Firmware

Update Manual

Version 1.0.0 June 2019

iWSN-2200-E

(iWSN Wireless Data Concentrator)

Table of Contents

Important Information

Warranty

All products manufactured by ICP DAS are under warranty regarding defective materials for a period of one year, beginning from the date of delivery to the original purchaser.

Warning

ICP DAS assumes no liability for any damage resulting from the use of this product.ICP DAS reserves the right to change this manual at any time without notice. The information furnished by ICP DAS is believed to be accurate and reliable. However, no responsibility is assumed by ICP DAS for its use, not for any infringements of patents or other rights of third parties resulting from its use.

Copyright

Trademark

Names are used for identification purpose only and may be registered trademarks of their respective companies.

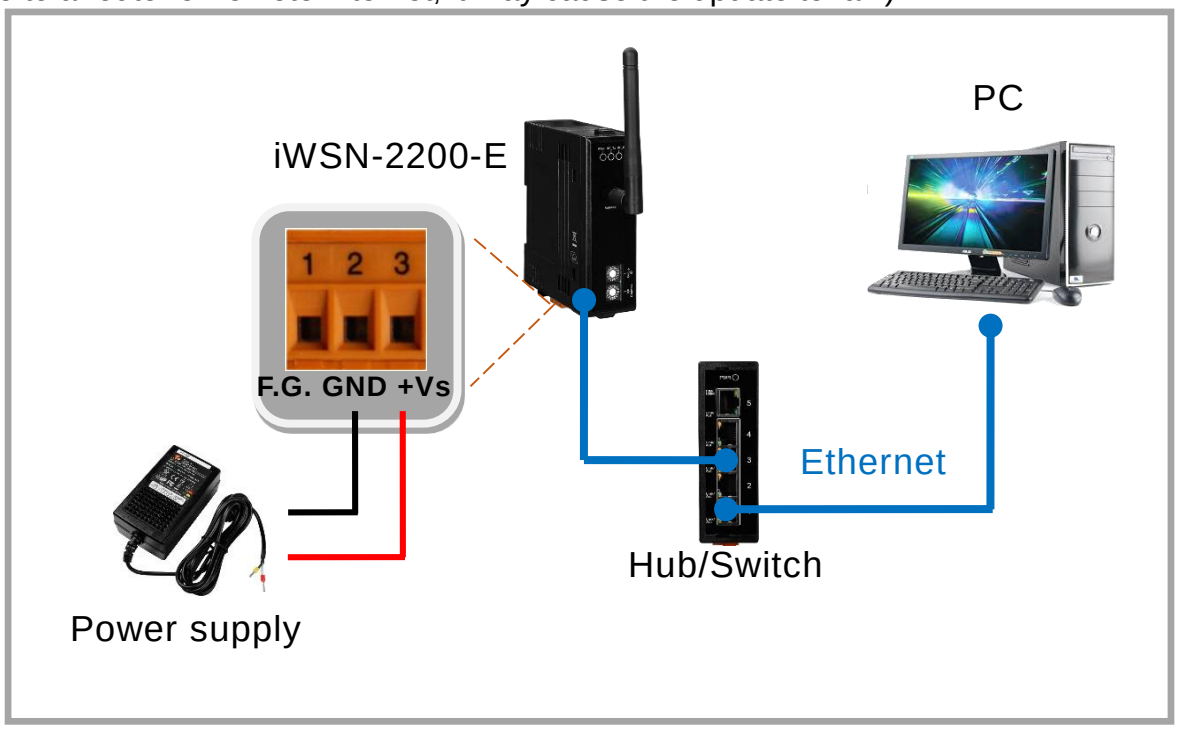
Contact us

If you encounter any problems while operating this device, feel free to contact us via mail at: service@icpdas.com .We guarantee to repond within 2 working days.

1. Getting Started

Before beginning to update Firmware, the wiring test, Ethernet configuration and search/Modbus utility driver installation procedures must first be fully completed. Follow the procedure described below:

Step 1: Connect both the module and the Host computer to the same sub-network or the same Ethernet Switch, and then supply power (+12 to +30 VDC) to the module. (Do not connect the module to a router or remote Internet, it may cause the update to fail.)



