellation screen as shown in [Figure 40](#). [Table 14](#) lists the Echo-Cancellation Options.

NOTE

To configure echo canceller type as DFEC, use the Global Config subtab.

Figure 40. Echo Cancellation Screen

Status System Network Firewall VPN QoS **Telephony** Graphs

Extensions Service Numbers Global Config Conferencing Unified-Diag External SIP Proxy

Dial Plan

Analog Extensions:

Phone ID	Phone Number	Display Name	Actions
1	101	pots1	
2	102	pots2	

Edit Echo Cancellation for Analog Phone 1:

Analog Phone ID

Name pots1

Number 101

Enable Echo Cancellation ☒

Enable DC Removal Filter ☒

Freeze HEC Filter Coefficient ☐

Enable NLP Control ☒

NLP Tune

Comfort Noise Generation ☒

Network Echo Cancellation Tail Length

APPLY REVIEW CLEAR

Table 14. Echo Cancellation Options

Option	Description
Enable Echo Cancellation	Enable/Disable echo cancellation.
Enable DC Removal Filter	Enable/Disable DC Removal Filter
Freeze Hardware Echo Canceller (HEC) Filter Coefficient	Enable/Disable the updated of HEC.
Enable Non-Linear Processor (NLP) Control	Enable/Disable the Non-Linear Processor.
NLP Tune	Controls the level of NLP engagement
Comfort Noise Generation	Enable/Disable the Comfort Noise Generation
Network Echo Cancellation Tail Length	Echo Canceller Tail Length is adjustable to {16, 32, 48, 64} ms.

1. In the Advance Configuration section of the Edit Analog Phone, the user can edit various parameters for enhanced echo cancellation. Click the **Enhanced Echo-Canceller** link to open the Enhanced Echo-Cancellation Screen as shown in [Figure 41](#).

Figure 41. Enhanced Echo-Cancellation

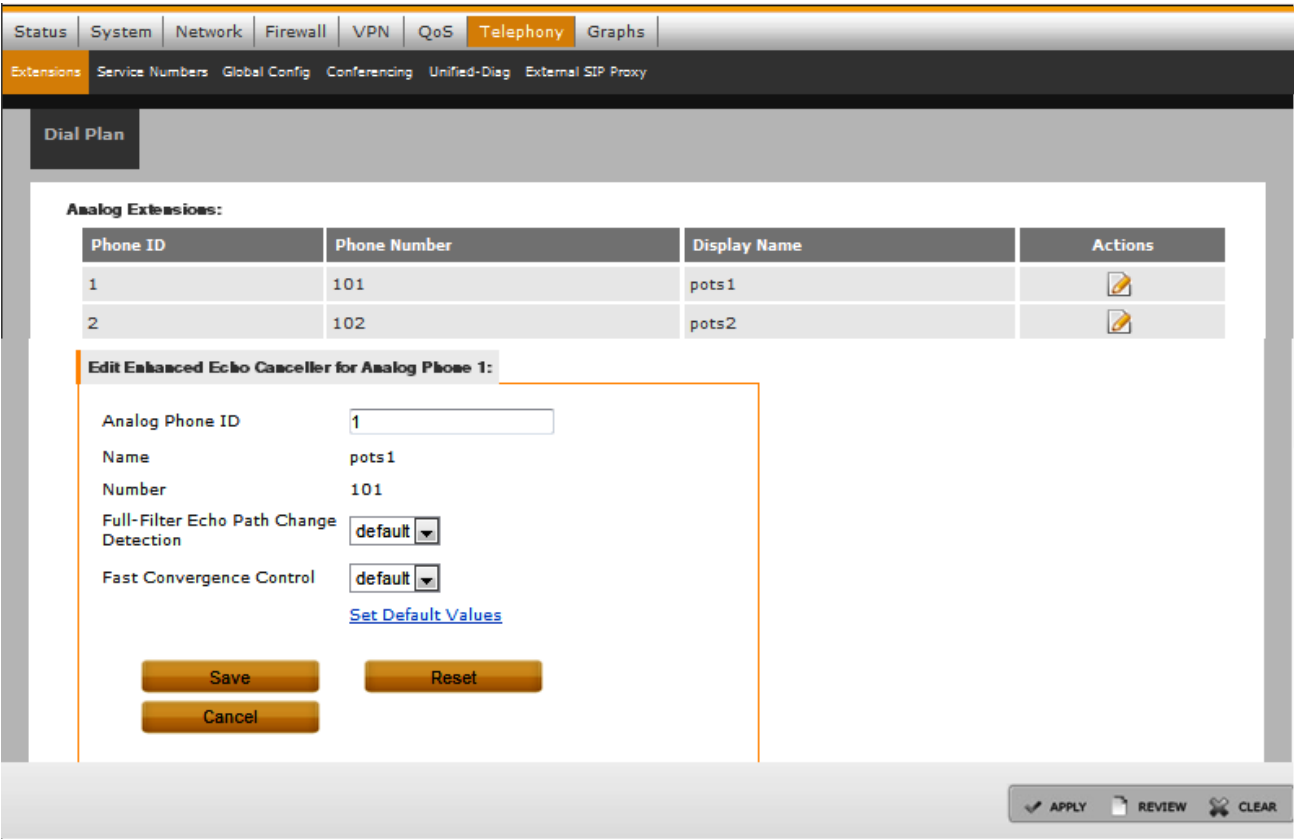


Table 15. Enhanced Echo Cancellation Options

Option	Description
Full Filter Echo Path Change Detection	Enable/Disable echo path change detection
Fast Convergence Control	Enable/Disable fast convergence control

7. If Echo canceller type is DFEC, then in the Advance Configuration section of the Edit Analog Phone, the user can edit various parameters for DFEC. Click the **Dual Filter Echo Cancellation** link to open the DFEC configuration screen as shown in [Figure 42](#).

NOTE

From Global config sub-tab, the user should select Echo Cancellation type as DFEC and click Save to enable DFEC type.

Figure 42. DFEC Basic Configuration

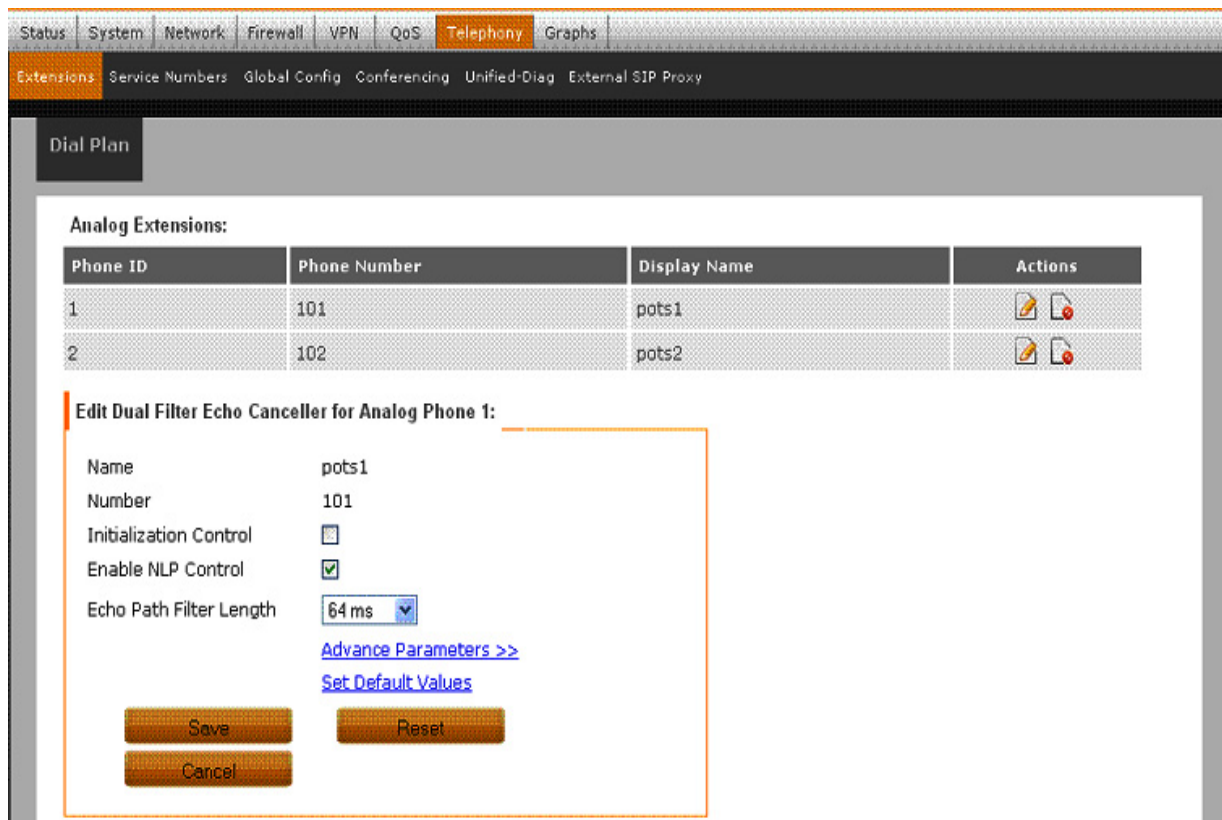


Table 16. DFEC Basic Options

Option	Description
Initialization	Enable/Disable
Enable NLP Control	Enable/Disable the Non-Linear Processor Control.
Echo Path Filter Length	Filter length

8. Click **Set Default Values** to set the default values for all basic and advanced DFEC parameters.
9. Click **Reset** to restore the saved configuration and click **Cancel** and return to the extensions main page.
10. For advance configuration, click **Advance Parameters**. Figure 43 shows the DFEC advance parameter configuration.

