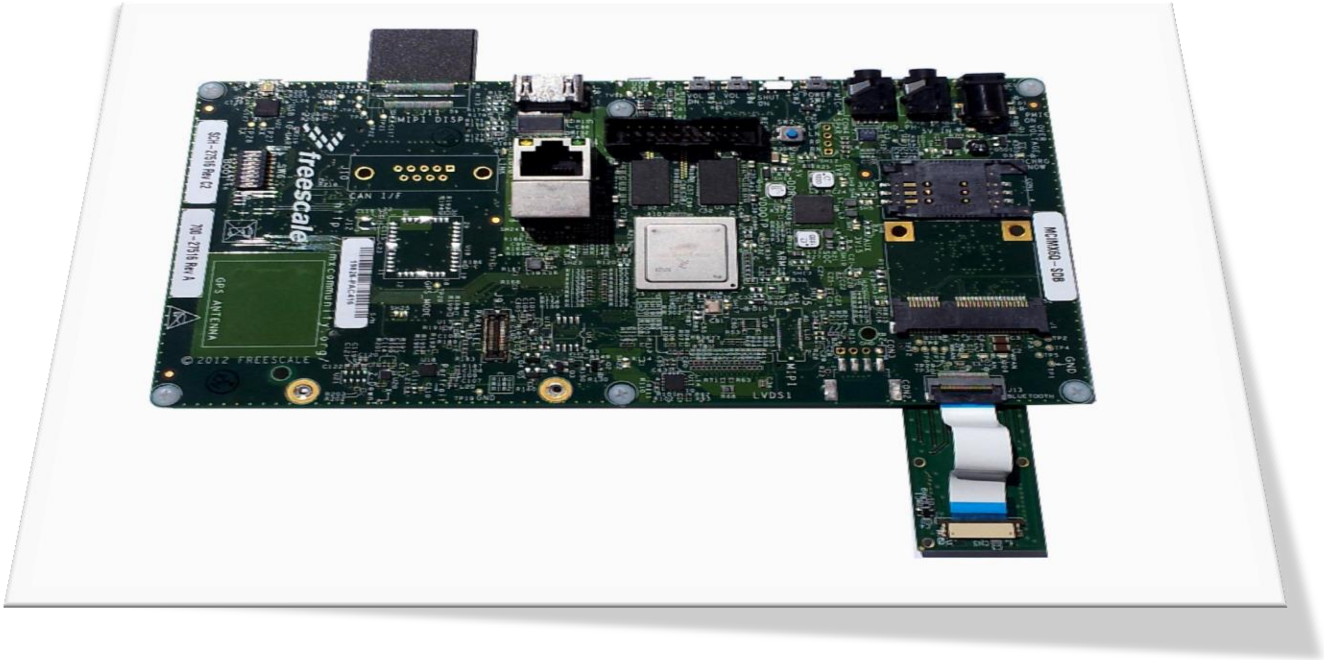


SX-6K3-EVK-SD

User Guide

Part Number 140-00207-150

Revision A

Copyright & Trademark

Silex Technology America SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS OF THIS PRODUCT FOR A PARTICULAR PURPOSE. Silex shall not be liable for any errors contained in this manual or for any damages resulting from loss of use, data, profits, or any incidental or consequential damages arising from the use of SILEX products or services. The information contained in this documentation is subject to change without notice.

Information and descriptions contained herein are the property of Silex. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Silex. This publication is subject to change without notice.

The software embedded in this SX-6K3-EVK includes the Linux operating system. Linux and certain other software programs used in the SX-6K3-EVK are licensed under GNU GPL compatible Free Software Licenses. In compliance with these licenses, you can obtain the relevant source code at no charge by contacting Silex at support@silexamerica.com.

Silex Technology America, Inc.
www.silexamerica.com

Table of Contents

Figures

Tables

1 Document Conventions

The following section describes the conventions used within the document to identify and highlight the different applications of displayed text and provide value contextual information related to a section or paragraph.

Note that any identified context provided in proximity to any text overrides the conventions listed below.

1.1 Text Conventions

Bold Bold type within paragraph text indicates commands, file names, directory names, paths, output, or returned values.

italic Within commands, italics indicate a variable that the user must specify.

`Courier` The Courier font indicates output or display.
Example: `Error:Unable to allocate memory for transfer!`

[ ] Within commands, items enclosed in square brackets are optional parameters or values that the user can choose to specify or omit.

{ } Within commands, items enclosed in braces are options from which the user must choose.

| Within commands, the vertical bar separates options.

… An ellipsis indicates a repetition of the preceding parameter.

> The right angle bracket separates successive menu selections.
Example: Applications > Accessories > Terminal

1.2 Notes

A note contains information that requires special attention or provides specific information relating to the section or paragraph displayed above it. The following highlighted icon will be used. The area next to the icon will identify the specific information and make any references necessary.

This is a note section that contains supplemental information required to fully understand the contents of the inline text.
Additionally it will grow with the size of the contents.

1.3 Caution

A caution contains information that, if not followed, may cause permanent damage to the product, render the product inoperable or cause injury to the user. The following highlighted icon will be used. The area next to the icon will identify the specific information and make any references necessary.

All cautions MUST be read and understood.

This is a caution section that contains supplemental information required to fully understand the contents of the in-line text.

Additionally it will grow with the size of the contents.

2 Product Overview

This manual covers the SX-6K3-EVK-SD Wireless LAN evaluation kit for the Freescale Sabre Smart Devices (Sabre-SD) evaluation kit. The SX-6K3-EVK-SD is intended to provide a platform with which to evaluate the SX-SDMAN (dual-band) Wireless Module in conjunction with the i.MX6 processor. The evaluation platform includes a sample radio driver, supplicant and tools to test the following:

- Basic Wireless functionality
- Advanced Wi-Fi Security
- Data Throughput

Please contact your Silex sales representative to learn more about Silex Technology America, Inc. Embedded Wireless LAN solutions, including hardware options, production radio drivers with 802.1X authentication along with development and support services.

3 Contents of EVK

The following items should be present in the Evaluation Kit Box:

1. SX-SDCAN radio card.
2. SD Card with Silex Linux image and wireless utilities.
3. Quick Start Guide.

If any of the above items are missing please contact Silex Technology America technical support immediately:

Tel (US):	866.765.8761
Tel (International):	+1.801.748.1199
e.mail:	support@silexamerica.com

4 Installing the SX-6K3-EVK-SD

Before you can install the Silex SX-6K3-EVK-SD you must have purchased a Freescale Sabre-SD (Smart Devices) evaluation board from Freescale or one of their authorized distributors.

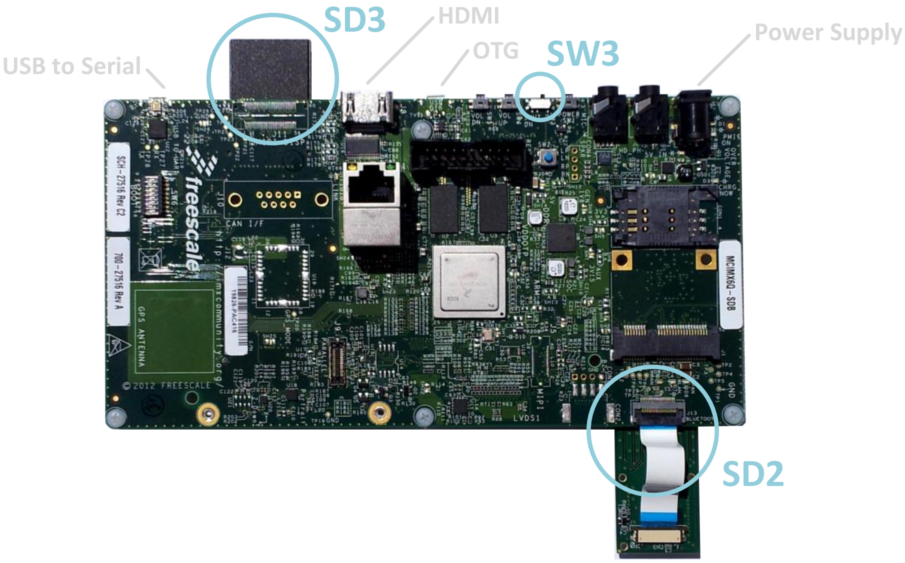
> The Sabre Smart Devices (Sabre-SD) EVK part number referenced in this Users Guide is **MCIMX6Q-SDB.**

The following steps assume you have already successfully verified the operation of the Sabre-SD EVK using the default Freescale SD card with the OS image that is shipped with it.

To install the Silex 6K3 EVK, perform the following steps:

1) Turn off the Sabre-SD EVK card using SW3.
2) Disconnect the power supply from the Sabre-SD card.
3) Go to SD3 (J507) and remove the SD Card containing the Freescale supplied OS image.
4) Go to the SX-6K3-EVK-SD and remove the Silex supplied SD card.
5) Insert the Silex SD card into SD3 card slot. This is the same location you just removed the Freescale SD card from (See Figure 1 for the location).
6) Go to the SX-6K3-EVK-SD and remove the SX-SDCAN.
7) Insert the SX-SDCAN card into SD2 (J500) SD card slot. This is located at the same end of the EVK card as the power supply connector but on the opposite side of the card (See Figure 1 for the location).
8) Insert the power supply.
9) Power up the Sabre-SD card using SW3.

Figure 1 - Sabre-SD Card Layout



Once the card has been powered up, the boot sequence will start. If you have connected the serial-to-USB console port to a PC or laptop you will see the boot sequence in the console port output. During the boot sequence the LED indicators on the Sabre-SD may change state. This is expected.