Step 2: Downloaded the **eSearch Utility** and installed according to the installation instructions. The eSearch Utility can be obtained from the ICP DAS web site. The location of the download addresses is shown below:

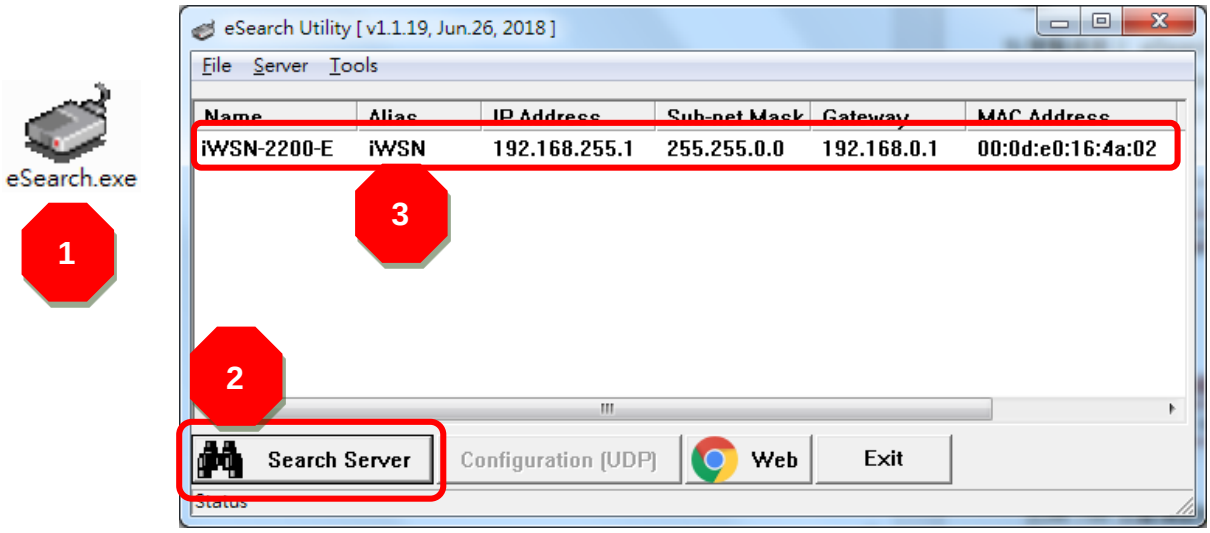
http://ftp.icpdas.com/pub/cd/tinymodules/napdos/software/esearch/

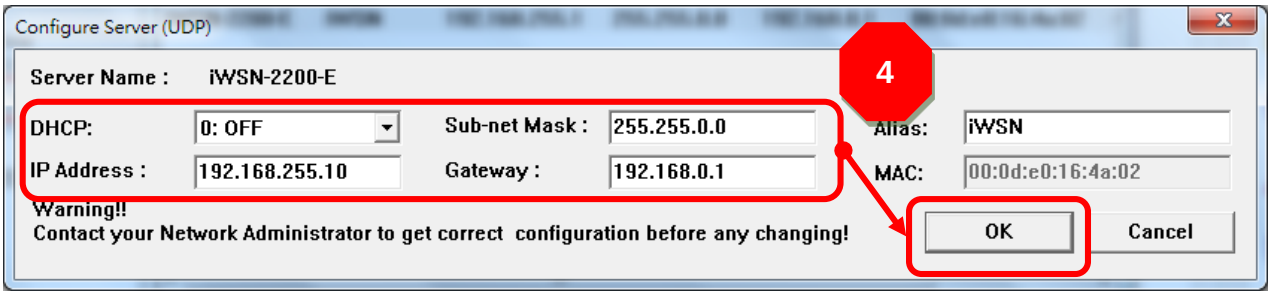
Step 3: Execute the eSearch Utility to search for the module and configure the correct and effective network settings.

1. Double click the eSearch Utility shortcut on the desktop.
2. Click the **"Search Servers"** button to search your module.
3. Once the search process is complete, double-click the name of the module

to open the **"Configure Server"** dialog box.

4. Enter the network settings information, including the **IP, Mask and Gateway addresses**, and then click **"OK"** button.





2. Start updating Firmware

The module can directly update the Firmware via Ethernet. The update procedure is as follows.