Figure 43. DFEC Advanced Parameter Configuration

Status

System

Network

Firewall

VPN

QoS

Telephony

Graphs

Extensions

Service Numbers

Global Config





Conferencing

Unified-Diag

External SIP Proxy

Dial Plan

Analog Extensions:

Phone ID	Phone Number	Display Name	Actions
1	101	pots1	 
2	102	pots2	 

Edit Dual Filter Echo Canceller for Analog Phone 1:

Name

pots1

Number

101


Initialization Control

☐

Enable NLP Control

☒

Echo Path Filter Length

64 ms 

<<Advance Parameters

Enable Master Echo Canceller

☒

Transmit Input DC Filter Disable

☒

Tone Transmitter

☐

Filter Coefficient Freeze

☒

Dynamic Attenuation

☐

Background Noise Replacement

☐

Sparse Foreground Filter

☐

NLP Comfort Noise Generation

☒

Echo Path Filter Control

☒

Recieve Input DC Filter Enable

☐

Set Default Values

Save

Reset

Cancel

5.7.2 VoIP Extensions

1. Click **Telephony** tab from the Main menu. The **Extensions** sub-tab opens.

- To add a new VoIP phone, click **Add New** in the VoIP Extension section. Figure 44 shows the VoIP Extension screen. Table 17 lists the VoIP Extension configuration details.

Figure 44. VoIP Extension

VoIP Extensions:

Phone ID	Phone Number	Display Name	Actions
1	201	201	
2	202	202	
3	203	203	
4	204	204	

Add New

New VoIP Extension:

Name

Number/Auth Name

Protocol

Type

Authentication Password

Voicemail ☐

Save **Reset** **Cancel**

APPLY **REVIEW** **CLEAR**

Table 17. VoIP Extension Configuration

Option	Description
Name	VoIP Phone ID.
Number/Auth Name	Phone number or the authentication name.
Type	Possible values are friend and peer. By default, it is friend.
Protocol	The type of protocol.
Authentication Password	Enter the authentication password.
Voicemail	Enable/Disable.

3. Specify the Name and Number of the telephone. For the protocol, only SIP is supported. For Authentication, provide the Authentication name and Authentication password. Enable Voicemail check-box to enable voicemail for that number.
4. Click **Save** and click **Apply** to apply the changes.
5. To edit the existing VoIP extensions, click the **edit** link. Edit the VoIP phone 1 extension details.
6. Click **Save** to save the changes made.

5.7.3 Service Numbers Configuration

1. Click **Telephony** tab in the Main menu, then click the **Service Numbers** sub-tab.
2. Configure Extension Number in Voicemail Retrieval Extension section.
3. Configure Extension Number in Voicemail Operator Extension section.
4. Click **Save** and click **Apply**.

Figure 45 shows the Service Number Configuration section. In Service Number Configuration section, the voicemail retrieval number is editable.

Figure 45. Service Number Configuration

The screenshot displays the 'Service Numbers' configuration page within a web interface. The top navigation bar includes tabs for Status, System, Network, Firewall, VPN, QoS, Telephony (selected), and Graphs. Below this, a sub-menu shows Extensions, Service Numbers (selected), Global Config, Conferencing, Unified-Diag, and External SIP Proxy. The main content area is titled 'Voice Mail Extension' and contains two sections: 'Voicemail Retrieval Extension' with an 'Extension Number' field set to '1234', and 'Voicemail Operator Extension' with an empty 'Extension Number' field. A 'Save' button is located at the bottom of the form.

5.7.4 Global Configuration

The user can configure many telephony features through the **Global Config** sub-tab. This helps the user to configure few options globally rather than configuring them in the individual pages. The **Global Config** sub-tab has link to configure Echo Canceller Type, Passthrough Mode, 3-Way Calling Support and so on.

1. Click **Telephony** tab in the Main menu, then click the **Global Config** sub-tab.
2. In the Phone Settings subtab, supported codecs are enabled by default. Figure 46 shows the Global Configuration section. Table 18 lists the Global Configuration details.

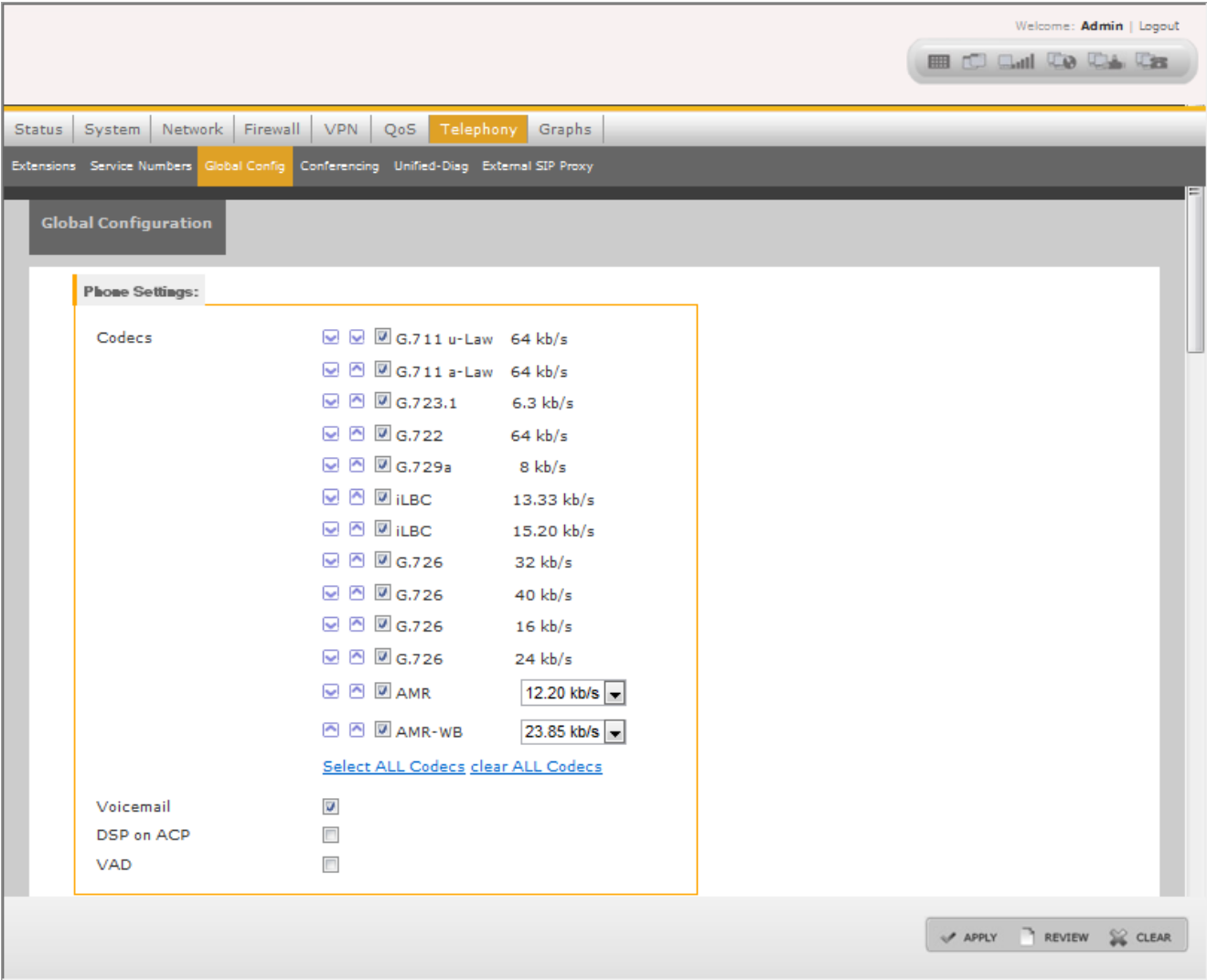
NOTE

Codec g729 indicates that a g729 channel can be created for that particular line on the Freescale device. This does not mean that an analog telephone supports codec g729.

Table 18. Global Configuration

Option	Description
Phone Settings	Codec Selection for PBX—Select the Codec channel. Voicemail—Enable/Disable DSP on ACP—Enable/Disable VAD—Enable/Disable
Echo Celler Type	DFEC or EC
Timeout Values	Dial timeout values and Interdigit timeout values can be set from this option.
NTT Caller ID Support	Enable or Disable
Fax Support	Select auto, T38, or Pass Through Mode

Figure 46. Global Configuration-Codec Selection



Welcome: Admin | Logout

Status System Network Firewall VPN QoS **Telephony** Graphs

Extensions Service Numbers **Global Config** Conferencing Unified-Diag External SIP Proxy

Echo Canceller:

Echo Canceller Type ☒ Standard EC ☐ DFEC

[EchoCanceller Parameters >>](#)

[Enhanced EchoCanceller Parameters >>](#)

Timeout Values:

Dial Timeout (msec)

Interdigit Timeout (msec)

Set to Default Values [Set Factory Default Values](#)

NTT Caller ID Support:

NTT Caller ID ☐

Fax Support:

Fax Mode

DECT Configuration:

HS registration

PIN code

HS REGISTRATION:
when you click "Enable" - HS registration is enabled
for short amount of time (1 minute). After that it is
automatically disabled.

Configuration Through Web User Interface

Welcome: Admin | Logout

Status System Network Firewall VPN QoS **Telephony** Graphs

Extensions Service Numbers **Global Config** Conferencing Unified-Diag External SIP Proxy

VoIP Calling Band Selection:

Band ☒ Narrow Band ☐ Wide Band

3-Way Calling Support:

Flash Mode ☒ Switch call ☐ Three-way call

3WC Conference Band ☒ Narrow Band ☐ Wide Band

Bandwidth extension for POTS/DECT phones:

BWE master ☐ Enable ☒ Disable

High Band

Low Band

Bandwidth extension for RSP participants:

BWE master ☐ Enable ☒ Disable

High Band

Low Band

RTP Cut-through Support:

RTP Cut-through ☐ Enable ☒ Disable

ACTIVATION:
After changing this option Asterisk must be restarted

APPLY REVIEW CLEAR

Select **ALL Codecs** and **Clear ALL Codecs** links help in selecting and clearing all codecs. This link helps when the user needs to select only one codec.

