SN82xx SNIC SPI Serial Interface User Manual

Version:	1.0
Release Date:	April 9, 2013

SyChip LLC reserves the right to make changes in specifications at anytime and without notice. The information furnished in this user guide is believed to be accurate and reliable. However, no responsibility is assumed by SyChip for its use, nor any infringements of patents or other rights of third parties resulting from its use. No license is generated under any rights of SyChip or its supporters unless specifically agreed.

Release Record

Version Number	Release Date	Comments
Version 1.0	4/9/2013	• Initial release

THE TABLE OF CONTENTS

TABLE of figures

1. Introduction

SN82xx is a complete low power embedded wireless solution to address the connectivity demand in home appliances and other applications. It integrates an ARM Cortex M3 micro-controller, WiFi BB/MAC/RF IC, RF front end, flash memory, clock, and on-board antenna into a small form factor module. The SN82xx Simple Network Interface Controller (SNIC) [2] is a complete platform for easy network connectivity. The SNIC contains a firmware running onboard SN82xx to support wireless network configuration, TCP/IP network stack, WiFi driver and I/O peripherals driver. It provides to the embedded network application a socket interface over a serial bus, enabling the creation of wireless IP-capable nodes in a simple and straight forward manner. This document provides an overview of the SNIC application development platform for using a host microcontroller to control SN82xx over SPI serial interface. See [5] for host MCU control of SN82xx over UART interface; see [4] for hostless web-based application development based on SN82xx EZ Web Wizzard.

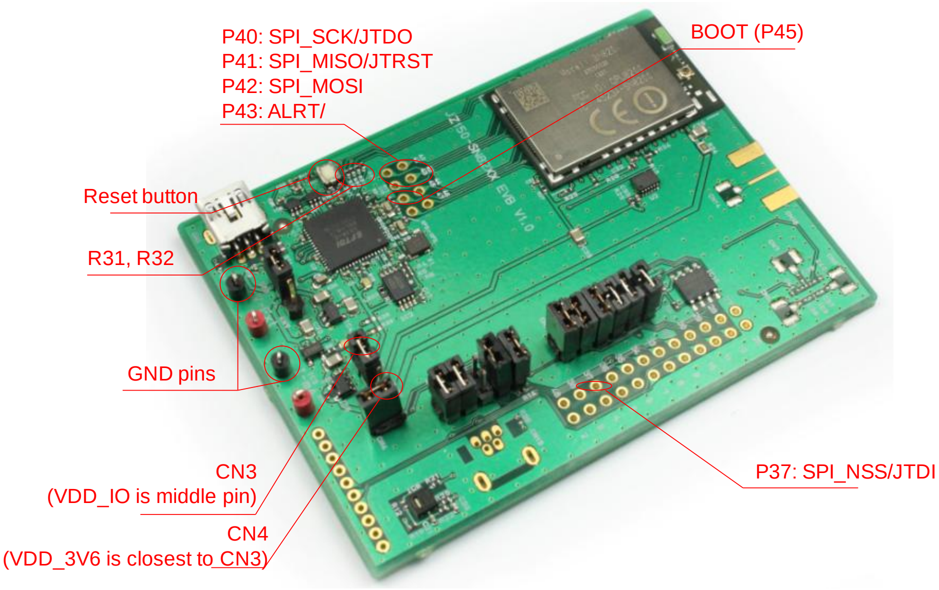


Figure 1 SN82xx EVB configuration for SPI interface

1.1 Acronyms

Acronym	Meaning
API	Application Programming Interface
EVB	Evaluation Board
EVK	Evaluation Kit
FW	Firmware
GPIO	General Purpose Input/Output
PC	Personal Computer
SNIC	Simple Network Interface Controller
SPI	Serial Peripheral Interface
SW	Software
UART	Universal Asynchronous Receiver/Transmitter

USB	Universal Serial Bus

1.2 References

[1] SyChip, “SN82xx EVB schematics”
[2] SyChip, “SN82xx SNIC Serial Interface Specification”
[3] SyChip, “SN82xx SNIC EVK+ User Guide”
[4] SyChip, “SN82xx SNIC EZ Web Wizzard Development Platform User Manual”
[5] SyChip, “SN82xx SNIC UART Serial Interface User Manual.doc”
[6] SyChip, “SN82xx EZ Web Wizzard Simple Web Services URIs”
[7] SyChip, “SN82xx SNIC SPI Sample Application User Guide”

2. Customize and download SNIC Firmare

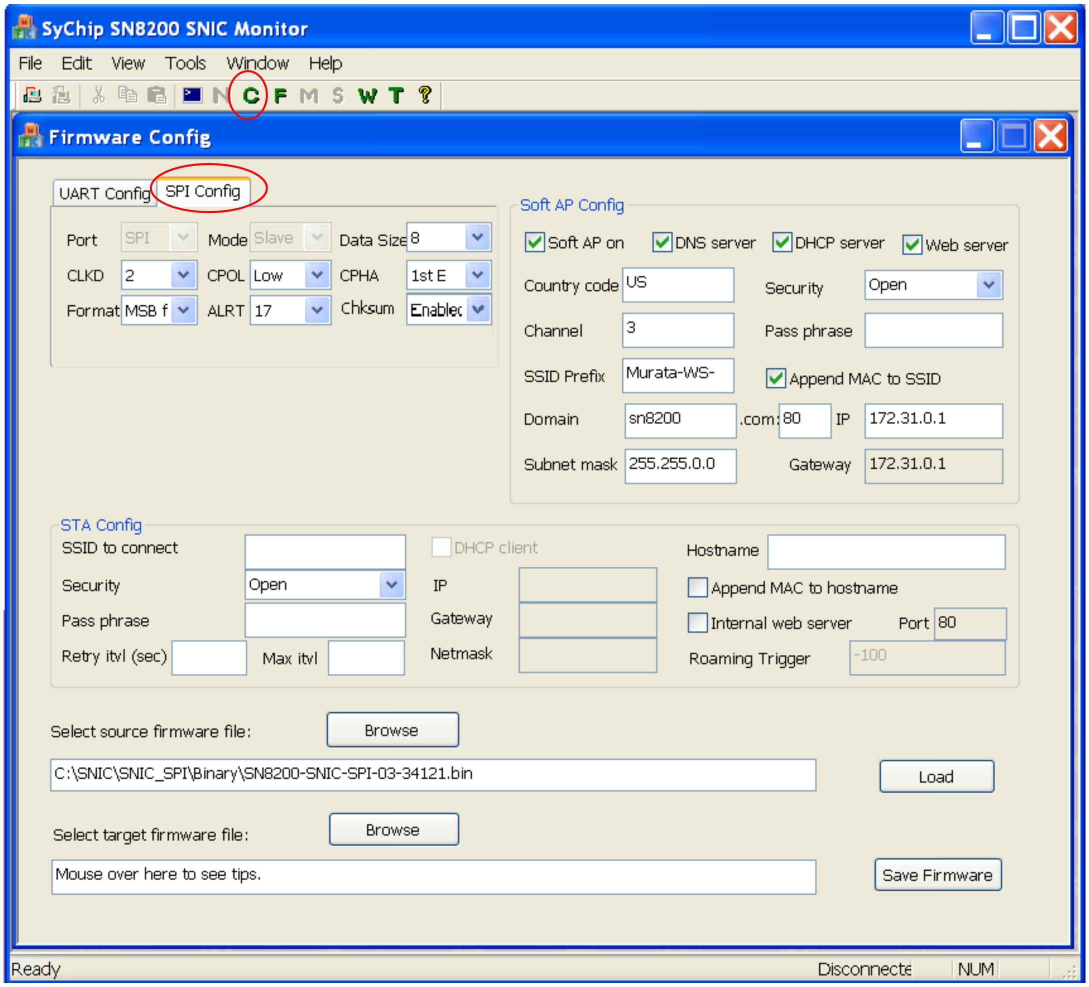
The SN82xx SNIC monitor is a PC application that can be used to customize the SPI interface, generate a new firmware and download that firmware.