When the boot sequence is complete the Ubuntu v11.10 splash will be displayed and you will be logged into the Ubuntu desktop (user **Linaro**). The following sections will cover shutting down the Sabre-SD board as well as configuring the WLAN interface using the Gnome GUI and console interfaces.

5 Shutting down the i.MX6 Sabre-SD

The i.MX6 Sabre-SD EVK board should be shut down from the GUI or console interfaces before power is removed.

DO NOT REMOVE POWER WITHOUT SHUTTING DOWN THE OS!

Removing power from the EVK without properly shutting down the operating system could result in the OS being unable to correctly boot due to corrupt system files.

To shut down the Ubuntu OS (Linux):

1) Click on the Power button on the top right side of the Gnome Desktop.
2) Select Shut Down.
3) Wait until the desktop has shut down and the LED’s near the power button on the Sabre-SD EVK have turned off.

6 Configuring WLAN using Ubuntu GUI

The following section will cover how to configure the WLAN interface using the Ubuntu graphical user interface. This is the default configuration interface for the EVK and provides the simplest way of successfully connecting and testing the Silex SX-6K3-SDK-SD hardware and software.

To configure the interface using the command line interface, please refer to section 8.

6.1 General Wireless Network Setup

The WLAN Linux driver that is included in the SX-6K3-EVK-SD will load automatically if the steps described in section 4 have been completed successfully. This section will explain the methods used to configure the SD card to communicate on your wireless network. This section cannot be attempted until section 4 has been successfully completed.

The Silex SX-6K3-EVK-SD will automatically boot into Ubuntu 11.10 using Gnome Desktop. The following procedure describes how to locate, select and configure the interface using the Gnome Desktop.

IP address, network mask and WLAN network settings in the examples below are for demonstration purposes only. Use the IP address, network mask and WLAN network settings that are appropriate for your network environment.

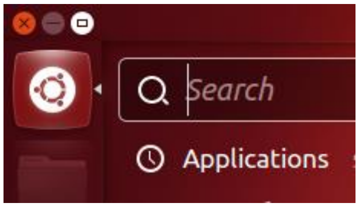
To configure the WLAN interface using the **Network Connections** manager follow these steps:

1) Prior to configuring the interface you will need to either set-up a test wireless network or know which available wireless network you want to connect the EVK to. In either case you will need to know the following information prior to attempting to connect:

   a) Network SSID.
   b) Security configuration and appropriate credentials. The credentials will vary depending upon the security being used by the WLAN e.g. If you are using WPA or WPA2 you will need to know the passphrase.

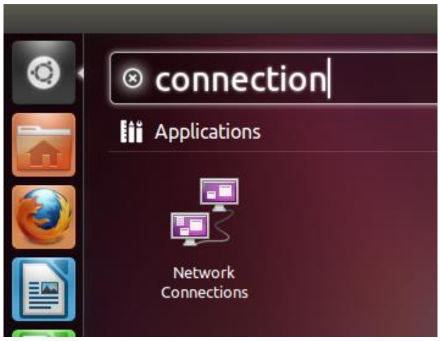
2) To open the **Network Connections** manager, click the **Dash home** button (Figure 2).

Figure 2 - Dash Home Button



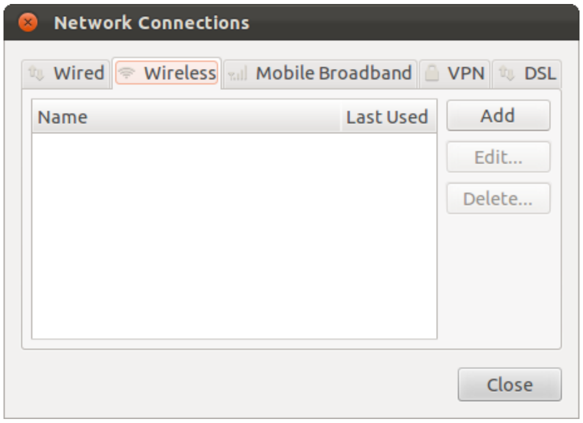
3) Enter *connection* in the search field. This will display the **Network Connections** in the **Applications** section.

Figure 3 - Dash - Connection Search



4) Click the **Network Connections** application.
5) Once the **Network Connections** manager opens, click on the **Wireless** tab (Figure 4).
6) To add your network click on the **Add** button (Figure 4).

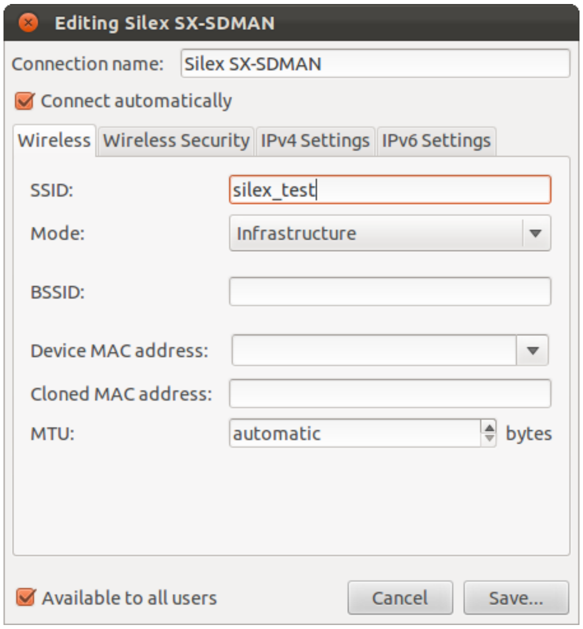
Figure 4 - Ubuntu Network Connections Wireless Tab



7) In the Dialog box that appears, enter the following information:

   a) **Connection name:** Enter the name that you want this network connection to appear as in the Network Connection Manager e.g. *Test Network*. This is not the SSID, unless you wish to use it as the identifier in the list of configured networks.
   b) **Connect Automatically**: Select this option to connect to this Access Point automatically when booting into Gnome.
   c) **SSID**: Enter the SSID of the Access Point that you want to connect to.
   d) **Infrastructure/Ad-hoc:** Select infrastructure to connect to an Access point on your Network. Select Ad-hoc to make a peer-to-peer connection to another wireless device in Ad-hoc mode (typically a PC or Laptop). AdHoc network configuration is not covered in this manual.
   e) **BSSID:** Do not enter anything into this field.
   f) **MAC address:** Do not enter anything into this field.
   g) **MTU:** Leave as default (Automatic).

Figure 5 - WLAN Network Configuration Wireless Tab



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

SSID: silex_test

Mode: Infrastructure

BSSID:

Device MAC address:

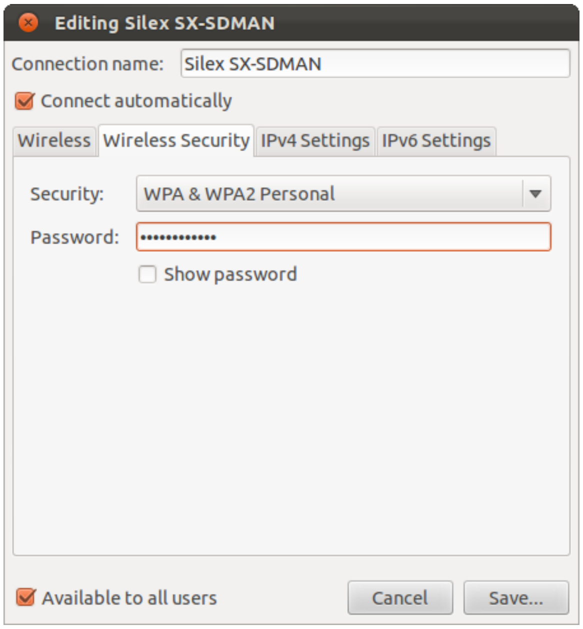
Cloned MAC address:

MTU: automatic bytes

☑ Available to all users

8) Next, click on the **Wireless Security** tab. Set security to none for an unencrypted connection or choose the appropriate security option to match your network and complete the credentials listed. Details of the security requirements will be covered in later sections.

Figure 6 - WLAN Network Configuration Security Tab



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

Security: WPA & WPA2 Personal

Password: ••••••••••••

□ Show password

☑ Available to all users

9) Click **Save...**

Once you click Apply the Connection Settings will be saved. If you have selected to automatically connect and the network is within range of the EVK within a short period of time the EVK will connect the network without any additional input.

If you selected to not automatically connect and the network is within range you will need to double click the network connection name in the **Network Connections** window to connect to the network.

6.2 WPA & WPA2 Personal (PSK) Security Setup

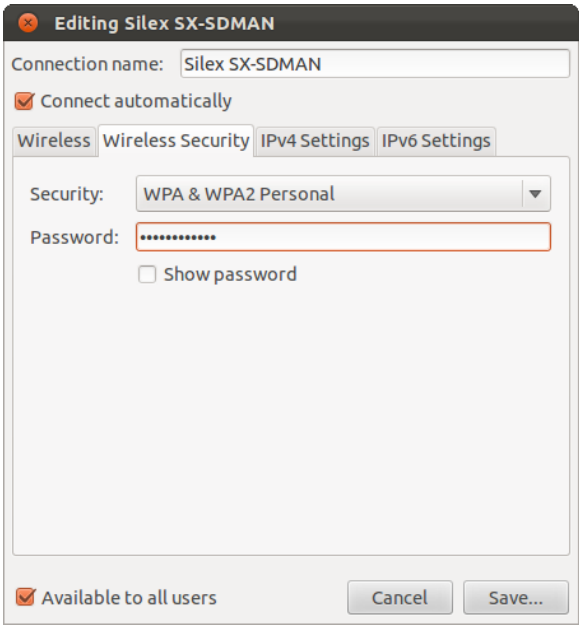
WPA and WPA2 with a pre-shared key (passphrase) are the most common basic security configuration used by WLAN networks. The driver is able to determine whether WPA or WPA 2 is being used for the wireless encryption.