5.7.5 Conference

1. Click **Telephony** tab in the Main menu, then click the **Conferencing** sub-tab.
2. A table with the list of conference numbers is added. Click the **edit** tab to edit the already existing Conference number. Click the **delete** tab to delete the conference number from the list.
3. In the Conferencing Configuration section, click **Add New**, to add more numbers to the list. Enter the Conference Name and the Conference Number. Figure 47 shows the Conference Configuration section.
4. The user can select the following options when configuring a conference:
 - Wide Band Mixer
 - Announce User Count

- Music on Hold
- Join/Leave Sound

Figure 47. Conferencing Configuration Section

List of Conference rooms:

No.	Conference Name	Conference Number	Admin Number	Conference mixer	Options	Actions
1	MSPD-Conf	6001	none	Narrow band	[m c s]	

Add New

New Conference Number:

Conf Name

Conf Number

Admin Number

Wide Band mixer ☐

Announce user count ☐

Music on hold ☐

Join/leave sound ☐

Save **Reset** **Cancel**

APPLY **REVIEW** **CLEAR**

5. Click **Save** to save the changes and click **Apply** to apply the saved changes.

5.7.6 Unified-Diag Configuration

1. Click **Telephony** tab in the Main menu, then click the **Unified-Diag** sub-tab to open the Unified Diag Configuration section.
2. Enter the Unified-Diag information. [Figure 48](#) shows the Unified Diag-Configuration screen.

Figure 48. Unified Diag Configuration

StatusSystemNetworkFirewallVPNQoS**Telephony**Graphs

ExtensionsService NumbersGlobal ConfigConferencing**Unified-Diag**External SIP Proxy

UD Global Information:

Dst IP Address

Src Port

Dst Port

16

32

Line Information:

☐ All☐ Pots 1☐ Pots 2☐ Pots 3☐ Pots 4

UD Types Information:

TDM TX

TDM RX

SPU I/O Parameters

SPU In Stream

SPU Out Stream

Packet TX

Packet RX

UD Report

☐

☐

☐

☐

☐

☐

☐

☐

Save

?

IP-ADDRESS:

IP Address is only one time configurable. If user reconfigure, it will be effective from next boot.

✓

APPLY

📄

REVIEW

✕

CLEAR

NOTE

IP Address configuration changes are effective after board reboot.

For more information about unified Diag configuration, Refer *LS1024A Command Reference Manual*.

5.7.7 External SIP Proxy

1. Click **Telephony** tab in the Main menu, then click the **External SIP Proxy** sub-tab to open the External SIP Proxy Configuration section. [Figure 49](#) shows the External Proxy connect screen.

Figure 49. External SIP Proxy Connect

External SIP Proxy Configuration

External SIP Proxy Configuration:

☐ Connect to External SIP Proxy

Save

APPLY REVIEW CLEAR

2. Enable **Connect to External SIP Proxy** checkbox to configure the External SIP Proxy. [Figure 50](#) shows the External SIP Proxy Configuration screen. [Table 19](#) lists the External SIP Proxy configuration details.
3. Configure the SIP proxy and click **Save** to save the changes.
4. Click **Apply** to apply the saved changes.

Figure 50. External SIP Proxy

External SIP Proxy Configuration

External SIP Proxy Configuration:

☒ Connect to External SIP Proxy

Login Name

Password

Address Type ☒ IP address ☐ Domain name

IP Address

SIP-Authentication ☒ Enable ☐ Disable

Phone No. Pattern

Save

APPLY REVIEW CLEAR

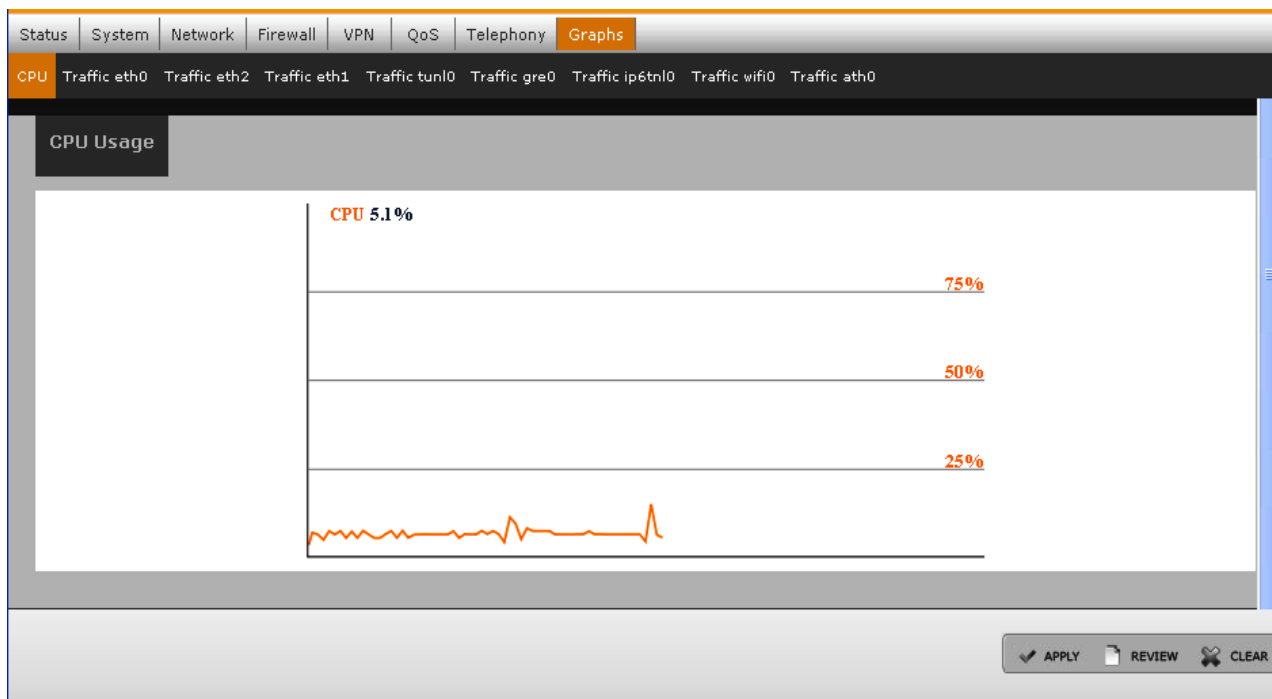
Table 19. External SIP Proxy

Option	Description
Login Name and Password	Configure the Login name and Password of the user for SIP-registration with the External SIP proxy.
Address Type	Select IP address or Domain name
SIP Authentication	Enable or Disable SIP Authentication
Phone Number Pattern	The pattern of the phone numbers that are connected to SIP proxy server. For example, _4xx.

For inter-Asterisk setup using the External SIP Proxy feature, see [Section 7.2, “Inter-Asterisk Setup.”](#)

5.8 Graphs

1. Click **Graphs** tab in the Main menu to view the CPU usage graph. [Figure 51](#) shows the options available in Graphs main menu.

Figure 51. Graphs

6 Flashing or upgrading software

This section describes the configurations and steps to upgrade software.

The following table provides a list of boot strap options available on the RDB:

System boot options code	Switch SW1	Pin1	Pin2	Pin3
Booting from LS SPI	000	off	off	off
Booting from LS I ² C	001	on	off	off
Booting from HS SPI	010	off	on	off
Booting from UART	011	on	on	off
Booting from NAND (Not Supported in LS1024A 1st stage boot loader.)	100	off	off	on
Booting from SATA (Not Supported in LS1024A 1st stage boot loader.)	101	on	off	on
Booting from 8bit NOR	110	off	on	on
Booting from 16bit NOR	111	on	on	on

NOTE

These boot strap options are only applicable for 1st stage boot loader (IBR).

6.1 Flashing board using UART boot

The following are the two scenarios to flash the board:

- Fresh board without any image
- Bricked board (Board with corrupted image)

To flash the board through UART using ymodem, perform the following:

1. Download the following onto on your PC:

```
- evm_uloader_ymodem_rc3_2.bin
- evm_barebox_ymodem_rc3_2.bin files
- uloader & barebox binaries
```

NOTE

Contact Freescale sales representative for `evm_uloader_ymodem.bin` and `evm_barebox_ymodem.bin`

2. Switch off the board.
3. Set the SW1 DIP Switch settings as below:

SW1.1, SW1.2 in ON position and SW1.3, in OFF position

4. Switch on the board.

The 'C' character appears on the terminal screen.

5. On Teraterm, send the `evm_uloader_ymodem_rc3_2.bin` using ymodem protocol as specified below:

```
FILE > TRANSFER> YMODEM > SEND
```

The below messages appears after loading:

```
uloader - C
barebox 2011.06.0 (May 17 2012 - 11:31:39)
Board: Freescale LS1024A
Copying Bb
2
Malloc space: 0x8300c000 -> 0x8300f000 (size 12 kB)
Stack space : 0x8300b000 -> 0x8300c000 (size 4 kB)
running /env/bin/init...
not found
uLoader >
uLoader >
```

6. Execute the following command at the `uloader` prompt.

```
uLoader >loady -a -o 0x01000000
```

NOTE

In case there is already a `uloader` in flash, press Enter to stop the boot in `uloader` and run `loady` at `uloader` prompt.

7. Send the `evm_barebox_ymodem.bin` using ymodem protocol as specified below:

```
FILE > TRANSFER> YMODEM > SEND
```

8. Run the barebox as specified below.

```
uLoader> go 0x01000000
```

9. Stop barebox-C2K by pressing Enter before Kernel loading.

10. Execute the following command to update microloader:

```
Barebox-C2K >/ loady -a -o 0x10000000
```

11. Load `uloader` via modem into DDR as specified below:

```
## Ready for binary (ymodem) download to 0x10000000 on DDR at 115200 bps...
```

12. Send the standard release binary `uloader` file using ymodem protocol as specified below:

```
FILE > TRANSFER> YMODEM > SEND
```

```
CCxyzModem - CRC mode, 0(SOH)/45(STX)/0(CAN) packets, 5 retries
```

```
## Total Size = 0x0000ac98 = 44184 Bytes
```

13. Execute the following command to copy `uloader` from DDR to NOR flash.

```
Barebox-C2K >/ update_nor 0x10000000 0x0 0xac98
```

Note: Change the size equal to the downloaded file size.