2.1 Setting up the SN82xx EVK for Windows

SNIC monitor must be installed along with the drivers for the SN82xx EVK. The procedures for those operations are detailed in *SN82xx SNIC EVK+ User Guide* ([3]).

2.2 Specify product-specific configurations

Application developers can modify the firmware startup parameters to suit their needs. The default software package released by Murata has a prebuilt binary firmware file for SN82xx. This file will be the input to generate a new binary firmware file to include any customized parameters.



Port: SPI
Mode: Slave
Data Size: 8
CLKD: 2
CPOL: Low
CPHA: 1st E
Format: MSB f
ALRT: 17
Chksum: Enablec

Soft AP Config
☑ Soft AP on ☑ DNS server ☑ DHCP server ☑ Web server
Country code: US
Security: Open
Channel: 3
Pass phrase:
SSID Prefix: Murata-WS-
☑ Append MAC to SSID
Domain: sn8200 .com: 80
IP: 172.31.0.1
Subnet mask: 255.255.0.0
Gateway: 172.31.0.1

STA Config
SSID to connect:
Security: Open
Pass phrase:
Retry itvl (sec):
Max itvl:
☐ DHCP client
IP:
Gateway:
Netmask:
Hostname:
☐ Append MAC to hostname
☐ Internal web server Port: 80
Roaming Trigger: -100

Select source firmware file: Browse
C:\SNIC\SNIC_SPI\Binary\SN8200-SNIC-SPI-03-34121.bin
Load

Select target firmware file: Browse
Mouse over here to see tips.
Save Firmware

Ready Disconnecte NUM

Figure 2 Customize firmware parameters (SPI)

Execute the following steps to generate a new firmware suited for the customer platform.

- Open SNIC monitor and click on the green “C” configuration button on the tool bar. The default screen is for configuring the SNIC over UART interface. Do not click on UART tab, because it is for a different host application that communicates with SN82xx via UART interface. Click the “SPI Config” tab to configure the SPI interface (Figure 2).
- Click the Browse button to select source firmware file, and click on Load button. This will populate the above fields according to the file. After loading, the Save Firmware button is enabled.
- The upper left area is interface configuration. Set the SPI parameters used by the host for the serial interface protocol.
    - Data Size: 8-bit or 16-bit data frame format;
    - CLKD: clock divider. Clock rate = 36MHz / CLKD;
    - CPOL: clock polarity. Choose clock to either low or high when idle;
    - CPHA: clock phase. Choose to capture data at either 1st or 2nd clock transition edge;
    - Format: choose to transmit either MSB or LSB first in a frame;
    - ALRT: alert pin. Choose the GPIO pin used as alert. Refer to section 7.5 in [2] for detailed I/O pin information.
    - Chksum: payload checksum calculation disabled.
- Modify any parameters for the following:
    - AP mode parameters (2.2.1)
    - STA mode parameters (2.2.2)
- Select or type in the name of the target firmware file name.
- Click on Save Firmware button. A message should pop up to indicate success or failure.
- Continue to the Section 2.3 to import web contents into the newly generated Firmware.

2.2.1 AP mode parameters

The Soft AP Config block specifies the startup parameters for the soft AP interface.

- Soft AP on: Soft AP will be on or off at startup
- DNS server: if enabled, it will return IP address for the value specified in the Domain name field (default is sn8200.com).
- DHCP server: if enabled, it will assign IP addresses to devices connected to it.
- Web server: if enabled, it will serve pages for STA to select a target AP, see details in Section 3.2.
- Country code: default is US.
- Security: open, WPA, WPA2, or mixed
- Pass phrase: 64 characters or less
- Channel: WiFi channel for soft AP
- SSID Prefix: this is broadcasted soft AP’s SSID prefix
- Append MAC to SSID: if checked, the soft AP’s SSID will be the prefix plus the last 3 bytes of the MAC address; otherwise, the SSID prefix will be used as the whole SSID.
- Domain name: default is sn8200.com, can be modified to any name.
- The edit box next to the Domain name is the HTTP port for the web server, default is 80.
- IP: default is 172.31.0.1, can be customized to be any valid IP.
- Subnet mask: default is 255.255.0.0.

- Gateway: should be same as IP.

2.2.2 STA mode parameters

The STA Config block specifies the startup parameters for STA interface.

- SSID to connect: enter SSID to connect when the module boots up (or after a reset).
- Security: the target AP’s security mode which can be open, WEP, WPA-PSK, WPA2-PSK, or mixed.
- Pass phrase: the target AP’s pass phrase.
- Retry itvl (T1): if the SSID specified is not on (or with wrong security settings) at the time SN82xx boots up, the auto-joining will fail. This parameter specifies the initial retry interval. If STA fails to connect for the first time, STA waits for T=T1. Once T expires, STA retries connection. Failed attempt will result in next attempt at T=min(2*T, Tmax). The unit of timeout is second(s), and the range is from 0x0000 - 0xFFFF. The value of 0 has a special meaning for T1, which indicates no retry.

  NOTE: this is only supported in SN82xx EVK+ and not SN82xx EVK.
- Max itvl (Tmax): maximum retry interval SN82xx waits to retry joining. If T1=10 and Tmax=1000, the following intervals (seconds) will be set for retries: 10, 20, 40, 80, 160, 320, 640, 1000, 1000, 1000… Either a Join request or a Leave request from other interface (e.g., web) will stop the retry process.

