HSC04-0 Gateway User Manual

Version: 1.0

Date: 2011-06-17

Table of Contents

1. Copyright and Confidential

2. Disclaimer

This document or diagram and the information contained herein is provided on an "AS IS" basis and Chromagic DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

3. Revision Record

Date	Version	Description
2011-06-17	1.0	The first release.
2009-08-24	0.1	The draft version.

4. Introduction

The gateway is a transceiver which belongs to the member of U-Net series and is fully compatible with any U-Net enabled devices. It is reliably and remotely control and monitor your U-Net enabled devices. Whether you'll be on site and logging in through your network, or away from the premises, logging in through the internet, you'll always have access to control and monitor your security system. You can achieve a better control of your home security, to make your life safer and easier than ever before.

5. Appearance

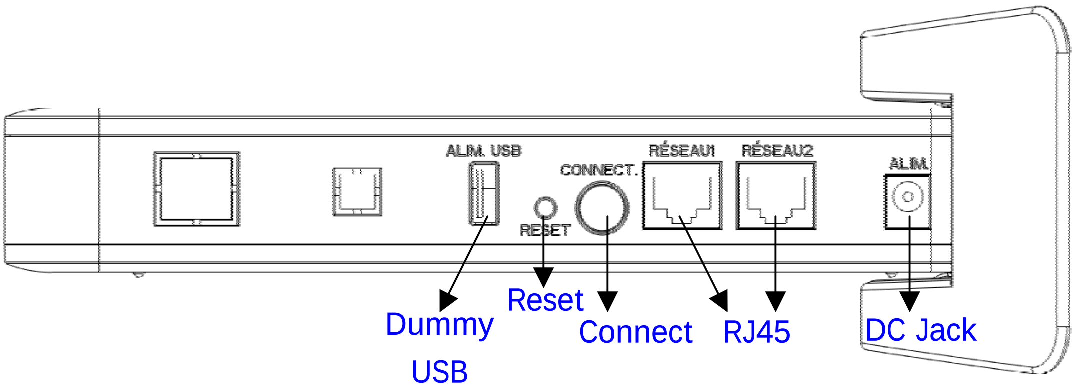


Figure 1: The appearance of the HSC04

5.1. Sockets

- DC Jack:

  Input the DC power voltage 9V and current 2A.
- RJ-45 Socket:

  There are two RJ-45 sockets, The HSC04 has the Ethernet hub function. These two sockets are linked. In SFR, one will connect to SFR modem; another will connect to SFR mini hub.

5.2. Buttons

There are two buttons in the HSC04, one is the reset button (near the dummy USB socket), and another is the connection button (near the RJ-45 socket).

- Reset Button:
  This button will reboot the system. If the system is halting, the user can press this button.

  Note: The HSC04 has the battery power inside, if the DC power be cut off, it will auto switch to use the battery power. So the device is still halting.
- Connection Button:
  - Enable the firmware upgrade function in boot time.
    After press the reset button or power on the device, press the connection button over three times. To ensure the function is enabled, please check the connection LED is blinking in red and green.
  - Set the all settings of the device to the factory default.
    After press the reset button or power on the device, press and hold the connection button until the connection LED is turn on the red and the green light and after the light are turn off. And then release the connection button.
  - Manual enable the bind function.
    After the system is boot up. Press the connection button one time.
  - Manual cancel the bind function.
    If the system is in the binding mode, Press the connection button one time.

5.3. LED

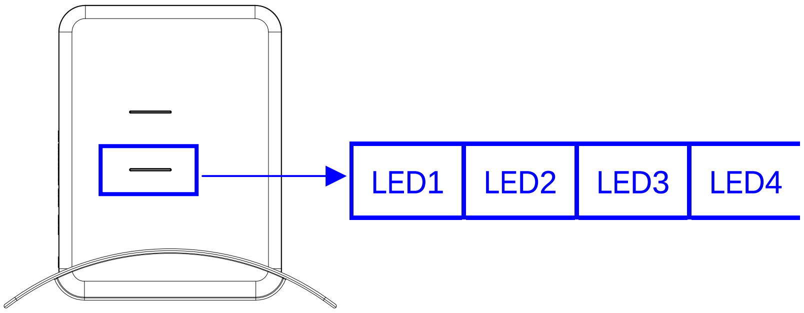


Figure 2: The definition of the LEDs.

We define the function name of these LED.

- LED1: Power LED.
- LED2: Connection LED.
- LED3: Network 1 LED.
- LED4: Network 2 LED.

5.3.1. Power LED

- The green light is on:
  The power is on.
- The red light is on:
  The Flash is writing data.
- The red light is flash once every 5 seconds:
  The system time is not synchronize after boot up.

5.3.2. Connection LED

- The green light is on:
  The OpenVPN is connecting to the server successful.
- The red light is on:
  The DHCP function is enabled but couldn’t got the IP information.

- Blinking in red and green:
  The firmware upgrade function is enabled in bootloader runtime.
- The green light is blinking in second: (0.5s On, 0.5s Off)
  The system is in the binding mode.
- The green light is turn on 2 seconds and turn off 2 seconds:
  The system is inclusion other U-Net device successful.
- The green light is blinking: (0.1s On, 0.1s Off)
  If the system is binding timeout, it will persistence in 4 seconds.
  If the system is abort binding mode, it will persistence in 1 second.
- The green light and the red light are blinking 3 times:
  The system is boot up OK.

5.3.3. Network 1 LED

- The green light is on:
  The RJ-45 socket that one near the connection button is connecting.

5.3.4. Network 2 LED

- The green light is on:
  The RJ-45 socket that one near DC power jack is connecting.

5.4. USB

There are four USB sockets, one is dummy, it is on the side of the appearance, and the other USB sockets are inside the box. In SFR, the dummy USB will provide the power to the mini hub. The other normal USB sockets could plug the 3G dongle.

6. How to search the device?

In default, the HSC04 will enable the DHCP function to get the IP address. If the DHCP function is failed, you will see the “Connection LED” is light on red. In this situation the HSC04 will set the default IP address 192.168.1.222.

Static IP: 192.168.1.222
Netmask: 255.255.255.0
Gateway: 192.168.1.1
DNS1: 192.168.1.1

Otherwise the HSC04 got the IP address from the DHCP server, and you can use the utility “Gateway Finder” to find out the assigned IP address.

The “Gateway Finder” is designed by .Net Framework; you must install it in your system first.

Execute the “GatewayFinder.exe”.

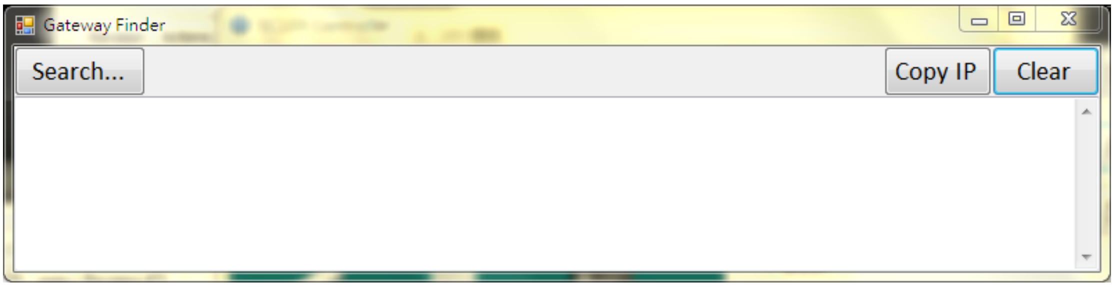
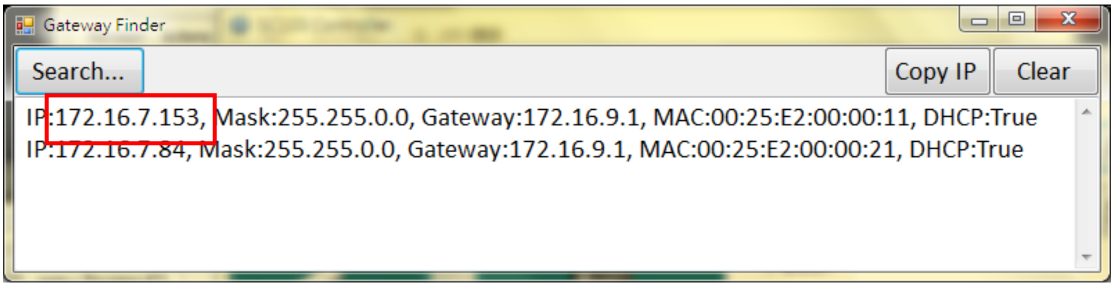