Unprotecting nor0...

cfi_protect: unprotect 0xc0000000 (size 44184)

Writing ...

Protecting...

cfi_protect: protect 0xc0000000 (size 44184)

DoneBarebox-C2K >/

Barebox-C2K >/

14. Update barebox with the production binary as follows:

a) Load Barebox via ymodem into DDR:

Barebox-C2K >/ loady -a -o 0x10000000

Ready for binary (ymodem) download to 0x10000000 on DDR at 115200 bps...

b) Send the standard release binary barebox file using ymodem protocol

file->transfer->ymodem->send

CCxyzModem - CRC mode, 0(SOH)/45(STX)/0(CAN) packets, 5 retries

Total Size = 0x000306e8 = 198376 Bytes

15. Program barebox from DDR to NOR flash @ address 0x20000.

Barebox-C2K >/ update_nor 0x10000000 0x20000 0x306e8 <- change size to that of the downloaded file

Unprotecting nor0...

cfi_protect: unprotect 0xc0020000 (size 198376)

[#####]

Writing ...

Protecting...

cfi_protect: protect 0xc0020000 (size 198376)

DoneBarebox-C2K >/

Barebox-C2K >/

16. Update kernel, rootfs as usual, using the barebox 'update' command.

17. Set SW1.3 switch to ON position and reboot (NOR boot) the board.

6.2 Flashing board using JTAG probe and debugger

The following are the software and the hardware requirements for updating the NOR flash memory:

Requirements

- JTAG probe

microloader and Barebox binaries - `microloader-nor.elf`, `barebox.elf` image and regular `microloader-nor.bin`, `barebox.bin` file for the target board. Both are available in LS1024A SDK of Freescale Reference Design Boards.

- Non-booting LS1024A Reference Design Board
- ARM DS-5 Developer Studio

Procedure

Perform the following procedure to update the NOR flash memory of the Reference Design Board:

1. Connect the JTAG probe and launch the debugger. Connect it to the core.
2. Connect a serial console to the Reference Design Board and load the `microloader-nor.elf` image in the debugger.

From the DS-5 command prompt run the following commands.

```
stop
loadfile microloader-nor.elf
run
```

3. Microloader will run and initialize the DDR. Stop the debugger again to load `barebox.elf` image.

```
stop
loadfile barebox.elf
run
```

4. Barebox will boot and provide the prompt. Stop the debugger again to store `microloader-nor.bin` binary to location `0x800000`.

```
stop
restore microloader-nor.bin binary 0x800000
run
```

5. Update the NOR flash `uloader` partition.

```
update -t uloader -d nor -m ddr -a 0x800000 -s 0x10000
```

NOTE

"-s" option should be provided with correct size of binary

6. Stop the debugger again to store `barebox.bin` binary to location `0x800000`.

```
stop
restore barebox.bin binary 0x800000
run
```

7. Update the NOR flash `barebox` partition.

```
update -t barebox -d nor -m ddr -a 0x800000 -s 0x843000
```

NOTE

"-s" option should be provided with correct size of binary

8. Stop the debugger and disconnect debugger from the target.
9. Reset the Reference Design Board.

6.3 Flashing or updating flash partitions

NOR microloader can reside in parallel NOR flash or in SPI serial NOR flash or I²C eeprom flash, and the boot loader code is booted from the same location. The boot loader will boot Linux and rootfs image, which resides in parallel NOR or NAND flash partitions based on the barebox environment configuration (`kernel_loc` and `rootfs_loc`).

Table 20. NOR and NAND microloader residence and target barebox

Microloader Image	Resident flash	Boots Barebox from
NOR microloader	NOR	NOR
NOR microloader	SPI-NOR	SPI-NOR
NOR microloader	I ² C	NOR
NAND microloader	NOR	NAND
NAND microloader	SPI-NOR	NAND
NAND microloader	I ² C	NAND

6.3.1 Configuring barebox

The µloader, barebox, kernel and rootfs images on the board are usually updated using TFTP. In preparation for this, the board needs to be configured with an IP address on the same subnet as your TFTP server. The board also needs to be configured with the IP address of the TFTP server.

To see the current network settings for the WAN port eth0, use the `devinfo` command as follows:

```
Barebox-C2K >/ devinfo eth0
base : 0x0
size : 0x0
driver: none
Parameters:
ipaddr = 192.168.1.130
ethaddr = 00:0A:0B:0C:0D:0E
gateway = <NULL>
netmask = <NULL>
serverip = 192.168.1.108
Barebox-C2K >/
```

Note that while the LAN ports may be used in barebox, these instructions assume the WAN port, eth0, is used. Key Barebox environment variables such as board IP address and server IP address are stored in file `/env/config`, so if you need to change these parameters, edit this file using the edit command as follows:

```
Barebox-C2K >/ edit /env/config
```

6.3.2 Flashing or updating NOR/NAND

To update images (microloader, barebox, bareboxenv, kernel and files system (jffs2 and UBI images)) use the following command at barebox prompt:

```
update -t <kernel|rootfs|barebox|bareboxenv> -d <nor|nand> [-m tftp|xmodem|ddr] [-f  
imagename|-a address] -c [-s <imagesize>]
```

Table 21. Command options

-t	Defines image to be flashed
-d	Defines storage device to be updated (NOR or NAND): Default is NOR
-m	Defines transfer mode. Default mode is tftp
-f	Image file name on the tftp server
-a	image address in ddr
-c	Check the crc32 for the image and flashed one
-s	Size of the image in ddr

Examples:

```
"update -t uloader -d <nor|i2c> [-m tftp|xmodem|ddr] [-f imagename|-a address] [-s  
<imagesize>]" to update uloader into flash
```

```
"update -t barebox -d <nor|nand> [-m tftp|xmodem|ddr] [-f imagename|-a address] [-s  
<imagesize>]" to update barebox into flash
```

```
"update -t kernel -d <nor|nand> [-m tftp|xmodem|ddr] [-f imagename|-a address] [-s  
<imagesize>]" to update kernel into flash
```

```
"update -t rootfs -d <nor|nand> [-m tftp|xmodem|ddr] [-f imagename|-a address] [-s  
<imagesize>]" to update rootfs into flash
```

```
"update -t bareboxenv -d <nor|nand> [-m tftp|xmodem|ddr] [-f imagename|-a address] [-s  
<imagesize>]" to update bareboxenv into flash
```

6.3.3 Flashing or updating serial NOR partition (SPI Boot)

SPI boot is NOT supported on LS1024A RDB. To use SPI boot, μ loader has to be present in SPI-Flash device connected at chip select 0 of the SPI controller. μ loader starts at 0x0 address at sector 0x0 in the SPI-Flash. Barebox can also be present in the SPI-Flash, and starts at 0x0 address of sector 0x2.

NOTE

Add a temporary partition at DDR address 0x800000 using the command
`addpart /dev/mem 10M@0x800000 (temp)`

6.3.3.1 Updating SPI-Flash for µloader

To update the µloader in the SPI-Flash, use the following command:

Barebox-C2K >/ tftp tftp_address_to_uLoader_binary /dev/mem.temp

Run the following command from Barebox prompt:

Barebox-C2K >/ update_spi <memory_addr> <flash_sector> <sector_offset> <uLoader_size>

Example:

Barebox-C2K >/ tftp uloader.bin /dev/mem.temp

Barebox-C2K >/ update_spi 0x800000 0x0 0x0 0xb0c0

6.3.3.2 Updating SPI-Flash for barebox

Use the following command to update the Barebox in the SPI-Flash:

NOTE

Add a temporary partition at DDR address 0x800000 using the command
`addpart /dev/mem 10M@0x800000 (temp)`

Barebox-C2K >/ tftp tftp_address_to_Barebox_binary /dev/mem.temp

Run the following command from Barebox prompt:

Barebox-C2K >/ update_spi <memory_addr> <flash_sector> <sector_offset> <barebox_size>

Example:

Barebox-C2K >/ tftp Barebox.bin /dev/mem.temp

Barebox-C2K >/ update_spi 0x800000 0x2 0x0 0x3847c

SPI Environment variables partition support

Barebox environment variables can be flashed in the SPI-Flash. Sector 10th and 11th are kept for the environment variables starting from 10th sector of the SPI-Flash. SPI-Flash is partitioned as shown in [Section Table 22., “SPI-Flash partition for µloader, barebox and ENV”](#). Each row in the table corresponds to one sector of 64KB size of SPI-Flash. Space allocation for µloader, Barebox and Environment variables is as shown below:

µloader: 128 KB (From Sec 0 to 1)

Barebox: 512 KB (From Sec 2 to 9)

Env: 128 KB (From Sec 10 to 11)

Table 22. SPI-Flash partition for μ loader, barebox and ENV

SPI-Flash Sec-0 for uloader
SPI-Flash Sec-1 for uloader
SPI-Flash Sec-2 for uloader
SPI-Flash Sec-3 for uloader
SPI-Flash Sec-4 for uloader
SPI-Flash Sec-5 for uloader
SPI-Flash Sec-6 for uloader
SPI-Flash Sec-7 for uloader
SPI-Flash Sec-8 for uloader
SPI-Flash Sec-9 for uloader
SPI-Flash Sec-10 for ENV
SPI-Flash Sec-11 for ENV

ENV partition can be updated using one of the following two methods:

1. Use SPI Boot and run the following commands from Barebox prompt after the first boot:


```
-erase /dev/env0
```

```
-save
```
2. To update the environment variables in the SPI-Flash, env file (barebox_default_env) has to be present at some DDR address and then the following command is used from Barebox prompt:

Barebox-C2K >/ update_spi <ddr_mem_addr> <flash_sector> <sector_offset> <ENV_size>

6.3.4 Flashing or updating Fast-SPI-Flash partition (Fast SPI Boot)

Fast SPI boot is supported on LS1024A RDB. To use Fast SPI boot, μ loader has to be present in Fast-SPI-Flash device connected at chip select 0 of the Fast SPI controller. μ loader starts at 0x0 address at sector 0x0 (offset 0x0) in the Fast-SPI-Flash and barebox starts at 0x0 address of sector 0x2 (at offset of 128KB).