> Passphrase, Pre-Shared Key and Password all relate to the same piece of information and are considered interchangeable when referring to the secret used to authenticate to a WLAN network using WPA/WPA2-PSK.

To setup WPA or WPA2 Personal (Pre-Shared Keys) follow these steps:

1) Open the network Connection Edit window System > Preferences > Network Connections>Edit
2) Select the network configuration you wish to edit.
3) Select the Wireless Security tab.
4) Under the **Security** parameter set the Security type to **WPA & WPA2 Personal**
5) In the **Password** field enter your Pre-Shared Key.
6) You can check the Pre-Shared key by selecting the **Show Password** box.
7) Click **Save...**

Figure 7 - WLAN Network Configuration WPA/WPA2 Setup



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

Security: WPA & WPA2 Personal

Password: ••••••••••••

□ Show password

☑ Available to all users

6.3 WPA & WPA2 Enterprise Security Setup

A more advanced security type is called Enterprise security; this is often used to secure large corporate networks and requires a higher level of authentication than the more common WPA/WPA2 pre-shared key type. There are several methods of Enterprise security; the following types are supported by the Gnome Network Manager:

- TLS
- LEAP
- Tunneled TLS (TTLS)
- Protected EAP (PEAP)

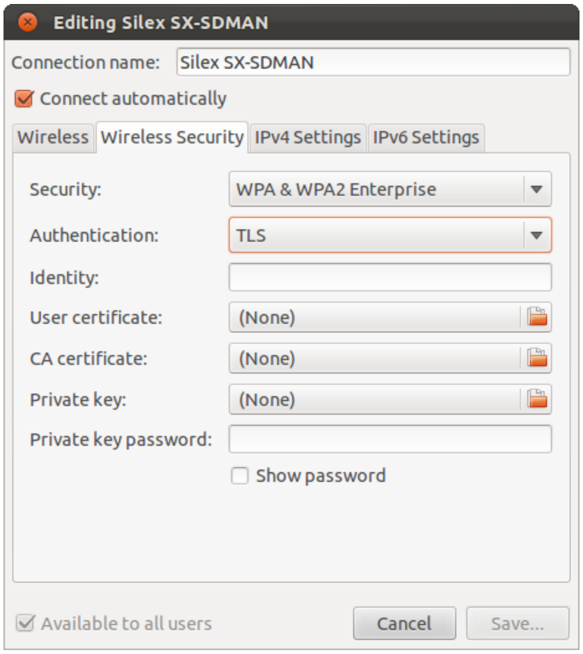
The following section will cover how to configure these types of security using the network manager and the Silex SX-6K3-EVK-SD.

> Due to the potential security risk an unauthorized network connection creates, it is recommended that before placing the Sabre-SD and SX-6K3-EVK-SD on a corporate network, approval from the IT administrator of the network should be obtained.

Prior to attempting to place the Sabre-SD and SX-6K3-EVK-SD on your corporate network it will be necessary to obtain the appropriate credentials for the network. These should be obtained from the network administrator prior to attempting to connect. In addition to the credentials you will need to know the Security or EAP type and settings for each. Check the following sections to confirm what is required.

1) Open the network Connection Edit window **System > Preferences > Network Connections>Edit**
2) Select the network configuration you wish to edit.
3) Select the **Wireless Security** tab.
4) Under the **Security** parameter set the Security type to **WPA & WPA2 Enterprise**.
5) Setting up TLS Authentication:
    a) Select **TLS** for the Authentication type
    b) Enter the Identity associated with your Radius server. This is the user name provided by the network administrator.
    c) Enter the User and CA certificate names or click on the folder and browse to their location and select. These are files provided by the network administrator. The certificates must be downloaded to the EVK before they can be selected.
    d) Enter the Private Key name or click on the folder and browse to their location and select. This is a file provided by the network administrator. The private key must be downloaded to the EVK before it can be selected.
    e) Select the **Private key password** and enter it. This should be provided by the network administrator.
    f) Click **Save...**

Figure 8 - Configuring TLS using GUI



Connection name: Silex SX-SDMAN

☑ Connect automatically

Security: WPA & WPA2 Enterprise

Authentication: TLS

Identity:

User certificate: (None)

CA certificate: (None)

Private key: (None)

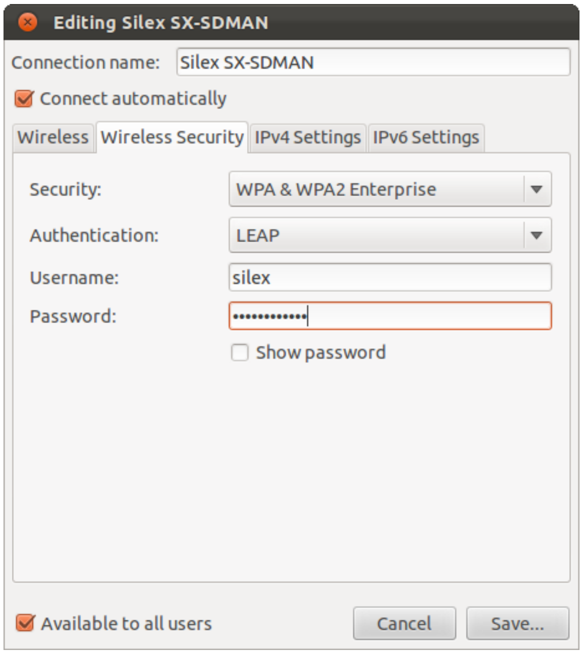
Private key password:

□ Show password

☑ Available to all users

6) Setting up LEAP Security:
   a) Select **LEAP** for the Authentication type.
   b) Enter the **Username**.
   c) Enter the **Password**.
   d) Click **Save...**

Figure 9 - Configuring LEAP using GUI



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

Security: WPA & WPA2 Enterprise

Authentication: LEAP

Username: silex

Password: ••••••••••••

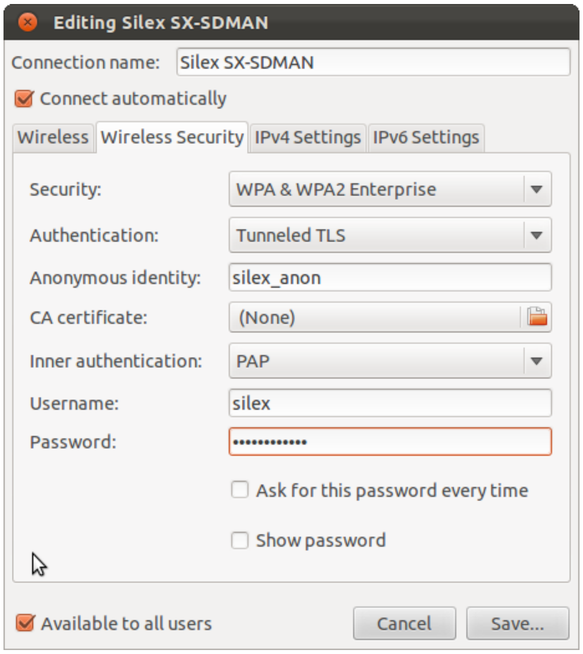
□ Show password

☑ Available to all users

LEAP is a depreciated network security type and will compromise the integrity of the network if used. Long term support for this security type is not guaranteed.

7) Setting up Tunneled TLS (TTLS) Security:
   a) Select **Tunneled TLS** for the Authentication type.
   b) Enter the **Anonymous Identity**. This parameter is optional if it is not provided by the network administrator leave blank.
   c) Enter the **CA certificate** name or click on the folder and browse to its location and select. This is a file provided by the network administrator. The certificates must be downloaded to the EVK before they can be selected. This is optional for some implementations of TTLS.
   d) Select the **Inner Authentication** type. This will be defined by the network administrator.
   e) Enter your **Username**
   f) Enter the **Password**.
   g) Click **Save...**

Figure 10 - Configuring TTLS using GUI



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

Security: WPA & WPA2 Enterprise

Authentication: Tunneled TLS

Anonymous identity: silex_anon

CA certificate: (None)

Inner authentication: PAP

Username: silex

Password: ••••••••••••

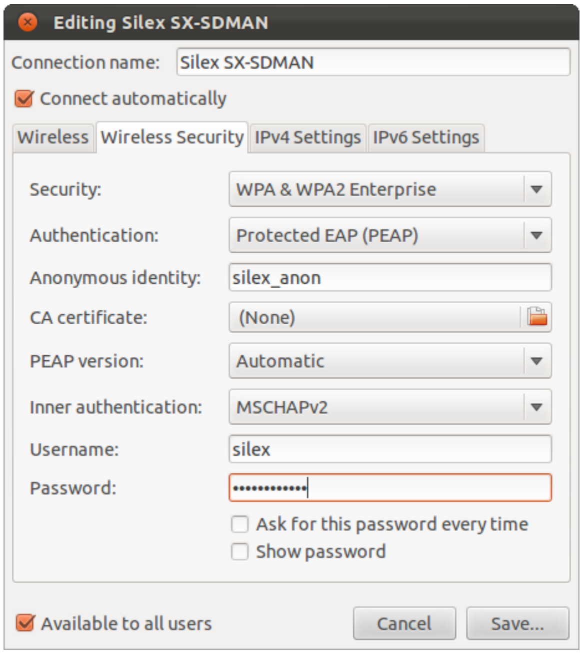
□ Ask for this password every time

□ Show password

☑ Available to all users

8) Setting up PEAP Authentication
   a) Select **Protected EAP (PEAP)** for the Authentication type.
   b) Enter the **Anonymous Identity**. This parameter is optional if it is not provided by the network administrator leave blank.
   c) Enter the **CA certificate** name or click on the folder and browse to its location and select. This is a file provided by the network administrator. The certificates must be downloaded to the EVK before they can be selected. This is optional for some implementations of PEAP.
   d) Enter the **PEAP version**. It is recommended you leave it as the default automatic, unless the network administrator has identified the specific version being used.
   e) Select the **Inner Authentication** type. This will be provided by the network administrator.
   f) Enter the **Username**.
   g) Enter the **Password**.
   h) Click **Save...**

Figure 11 - Configuring PEAP using GUI



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

Security: WPA & WPA2 Enterprise

Authentication: Protected EAP (PEAP)

Anonymous identity: silex_anon

CA certificate: (None)

PEAP version: Automatic

Inner authentication: MSCHAPv2

Username: silex

Password: ••••••••••••

□ Ask for this password every time

□ Show password

☑ Available to all users

Some implementations of PEAP do not require the use of a CA certificate. This is a compromised implementation and reduces the integrity of the network. It is not recommended.