Figure 3: Gateway Finder

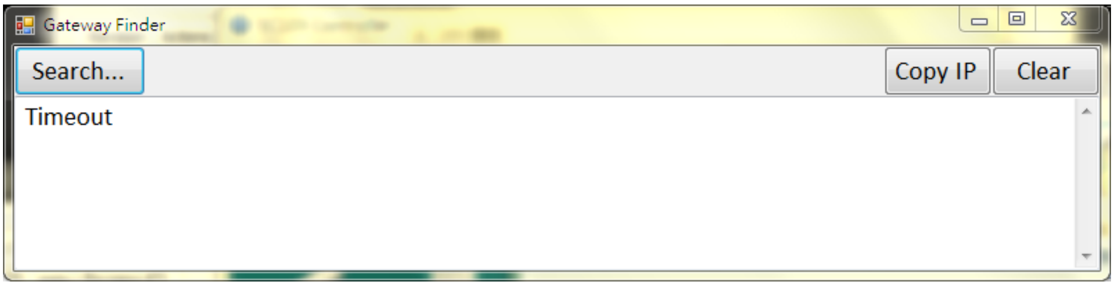
Just click the “Search” button, you will find out the HSC04 IP address.



```
IP:172.16.7.153, Mask:255.255.0.0, Gateway:172.16.9.1, MAC:00:25:E2:00:00:11, DHCP:True
IP:172.16.7.84, Mask:255.255.0.0, Gateway:172.16.9.1, MAC:00:25:E2:00:00:21, DHCP:True
```

Figure 4: Gateway Finder Find Out the IP Address

If it can’t get the response, after about 5 seconds, it will show timeout.

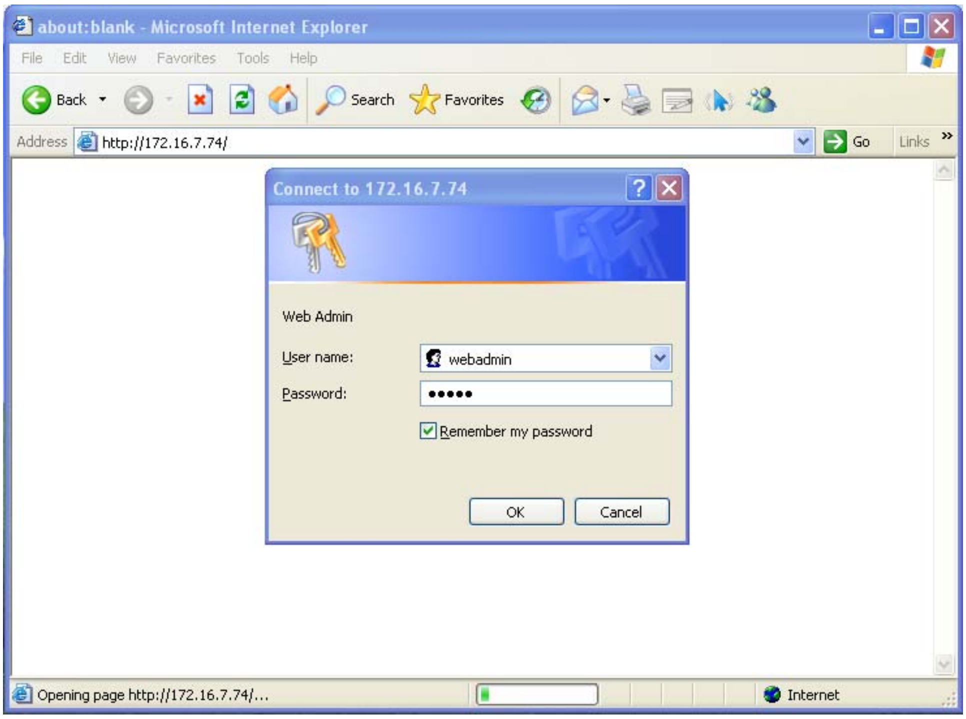


Timeout

Figure 5: Gateway Finder Timeout

7. Web Configuration

Using the browser (IE or Firefox) to access the HSC04, just enter the URL http://(IP Address)/ in browser, The first time access the HSC04 web server, it will request login, the default user name is “webadmin” and the password is “admin”.


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Connect to 172.16.7.74
OK
Cancel
Internet

Address: http://172.16.7.74/

Web Admin

User name: webadmin

Password: •••••

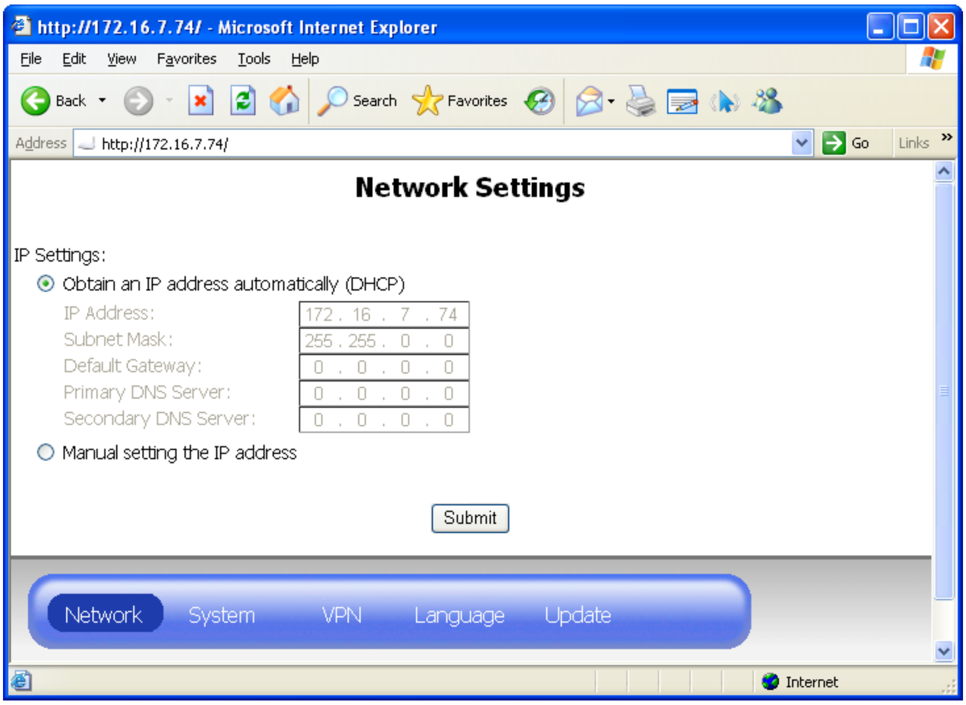
☑ Remember my password

Opening page http://172.16.7.74/...

Figure 6: First Time Access the HSC04 Web Server.

7.1. Network Settings

Set the IP address using the DHCP or the static IP address.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://172.16.7.74/
Go
Links
Submit
Network
System
VPN
Language
Update
Internet

Network Settings

IP Settings:

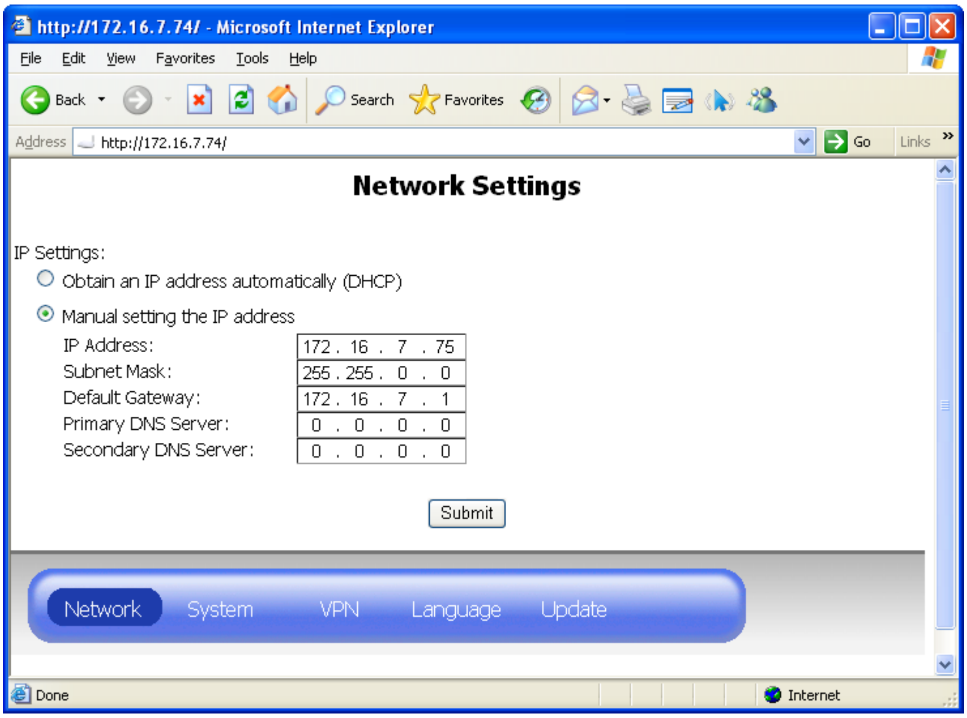
● Obtain an IP address automatically (DHCP)