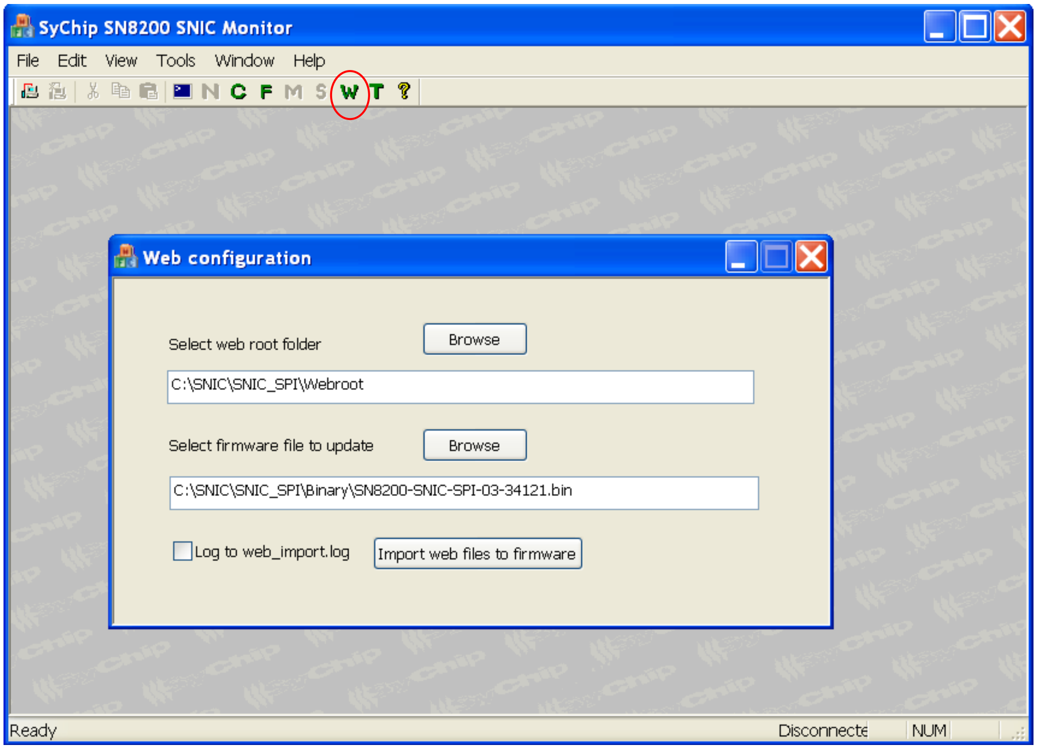
  NOTE: this is only supported in SN82xx EVK+ and not SN82xx EVK.
- Internal web server: if enabled, it will serve pages for the STA interface. Default is enabled.
- Port: HTTP (internal web server) port, default is 80.
- DHCP client: if checked, the module will send DHCP request out to obtain IP after connecting to AP.
- IP, Gateway and Netmask: if DHCP client is not checked, specify the static IP info here.
- Hostname prefix: this is the prefix of the hostname that will be advertised through the DHCP host name option (12). Default value is NUL string which means no hostname is used.
- Append MAC to hostname: if checked, the hostname will be the hostname prefix plus the last 3 bytes of the MAC address; otherwise, the hostname prefix will be used as the hostname.

2.3 Customize web content in firmware

The soft AP interface in SN82xx includes a built-in web server, see Section 3.2. Customers can modify the web content to suit their needs. The software package released by Murata has a prebuilt binary firmware file for SN82xx. This file can be the input to generate a new binary firmware file to include any customized web content.

Execute the following steps to generate a new firmware suited for the customer platform.

- Open SNICMonitor and click on the green “W” configuration button on the tool bar.
- Follow steps described in [4] to update firmware with customized web contents. Ensure that the SPI port is not also being used by the EZ Web Wizzard based web-interface ([6]).


SyChip SN8200 SNIC Monitor
File Edit View Tools Window Help
N C F M S W T ?
Web configuration
Browse
Browse
Import web files to firmware
Ready
Disconnecte
NUM

Select web root folder: C:\SNIC\SNIC_SPI\Webroot

Select firmware file to update: C:\SNIC\SNIC_SPI\Binary\SN8200-SNIC-SPI-03-34121.bin

□ Log to web_import.log

Figure 3 Web content configuration

2.4 Import TLS certificate to firmware

The firmware has a default certificate (generated by Broadcom) and private key for secure sockets layer (SSL) communication. They are used when a secure socket is used or a HTTPS request is sent from the host application. New certificate and private key can be imported to the firmware by customer using the SNICMonitor.

The generation of TLS certificate and private key file is out of the scope of this document. Usage of secure sockets and HTTPS request are described in the SN82xx SNIC Serial Interface Specification [2]. Here is a typical procedure of using a secure socket.

- TLS TCP server
  - Ensure IP is valid on the interface, either STA or soft AP.
  - Create a secure TCP socket and bind to local IP and a port.
  - Start TCP connection on the socket (listening socket).
  - Accept one incoming connection.
  - Send and receive data on the connection socket.
  - Close the connection socket if no more data needs to exchange on this connection, this also allows the listening socket to accept new connection.
  - Close the listening socket to terminate the TLS server.
- TLS TCP client
  - Ensure IP is valid on the interface, either STA or soft AP.

- Create a secure TCP socket
- Connect to a TLS TCP server
- Send and receive data on the same socket
- Close the socket to terminate the TLS client

Click on the “T” button to open the certificate import window. Select certificate file, private key file, and the target firmware file. The maximum file size of the certificate and private key are 4K and 2K bytes, respectively. Certificate and private key files are in BASE 64 format (PEM format).

Open the certificate file in a text editor. The certificate should be enclosed with the following two lines.