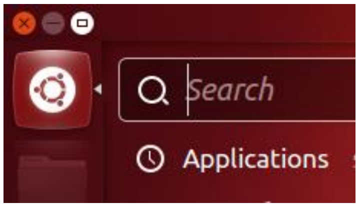
6.4 TCP/IP Setup

Once the WLAN interface has authenticated to a network it will be necessary for the interface to have an IP address if network communications are to follow. The EVK supports both automatic assigning (DHCP) and static assigning of an IP address. The following section covers how to configure each of these.

To configure the interface for automatic assignment (DHCP) of an IP address, follow these steps:

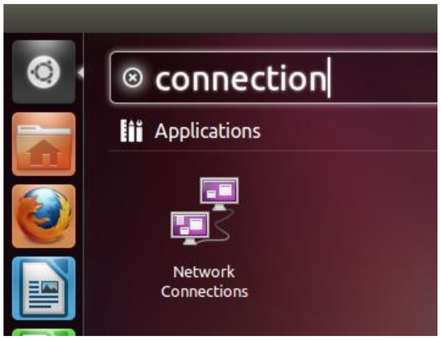
1) To open the **Network Connections** manager, click the **Dash home** button (Figure 12).

Figure 12 - Dash Home Button



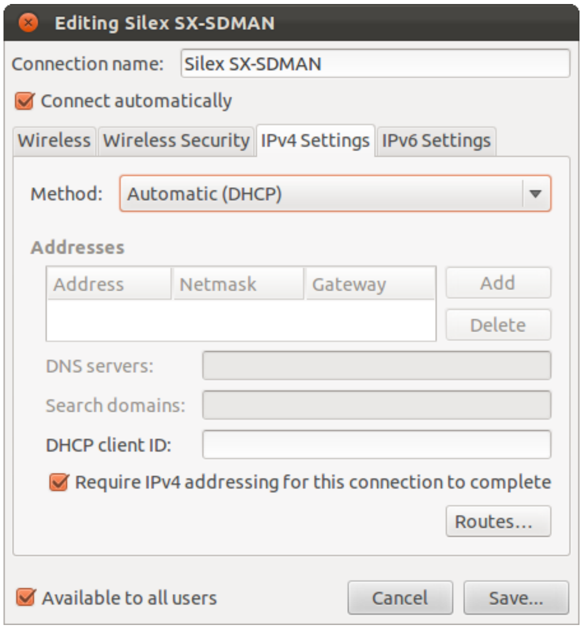
2) Enter *connection* in the search field. This will display the **Network Connections** in the **Applications** section.

Figure 13 - Dash - Connection Search



3) Click the **Network Connections** application.
4) Click on the **Wireless** tab.
5) If you wish to change an existing configuration, select the network configuration you wish to edit and click the **Edit** button.
6) If you wish to create a new network configuration click the **Add** button.
7) The edit connection window will open.

Figure 14 - WLAN Network Configuration IPv4 Tab - DHCP



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

Wireless | Wireless Security | IPv4 Settings | IPv6 Settings

Method: Automatic (DHCP)

Addresses

Address	Netmask	Gateway

Add
Delete

DNS servers:

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

Routes...

☑ Available to all users

Cancel Save...

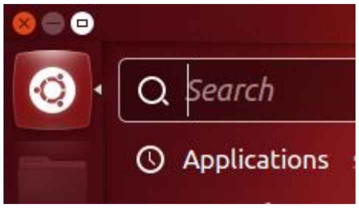
8) Select the **IPV4 Settings** tab.
9) Select the **Method** dropdown box and choose **Automatic (DHCP)**.
10) Click **Save...**

For DHCP to work it is necessary to have a DHCP server on the network.
Most Wireless Routers include a DHCP server by default. Check with your network administrator to confirm your corporate network uses DHCP.

To configure the interface for static assignment of an IP address, follow these steps:

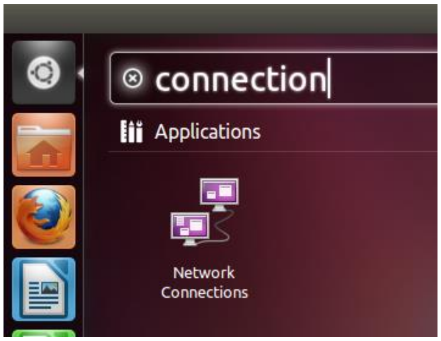
1) To open the **Network Connections** manager, click the **Dash home** button (Figure 15).

Figure 15 - Dash Home Button



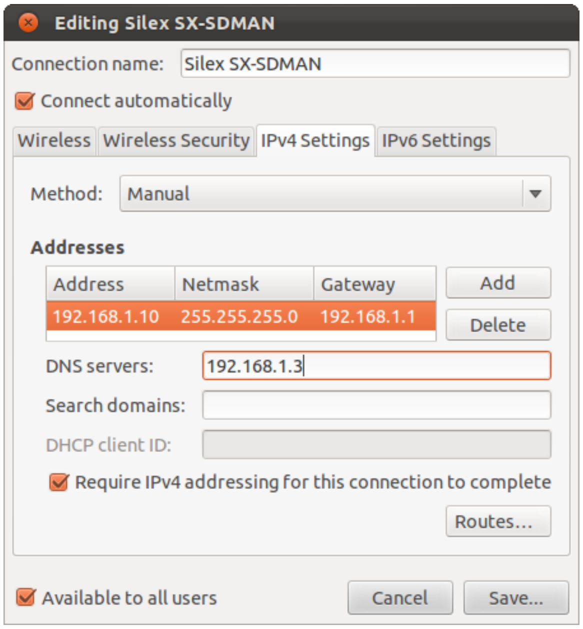
2) Enter *connection* in the search field. This will display the **Network Connections** in the **Applications** section.

Figure 16 - Dash - Connection Search



3) Click the **Network Connections** application.
4) Click on the **Wireless** tab.
5) If you wish to change an existing configuration, select the network configuration you wish to edit and click the **Edit** button.
6) If you wish to create a new network configuration click the **Add** button.
7) The edit connection window will open.

Figure 17 - WLAN Network Configuration IPv4 Tab - Static IP



Editing Silex SX-SDMAN

Connection name: Silex SX-SDMAN

☑ Connect automatically

Wireless | Wireless Security | IPv4 Settings | IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.10	255.255.255.0	192.168.1.1

DNS servers: 192.168.1.3

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

☑ Available to all users

8) Select the **IPV4 Settings** tab.
9) Select the **Method** dropdown box and choose **Manual**.
10) Click the **Add** button.
11) To configure the IP settings.
    a) In the **Address** field enter the Static IP address you want to assign. This must be a unique IP address within the subnet of the network the device is connected to.
    b) In the **Netmask** field enter your network mask.
    c) In the **Gateway** field enter your default gateway (only require when communicating between different subnets or the internet).
    d) In the **DNS servers** field enter your networks DNS server IP address (required to communicate using names/URL rather than IP Addresses).
12) Check the **Available to all users** box.
13) Click **Save...**

7 Configuring Ethernet using Ubuntu GUI

7.1 Wired Network Connection Manager

The Sabre-SD and SX-6K3-EVK-SD support networking using the Ethernet connection on the Sabre-SD card. To use the Ethernet interface first plug a network connection into the RJ45 socket (J7) on the Sabre-SD card.

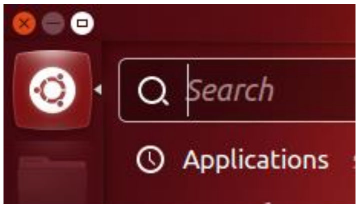
By default, the Ethernet connection is set to obtain an IP address via DHCP. To support DHCP the network you have connected the Sabre-SD card to must have a DHCP server available.

> Due to the potential security risk an unauthorized network connection creates, it is recommended that before placing the Sabre-SD and SX-6K3-EVK-SD on a corporate network, approval from the IT administrator of the network should be obtained.

To configure the interface for DHCP (Dynamic) assignment of an IP address, follow these steps:

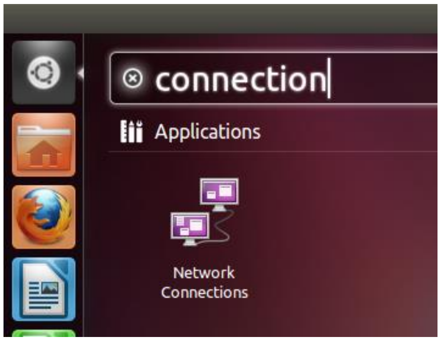
1) To open the **Network Connections** manager, click the **Dash home** button (Figure 18).