IP Address:	172 . 16 . 7 . 74
Subnet Mask:	255 . 255 . 0 . 0
Default Gateway:	0 . 0 . 0 . 0
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

○ Manual setting the IP address

Figure 7: Network Settings DHCP

Click the “Manual Setting the IP address” to set the static IP address.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://172.16.7.74/
Go
Links
Submit
Network
System
VPN
Language
Update
Done
Internet

Network Settings

IP Settings:

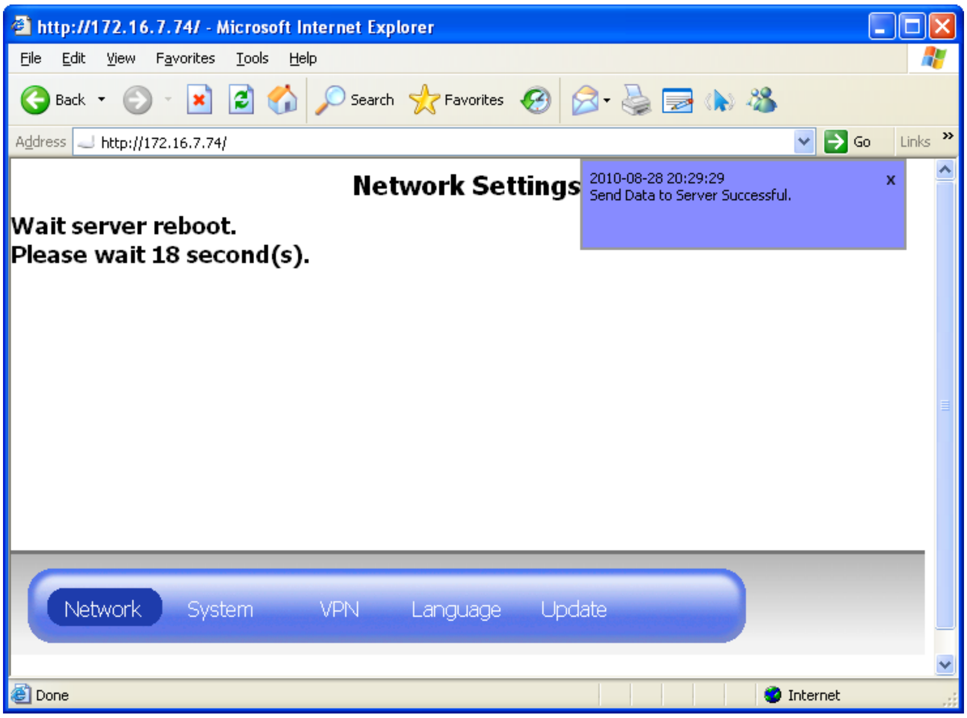
○ Obtain an IP address automatically (DHCP)

● Manual setting the IP address

IP Address:	172 . 16 . 7 . 75
Subnet Mask:	255 . 255 . 0 . 0
Default Gateway:	172 . 16 . 7 . 1
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

Figure 8: Network Settings DHCP

After setting OK, don't forget to press the "submit" button.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Network System VPN Language Update
Done Internet

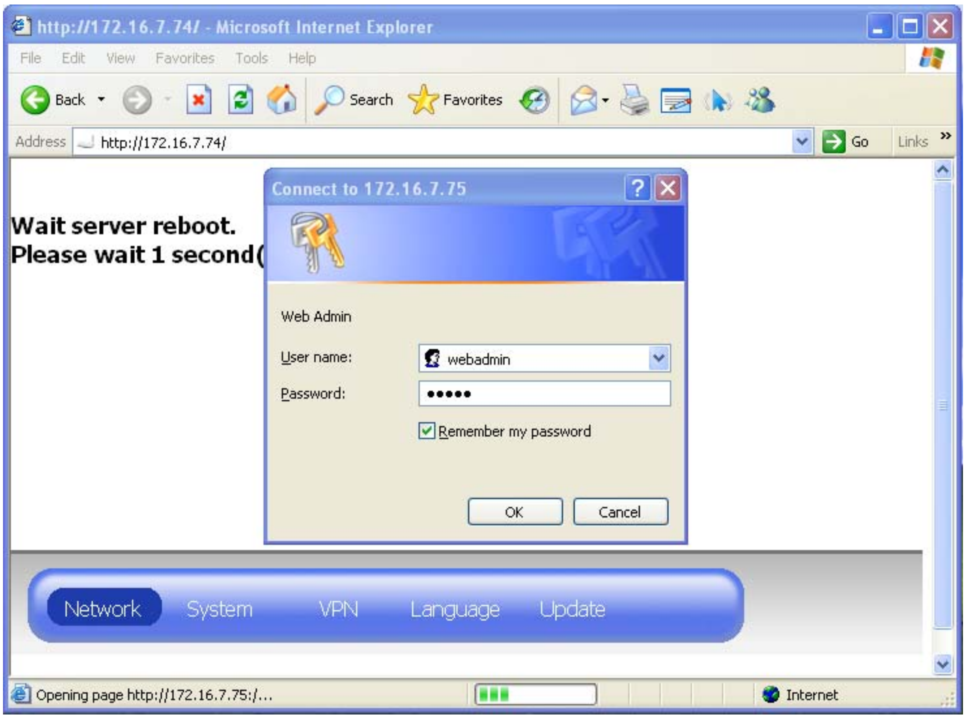
Network Settings

2010-08-28 20:29:29
Send Data to Server Successful.

Wait server reboot.
Please wait 18 second(s).

Figure 9: Network Setting Submit

After 20 seconds, the browser will connect to new IP address.
And you must re-login.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Connect to 172.16.7.75
OK Cancel
Network System VPN Language Update
Opening page http://172.16.7.75:/...
Internet

Wait server reboot.
Please wait 1 second(

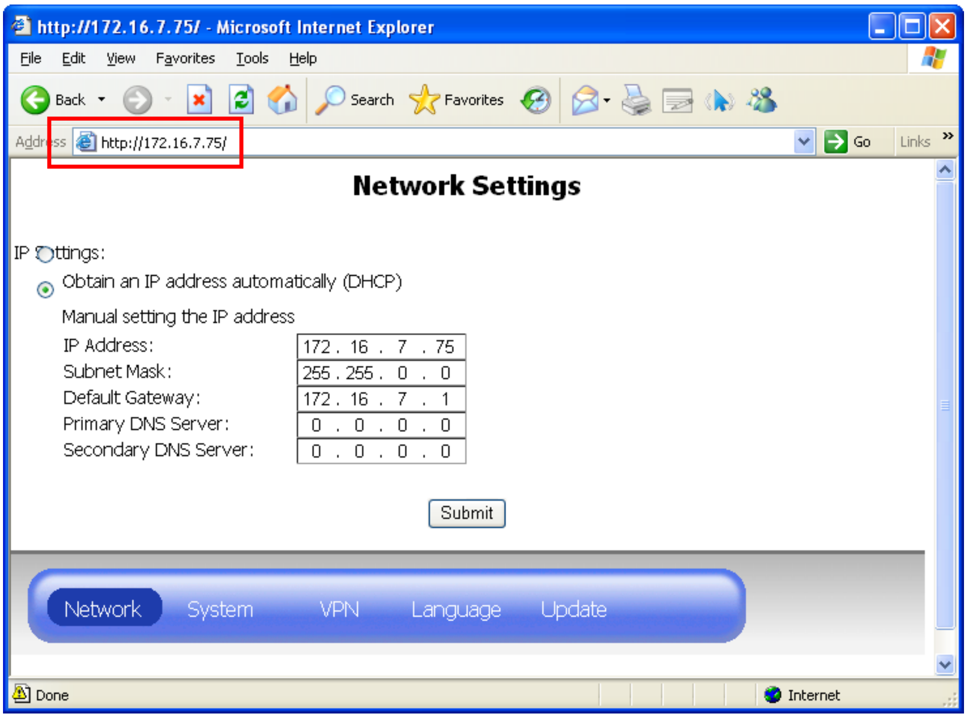
Web Admin

User name: webadmin

Password: •••••

☑ Remember my password

Figure 10: Browser Auto Connect to New IP Address


http://172.16.7.75/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.75/ Go Links
Network System VPN Language Update
Done Internet