-----BEGIN CERTIFICATE-----

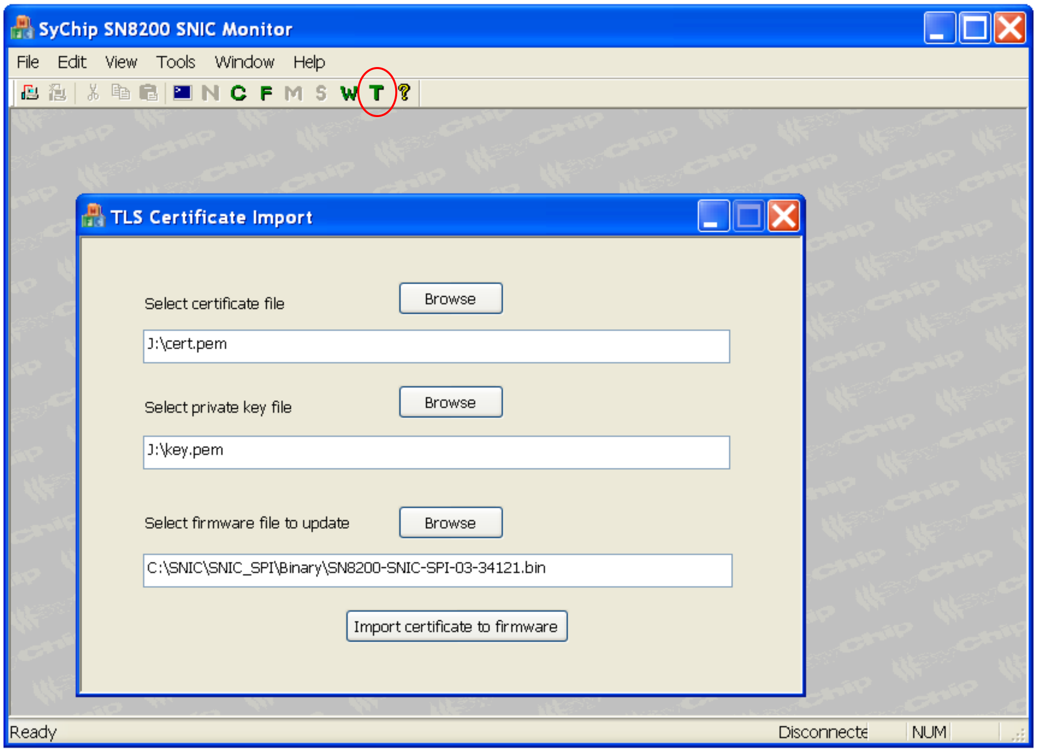
-----END CERTIFICATE-----

Similarly, open the private key file in a text editor. The private key should be enclosed with the following two lines.

-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----

Click “Import certificate to firmware” button after correct files are selected.



Select certificate file

J:\cert.pem

Select private key file

J:\key.pem

Select firmware file to update

C:\SNIC\SNIC_SPI\Binary\SN8200-SNIC-SPI-03-34121.bin

Figure 4 Import certificate and private key

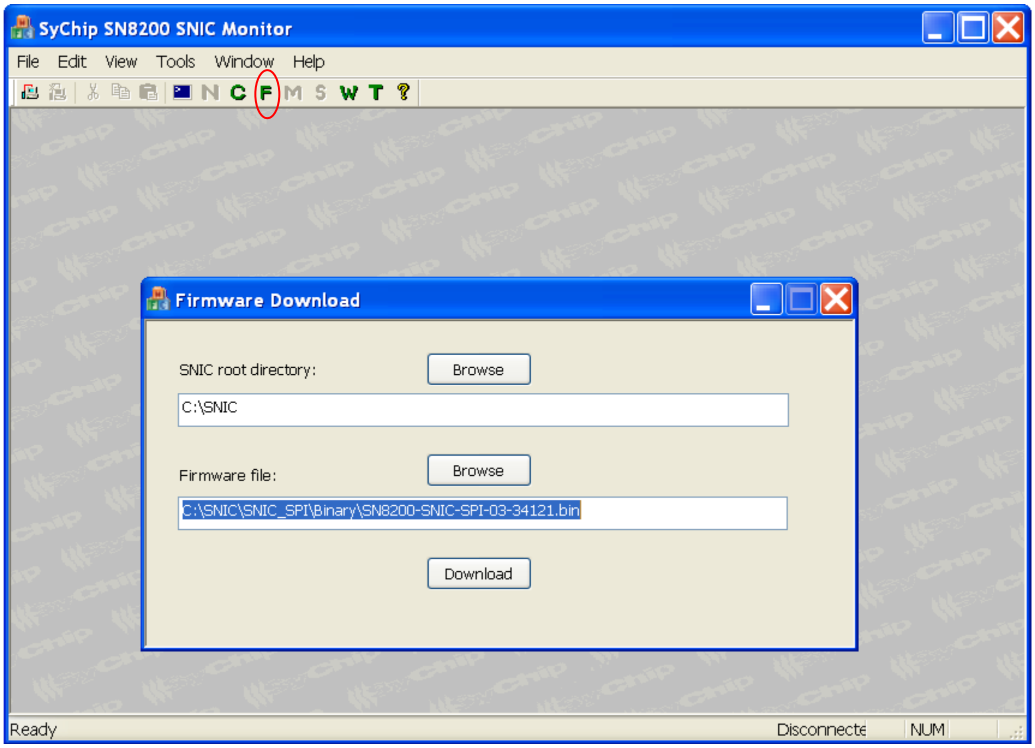
2.5 Download SNIC firmware

The following step must be used to upgrade the SN82xx FW. Once the module has been flashed with the SPI FW, it no longer works with the SNIC Monitor [5] for SNIC UART serial interface operations. However, SNIC Monitor can still be used for FW configuration and download.

1. Pull BOOT (pin 45) high
2. Reset the board
3. Follow the FW download procedure as described below
4. Remove pull-up for BOOT
5. Reset the board to run the updated FW

The SN82xx EVB is preloaded with the SNIC EWW FW image. This section describes the procedure for loading into SN82xx a different SNIC FW image.

1. Ensure the SN82xx EVK has been setup properly and the PC drivers have been installed
2. Ensure that there is no other FTDI-based USB connection besides the SN82xx EVB
3. On SNICMonitor window, click on the green "F" button. It does not matter if the UART Connect button has been clicked or not. The following screen should pop up (with Connect button clicked previously).
4. Click on the green "F" button, the following screen should pop up.