Figure 18 - Dash Home Button



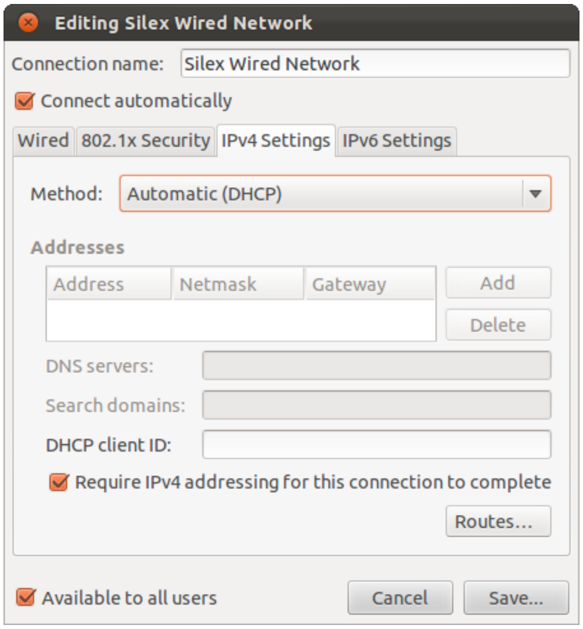
2) Enter *connection* in the search field. This will display the **Network Connections** in the **Applications** section.

Figure 19 - Dash - Connection Search



3) Click the **Network Connections** application.
4) Click on the **Wired** tab.
5) If you wish to change an existing configuration, select the network configuration you wish to edit and click the **Edit** button.
6) If you wish to create a new network configuration click the **Add** button.
7) The edit connection window will open.

Figure 20 - Ethernet Network Configuration IPv4 Tab - DHCP



Editing Silex Wired Network

Connection name: Silex Wired Network

☑ Connect automatically

Wired | 802.1x Security | IPv4 Settings | IPv6 Settings

Method: Automatic (DHCP)

Addresses

Address	Netmask	Gateway

Add

Delete

DNS servers:

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

Routes…

☑ Available to all users

Cancel

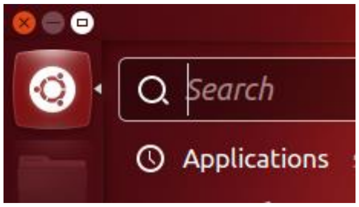
Save...

8) Select the **IPV4 Settings** tab.
9) Select the **Method** dropdown box and choose **Automatic (DHCP)** option (default).
10) Check the Available to all users box.
11) Click **Save...**

To configure the interface for static assignment of an IP address, follow these steps:

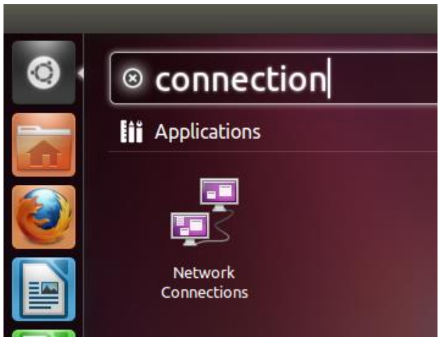
1) To open the **Network Connections** manager, click the **Dash home** button (Figure 21).

Figure 21 - Dash Home Button



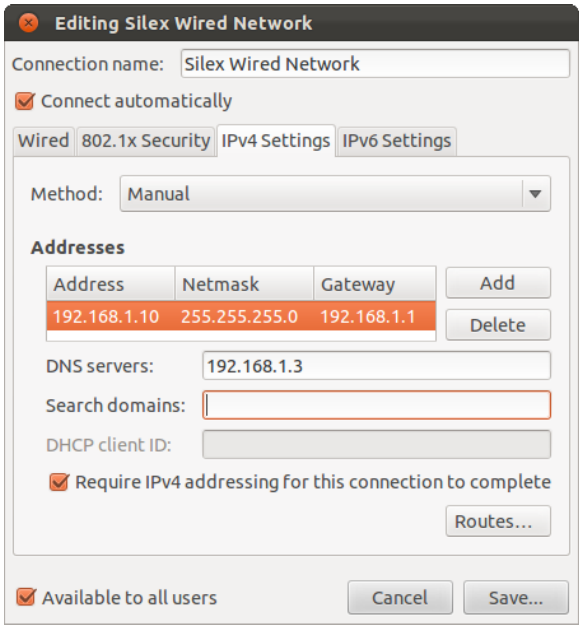
2) Enter *connection* in the search field. This will display the **Network Connections** in the **Applications** section.

Figure 22 - Dash - Connection Search



3) Click the **Network Connections** application.
4) Click on the **Wired** tab.
5) If you wish to change an existing configuration, select the network configuration you wish to edit and click the **Edit** button.
6) If you wish to create a new network configuration click the **Add** button.
7) The edit connection window will open.

Figure 23 - Ethernet Network Configuration IPv4 Tab - Static IP


Editing Silex Wired Network

Connection name: Silex Wired Network

☑ Connect automatically

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.10	255.255.255.0	192.168.1.1

DNS servers: 192.168.1.3

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

☑ Available to all users

8) Select the **IPV4 Settings** tab.
9) Select the **Method** dropdown box and choose **Manual**.
10) Click the **Add** button.
11) To configure the IP settings.
    a) In the **Address** field enter the Static IP address you want to assign. This must be a unique IP address within the subnet of the network the device is connected to.
    b) In the **Netmask** field enter your network mask.
    c) In the **Gateway** field enter your default gateway (only require when communicating between different subnets or the internet).
    d) In the **DNS servers** field enter your networks DNS server IP address (required to communicate using names/URL rather than IP Addresses).
12) Check the Available to all users box.
13) Click **Save...**

8 Command Line Setup

The S6K3-EVK-SD supports command line control through the Linux console. Access to the Linux console can be found through the USB-Serial interface provided on the Sabre-SD card. Additionally it is necessary to have a telnet/terminal emulator application. With the Command Line interface it is possible to configure, enquire and interrogate the network interfaces on the Sabre-SD EVK directly.

The following section will cover how to establish the Linux console connection, provide common console commands and actions for the WLAN device, all supported by the Sx-6K3-EVK-SD form Silex.

8.1 Connecting the USB-Serial Interface

This interface is provided as part of the Sabre-SD card and is used for general Linux console access. It requires that the Sabre-SD card by connected to a target laptop or desktop via a USB-Micro-B to USB-A connector cable, provided by Freescale.

If you have not already connected this interface the following will describe the steps necessary:

1) Turn off the Sabre-SD EVK card using SW3.
2) Connect the micro-B end of the cable into the debug port (J509) on the Sabre-SD card.
3) Plug the other end into the PC to be used as the terminal.
4) Turn on the Sabre-SD EVK using SW3.

8.2 Loading USB-Serial Driver

The PC connected to the Sabre debug port must load a driver to interact with the interface and create a virtual COM port on the debug PC. This should happen automatically when the Sabre-SD board is first powered up.

When the install is complete a COM port number will be assigned to the Sabre0SD card. You will need to know this when using the terminal emulator application.

If needed, the Serial-to USB drivers can be found at
www.ftdichip.com/FTDrivers.htm

8.3 Opening a Linux Console Session

Open the terminal emulator of choice and enter the following:

Type:	**Serial interface**
COM Port:	**<assigned when the virtual COM port driver was installed>**
Configuration:	**115.2K BAUD, 8 data bits, 1 stop bit, no parity**

When the session is opened the Ubuntu Linux prompt will be displayed.

There are a number of available terminal emulators. The following list is not comprehensive but provides guidance on the type of application required a list of available emulators can be found here.

The following two are widely used and are known to function correctly with the Sabre-SD debug port:

PuTTY	www.putty.org
TeraTerm	ttssh2.sourceforge.jp/index.html.en

8.4 Temporary Wireless Network Setup

There is more than one way to configure a network connection from the command line. The method described below uses the commands ifconfig, iw, iwconfig and dhclient. The applications are built into the SX-6K3-EVK-SD image.

PLEASE NOTE THAT USING THESE COMMAND LINE UTILITIES DOES NOT CREATE A PERMANENT CONFIGURATION. ANY CONFIGURATION INFORMATION WILL BE LOST AFTER RESTARTING THE OPERATING SYSTEM.

A method for creating a permanent configuration is described below in section 9.