Network Settings

IP Settings:

● Obtain an IP address automatically (DHCP)

Manual setting the IP address

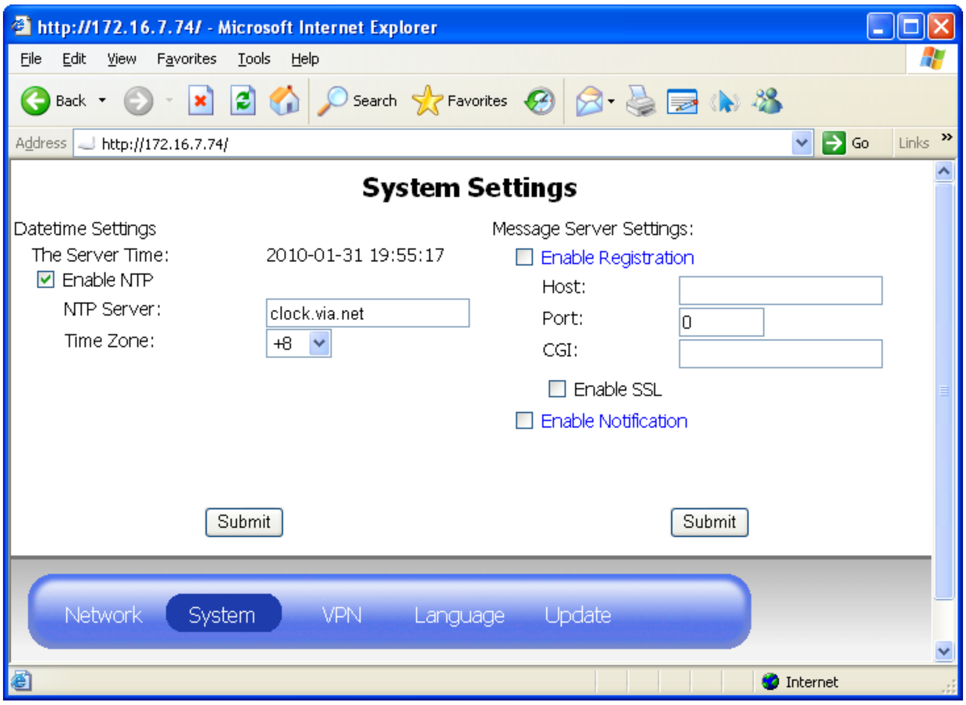
IP Address:	172 . 16 . 7 . 75
Subnet Mask:	255 . 255 . 0 . 0
Default Gateway:	172 . 16 . 7 . 1
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

Submit

Figure 11: The Browser Connected to New IP Address

7.2. System Settings

The system settings will set the NTP function and the message server.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Network System VPN Language Update
Internet

System Settings

Datetime Settings

The Server Time: 2010-01-31 19:55:17

☑ Enable NTP

NTP Server: clock.via.net

Time Zone: +8

Submit

Message Server Settings:

□ Enable Registration

Host:

Port: 0

CGI:

□ Enable SSL

□ Enable Notification

Submit

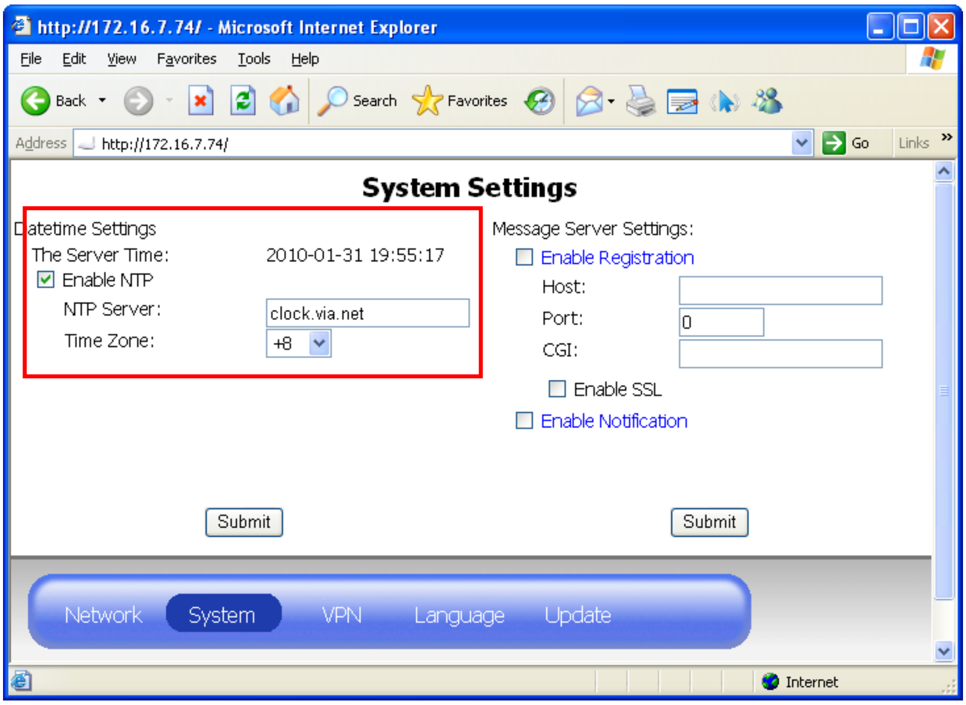
Figure 12: System Settings

7.2.1. NTP Settings

The HSC04 has not the RTC, which means if the power is off, the system time will be reset or stopped.
So at the boot time, the HSC04 will synchronize the system time with the NTP server.
The default NTP settings:

NTP function enable: Yes
NTP Server: clock.via.net
Time Zone: 0

If connect to NTP server failed, it will try again after 1 hour.
If synchronize the time OK, after 4 hours it will synchronize again.
After boot up, the HSC04 detected the system time is not be set. The power LED will flash once every 5 seconds.
The user can set the NTP settings from the browser.



System Settings

Datetime Settings
The Server Time: 2010-01-31 19:55:17
☑ Enable NTP
NTP Server: clock.via.net
Time Zone: +8

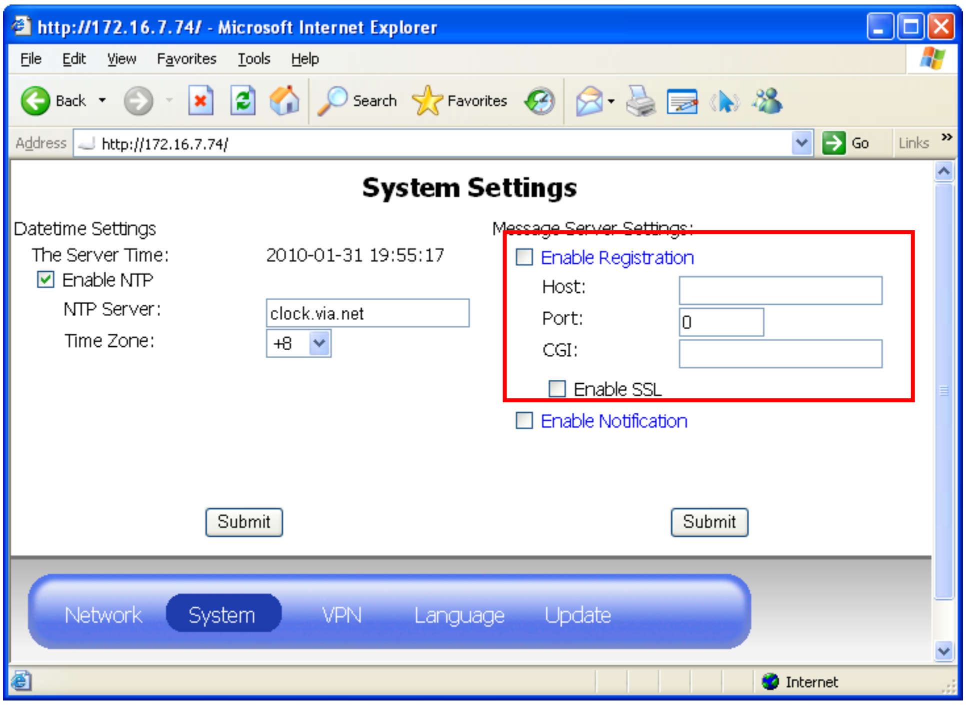
Message Server Settings:
□ Enable Registration
Host:
Port: 0
CGI:
□ Enable SSL
□ Enable Notification

http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Submit
Submit
Network System VPN Language Update
Internet