2.1 Firmware updating

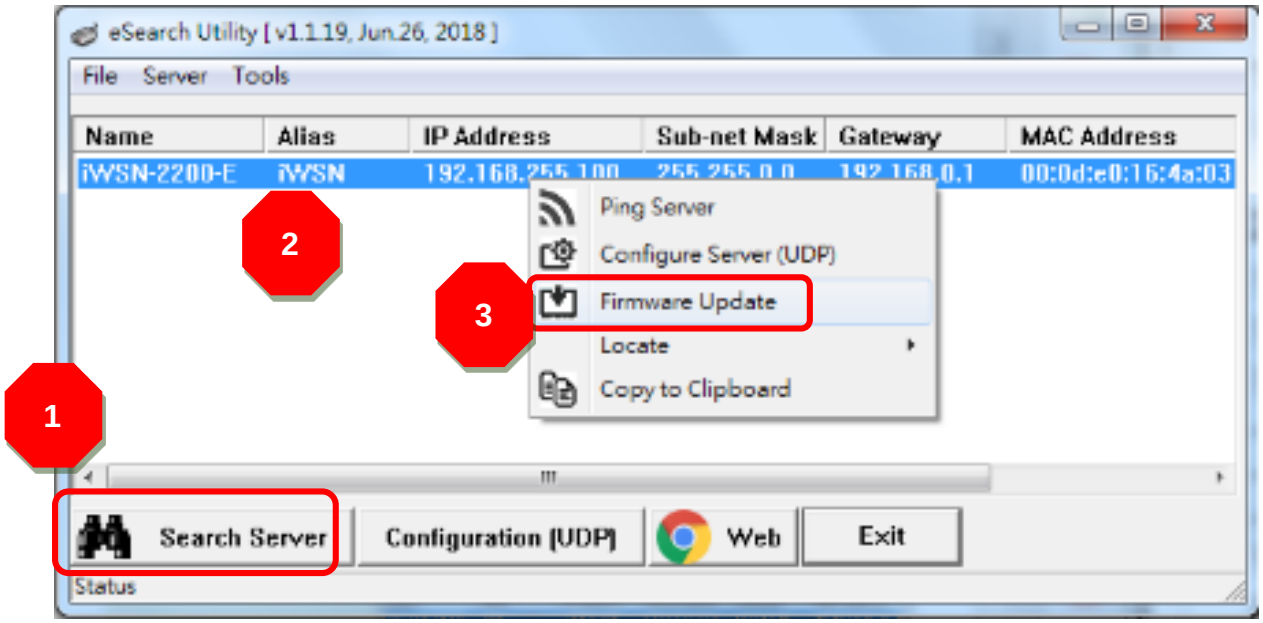
The firmware update can fail when the computer has multiple network interfaces (e.g., LAN and Wi-Fi). Therefore, enable only one network interface for updating the firmware, and temporarilyturn off other network interfaces, firewalls, and anti-virus software first. Two methods can be used to update the firmware: **“Local FirmwareUpdate” (traditional)** and **“Remote Firmware Update” (TeamViewer)**. The Local Firmware Update method requires the user to manually adjust the position of the Init/Run Switch and reboot the module in order toinitializethe firmware update. Refer to Section 2.1.1“Local Firmware Update”for more details. The Remote Firmware Update method allows the user to initialize the module via a web interface withoutneeding to adjust the hardware switch. Initialization via the web interface is useful when the module is installed ata remote site and can be accessed viatheTeamViewerapplication installed on a remote PC. Refer to Section 2.1.2 “Remote Firmware Update” for more details.

2.1.1 Local Firmware Update

Step 1: In the eSearch Utility, click the **“Search Servers”** button to searchthe for any modules connected to the network .

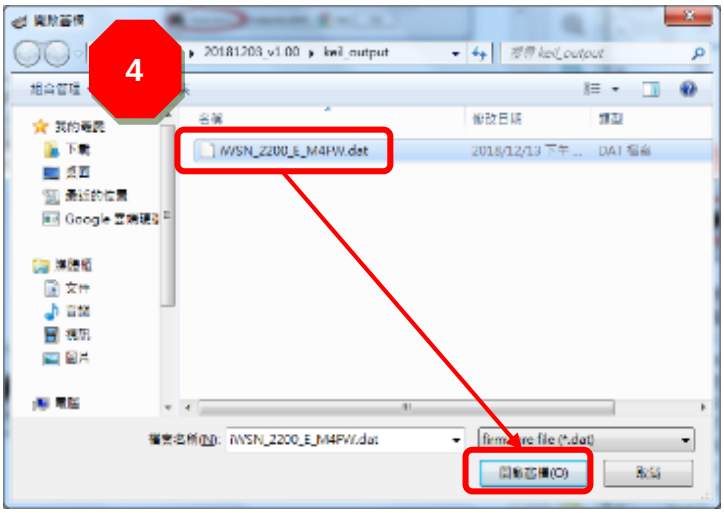
Step 2: Right clickon the name of the module to be updated.