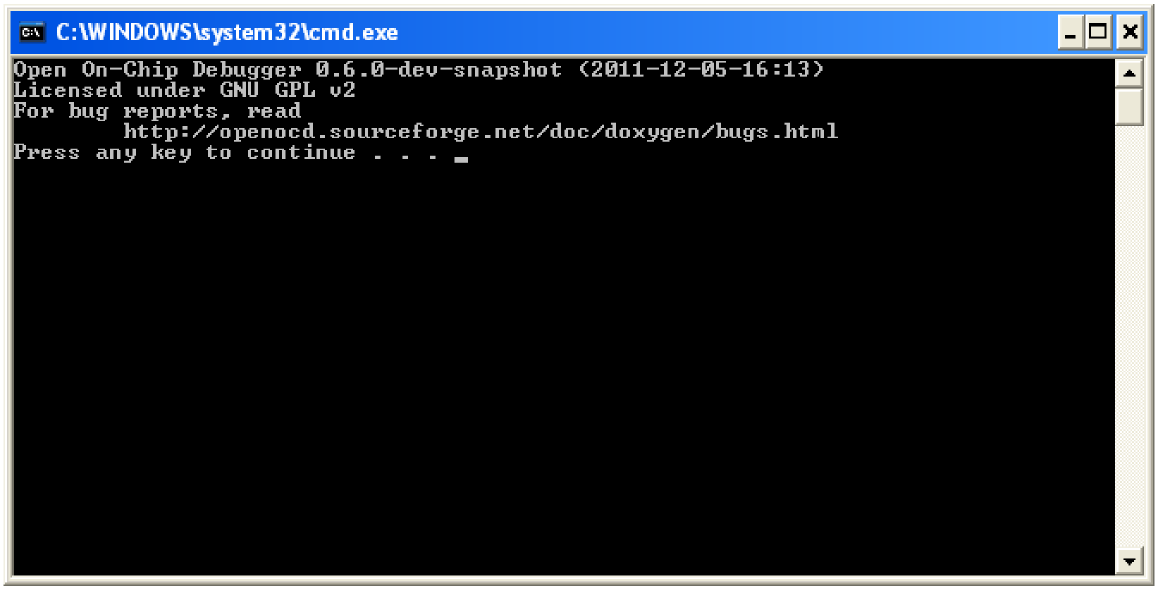
SNIC root directory: C:\SNIC

Firmware file: C:\SNIC\SNIC_SPI\Binary\SN8200-SNIC-SPI-03-34121.bin

Figure 5 Firmware download

5. The correct SNIC root directory must be entered. By default, the *C:\SNIC* folder is populated in the SNIC root directory text box. If it is indeed the SNIC root installation directory, the available Firmware file should also be shown in Firmware file text box.

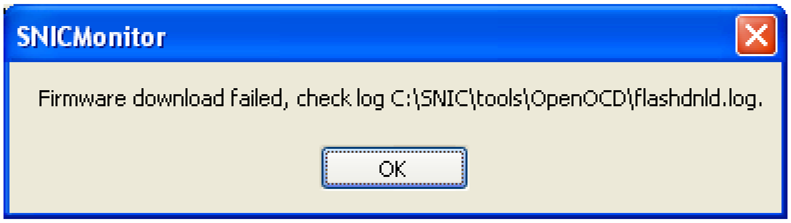
6. If the <*Install Folder*> is not *C:\SNIC*, click on the upper Browse button to select the SNIC root directory. If correct, the Firmware file coming from the installation should be shown; otherwise, the Firmware file text box is empty. If a firmware file other than the installation version is desired, click on the lower Browse button to select it.
7. After SNIC root and Firmware file are selected, click on Download button. A black Command screen should show up as below. A normal download takes about 12 seconds. Press any key to dismiss the Command window when prompted after firmware download is completed. If the firmware file size is bigger than the SN82xx's flash size, an error message is displayed.



```
Open On-Chip Debugger 0.6.0-dev-snapshot (2011-12-05-16:13)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.sourceforge.net/doc/doxygen/bugs.html
Press any key to continue . . . _
```

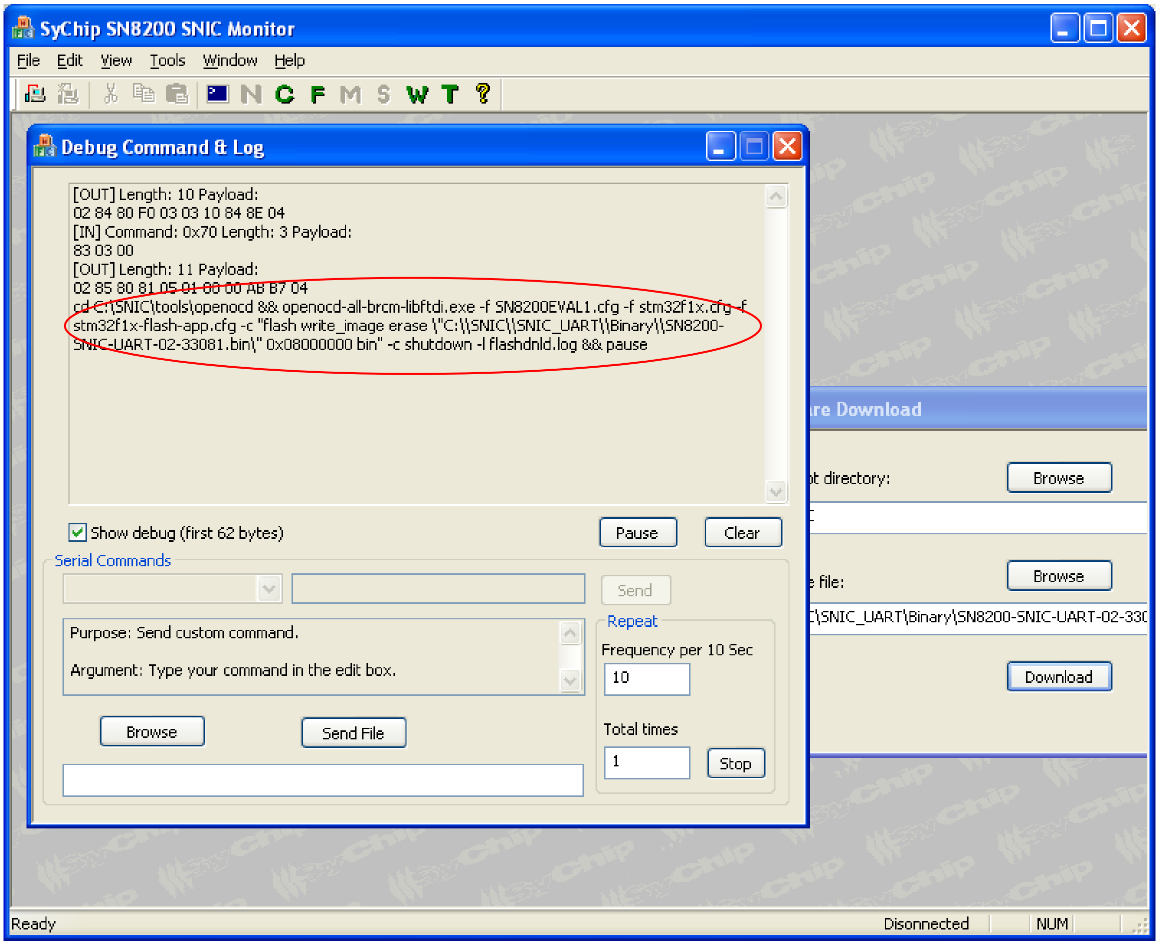
Figure 6 Firmware download window

8. If the black download screen disappears in a second, the download fails. A popup box should show the error log location. Check the log for errors. The command line that is actually used to download firmware should be shown on the Debug window. If the download failed, double check that the correct values are entered in steps 5-6. It is also possible to do the following to capture more detailed error messages.
   - Open a command window by running **Start->Run->cmd** on PC
   - Copy the command line from Debug window (see Figure 8) and paste it on the command window
   - Hit Enter key to run it.
   - Check for any error.