Figure 13: System Settings

7.2.2. Gateway Registration

If this function is enabled, after boot up OK, the HSC04 will send the registration information to the server every 150 seconds.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Network System VPN Language Update
Internet

System Settings

Datetime Settings
The Server Time: 2010-01-31 19:55:17
☑ Enable NTP
NTP Server: clock.via.net
Time Zone: +8

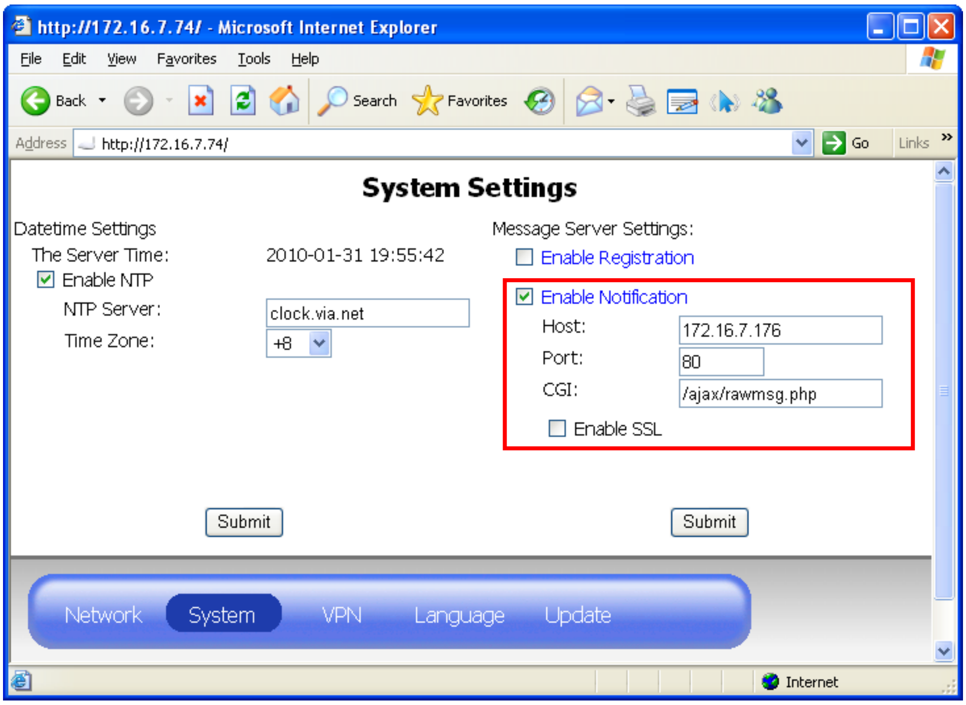
Message Server Settings:
☐ Enable Registration
Host:
Port: 0
CGI:
☐ Enable SSL
☐ Enable Notification

Submit Submit

Figure 14: System Setting Gateway Registration

7.2.3. U-Net Message Forward

If this function is enabled, when the U-Net devices report the state to the HSC04, it can forward the message to the server.



http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Network System VPN Language Update
Internet

System Settings

Datetime Settings
The Server Time: 2010-01-31 19:55:42
☑ Enable NTP
NTP Server: clock.via.net
Time Zone: +8

Message Server Settings:
□ Enable Registration
☑ Enable Notification
Host: 172.16.7.176
Port: 80
CGI: /ajax/rawmsg.php
□ Enable SSL

Submit Submit

Figure 15: System Setting Message Notification

7.3. VPN Settings

A VPN (Virtual Private Network) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

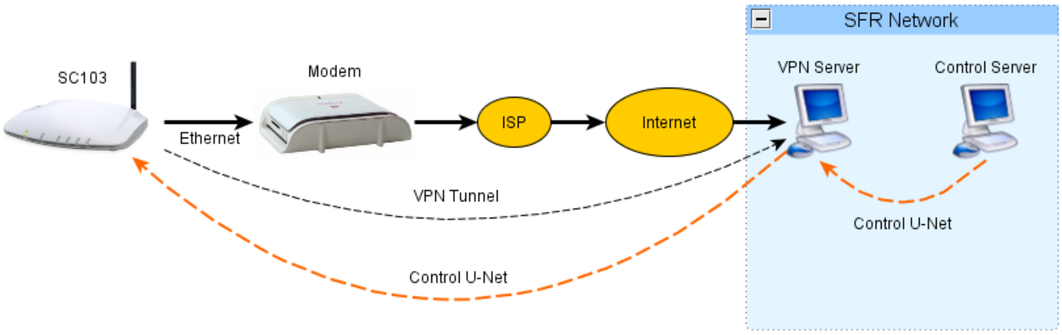
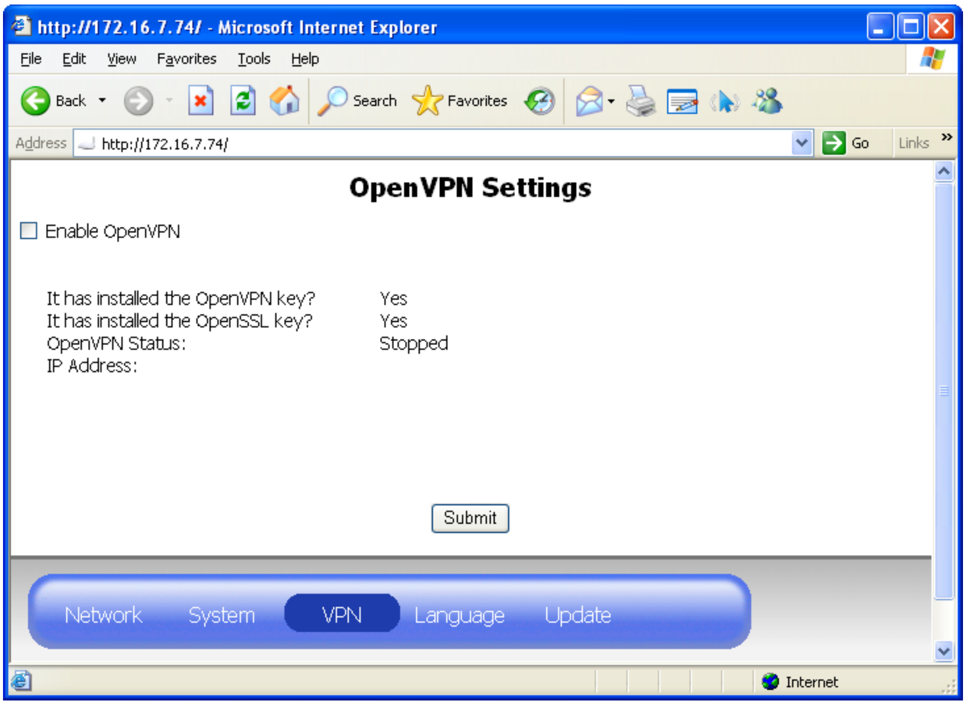


Figure 16: The VPN link.

The HSC04 will use the OpenVPN to provide the VPN function.