μ loader size: 128 KB (From Sec 0 to 1)

Barebox size: 512 KB (From Sec 2 to 9)

6.3.4.1 Updating Fast-SPI-Flash for μ loader

Use the following command, to update the μ loader in the Fast-SPI-Flash:

NOTE

Add a temporary partition at DDR address 0x800000 using the command

```
addpart /dev/mem 10M@0x800000(temp)
```

```
Barebox-C2K >/ tftp tftp_address_to_uLoader_binary /dev/mem.temp
```

Use the following command from Barebox prompt:

```
Barebox-C2K >/ update_fast_spi <memory_addr> <flash_sector> <sector_offset> <uLoader_size>
```

Example:

```
Barebox-C2K >/ tftp uloader.bin /dev/mem.temp
```

```
Barebox-C2K >/ update_fast_spi 0x800000 0x0 0x0 0xb0c0
```

6.3.4.2 Update SPI-Flash for Barebox

To update the Barebox in the Fast-SPI-Flash, use the following command:

NOTE

Add a temporary partition at DDR address 0x800000 using the command

```
addpart /dev/mem 10M@0x800000(temp)
```

```
Barebox-C2K >/ tftp tftp_address_to_Barebox_binary /dev/mem.temp
```

Following command is used from Barebox prompt:

```
Barebox-C2K >/ update_fast_spi <memory_addr> <flash_sector> <sector_offset> <barebox_size>
```

Example:

```
Barebox-C2K >/ tftp Barebox.bin /dev/mem.temp
```

```
Barebox-C2K >/ update_fast_spi 0x800000 0x2 0x0 0x3847c
```

NOTE

The ENV partition resides in NOR.

6.3.5 Flashing or updating I²C EEPROM (I²C Boot)

I²C boot is supported on LS1024A and LS10xMA boards. To use I²C boot and μ loader have to be present in I²C-EEPROM. μ loader starts at 0x0 address. Only μ loader can be accommodated in the EEPROM. This can be NAND or NOR μ loader, which expects the corresponding barebox to reside on NAND or NOR respectively.

6.3.5.1 Updating I²C-EEPROM for μ loader

To update the μ loader in the I²C-EEPROM, use the following command:

```
Barebox-C2K >/update -t uloader -d i2c -m tftp -f uloader.bin
```

6.3.6 Flashing or updating UBI image on rootfs partition

SDK supports both JFFS2 and UBIFS file systems on NOR flash. Only UBIFS is supported on NAND flash.

6.3.6.1 Updating Environment partition (/dev/env0)

To support both file systems environment partition is updated. To get this new environment, it is necessary to erase the environment (/dev/env0) partition after new Barebox update and before reboot. It gets the new environment configuration after reboot.

```
Barebox-C2K > unprotect /dev/env0
```

```
Barebox-C2K > erase /dev/env0
```

6.3.6.2 Flashing UBI Image on rootfs partition

By default Linux boots with `ubifs` file system, the environment configuration parameter `rootfs_type` set to UBIFS. Flashing UBI NOR/NAND image on rootfs partition is similar to flashing the JFFS2 NOR image on rootfs partition. Instead of JFFS2 image name, pass the UBI image name to the update command.

```
"update -t rootfs -d <nor|nand> [-m tftp|xmodem|ddr] [-f imagename|-a address] [-s <imagesize>]"
```

to update rootfs into flash.

Here `imagename` is UBI NOR/NAND image name.

6.3.6.3 Booting with JFFS2 image

To boot with JFFS2 file system, after JFFS2 image flash on rootfs partition and before reboot change the `rootfs_type` Barebox environment configuration parameter value to JFFS2 from UBIFS. To do this, use this command:

```
Barebox-C2K > edit /env/config
```

Change the `rootfs_type` to `jffs2` from `ubifs`. To save and exit from editor press CTRL+D. Save the configuration using this command:

```
Barebox-C2K > sa
```

6.4 Environment variables

If the environment partition is empty, Barebox loads a set of default parameters. Sometimes a new version of Barebox will add an environment variable, and in this case, after updating Barebox to the new version, you should erase the current environment variables and reboot the board to ensure the environment variables are consistent with this version of Barebox. Therefore we recommend that if you update barebox to a new version, you also erase the environment partition.

To erase the ENV partition of NOR, NAND and SPI, run the following commands from the Barebox prompt:

```
erase /dev/env0
```

```
save
```

Now reboot the board. You will see that Barebox doesn't find any environment variables and so loads its defaults.

Update `/env/config` for your network environment as described in [Section 6.3.1, “Configuring barebox”](#)

Barebox. Don't forget to use `saveenv` after you've updated `/env/config`

- o Another method to update the env partition of SPI, is to use the

following command from the Barebox prompt:

- `/update_spi <ddr_mem_addr> <flash_sector> <sector_offset>`
`<ENV_size>`
- The env file (`barebox_default_env`) has to be present at some DDR address.

6.5 U-Boot - Flashing or upgrading software

If U-Boot is used as third stage bootloader instead of Barebox, the following steps will be useful for flashing and upgrading software.

NOTE

All features supported by Barebox are not supported by U-Boot.
 Refer QorIQ LS1024A Linux BSP Architecture Specification document for more details.

6.5.1 Flashing the board using UART Boot

1. Follow the steps 1 to 13 to flash microloader to NOR flash (See [Section 6.1, “Flashing board using UART boot”](#))
2. Update U-Boot with the production binary as follows:
 - a) Load U-Boot via ymodem into DDR:

```
Barebox-C2K >/ loady -a -o 0x10000000
## Ready for binary (ymodem) download to 0x10000000 on DDR at 115200 bps...
```

- b) Send the standard release binary U-Boot file using ymodem protocol

```
file->transfer->ymodem->send
CCxyzModem - CRC mode, 0(SOH)/45(STX)/0(CAN) packets, 5 retries
## Total Size = 0x000306e8 = 198376 Bytes
```

3. Program U-Boot from DDR to NOR flash @ address 0x20000.

```
Barebox-C2K >/ update_nor 0x10000000 0x20000 0x306e8 <- change size to that of the
downloaded file
Unprotecting nor0...
cfi_protect: unprotect 0xc0020000 (size 198376)
[#####]
Writing ...
Protecting...
cfi_protect: protect 0xc0020000 (size 198376)
```

```
DoneBarebox-C2K >/
```

```
Barebox-C2K >/
```

4. Set SW1.3 switch to ON position and reboot (NOR boot) the board.
5. Update kernel, rootfs from U-Boot. The steps are described in the following sections.

6.5.2 Flashing board using JTAG probe and debugger.

1. Follow the steps 1 to 5 to flash microloader to NOR flash. (See [Section 6.2, “Flashing board using JTAG probe and debugger”](#))
2. Stop the debugger again to store u-boot.bin binary to location 0x800000.

```
stop
```

```
restore u-boot.bin binary 0x800000
```

```
run
```

3. Update the NOR flash barebox partition.

```
update -t barebox -d nor -m ddr -a 0x800000 -s 0x843000
```

NOTE

"-s" option should be provided with correct size of binary

4. Stop the debugger and disconnect debugger from the target.
5. Reset the Reference Design Board.

6.5.3 Upgrading software from U-Boot

1. To upgrade µloader use the following command in the U-Boot prompt.

```
U-Boot> run updateeuloader
```

2. To upgrade U-Boot use the following commands in the U-Boot prompt.

Modify bootfile using the setenv command.

```
U-Boot> setenv bootfile u-boot.bin
```

Run the updateboot command.

```
U-Boot> run updateboot
```

3. To upgrade kernel use the following commands in the U-Boot prompt.

Modify kernelfile using the setenv command.

```
U-Boot> setenv kernelfile uImage
```

Run the updatekernel command.

```
U-Boot> run updatekernel
```

4. To upgrade rootfs use the following commands in the U-Boot prompt.

Modify fsfile using the setenv command.

```
U-Boot> setenv fsfile rootfs
```

Run the updatekernel command.

```
U-Boot> run updatefs
```

5. To save U-Boot environment.

```
U-Boot> save
```

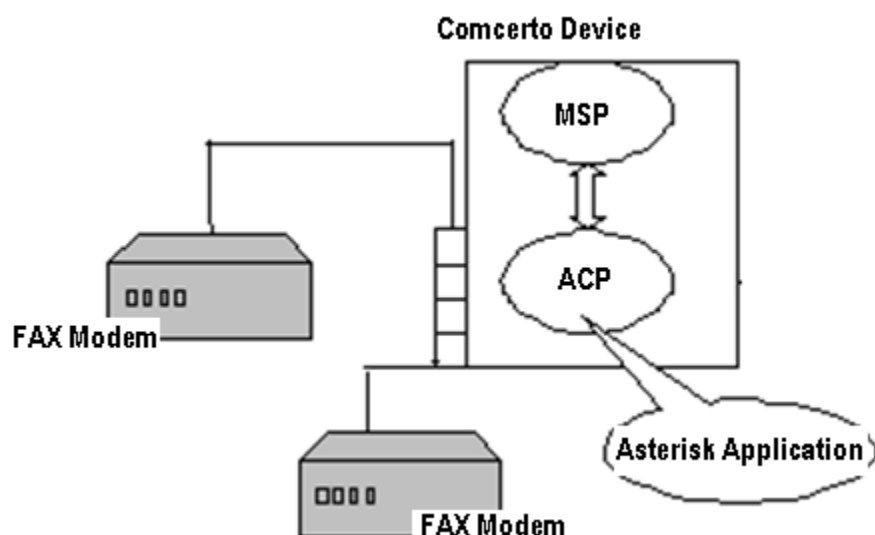
7 Appendix

This section explains the Fax testing setup and Inter-asterisk setup.