Firmware download failed, check log C:\SNIC\tools\OpenOCD\flashdnld.log.

Figure 7 Popup box if firmware download fails



```
[OUT] Length: 10 Payload:
02 84 80 F0 03 03 10 84 8E 04
[IN] Command: 0x70 Length: 3 Payload:
83 03 00
[OUT] Length: 11 Payload:
02 85 80 81 05 01 00 00 AB B7 04
cd C:\SNIC\tools\openocd && openocd-all-brcm-libftdi.exe -f SN8200EVAL1.cfg -f stm32f1x.cfg -f
stm32f1x-flash-app.cfg -c "flash write_image erase \"C:\\SNIC\\SNIC_UART\\Binary\\SN8200-
SNIC-UART-02-33081.bin\" 0x08000000 bin" -c shutdown -l flashdnld.log && pause
```

☑ Show debug (first 62 bytes)

Purpose: Send custom command.

Argument: Type your command in the edit box.

Frequency per 10 Sec: 10

Total times: 1

C\SNIC_UART\Binary\SN8200-SNIC-UART-02-330

Figure 8 Download firmware command line

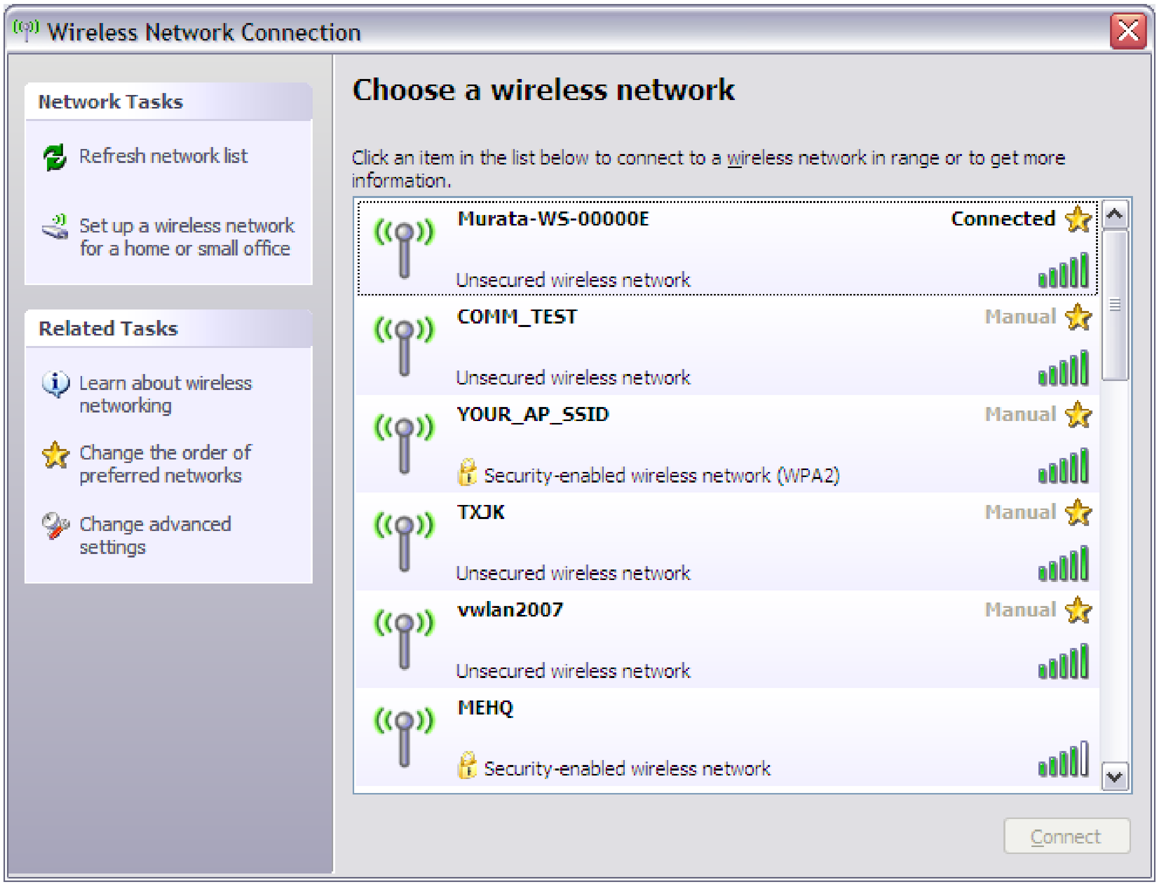
3. Soft AP functions

SN82xx supports both soft AP mode and STA mode at the same time. Soft AP is started by default when powered up, along with DNS server, DHCP server and web server. The web server provides user a sample web interface to configure the STA to scan and join a target AP. This is useful for a display-less implementation using SN82xx, i.e., if a device does not have a key pad to enter SSID and security info, it will not be possible to use the serial command WIFI_JOIN_REQ to join any AP. The soft AP will serve as the input device in this case.

Use the following steps to access the soft AP functions.

3.1 Connecting to the soft AP

1. Reset SN82xx.
2. From a laptop computer with WiFi enabled, scan and join the soft AP's default SSID: Murata-WS-xxxxxxx. The xxxxxx is the last 3 bytes hex of the MAC address of the SN82xx module. Default security is Open.
3. The laptop obtains an IP from the soft AP's DHCP server after joining the soft AP.