8.5 Logging into the Linux Console

There is no requirement to log into the Linux console after the OS has successfully booted. However to log in as root, once a terminal session is opened, type the following:

```
sudo su
```

8.6 Stopping the Gnome Network Manager

To allow network configuration from the command line the Gnome Network Manager must first be disabled. To temporarily disable the Network Manager enter the following command from the terminal prompt:

```
stop network-manager
```

8.7 Starting Gnome Network Manager

If you have stopped the Gnome Network Manager and need to re-start it to allow you to configure your network from the Gnome Desktop, run the following command from the terminal prompt.

```
start network-manager
```

8.8 Making the WLAN Interface Available

By default after the network manager has been stopped the WLAN interface will be disabled. To enable the WLAN issue the following command:

```
ifconfig wlan0 up
```

8.9 List Available Network Interfaces

The first thing you should confirm is that the WLAN interface driver has loaded and the interface is available. To see the available network interfaces enter:

```
ifconfig –a
```

Sample output:

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1020 (1.0 KB)  TX bytes:1020 (1.0 KB)

wlan0     Link encap:Ethernet  HWaddr 00:80:92:4d:e5:42
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5262 errors:0 dropped:1 overruns:0 frame:0
          TX packets:1638 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6636802 (6.6 MB)  TX bytes:72608 (72.6 KB)
```

The listed **wlan0** interface indicates the Silex SX-SDCAN WLAN device driver has been loaded and the network interface is available for configuration.

8.10 Check Current Connection Status

To check the current connection status of the WLAN interface, enter the following command:

```
iw dev wlan0 link
```

Sample Output:

```
Connected to 08:86:3b:28:90:1c (on wlan0)
        SSID: Silex_Test_G
        freq: 2462
        RX: 4329333 bytes (19234 packets)
        TX: 463343 bytes (7356 packets)
        signal: -22 dBm
        tx bitrate: 40.5 MBit/s MCS 2 40MHz

        bss flags:
        dtim period:    1
        beacon int:     100
```

If the interface is not associated to a network, the interface will indicate that no connection has been established.

Alternately you can use the depreciated command:

```
iwconfig
```

Sample Output:

```
wlan0     IEEE 802.11abgn  ESSID:"Silex_Test_G"
          Mode:Managed  Frequency:2.462 GHz  Access Point:
08:86:3B:28:90:1C
          Bit Rate=40.5 Mb/s   Tx-Power=13 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-20 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

8.11 Scanning for WLAN Networks

Once the WLAN network interface is available looking for available networks can provide feedback on the RF environment and provide confirmation your target network can be seen by the SX-6K3-EVK-SD. The scan has many options that allow control of the scanning function in order to limit the frequencies scanned, active or passive scanning and scanning for specific SSID's.

To scan for available networks on all channels issue the following command:

```
iw dev wlan0 scan
```

Sample output:

```
BSS 08:86:3b:28:90:1c (on wlan0) -- associated
        TSF: 826785183 usec (0d, 00:13:46)
        freq: 2462
        beacon interval: 100
        capability: ESS ShortSlotTime (0x0401)
        signal: -16.00 dBm
        last seen: 210 ms ago
        Information elements from Probe Response frame:
        SSID: Silex_Test_G
        Supported rates: 1.0* 2.0* 5.5* 11.0* 9.0 18.0 36.0 54.0
        DS Parameter set: channel 11
        ERP: Barker_Preamble_Mode
        Extended supported rates: 6.0 12.0 24.0 48.0
        HT capabilities:
                Capabilities: 0x6c
                        HT20
                        SM Power Save disabled
                        RX HT20 SGI
                        RX HT40 SGI
                        No RX STBC
                        Max AMSDU length: 3839 bytes
                        No DSSS/CCK HT40
                Maximum RX AMPDU length 65535 bytes (exponent: 0x003)
                Minimum RX AMPDU time spacing: 4 usec (0x05)
                HT RX MCS rate indexes supported: 0-15
                HT TX MCS rate indexes are undefined
        HT operation:
                 * primary channel: 11
                 * secondary channel offset: no secondary
                 * STA channel width: 20 MHz
                 * RIFS: 0
                 * HT protection: nonmember
                 * non-GF present: 1
                 * OBSS non-GF present: 0
                 * dual beacon: 0
                 * dual CTS protection: 0
                 * STBC beacon: 0
                 * L-SIG TXOP Prot: 0
                 * PCO active: 0
                 * PCO phase: 0
        Secondary Channel Offset: no secondary (0)
        WMM:     * Parameter version 1
                 * BE: CW 15-1023, AIFSN 3
                 * BK: CW 15-1023, AIFSN 7
                 * VI: CW 7-15, AIFSN 2, TXOP 3008 usec
                 * VO: CW 3-7, AIFSN 2, TXOP 1504 usec
        BSS Load:
                 * station count: 1
                 * channel utilisation: 145/255
                 * available admission capacity: 31250 [*32us]
        Extended capabilities: HT Information Exchange Supported
        Country: TW     Environment: bogus
                Channels [1 - 11] @ 16 dBm
        WPS:     * Version: 1.0
                 * Wi-Fi Protected Setup State: 2 (Configured)
                 * Response Type: 3 (AP)
                 * UUID: bc329e00-1dd8-11b2-8601-08863b28901c
                 * Manufacturer: Belkin International
                 * Model: Belkin N750DB Wireless Router
                 * Model Number: F9K1103 v1
                 * Serial Number: 121119GG106784
                 * Primary Device Type: 6-0050f204-1
                 * Device name: Belkin N750DB Wireless Router
                 * Config methods: Label, PBC
                 * RF Bands: 0x1
```

8.12 Connecting to an Access Point (No security)

The easiest way to get connected and learn how to use the command line interface is to initially connect to an open Access Point (AP). This is an AP with no security enabled. Later in the section we will cover connecting to AP's with network security enabled.

To connect to an AP enter the following command. You will need to know the SSID or network name you wish to connect to:

```
iw dev wlan0 connect <Network SSID>
```

After issuing the above command, you can confirm the Sabre-SD has associated to the AP by repeating the command in section 8.10.

8.13 Connecting to/Creating an AdHoc Network

The SX-6K3-EVK supports peer-to-peer WLAN connectivity. This can be established using the AdHoc network configuration. To put the SX-6K3-EVK-SD in to AdHoc mode to either establish or join and existing AdHoc network the following commands are an example of you can connect to an AdHoc network:

```
ifconfig wlan0 down
ifconfig wlan0 set type ibss
ifconfig wlan0 up
iw dev wlan0 ibss join <Network SSID> 2437 HT20
```

The above configuration starts an AdHoc network on channel 6 in the 2.4GHz ISM band and enables 11n channel 6.

> Since AdHoc networks do not typically support DHCP servers it is necessary to assign a static IP address to the Sabre-SD WLAN interface, when using an AdHoc network. See section 8.15 to understand how to do configure the interface to use a static IP address.

8.14 Configuring DHCP

Setting up the WLAN interface to obtain an IP address dynamically requires the following command:

```
dhclient wlan0
```

To determine if the WLAN interface has successfully obtained an IP address, refer to section 8.8. If an IP address has been leased to the interface it will be displayed in the returned results for the WLAN interface.

8.15 Configuring a Static IP Address

If the target network does not support DHCP or you are using an AdHoc network it may necessary to assign a static IP configuration to the WLAN interface. As a minimum an IP address and subnet mask must be configured, additional settings like a gateway address and DNS server addresses are optional.

To configure a static IP address use the following command:

```
ifconfig wlan0 <IP Address> netmask <network mask>
e.g. ifconfig wlan0 192.168.10.120 netmask 255.255.255.0
```

To configure a gateway IP address use the following command:

```
ip route add default via <gateway IP>
e.g. ip route add default via 192.168.10.1
```

A gateway IP address is required if access to devices on a different subnet to the one the Sabre-SD EVK is connected, is required e.g. access to the internet.

To configure a DNS server IP address, use the following procedure:

1) Edit **resolv.conf** using the following command:

```
gedit /etc/resolv.conf
```

2) Add your name servers by entering the following information to the **resolv.conf** file:

```
nameserver {DNS_Server_1_IP_Address}
nameserver {DNS_Server_2_IP_Address}
```

3) Save your changes.

One or more DNS server addresses are required if URL’s are to be used to access network resources.

9 Persistent WLAN Configuration

To create a persistent configuration (one which survives power cycles) you must use the wpa_supplicant.conf file to store WLAN network profiles. The following sections provide guidelines and examples of supplicant configuration files.

Multiple supplicant configuration files may be created and stored on the device. The different files can be invoked when the WPA supplicant process is started. This will be covered in the section 9.2.

> If you intend to use the command line for configuration of the WLAN interface it is recommended the Gnome Network Manager be uninstalled. To uninstall the network manager issue the following command:
>
> **`apt-get uninstall network-manager`**

To use the WPA supplicant you must first establish a network configuration in an appropriately named file. Within the file each network configuration must be defined in a network block. A single configuration file may contain several network blocks, each containing a different network and network security setting. There is no naming convention but references to the security or networks stored in the file will help manage the supplicant configuration files.

The files are text based and must be stored in the file system. There is no set location for the storage of the configuration files. The full path and file name will be needed when the WPA supplicant is started.

To get started with establishing a persistent WLAN configuration copy one of the example files below and save it to the EVK. You can pick any location you wish but the example below is using the /etc/wpa_supplicant subdirectory.

9.1 Stopping the wpa_supplicant process

Before changing the WLAN configuration using WPA supplicant it is necessary to halt any existing wpa supplicant processes. This section assumes the network manager has been stopped (section 9).

To stop any existing wpa supplicant processes follow these steps:

1) Run the following command:

```
ps –A | grep wpa
```

2) The command will output the process information to allow the **wpa_supplicant** process to be stopped.

   Example output:

```
root@linaro-ubuntu-desktop:/etc/wpa_supplicant# ps -A |grep wpa
6747 ?        00:00:00 wpa_supplicant
```

3) The process ID is located to the left of the information that is displayed. In the above example, the process ID is **6747**.
4) To stop the wpa_supplicant process in the above example type the following command and hit enter (replace the example process ID with your EVK’s process ID when running the command):

```
kill 6747
```

An alternate and simpler way to kill the wpa_supplicant process is to issue the following command:

```
killall wpa_supplicant
```

Once the kill command is issued the WPA supplicant process will terminate and an updated process can be started. Repeating the command in step 1 will return no found processes if the process is killed.

9.2 Configuring WPA/WPA2-PSK using WPA Supplicant

If the target network is using security, it will most likely be a pre-shared key type using WPA or WPA2 encryption. The following covers how to configure the Sabre-SD EVK and SX-6K3-EVK-SD to use WPA-PSK or WPA2-PSK.