The user can see the OpenVPN state or settings from the browser.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Submit
Network System VPN Language Update
Internet

OpenVPN Settings

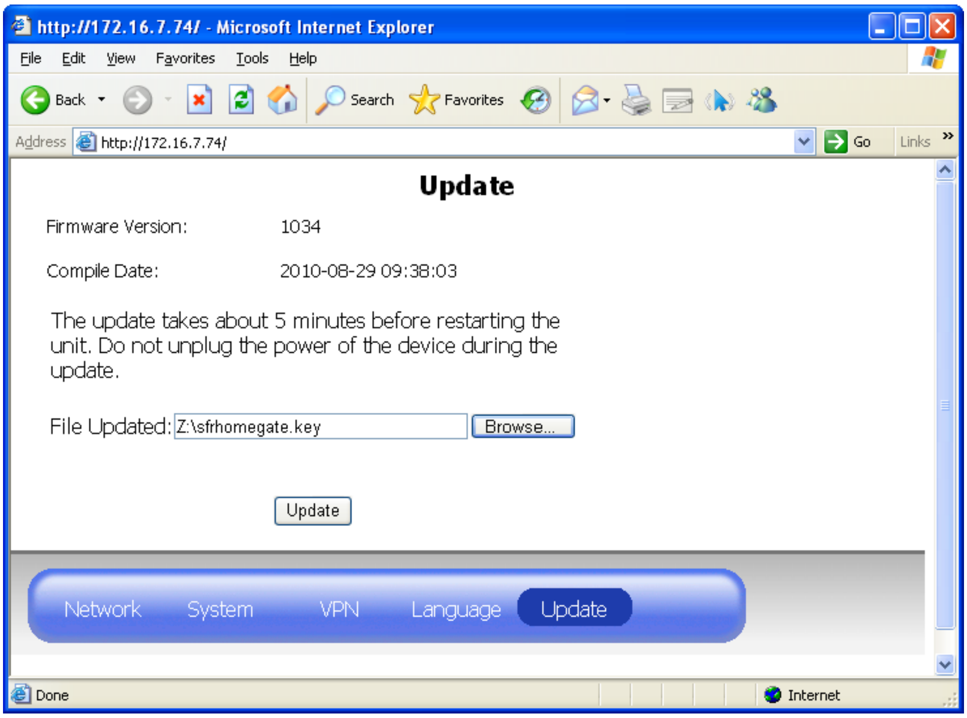
□ Enable OpenVPN

It has installed the OpenVPN key? Yes
It has installed the OpenSSL key? Yes
OpenVPN Status: Stopped
IP Address:

Figure 17 VPN Settings

There are two secret keys in OpenVPN, one is for OpenVPN, and another is for OpenSSL. The keys do not store in the Linux file system. They will be store in the Flash, and encrypted.

Before running the OpenVPN, these keys must be existed. The user can upload the key by “Update” page. Just upload the key file instead of the firmware file.


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Browse...
Update
Network System VPN Language Update
Done
Internet

Update

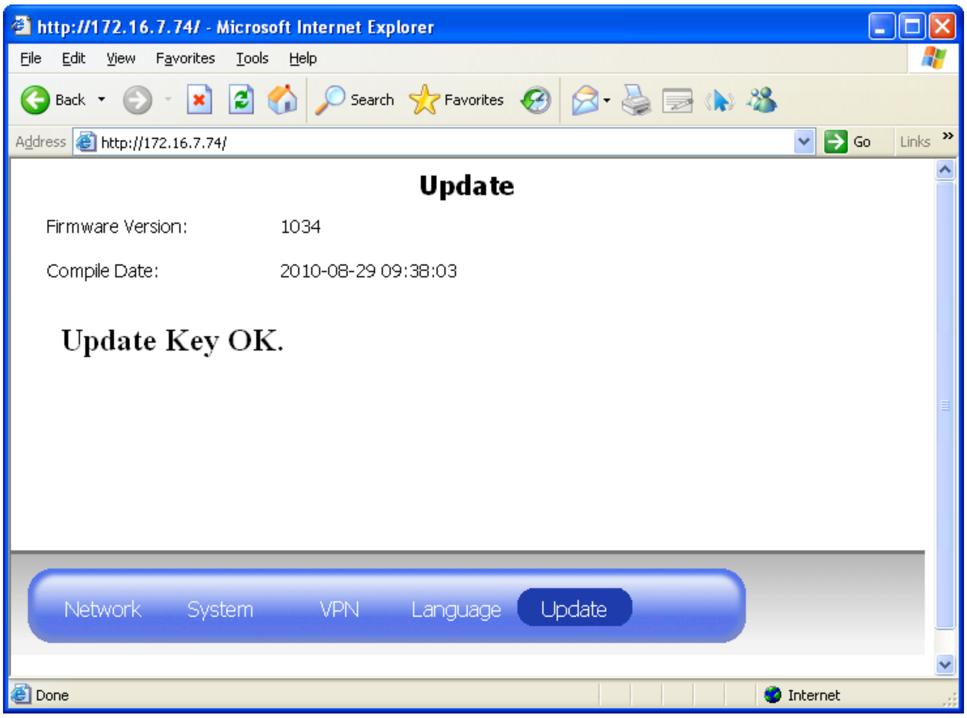
Firmware Version: 1034

Compile Date: 2010-08-29 09:38:03

The update takes about 5 minutes before restarting the unit. Do not unplug the power of the device during the update.

File Updated: Z:\sfrhomegate.key

Figure 18: Upload the Key File


http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/
Go Links
Network System VPN Language Update
Done
Internet

Update

Firmware Version: 1034

Compile Date: 2010-08-29 09:38:03

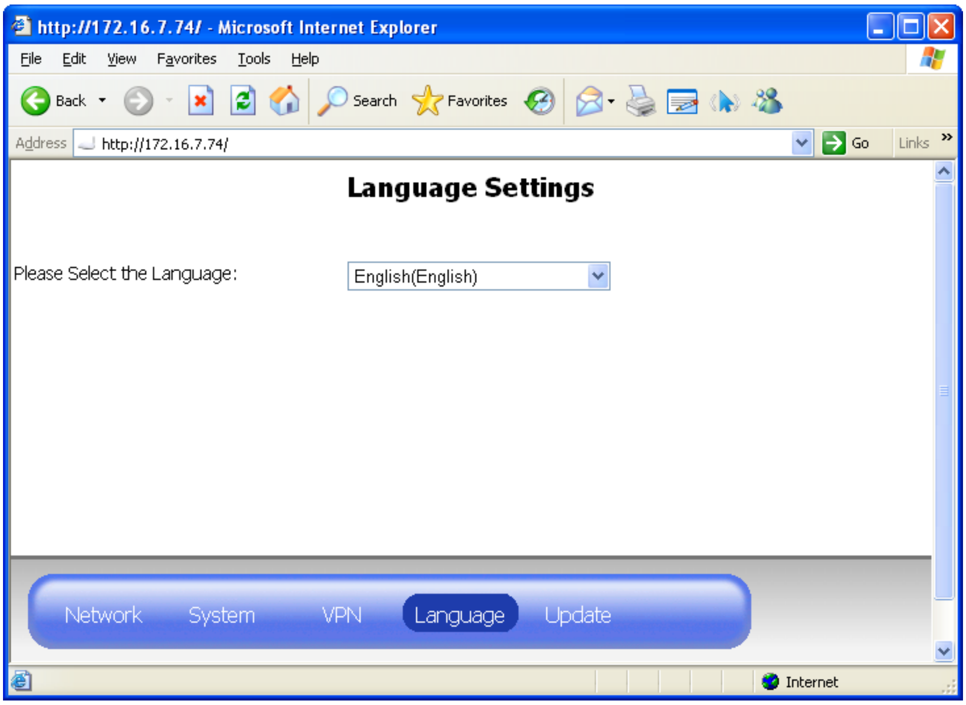
Update Key OK.

Figure 19: Upload Key OK

If the VPN function is enabled and established. The connection LED will turn the green light on.

7.4. Language Settings

Change the web page language to display.