Wireless Network Connection

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

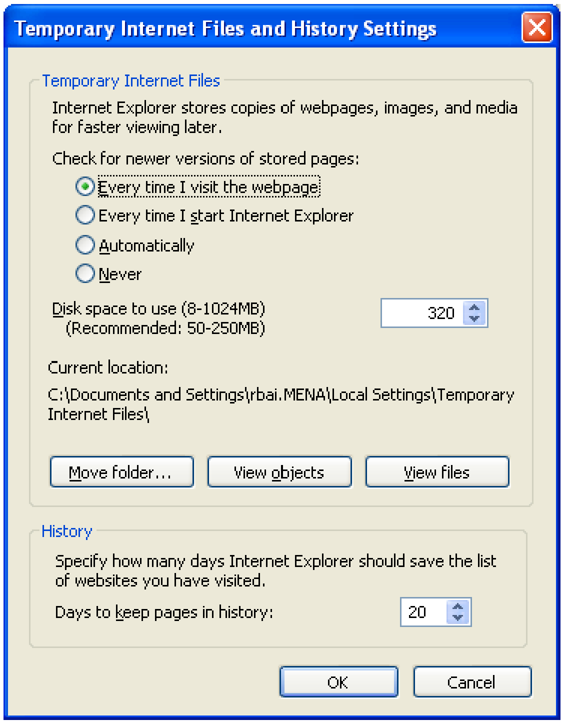
Murata-WS-00000E	Unsecured wireless network	Connected
COMM_TEST	Unsecured wireless network	Manual
YOUR_AP_SSID	Security-enabled wireless network (WPA2)	Manual
TXJK	Unsecured wireless network	Manual
vwlan2007	Unsecured wireless network	Manual
MEHQ	Security-enabled wireless network	

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Figure 9 Join the soft AP from a laptop

3.2 Web browser configuration

Set web browser options so that it sends out HTTP requests every time when a button is clicked. In another word, the browser should not use any cached information. For example, Internet Explorer users can open Tools->Internet Options->Browsing history->Settings, and set the "Check for newer versions of stored pages:" to "Every time I visit the webpage".



Temporary Internet Files and History Settings

Temporary Internet Files

Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

● Every time I visit the webpage
○ Every time I start Internet Explorer
○ Automatically
○ Never

Disk space to use (8-1024MB) (Recommended: 50-250MB): 320

Current location:

C:\Documents and Settings\rbai.MENA\Local Settings\Temporary Internet Files\

History

Specify how many days Internet Explorer should save the list of websites you have visited.

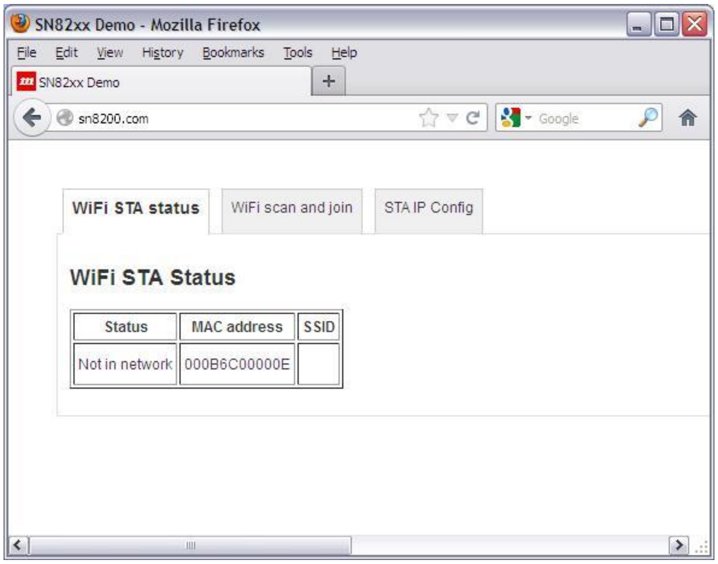
Days to keep pages in history: 20

Figure 10 IE Internet options

3.3 Web pages of the soft AP

The web files used for the soft AP web pages are under *<Install folder>\SNIC_SPI\webroot*, e.g., *C:\SNIC\SNIC_SPI\webroot*.

1. After the laptop joins the soft AP, open a web browser on the laptop. In the address bar, type in sn8200.com. The following web page should appear. If the STA interface has not joined a network, the SSID field should be empty.



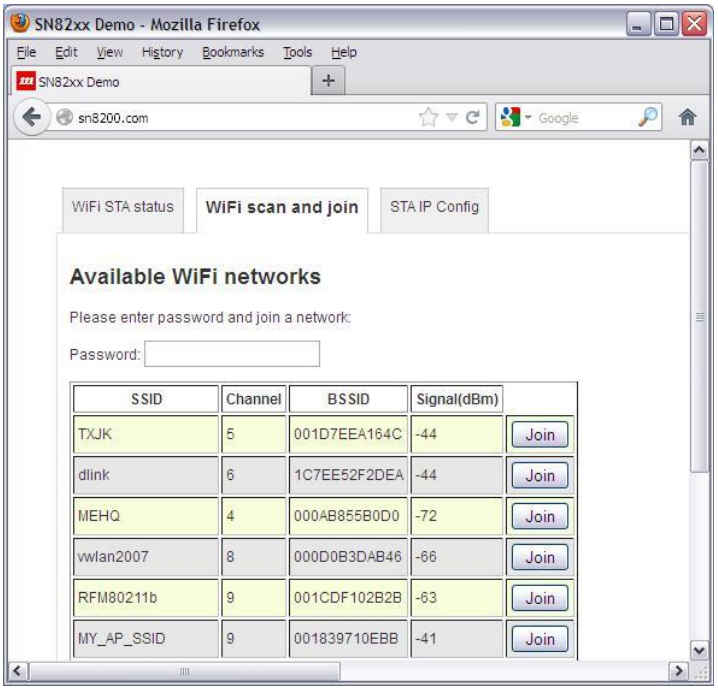
WiFi STA Status

Status	MAC address	SSID
Not in network	000B6C00000E	

Figure 11 Soft AP main page

The initial main page is served by *index.html*, which invokes *wifi_sta_status.html* showing STA is not connected to any network.

2. On the main page, click on “WiFi scan and join” tab.



Available WiFi networks

Please enter password and join a network:

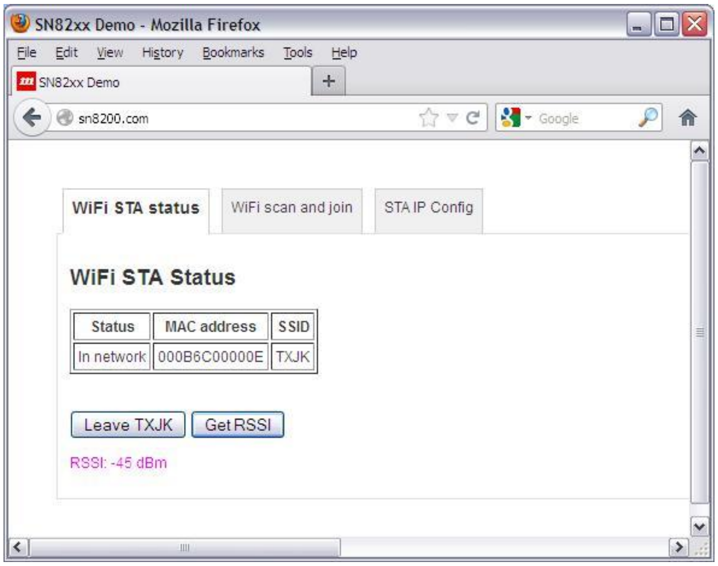
Password:

SSID	Channel	BSSID	Signal(dBm)	
TXJK	5	001D7EEA164C	-44	Join
dlink	6	1C7EE52F2DEA	-44	Join
MEHQ	4	000AB855B0D0	-72	Join
vwlan2007	8	000D0B3DAB46	-66	Join
RFM80211b	9	001CDF102B2B	-63	Join
MY_AP_SSID	9	001839710EBB	-41	Join

Figure 12 AP list

3. Select SSID, enter password and click on Join.

When the join is successful, the channel of the soft AP will change to the channel of the selected AP. Wait for about 10 seconds for the new status. The delay is due to the channel change of the soft AP, which causes the Laptop to reconnect to the soft AP in the new channel. The result page is served by *wifi_sta_status.html*, but two more buttons are added for options to leave the network or get the signal strength of the current connected AP.