Configuration of the EVK requires editing the WPA supplicant configuration file. Prior to editing the file the network SSID, encryption type and pre-shared key must be known.

To configure the EVK for WPA or WPA2 security, follow these steps:

1) Change the current directory to the one that contains the **wpa_supplicant.conf** file:

```
cd //etc/wpa_supplicant/
```

> If no WPA supplicant configuration file exists you must create one. To do this follow step 1 and enter the name of the configuration file you want to use in step 2.

a) Edit the **wpa_supplicant.conf** file:

```
gedit wpa_suplicant.conf
```

> The WPA supplicant configuration file does not have to be named wpa_supplicant.conf.
>
> Providing a file name that suggests the contents of the file can be advantageous when maintenance and use of the files is required e.g. a configuration file holding the network blocks for the manufacturing plant could be named wpa_supplicant_manuf.conf.
>
> See section 11.2 for a description of the WPA configuration file structure/format.

2) To configure the EVK for use with a network using WPA-PSK:

a) Find the first line containing the following. This is the first network block and will be used as the network configuration example:

```
network={
```

b) Edit the lines in the block under the network line, shown in RED, with the details of your specific network configuration:

```
ssid="replace with your network name"
scan_ssid=1
proto=WPA  # for WPA-PSK
key_mgmt=WPA-PSK
pairwise=TKIP
group=TKIP
psk="replace with your passphrase"
```

3) To configure the EVK for use with a network using WPA2-PSK:
   a) Find the first line containing the following. This is the first network block and will be used as the network configuration example:

      ```
      network={
      ```

   b) Edit the lines in the block under the network line, shown in RED, with the details of your specific network configuration:

      ```
      ssid="replace with your network name"
      scan_ssid=1
      proto=RSN  # for WPA2-PSK
      key_mgmt=WPA-PSK
      pairwise=CCMP
      group=CCMP
      psk="replace with your passphrase"
      ```

4) Each network block must be terminated with a }.
5) Save the edited file to the chosen location **(/etc/wpa_supplicant/** in the example above).
6) We can now run the WPA supplicant with the modified configuration file. Enter the following command:

   ```
   wpa_supplicant -B -Dnl80211 -c/etc/wpa_supplicant/wpa_supplicant.conf  -i wlan0
   ```

7) If the WPA supplicant is successfully initialized the system will report back that the initialization was successful. Any other message will identify the errors in the configuration file. If initialization is unsuccessful read the debug message response and adjust the WPA supplicant configuration file accordingly.
8) Successful initialization of the WPA supplicant does not guarantee connection to the target network. For this both the configuration must be correct and the network must be in range. To confirm association to the target network issue the following command:

   ```
   iw wlan0 link
   ```

9) If the response is **Not connected.** Check the contents in the WPA configuration file, edit accordingly, save it and issue the following command:

   ```
   killall -HUP wpa_supplicant
   ```

10) This will apply the changes made to the WPA supplicant configuration file in step 8. The edited file must be the one initially called during step 5. Repeat steps 7 and 8 until you successfully associate and authenticate to the network.
11) Once connected you will need an IP address to communicate on the network, see sections 8.14 or 8.15 for the available options.

9.3 Configuring EAP-TLS

Configuring the WPA supplicant to use EAP-TLS is the same as WPA-PSK with the exception of the WPA supplicant network block contents. To configure the WLAN interface for EAP-TLS follow the steps in section 9.2, replacing the block contents in step 2c with the one listed below:

```
ssid="replace with your network name"
scan_ssid=1
key_mgmt=WPA-EAP
pairwise=CCMP TKIP
```

```
group=CCMP TKIP
eap=TLS
identity="user@example.com"
ca_cert="/etc/cert/ca.pem"
client_cert="/etc/cert/user.pem"
private_key="/etc/cert/user.prv"
private_key_passwd="replace with your private key password"
```

EAP-TLS requires the use of three certificates, the Certificate Authority (CA) certificate, the user certificate and the Private Key certificate. Prior to authentication you will need to source the certificates form the network administrator and load them on the Sabre-SD EVK. The certificates are required to complete authentication on the network.

Loading certificates will be covered in section 10 of the manual.

9.4 Configuring EAP-TTLS

Configuring the WPA supplicant to use EAP-TTLS is the same as WPA-PSK with the exception of the WPA supplicant network block contents. To configure the WLAN interface for EAP-TLS follow the steps in section 9.2, replacing the block contents in step 2c with the one listed below:

```
ssid="replace with your network name"
scan_ssid=1
key_mgmt=WPA-EAP
eap=TTLS
identity=user@example.com
anonymous_identity="anonymous@example.com"
ca_cert="/etc/cert/ca.pem"
password="replace with your password"
client_cert="/etc/cert/user.pem"
phase2="auth=MD5"
```

EAP-TTLS requires the use of a Certificate Authority (CA) certificate. Prior to authentication you will need to source the certificate form the network administrator and load it on the Sabre-SD EVK. The certificate is required to complete authentication on the network.

Loading certificates will be covered in section 10 of the manual.

9.5 Configuring PEAP/MsCHAPv2 (PEAPv0)

Configuring the WPA supplicant to use PEAP is the same as WPA-PSK with the exception of the WPA supplicant network block contents. To configure the WLAN interface for EAP-TLS follow the steps in section 9.2, replacing the block contents in step 2c with the one listed below:

```
ssid="replace with your network name"
scan_ssid=1
key_mgmt=WPA-EAP
eap=PEAP
identity="user@example.com"
password="replace with your password"
ca_cert="/etc/cert/ca.pem"
phase1="peaplabel=0"
phase2="auth=MSCHAPV2"
```

PEAP requires the use of a Certificate Authority (CA) certificate. Prior to authentication you will need to source the certificate form the network administrator and load it on the Sabre-SD EVK. The certificate is required to complete authentication on the network.

> Many PEAP implementations ignore the need for the CA Cert. If the certificate is not provided by the network administrator comment out the **`ca_cert`** line in the configuration file.

Loading certificates will be covered in section 10 of the manual.

9.6 Configuring EAP-FAST

Configuring the WPA supplicant to use EAP-FAST is the same as WPA-PSK with the exception of the WPA supplicant network block contents. To configure the WLAN interface for EAP-FAST follow the steps in section 9.2, replacing the block contents in step 2c with the one listed below:

```
ssid="replace with your network name"
scan_ssid=1
key_mgmt=WPA-EAP
eap=FAST
anonymous_identity="optional user identity"
identity="replace with your user identity"
password="replace with your user password"
phase1="fast_provisioning=1"
pac_file="/tmp/wpa_supplicant.eap-fast-pac"
```

10 Loading Certificates

The following section covers how to load certificates on to the file system for use with the EAP-TLS/TTLS/PEAP security modes.

Before loading any certificates you will need to obtain them from the network administrator.

The WPA supplicant supports X.509 certificates in .PEM and .DER formats for the CA, user and private key certificates. If the certificates are received in the .PFX or .P12 formats they will need to be converted to the suitable format before being used, see steps below on how to do this.

There are several methods for load certificates to the EVK using the Gnome GUI:

- Load the certificates on to a USB memory stick
- FTP transfer the certificates to the EVK
- Cloud based file storage transfer

Whichever method you choose place the certificates in to the `/etc/cert/` subdirectory.

To convert .PFX or .P12 certificates in to a compatible format for the WPA supplicant follow these steps:

1) Copy certificates to the /etc/cert/ subdirectory.
2) Move to the /etc/cert/ subdirectory:

```
cd /etc/cert
```

3) To extract the CA certificate from the PFX file and convert to .PEM format, issue the following command:

```
openssl pkcs12 -in example.pfx -out ca.pem -cacerts -nokeys
```

4) To extract the user certificate and private keys and convert to .PEM format, issue the following command:

```
openssl pkcs12 -in example.pfx -out user.pem -clcerts
```

The above steps will create a `user.pem` and `ca.pem` file and place them in the /etc/cert/ subdirectory. These files will be the ones referenced in the WPA supplicant network block configuration.

11 Appendix

11.1 Bluetooth Support

The SX-6K3-EVK-SD provides the ability to examine the Wi-Fi capability of the SX-SDMAN module, but does not provide any support to evaluate its Bluetooth capability.

Although the SX-SDCAN used on the SX-6K3-EVK-SD has a custom connector which provides access to the Bluetooth functionality of the module, this interface is at a logic level and is not suitable for quick connection to a host device for evaluation.

If you would like to evaluate the Bluetooth capability of the SX-SDMAN, please contact your Silex sales representative at **866-765-8761** to obtain the necessary hardware and documentation.

11.2 wpa_supplicant

The WPA supplicant used in the SX-6K3-SDK-SD is a cross platform WPA supplicant implementation of 802.11i, with support for a number of operating systems, including Linux. Not only is it a full featured WPA2 supplicant, it also supports WPA and older wireless LAN security protocols.

wpa_supplicant can authenticate with any of the following EAP (Extensible Authentication Protocol) methods:

- EAP-TLS
- EAP-PEAP (both PEAPv0 and PEAPv1)
- EAP-TTLS
- EAP-SIM
- EAP-AKA
- EAP-PSK (experimental)
- EAP-FAST
- EAP-PAX
- EAP-SAKE
- EAP-GPSK
- LEAP (note: requires special functions in the driver)

The above list of EAP types is included for reference only and does not represent the supported and tested capabilities of the WPA supplicant included in the SX-6K3-EVK-SD.