7.1 FAX Testing Setup

This section describes the fax testing setup for the device. VentaFax[®] software is used for fax testing. VentaFax is a full-featured computer fax software and answering machine software. Ventafax must be set for **Signaling as TonePulsemode** setting, which is available under **Signal Recognition** of **Miscellaneous** tab. [Figure 52](#) illustrates the FAX setup.

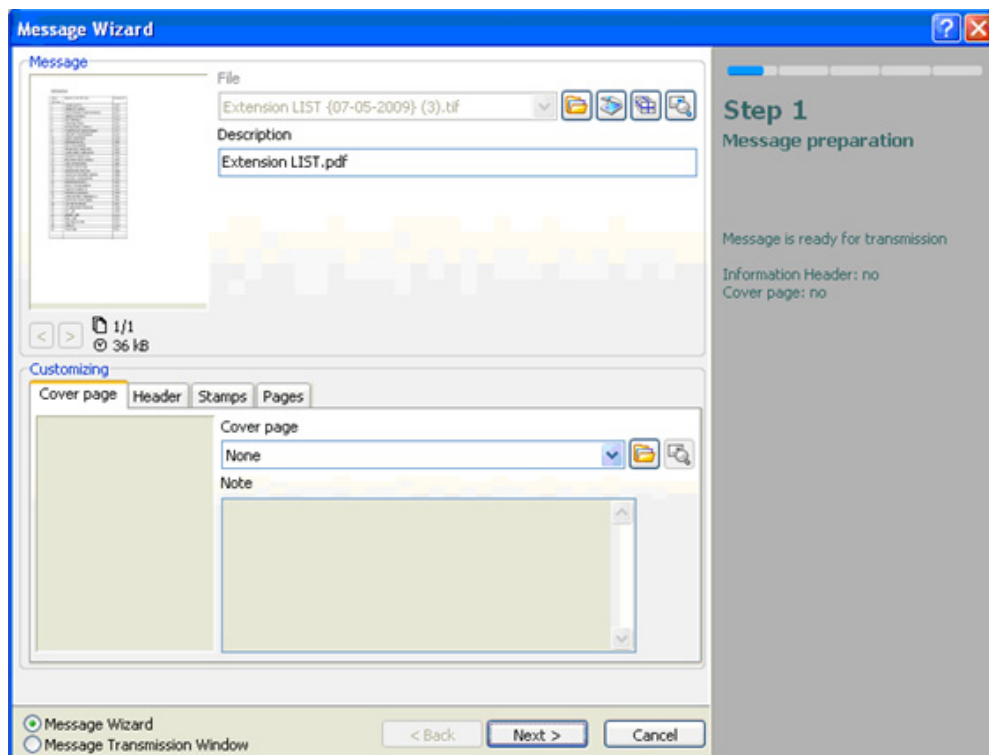
Figure 52. FAX Setup



The following procedure describes how to send or receive fax across two fax modems that are connected to SLIC devices. In this example, the sender fax modem is connected to SLIC 0, and the receiver fax modem is connected to SLIC 3.

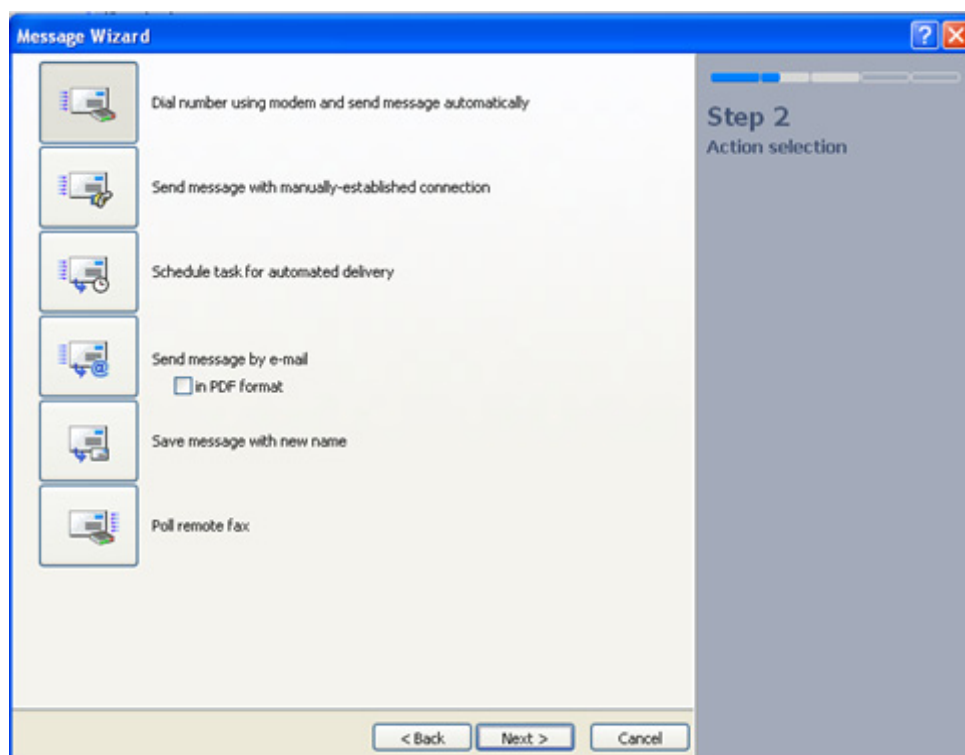
1. Open the document to be faxed and click **Print**. Select VentaFax and click **OK** to open the VentaFax message-wizard.
2. In Step 1 of the VentaFax-message wizard, if required, set the cover page options and click **Next**. [Figure 53](#) shows the Step 1 of VentaFax-message wizard.

Figure 53. Step 1 Message Preparation



3. In Step 2 of the VentaFax-message wizard, chose **Dial number using modem and send message automatically** option and click **Next**.

Figure 54. Step 2 Action Selection



4. In the Step 3 of the VentaFax-message wizard, enter the receiver SLIC number and click **finish**.

Figure 55. Step 3 Data Input

The fax transmission starts and the Ventafax main window of the sender shows that the call is setting up. The VentaFax main window on receiver side will start ringing and the receiver should press **Start** to begin the fax transmission.

7.2 Inter-Asterisk Setup

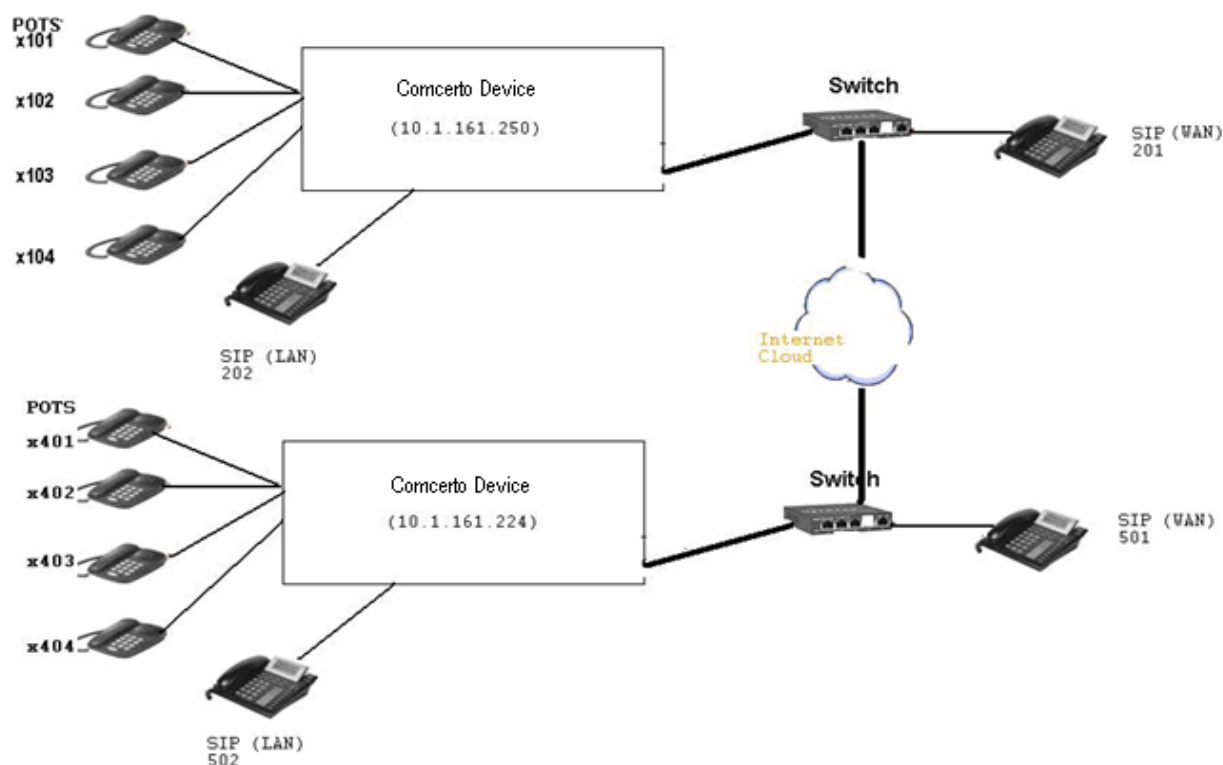
Asterisk supports the SIP call-control protocol. This establishes a VoIP call between the Asterisks running on two Reference Design Board. Asterisk is configured as SIP Back to Back User Agent (B2BUA) and handles calls involving SIP endpoints. However, in this setup two Reference Board both running on Asterisk, are connected back-to-back. Each instance of Asterisk registers with the other instance of Asterisk by registering itself as a peer.

In Asterisk, the configuration information is held in the following files:

- Sip.conf
- Extensions.conf
- mspd.conf

Figure 56 illustrates the inter-asterisk setup.

Figure 56. Inter-Asterisk Setup



For Reference Board1 (10.1.161.250), the POTS phones (connected to the four FXS ports) will have pre-configured extensions of 101,102,103, and 104. The SIP phones, connected to the LAN port of Reference Board1, will have pre-configured extensions of 201, 202, 203, and 204.