Step 3: Select the **“Firmware Update”** item from the popup menu and the **“Open”** dialog box will be displayed.



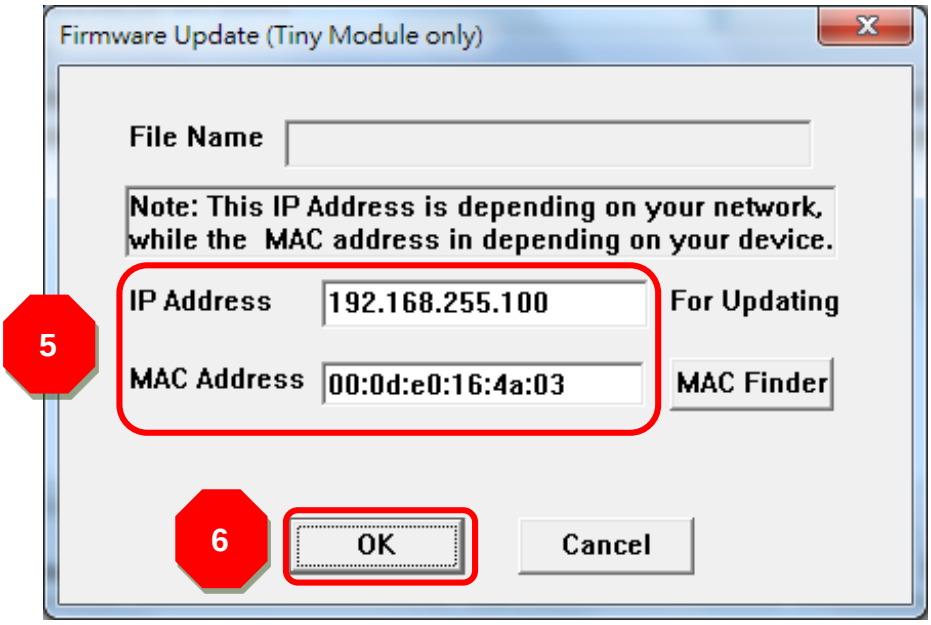
Step 4: In the **“Open”** dialog box, select the firmware file (iWSN_2200_E_M4FW_vxxx.dat) that will be used to update the moduleand then click the **“Open”** button.

Downloadthe Firmware File.



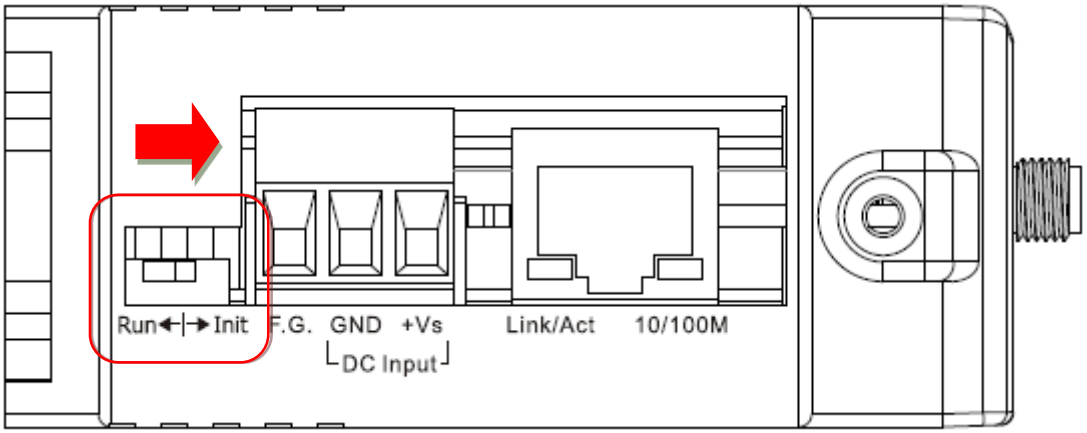
Step 5: Assign a valid IP Address (canbe different with the current IP) and the factory-default MAC Address for the module. If this IP address is invalid (e.g. IP Address: 0.0.0.0) or a user-defined MAC addressis assigned. Refer to note2 and note3 for more details.