When initiated the wpa_supplicant requires a configuration file to identify the available network configurations that should be used to authenticate. The configuration file contains a number of parameters, a control interface, scanning selection and one or more network blocks. An example of the configuration file contents is shown below:

```
ctrl_interface=/var/run/wpa_supplicant
ap_scan=2
network={
        ssid="Network_SSID1"
        scan_ssid=1
        proto=RSN  # for WPA2-PSK
        key_mgmt=WPA-PSK
        pairwise=CCMP TKIP
        group=CCMP TKIP
        psk="password1"
}
network={
        ssid="Network_SSID2"
        scan_ssid=1
        proto=WPA  # for WPA-PSK
        key_mgmt=WPA-PSK
        pairwise=CCMP TKIP
        group=CCMP TKIP
        psk="password2"
}
```

Full descriptions of the wpa_supplicant and the wpa_supplicant.conf file can be found on-line. The following table outlines the commonly used parameters in the network blocks

Table 1 - WPA Supplicant Configuration File Parameters

Parameter	Options	Description
ssid	<network name>	Network name [Mandatory]
scan_ssid	Control device probe format	
	0	Do not scan this SSID with specific Probe Request frames (default)
	1	Scan with SSID-specific Probe Request frames (this can be used to find APs that do not accept broadcast SSID or use multiple SSIDs; this will add latency to scanning, so enable this only when needed)
proto	List of acceptable protocols	
	WPA	WPA/IEEE 802.11i/D3.0
	RSN	WPA2/IEEE 802.11i (WPA2 is an acceptable alias for RSN)
key_mgmt	List of acceptable authenticated key management protocols	
	WPA-PSK	WPA pre-shared key
	WPA-EAP	WPA using EAP authentication
	IEE8021X	IEEE 802.1X using EAP authentication and (optionally) dynamically generated WEP keys.
	NONE	WPA is not used. Plain text or static WEP can be used.
pairwise	List of accepted pairwise (unicast) ciphers for WPA	
	CCMP	AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i/D7.0]
	TKIP	Temporal Key Integrity Protocol [IEEE 802.11i/D7.0]
	NONE	Use only Group Keys (deprecated, should not be included if APs support pairwise keys)
group	List of accepted group (broadcast/multicast) ciphers for WPA	
	CCMP	AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i/D7.0]
	TKIP	Temporal Key Integrity Protocol [IEEE 802.11i/D7.0]
	WEP104	WEP (Wired Equivalent Privacy) with 104-bit key
	WEP40	WEP (Wired Equivalent Privacy) with 40-bit key
psk	<network passphrase>	The 256-bit pre-shared key used in WPA-PSK mode can be entered either as 64 hex-digits, i.e., 32 bytes or as an ASCII passphrase (in which case, the real PSK will be generated using the passphrase and SSID). ASCII passphrase must be between 8 and 63 characters (inclusive). This field is not needed, if WPA-EAP is used.
eap	List of accepted EAP methods	
	TLS	EAP-TLS. Requires client and server (CA) certificates.
	PEAP	EAP-PEAP with tunneled EAP authentication. Requires server (CA) certificate.
	TTLS	EAP-TTLS with tunneled EAP or PAP/CHAP/MSCHAP/MSCHAPV2 authentication.

Parameter	Options	Description
		Requires client and server (CA) certificates.
	FAST	EAP-FAST.
identity	<identity>	Identity string for EAP authentication
anonymous_identity	<anon_identity>	Identity string for EAP authentication to be used as the unencrypted identity with EAP types that support different tunneled identity e.g. EAP-TTLS.
password	<password>	A password string for EAP authentication.
ca_cert	<cert path and file name>	File path to CA certificate file (PEM/DER). This file can have one or more trusted CA certificates. If ca_cert and ca_path are not included, server certificate will not be verified. This is insecure and a trusted CA certificate should always be configured when using EAP-TLS/TTLS/PEAP. Full path should be used since working directory may change when wpa_supplicant is run in the background.
client_cert	<cert path and file name>	File path to client certificate file (PEM/DER). Full path should be used since working directory may change when wpa_supplicant is run in the background.
private_key	<cert path and file name>	File path to client private key file (PEM/DER/PFX). When PKCS#12/PFX file (.p12/.pfx) is used, client_cert should be commented out. Both the private key and certificate will be read from the PKCS#12 file in this case. Full path should be used since working directory may change when wpa_supplicant is run in the background.
private_key_passwd	<password>	Password for Private key file.
phase1	<phase1 parameter>	outer authentication parameters.
	peaplabel=0	EAP-PEAP. Required for PEAPv0.
	fast_provisioning=1	EAP-FAST. Allows unauthenticated provisioning.
phase2	<phase 2 parameter>	Inner authentication parameters
	auth=MSCHAPV2	EAP-PEAP (required)
	autheap=MSCHAPV2	EAP-TTLS (required)
	autheap=MD5	
pac_file	<file path and name>	File path for the PAC entries. wpa_supplicant will need to be able to create this file and write updates to it when PAC is being provisioned or refreshed. Full path to the file should be used since working directory may change when wpa_supplicant is run in the background.

The above table is NOT comprehensive and is not meant as a complete guide to the wpa_supplicant parameter list and options. Please refer to a full description for completeness:

wpa_supplicant full description...

11.3 Network Manager Command Line Tool

Included with Ubuntu is a tool that allows interaction with the network manager using the command line. The following section will show some common examples and provide a full overview of the tools capabilities. The tool is called **nmcli** and is usable from any console interface (serial based or GUI based).

11.3.1 Checking Status of the WLAN Interface

To establish the status of the network interfaces the following command can be used:

```
nmcli –p nm status
```

(The –p is optional, it provide s a pretty output rather than a normal basic output.)

To establish the current connection status of the WLAN interface the following command can be used:

```
nmcli –p dev status
```

To get more information regarding the connection, once one is established using the WLAN interface use the following command:

```
nmcli –p con status
```

To list available AP's use the following command:

```
nmcli –p dev wifi list
```

Turning on the WLAN interface:

```
nmcli nm wifi on
```

Turning off thre WLAN interface:

```
nmcli nm wifi off
```

The full set of nmcli commands are identified in the table below.

The nmcli command has the following format:

```
nwmcli [OPTIONS] OBJECT {COMMAND | help}
```

Table 2 - nmcli Options Table

Option	Description
-t, --terse	Output is terse. This mode is designed and suitable for computer (script) processing.
-p, --pretty	Output is pretty. This causes *nmcli* to produce easy readable outputs for humans, i.e. values are aligned, headers are printed, etc.
-m, --mode tabular|multiline	Switch between *tabular* and *multiline* output. If omitted, default is *tabular* for most commands. For the commands producing more structured information that cannot be displayed on a single line default is *multiline*. *tabular* - Output is a table where each line describes a single entry. Columns define particular properties of the entry. *multiline* - Each entry comprises more lines, each property on its own line. The values are prefixed with the property name.
-f, --fields <field1,..>|all|common	This option is used to specify what fields (column names) should be printed. Valid field names differ for specific commands. List available fields by providing an invalid value to the --*fields* option. *all* is used to print all valid field values of the command. *common* is used to print common field values of the command. If omitted, default is *common*. The option is mandatory when --*terse* is used. In this case, generic values *all* and *common* cannot be used.
-e, --escape yes|no	Whether to escape ':' and '\' characters in terse tabular mode. The escape character is '\'. If omitted, default is *yes*.
-v, --version	Show *nmcli* version.
-h, --help	Print help information.

Table 3 - nmcli Object & Command Options

Object	Command	Option 1	Option 2	Comment
nm	status	Show overall status of NetworkManager. This is the default action, when no command is provided to *nm* object.		
	sleep	Put NetworkManager into sleep mode. When placed in this mode all interfaces that NetworkManager manages are deactivated.		
	wakeup	Awake NetworkManager from sleep. When NetworkManager is awakened, devices are available to be activated.		
	wifi	Inquire or set status of WiFi interface in NetworkManager.		
		on		Enables WiFi Interface
		off		Disables WIFi Interface
	wwan	Inquire or set status of WWAN interface in NetworkManager.		
		on		Enables WWAN interface
		off		Disables WWAN interface
con	list	List configured connections. Without a parameter, configured connection from both system and user settings services are listed.		
		id	<id>	
		uuid	<id>	
		system		argument filters only system-wide connections
		user		prints user connections only
	status	Print status of active connections.		
	up	Activate a connection. Following options allow specific interfaces and behaviors to be defined.		
		id <id>	iface <iface>	
			ap <hwaddr>	Specifies the AP to be connected to.
			--nowait	Causes *nmcli* to exit immediately and not to wait for command completion.
			--timeout <sec>	Provides a means to specify how long to wait for operation completion.
		uuid <id>	iface <iface>	
			ap <hwaddr>	Specifies the AP to be connected to.
			--nowait	Causes *nmcli* to exit immediately and not to wait for command completion.
			--timeout <sec>	Provides a means to specify how long to wait for operation completion.
	down	Deactivate a connection. The connection is identified by its name using *id* or UUID using *uuid*.		
		id	<id>	
		uuid	<id>	
dev	status	Print status of devices. This is the default action, when no command is specified to *dev* object.		
	list	Get detailed information about devices. Without an argument, all devices are examined.		
		iface	<iface>	Gets information for a specific device.
	disconnect	Disconnect a device and prevent the device from automatically activating further connections without user/manual intervention.		
		iface <iface>	--nowait	Causes *nmcli* to exit immediately and not to wait for command completion.
			--timeout <sec>	Provides a means to specify how long to wait for operation completion.
	wifi	List available WiFi access points.		
		list	iface <iface>	List's AP's seen by specific interface
			hwaddr <hwaddr>	List's only specified AP's if seen in scan results.

12 Revision History

Rev No.	Date	By	Comments
A	10/1/2013	ACR	Initial Release

Silex Technology America, Inc.
www.silexamerica.com