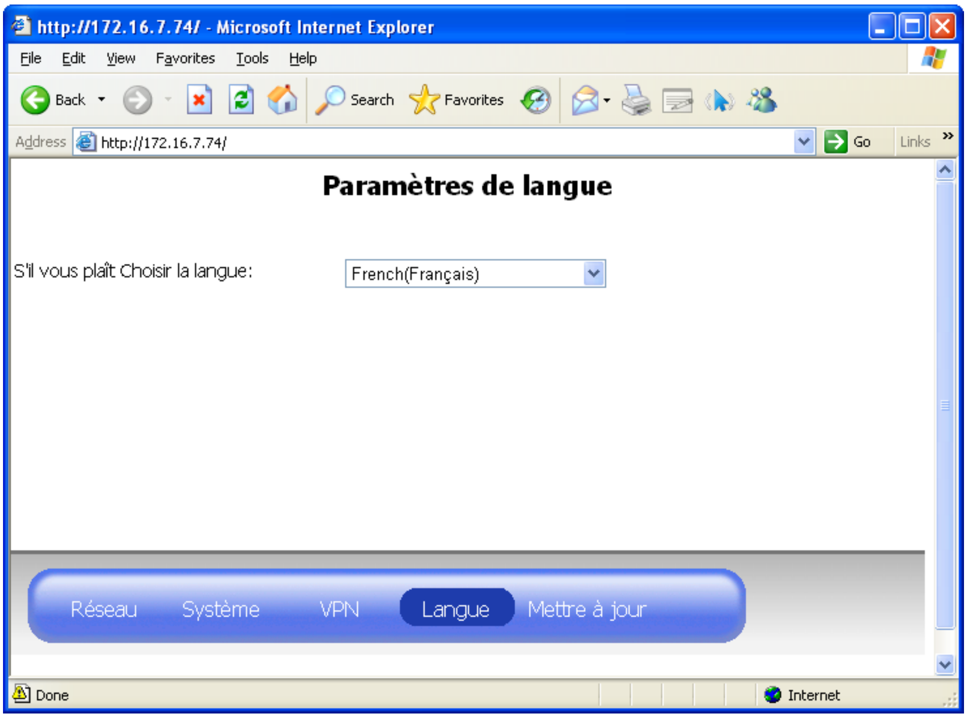

http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Internet
Network
System
VPN
Language
Update

http://172.16.7.74/

Language Settings

Please Select the Language: English(English)

Figure 20: Language Settings

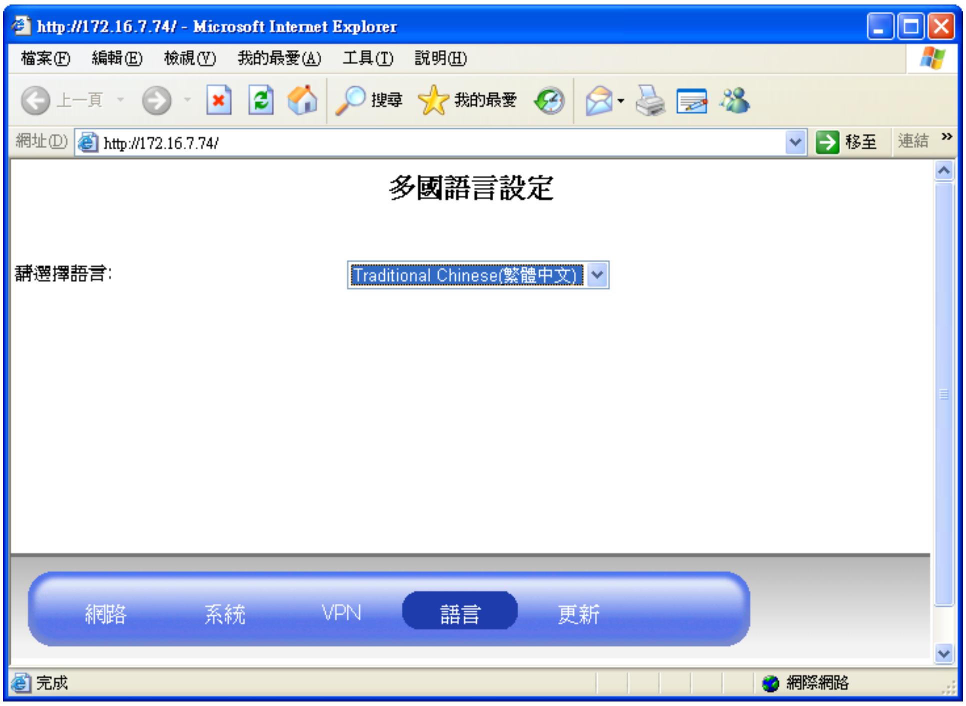

http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Done
Internet
Réseau
Système
VPN
Langue
Mettre à jour

http://172.16.7.74/

Paramètres de langue

S'il vous plaît Choisir la langue: French(Français)

Figure 21: Language Change to French.



http://172.16.7.74/ - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
網址(D) http://172.16.7.74/
移至
連結
網路
系統
VPN
語言
更新
完成
網際網路

多國語言設定

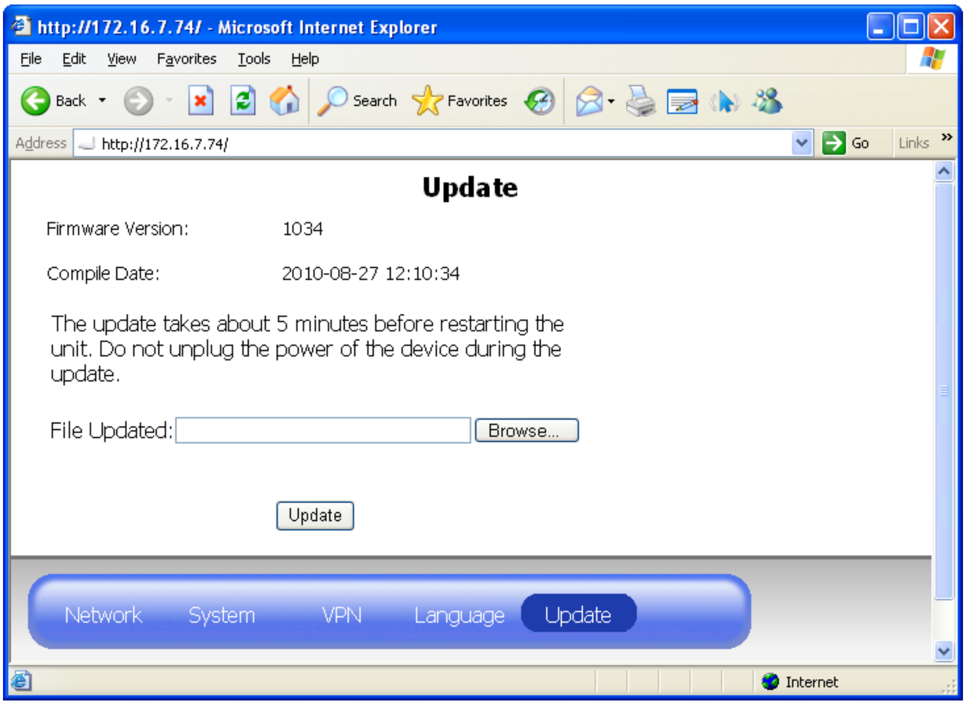
請選擇語言: Traditional Chinese(繁體中文)

Figure 22: Language Change to Chinese

7.5. Update Settings

There are two firmware upgrade function in the HSC04. One is in the bootloader runtime; another is in the Linux runtime. Normally, the user always upgrades the firmware in the Linux runtime. Unless the system occur error or the user want to manual enable the upgrade function, in these case it will operate in the bootloader runtime.

7.5.1. In Linux Runtime



Update

Firmware Version: 1034

Compile Date: 2010-08-27 12:10:34

The update takes about 5 minutes before restarting the unit. Do not unplug the power of the device during the update.

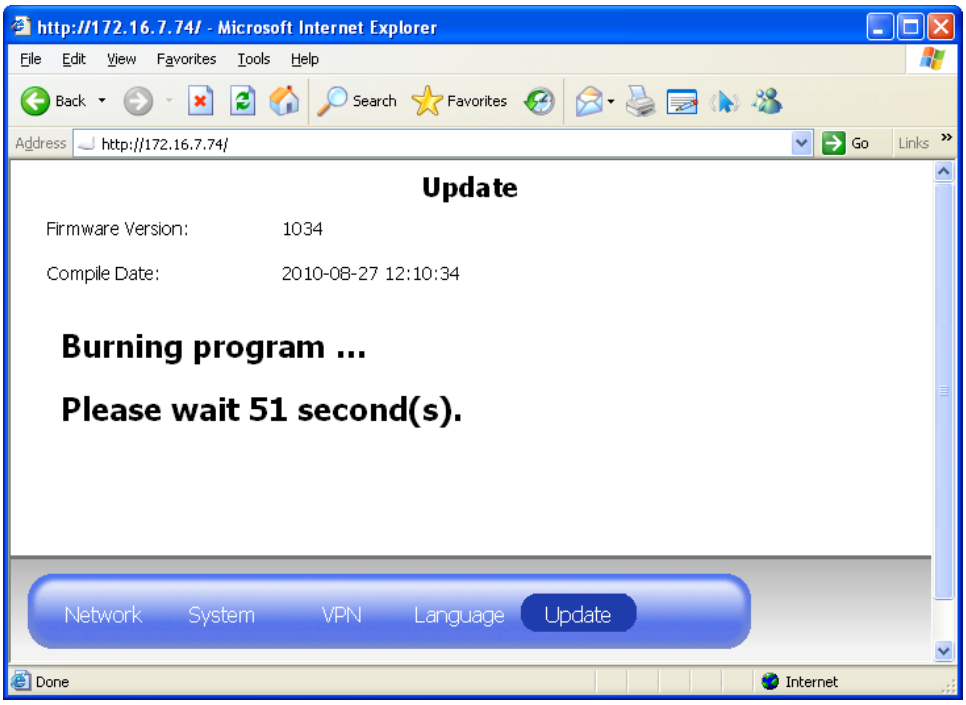
File Updated: Browse...