For Reference Board2, the POTS phones (connected to the four FXS ports) will have pre-configured extensions of 401, 402, 403, and 404. The SIP phones, connected to the LAN port of Reference Board1, will have pre-configured extensions of 501, 502, 503, and 504.

Perform the following steps for inter-asterisk setup:

1. On Reference board1 (10.1.161.250), a new peer must be added for registration. This information will be used by other asterisk for registering with this asterisk SIP Proxy. Add a new SIP extension from the **IP-PBX >>Extensions** tab with type as Peer and 1234 as extension and password. Save and apply changes.
2. On Reference board2 (10.1.161.224), a new peer must be added. Add a new SIP extension from the **IP-PBX >>Extensions** tab with type as Peer and 7890 as extension and password. Save and apply changes.
3. On Reference board2 (10.1.161.224), change the POTS extensions to 4xx format. Similarly, change SIP extensions to 5xx format. Save and apply changes.
4. From Reference board1, navigate to **IP-PBX >>External SIP Proxy** sub-tab and enable **Connect to External SIP Proxy** checkbox.
 - Enter the Login-Name and Password for the new peer configured on Reference board2 as per Step 2. In this example, it is 7890 with password 7890.

- Enter the address type as IP Address and enter the ip-address of Reference board2. In this case it is 10.1.161.224.
 - SIP Authentication can be enabled or disabled.
 - Phone number pattern must be updated as _4xx.
 - Save and apply changes.
5. On Reference board2, navigate to **IP-PBX >>External SIP Proxy** and enable **Connect to External SIP Proxy**.
 - Enter the Login-Name and Password for the new peer configured on Reference board1 as per Step1. In this example, it is 1234 with password 1234.
 - Enter the address type as IP Address and enter the ip-address of Reference board1. In this case it is 10.1.161.250.
 - SIP Authentication can be enabled or disabled.
 - Phone number pattern must be updated as _1xx.
 - Save and apply changes.
 6. To verify the registration, execute the following command on each of the Reference board:

```
asterisk -rx "sip show peers"
```

Sample output of `asterisk -rx "sip show peers"` on Reference board1:

Name/username	Host	Dyn	Nat	ACL	Port	Status
1234/s	10.1.161.224	D			5060	Unmonitored
202/202	192.168.1.50	D			5060	Unmonitored
201/201	10.1.161.214	D			5060	Unmonitored

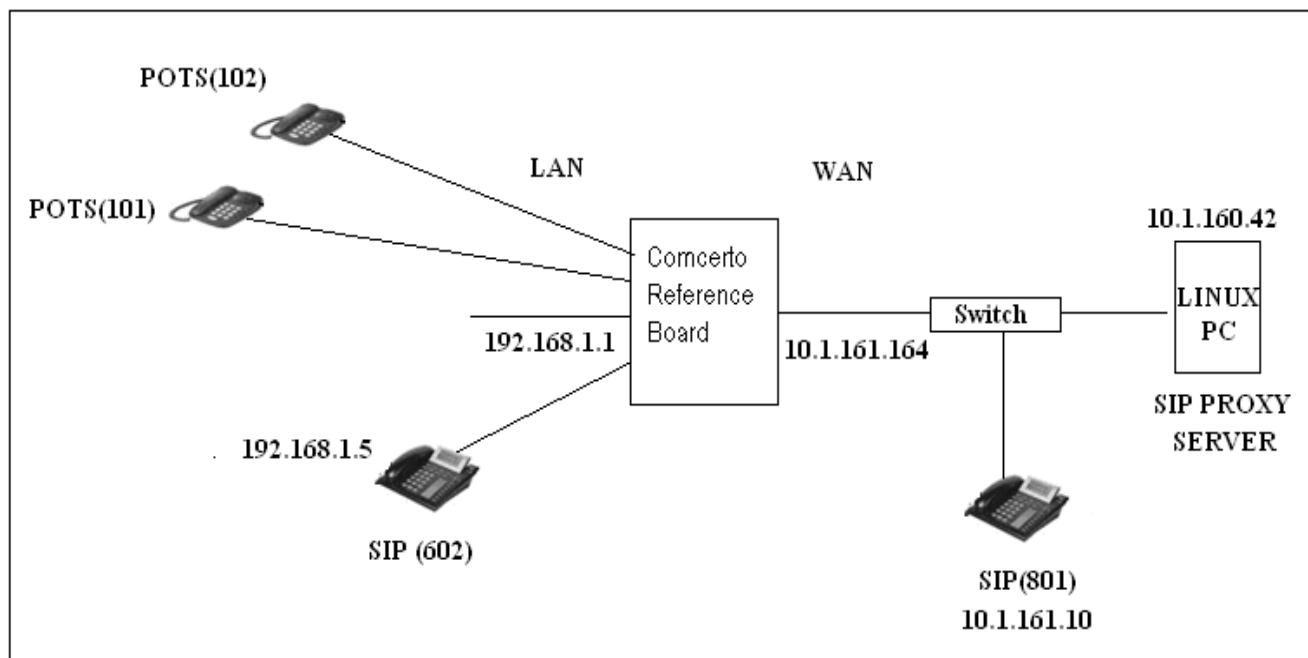
3 sip peers [3 online, 0 offline]

Check if 1234 has IP-Address of Reference board2.

7.3 External SIP Proxy Server Configuration

The integration of Asterisk with external SIP proxy, enables the user to make a call from an external SIP Proxy to Asterisk running on the LS1024A Reference board. [Figure 57](#) shows external SIP Proxy Server setup.

Figure 57. External SIP Proxy Topology



The following sections describe an example configuration as per the topology given in [Figure 57](#).

GUI Configurations

1. Enter the IP address, 192.168.1.1 in the local network, followed by the user name and password. The web Username and Password is set as `admin`.
2. Click the **Network** tab in the Main menu, and then click the **NAT-Rules** sub-tab in Network menu. Disable NAT.
3. Click the **IP-PBX** tab in the Main menu, and then click the **Extensions** tab. Add one new VoIP extension as peer with the configurations shown in [Table 23](#).

Table 23. VoIP Extension Configuration

Option	Description
Name	601
Number/Auth Name	601
Type	SIP
Protocol	Peer
Authentication Password	601

4. Save and apply changes.
5. Click the **IP-PBX** tab in the Main menu, and then click the **External SIP Proxy** tab. Select the External SIP Proxy configurations as shown in [Table 24](#).

Table 24. External SIP Proxy

Option	Description
Login Name and Password	601
Address Type	IP address
SIP Authentication	Enable
Phone Number Pattern	_8xx

6. Save and Apply Changes.

SIP Proxy Server Configurations (10.1.160.42)

```
root@newubuntu: /etc/init.d/mysql start
```

```
root@newubuntu: openser -f /home/user/openser.cfg ("killall openser" before starting the openser.cfg)
```

The Configuration file *Openser.cfg* must be updated with the IP address of asterisk-sip-server. In this case, the IP-address is **10.1.161.164**. The IP address is highlighted in the following configuration file:

```
root@newubuntu: cat openser.cfg
#
# $Id: openser.cfg,v 1.5 2005/10/28 19:45:33 bogdan_iancu Exp $
#
# simple quick-start config script
#

# ----- global configuration parameters -----

debug=8          # debug level (cmd line: -dddddddddd)
#fork=yes
#log_stderr=no    # (cmd line: -E)

#Uncomment these lines to enter debugging mode
fork=yes
log_stderr=yes

check_via=no      # (cmd. line: -v)
dns=no           # (cmd. line: -r)
rev_dns=no       # (cmd. line: -R)
port=5060
children=4
fifo="/tmp/openser_fifo"
fifo_db_url="mysql://openser:openserrw@localhost/openser"
#
# uncomment the following lines for TLS support
#disable_tls = 0
#listen = tls:your_IP:5061
#tls_verify = 1
#tls_require_certificate = 0
#tls_method = TLSv1
#tls_certificate = "/usr/local/etc/openser/tls/user/user-cert.pem"
#tls_private_key = "/usr/local/etc/openser/tls/user/user-privkey.pem"
#tls_ca_list = "/usr/local/etc/openser/tls/user/user-calist.pem"
```

```

# ----- module loading -----

# Uncomment this if you want to use SQL database
loadmodule "/usr/local/lib/openser/modules/mysql.so"

loadmodule "/usr/local/lib/openser/modules/sl.so"
loadmodule "/usr/local/lib/openser/modules/tm.so"
loadmodule "/usr/local/lib/openser/modules/rr.so"
loadmodule "/usr/local/lib/openser/modules/maxfwd.so"
loadmodule "/usr/local/lib/openser/modules/usrloc.so"
loadmodule "/usr/local/lib/openser/modules/registrar.so"
loadmodule "/usr/local/lib/openser/modules/textops.so"

# Uncomment this if you want digest authentication
# mysql.so must be loaded !
loadmodule "/usr/local/lib/openser/modules/auth.so"
loadmodule "/usr/local/lib/openser/modules/auth_db.so"

# ----- setting module-specific parameters -----

# -- usrloc params --

modparam("usrloc|auth_db|avpops|group",
    "db_url", "mysql://openser:openserrw@localhost/openser")

#modparam("usrloc", "db_mode", 0)

# Uncomment this if you want to use SQL database
# for persistent storage and comment the previous line
modparam("usrloc", "db_mode", 2)

# -- auth params --
# Uncomment if you are using auth module
#
modparam("auth_db", "calculate_ha1", yes)
#
# If you set "calculate_ha1" parameter to yes (which true in this config),
# uncomment also the following parameter)
#
modparam("auth_db", "password_column", "password")

# -- rr params --
# add value to ;lr param to make some broken UAs happy
#modparam("rr", "enable_full_lr", 1)

# ----- request routing logic -----

# main routing logic

route{

    # initial sanity checks -- messages with
    # max_forwards==0, or excessively long requests
    if (!mf_process_maxfwd_header("10")) {
        sl_send_reply("483", "Too Many Hops");
        exit;
    };
};