Step 6: Click the “OK”button.



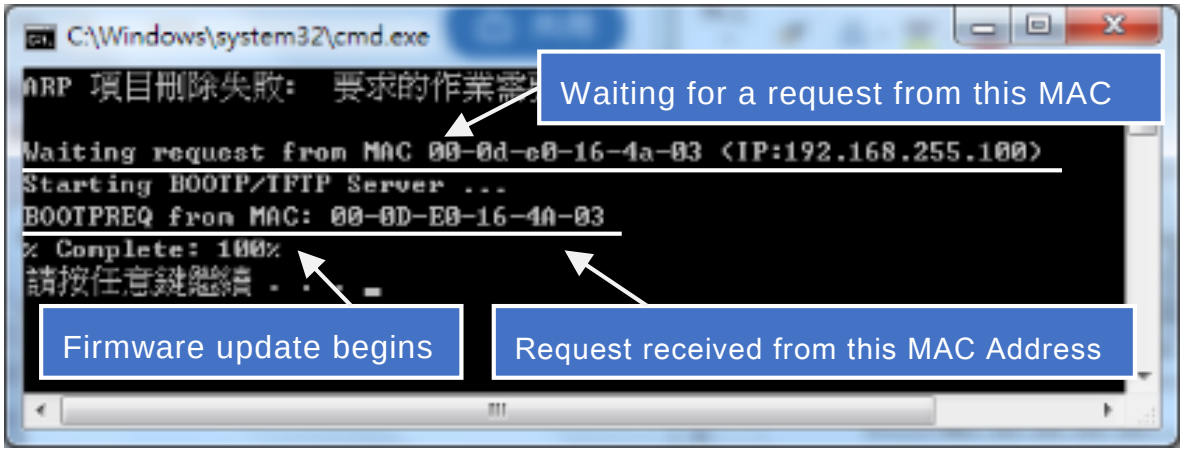
Step 7: You are now ready to update the firmware. A Command Prompt windows will be displayed the progress of the update.

Step 8: Set the **"Init Switch"** on the module to the **"Init"** position.



Step 9: Power-onreset the module in **"Init Mode"** to initiatethe update.

Step 10: Confirm that the two MAC addresses (factory-default) listed in the Command Prompt window, **"Waiting request from MAC x.x.x.x"** and **"BOOTPREQ from MAC: x.x.x.x"**, are the same, as indicated in the image below. If these addresses do not match, the update cannot proceed. Refer to note4 below for more details.



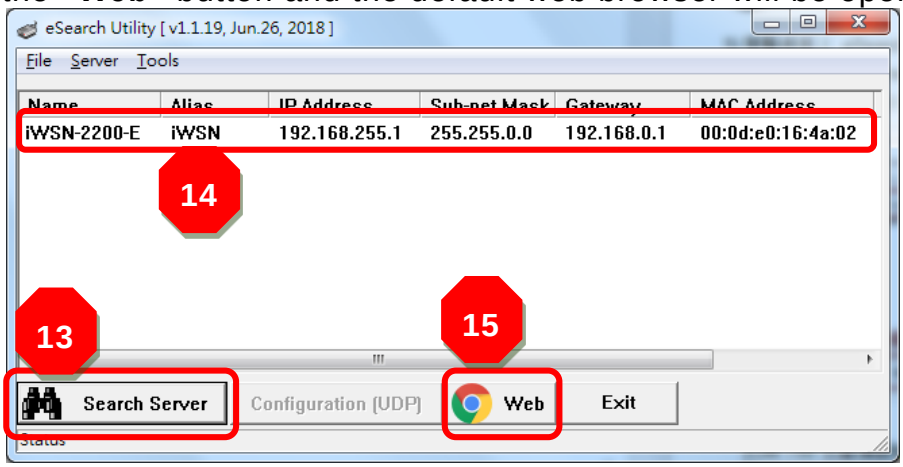
Step 11: Once the update is complete (i.e., when the progess indicator reaches 100%), set the **“Init Switch”** to the **“Run”** position.

Step 12: Power-on reset the module to operate the module in **“Run Mode”**.

Step 13: In the eSearch Utility, search for the module again to verify thatit is functioning correctly. Note that the network settings for the module may need to be reconfigured after updating the firmware. Refer to Step3 in Chapter1 above for more details.