Update

http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Network System VPN Language Update
Internet

Figure 23: The Upgrade Page in the Linux Runtime

Choose the firmware file and click the “Update” button. It will start to upload the firmware and write to the flash. It will start to count down. At this time, the user should not cut off the power of the HSC04.



Update

Firmware Version: 1034

Compile Date: 2010-08-27 12:10:34

Burning program ...

Please wait 51 second(s).

http://172.16.7.74/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://172.16.7.74/ Go Links
Network System VPN Language Update
Done
Internet

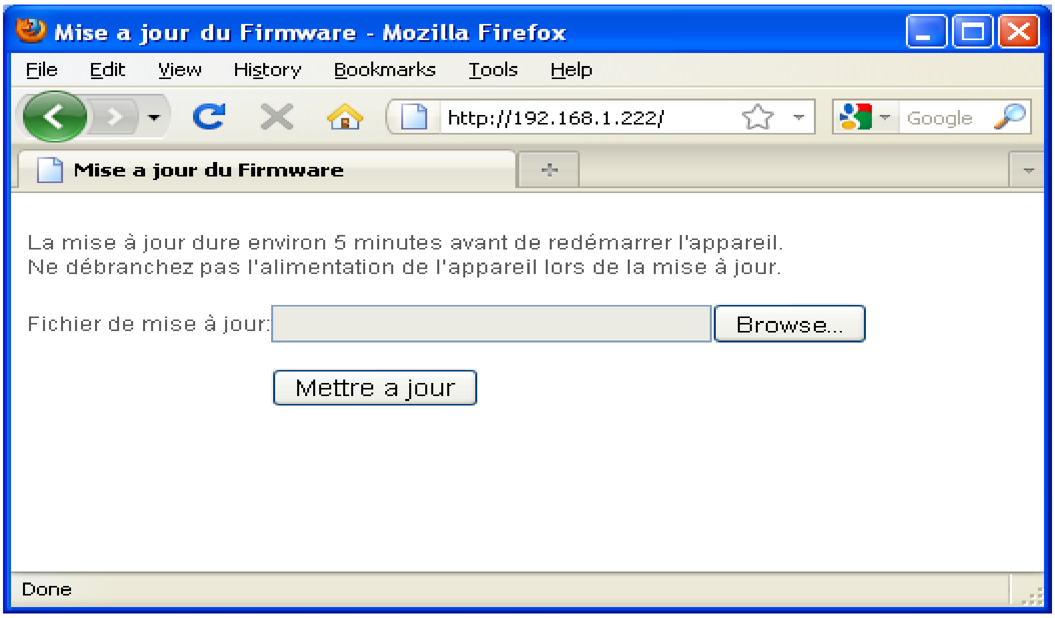
Figure 24: Upgrade and Count Down to Reboot.

After the count down, the browser will auto re-connect to the homepage of the HSC04.
When the firmware is writing to the Flash, the power LED is light on red.

7.5.2. In the Boot Time

In the boot time, if the HSC04 found error image cause to fail boot. The HSC04 will auto into the upgrade mode. At this moment, the connection LED will flash on green and red.
You can manual to into upgrade mode in boot time, press the reset button, and then press the connect button over three times, check the connection LED to make sure the HSC04 into the upgrade mode successes.

Using the browser connect to 192.168.1.222.


Mise a jour du Firmware - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.222/
Google
Mise a jour du Firmware

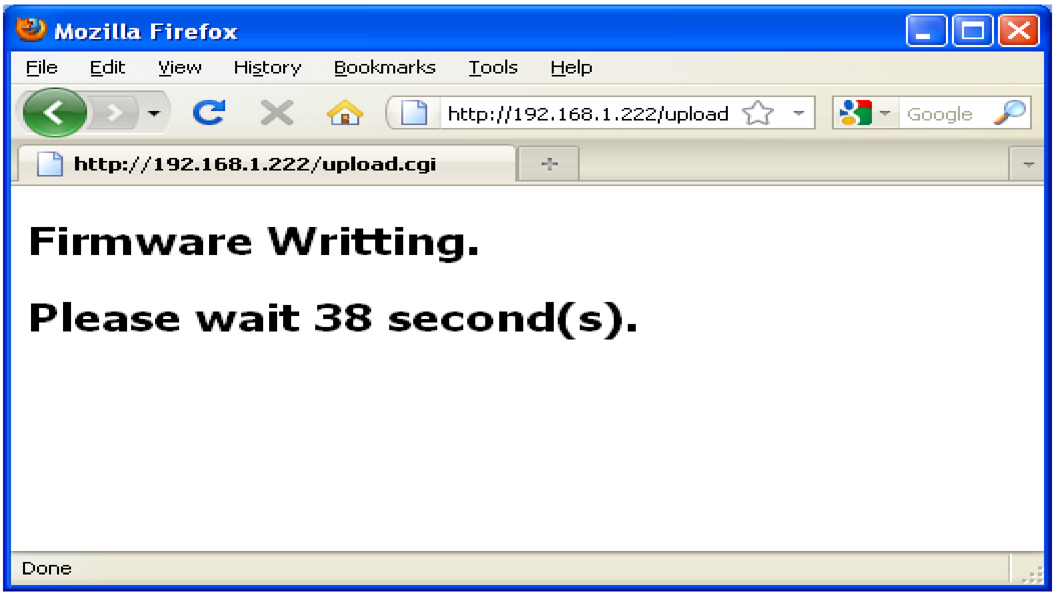
La mise à jour dure environ 5 minutes avant de redémarrer l'appareil.
Ne débranchez pas l'alimentation de l'appareil lors de la mise à jour.

Fichier de mise à jour:

Browse...
Mettre a jour
Done

Figure 25: The upgrade page in the bootloader runtime.

Choose the firmware file and click the "Mettre a jour" button. It will start to upload the firmware and write to the flash. It will start to count down. At this time, the user should not cut off the power of the HSC04.



Firmware Writting.

Please wait 38 second(s).

Figure 26: The count down in the bootloader runtime.

After the count down, the browser will re-connect to 192.168.1.222. But if the HSC04 has enabled the DHCP function, the IP will be changed, the user needs to connect to the newest IP manually.

8. U-Net Bind

The bind is an operation of the U-Net, it is for include the other U-Net devices to the HSC04.

Here will describe how to use the connection button to operate the binding function.

- Start binding:
  Push the connection button once. The connection LED will start to blink the green light.
- Bind device:
  Let other U-Net device start binding, For example: the SR801, press the disarm key and hold over three seconds. If bind successful, the connection LED of the HSC04 will stop blinking, and turn on 2 seconds, and then turn off 2 seconds.
- Cancel binding:
  In the binding mode, the connection LED is blinking, push the connection button again, the connection LED will quickly flashing. It will stop binding.

- Binding timeout:
  If enter the binding mode over 30 seconds, it will occurs the timeout, the connection LED will quickly flashing in 4 seconds.

The user can read the device information from the browser.
Ex: http://192.168.1.100/unet/deviceinfo.cgi?uid=0
It will list all device information in the HSC04.

```
0200 OK uid=0
--device
uid=2
type=7:Remote
code=7124/7801/7803/7128
subcode=0000
rssi=3
battery=0
mac=01:90:02:04:0F:00:00:30
partialarm=0:0
alias=Remote
posx=0
posy=0
width=0
height=0
entrydelay=0
```

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/ TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

Labeling requirements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF exposure warning

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