```

```

if (msg:len >= 2048 ) {
    sl_send_reply("513", "Message too big");
    exit;
};

# we record-route all messages -- to make sure that
# subsequent messages will go through our proxy; that's
# particularly good if upstream and downstream entities
# use different transport protocol
if (!method=="REGISTER")
    record_route();

if (method=="REGISTER") {
    log(1, "Mindspeed---REGISTER received !!!!! \n");
    sl_send_reply("100", "OK");
    log(1, "Mindspeed---REGISTER received !!!!! \n");
    if (!www_authorize("10.1.160.42", "subscriber")) {
        www_challenge("10.1.160.42", "0");
    };
    log(1, "Mindspeed---after auth-----\n");
};

if (method=="INVITE") {
    log(1, "Mindspeed---INVITE received !!!!! \n");
    sl_send_reply("100", "TRYING");
    if (!www_authorize("10.1.160.42", "subscriber")) {
        www_challenge("10.1.160.42", "0");
    };
    #log(1, "-----Mindspeed---REDIRECTING to 112-----\n");
    rewritehostport("10.1.161.164:5060");
    #route(1);
    log(1, "Mindspeed---after auth-----\n");
};

# subsequent messages withing a dialog should take the
# path determined by record-routing
if (loose_route()) {
    # mark routing logic in request
    append_hf("P-hint: rr-enforced\r\n");
    route(1);
};

# if (!uri==myself) {
#     # mark routing logic in request
#     append_hf("P-hint: outbound\r\n");
#     # if you have some interdomain connections via TLS
#     if(uri=~"@tls_domain1.net") {
#         t_relay_to_tls("IP_domain1","port_domain1");
#         exit;
#     } else if(uri=~"@tls_domain2.net") {
#         t_relay_to_tls("IP_domain2","port_domain2");
#         exit;
#     }
#     route(1);
# };

# if the request is for other domain use UsrLoc

```

```

# (in case, it does not work, use the following command
# with proper names and addresses in it)
if (uri==myself) {

    if (method=="REGISTER") {
        log(1, "REGISTER received\n");
        # Uncomment this if you want to use digest authentication
        if (!www_authorize("10.1.160.42", "subscriber")) {
            www_challenge("10.1.160.42", "0");
            exit;
        };

        save("location");
        exit;
    };

    lookup("aliases");
    if (!uri==myself) {
        append_hf("P-hint: outbound alias\r\n");
        route(1);
    };

    # native SIP destinations are handled using our USRLOC DB
    if (!lookup("location")) {
        sl_send_reply("404", "Not Found");
        exit;
    };
    append_hf("P-hint: usrloc applied\r\n");
};
route(1);
}
route[1] {
    # send it out now; use stateful forwarding as it works reliably
    # even for UDP2TCP
    if (!t_relay()) {
        sl_reply_error();
    };
    exit;
}

```

7.4 Diagnostics Test

Boards developed based on LS1024A platform have various hardware application interfaces. The Manufacturing Diagnostics software tests the functionality of all the hardware interfaces on LS1024A based boards. If all the tests pass, the board is considered to be free of any manufacturing defects and is selected for deployment. The software runs as part of the board manufacturing process.

Every board that is manufactured have this software burned into the NOR flash before mounting it on the board. When the operator powers up the board, the software runs and presents a command-line prompt to the operator through serial interface. The software supports writing the NOR flash and this capability is used to over-write the NOR flash with the secondary bootloader (SBL). If the board does not have NOR

flash and only has NAND flash, the software will be burned into the NAND flash before mounting it on the board. Table 6-3 list the testing interfaces.

Table 25. List of Testing Interfaces

Sr.No.	Functionality/Interface	Description
2	NOR	This test will write/read specific patterns (0xAA, 0x55) to all the memory locations.
3	SPI	This test will erase 2 sectors, write predefined data to those 2 sectors, read data back from those 2 sectors and finally verify the read data and written data.
4	Fast SPI	This test will erase 2 sectors, write predefined data to those 2 sectors, read data back from those 2 sectors and finally verify the read data and written data.
5	L2CC	
8	PCIe	
10	ZDS/TDM	This will perform the TDM Rx/Tx external loopback through TDM interface ZDS.
11	Fast UART	This test will perform read/write transactions with/without DMA and the error checking & correction.
12	USB	Command to run the USB diags test- Diags-C2K >/ diags -r usb3phyber
13	IPSEC through utilpe	These tests the ipsec functionality from utilpe.
14	I ² C	This test will read/write predefined data bytes to I ² C device.
15	MSIF/TDM	This will perform the TDM Rx/Tx external loopback through TDM interface MSIF.
16	MSIF/SLIC	This will initialize the MSIF block, SLIC device and identifies OFF-HOOK and ON-HOOK of the POTS phones connected.
18	OTP	This test is used to program the OTP memory and then verifies whether correct data has written.
20	NAND ECC	This test will erase raw write/read to NAND flash. This will also verify the ECC error detection and correction.
21	I2S	This test, the data is transferred to I2S controller via a DMA access and is received from the input line then transferred into the Rx FIFO. The received data will be read using DMA access and compared with the sent data.
22	SATA	This test is used to read/write the base registers of the SATA controller and also send/receive packets in a loopback fashion then checks whether the correct packet has received.

7.5 Procedure to Build the Diags Binary

1. Extract the LS1024A Diags tar file provided.
2. Configure the Diags build using the following command.

\$ make menuconfig

3. To select the USB3 test, go to “System Type -> Comcerto Diagnostic Configuration” and select “USB3.0 Diag Testing” option.
4. To select the PCIe test, go to “System Type -> Comcerto Diagnostic Configuration” and select “PCIe Verification API” option.
5. To select the SATA test, go to “System Type -> Comcerto Diagnostic Configuration” and select “SATA Diag Testing” option.
6. Issue the following command to build the Diags binary.

```
$ make clean; make
```

NOTE

The PATH environment variable points to the required toolchain (for example for gcc version 4.5 and glibc library version 2.14.1 is “staging_dir/toolchain-arm_v7-a_gcc-4.5-linaro_glibc-2.14.1_eabi/bin”)

Procedure to Update the Diags Binary

The following is the procedure to update the Diags binary using tftp from Barebox/Diags.

1. Erase the NOR partition where the Diags need to be flashed.

```
Barebox-C2K> unprotect /dev/nor0.barebox; erase /dev/nor0.barebox
```

2. Flash the Diags binary to NOR partition.

```
Barebox-C2K > tftp <diags_location> /dev/nor0.barebox
```

where <diags_location> - Location where Comcerto 2000 Diags binary is stored.

Test Commands

USB 3.0

The following hardware reworks must be done on the LS1024A Reference Board to get the USB hub working.

- Remove R345, R457, R458 and R446 resistors.
- Short or solder bridge R446 pad to R447. The side closest to the USB hub so that SM_DAT and SM_CLK are both pulled low.

Connect the USB stick to any of the USB ports after starting the test.

The command to run the USB 3.0 DIAGS test is:

```
Diags-C2K >/ diags -r usb3phyber
```

PCIe

Connect the GIGABYTE WiFi mini PCIe card with model number "GN-WS30N-RH" to slot 0.

The command to run the PCIe test is:

```
Diags-C2K >/ diags -r pcieperf
```

SATA

The present version of the test has two test cases.

SATA controller register read/write test

SBPHY initialization and Lane ready verification test

The command to run the SATA test is:

```
Diags-C2K >/ diags -r sata
```

DDR

The DDR Test is run from the μ loader only.

The command to run the DDR test is:

```
Diags-C2K >/ ddrtest
```

DPI

The command to run the DPI test is:

```
Diags-C2K >/ diags -r dpi
```

NOR

The command to run the NOR test is:

```
Diags-C2K >/ diags -r nor
```

NAND ECC

The command to run the NAND ECC test is:

```
Diags-C2K >/ diags -r nandecc
```

OTP

The command to run the OTP test is:

```
Diags-C2K >/ diags -r otp
```

ZDS/SLIC

The command to run the ZDS/SLIC test:

```
Diags-C2K >/ diags -r zdsslic
```

To validate the SPI block, the ZDS/SLIC Diags test is run since the ZDS SLIC is initialized through the SPI.

Connect a POTS phone to any of the ports before running the test.

The test waits for the off/on-hook events. So perform the off-hook and on-hook operations with the connected POTS phone and the status message will be displayed on the console. Press "Control + C" to exit from the test.

IPSEC

The command to run the IPsec is:

```
Diags-C2K >/ diags -r ipsec
```

I²C

The command to run the I²C Diags is:

```
Diags-C2K >/ diags -r i2c
```

Ethernet(LAN and WAN)

This command tests the WAN port and all four LAN ports one by one.

The command to run the ethernet test is:

```
Diags-C2K >/ diags -r eth
```

DSPG

Load the DSPG TH firmware file css.elf (provided in same zip file) at location 0x20000000 using the debugger.

The command to run the DSPG test is:

```
Diags-C2K >/ diags -r eth
```

8 Revision History

This table provides the revision history of this document

Table 26. Revision Table

Revision	Date	Substantive Changes
Rev2	03/2015	Updated with Telephony configuration page
Rev1	11/2014	Updated Section 6, “Flashing or upgrading software” .
Rev 0	10/2014	Initial public release

How to Reach Us:

Home Page:

www.freescale.com

Web Support:

<http://www.freescale.com/support>

Information in this document is provided solely to enable system and software implementers to use Freescale products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document.

Freescale reserves the right to make changes without further notice to any products herein. Freescale makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in Freescale data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including "typicals," must be validated for each customer application by customer's technical experts. Freescale does not convey any license under its patent rights nor the rights of others. Freescale sells products pursuant to standard terms and conditions of sale, which can be found at the following address: [freescale.com/Sales Terms and Conditions](http://freescale.com/Sales%20Terms%20and%20Conditions).

Freescale, the Freescale logo, and QorIQ are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. Layerscape, trademark of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org. ARM and Cortex are registered trademarks of ARM Limited. ARM is the trademark of ARM Limited.

© 2015 Freescale Semiconductor, Inc.

Document ID: LS1024ARDBUG
Rev. 2, 03/2015



Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

[NXP:](#)

[LS1024A-RDB](#)