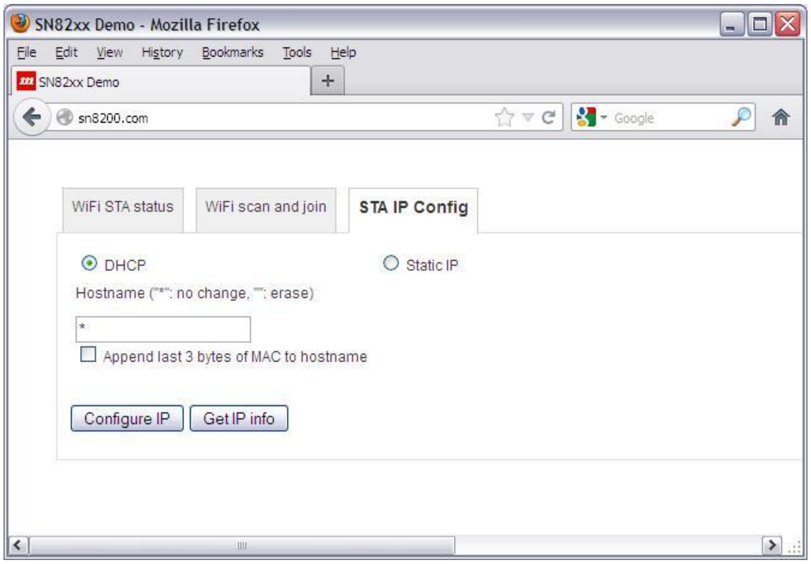
WiFi STA Status

Status	MAC address	SSID
In network	000B6C00000E	TXJK

RSSI: -45 dBm

Figure 13 Status page after join

4. At this point, the STA joins the network but has not obtained an IP. Click on the “STA IP Configuration” tab on web browser and then click on “Configure IP” with DHCP or static IP. The result page is served by *ip_config.html*.



● DHCP ○ Static IP

Hostname ("*": no change, "": erase)

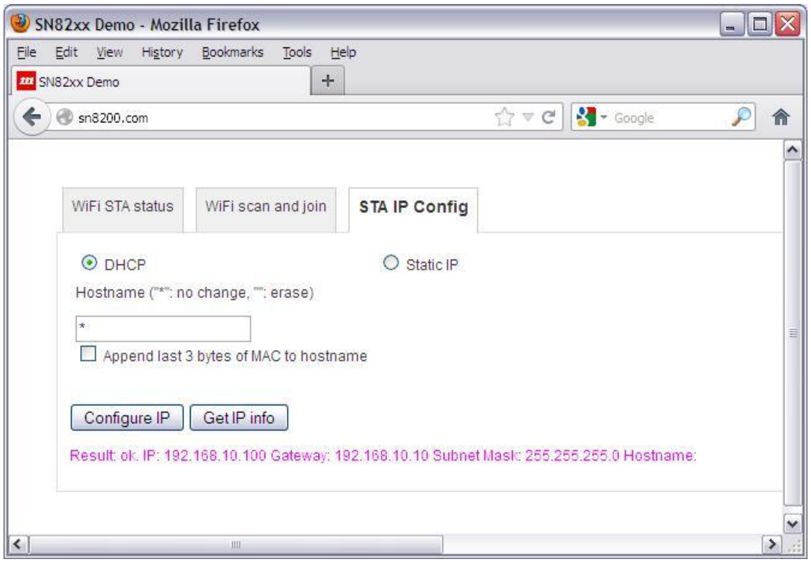
*

□ Append last 3 bytes of MAC to hostname

Figure 14 IP configuration

The hostname field is used to specify a hostname to be embedded into DHCP request. When "Append last 3 bytes of MAC to hostname" is checked, the last 3 bytes of MAC address will be appended to the hostname. Enter "*" if hostname does not need to be changed. Empty the field if hostname is to be erased so that it would not be embedded into DHCP request.

5. Click on "Get IP Info" button to show the IP address information of the STA interface.



● DHCP ○ Static IP

Hostname ("*": no change, "": erase)

*

☐ Append last 3 bytes of MAC to hostname

Result: ok. IP: 192.168.10.100 Gateway: 192.168.10.10 Subnet Mask: 255.255.255.0 Hostname:

Figure 15 IP information

For SNIC serial interface application, the above 3 tabs are sufficient for instructing SN82xx to join/leave an AP. If there is a need to modify the web content, follow the steps described in [4] to customize the web pages. Also check out the SNIC EWW firmware to see the web capabilities.

4. NVM function

Flash space (NVM) is reserved to store startup parameters in SN82xx for both the soft AP and the STA. The purpose is to allow the SN82xx to join the last SSID and preserve the IP info, if it is restarted for any reason. Only STA's parameters can be dynamically changed at run time.

The stored parameters for both soft AP and STA are: Soft AP on/off, Country code, SSID, Passphrase, Channel, DHCP or static IP, etc. The parameters will be used at power up. They can be configured in the Firmware configuration screen on the SNIC Monitor (Section 2.2). Whenever the STA tries to join an AP or obtain IP address, the information is saved in NVM. The latest saved information is used at module power up. The NVM configuration may be restored to the factory default using the GEN_RESTORE_REQ command. Please see reference [2] for details.

5. Third party licensing information

The demo application uses the following open source and vendor-specific libraries:

- FTDI (libftdi/libusb) open source driver
- FreeRTOS open source RTOS
- LwIP open source network stack
- ARM GNU open source gcc toolchain
- STM32F library
- Cortex-M3 CMSIS
- Broadcom WICED SDK
- jQuery

The means for obtaining the licenses and sources for those components is located in *<Install Folder>\License & Open Source Related*.

(END)