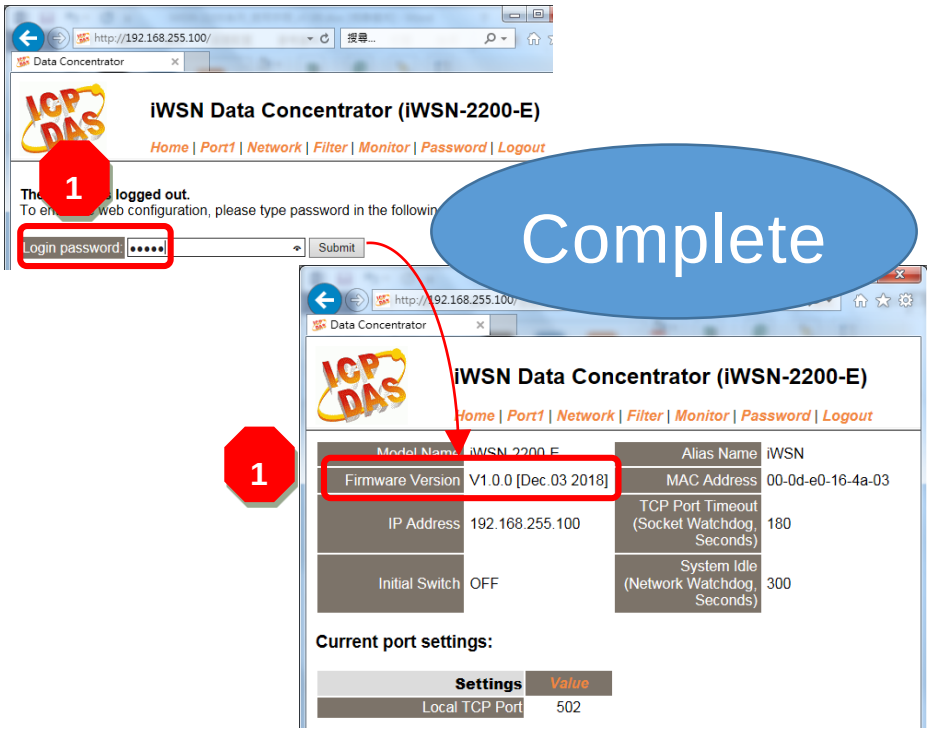
Step 14: Click the name of the module to highlight it.

Step 15: Click the **“Web”** button and the default web browser will be opened.



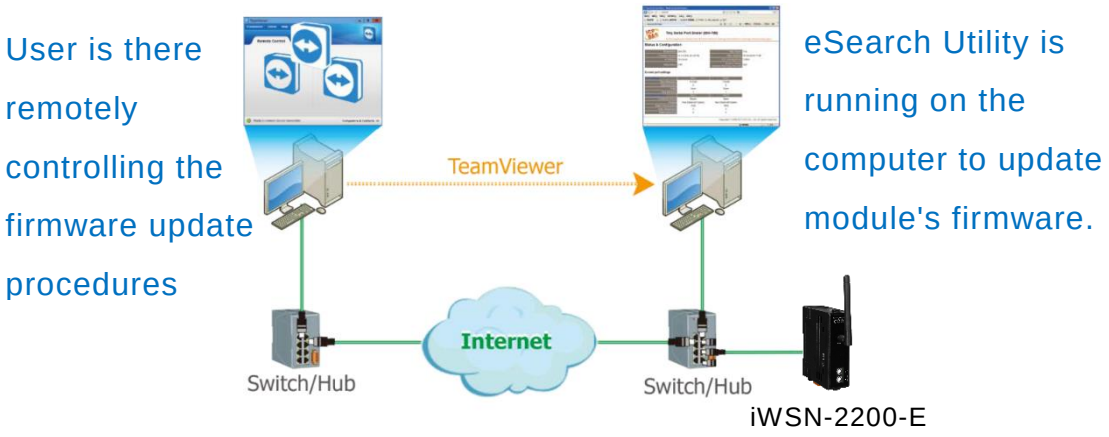
Step 16: Login to the web configuration pages for the module (use the default password **“admin”**).

Step 17: Verify that the firmware version and date details are correct.



2.1.2 Remote Firmware Update

In order to perform a Remote Firmware Update, use an application that allows an external system to be remotely controlled, such as TeamViewer, to createa connection between the localand the remote system.**Note that all firmware update procedures need to be carried out on the remote system.**

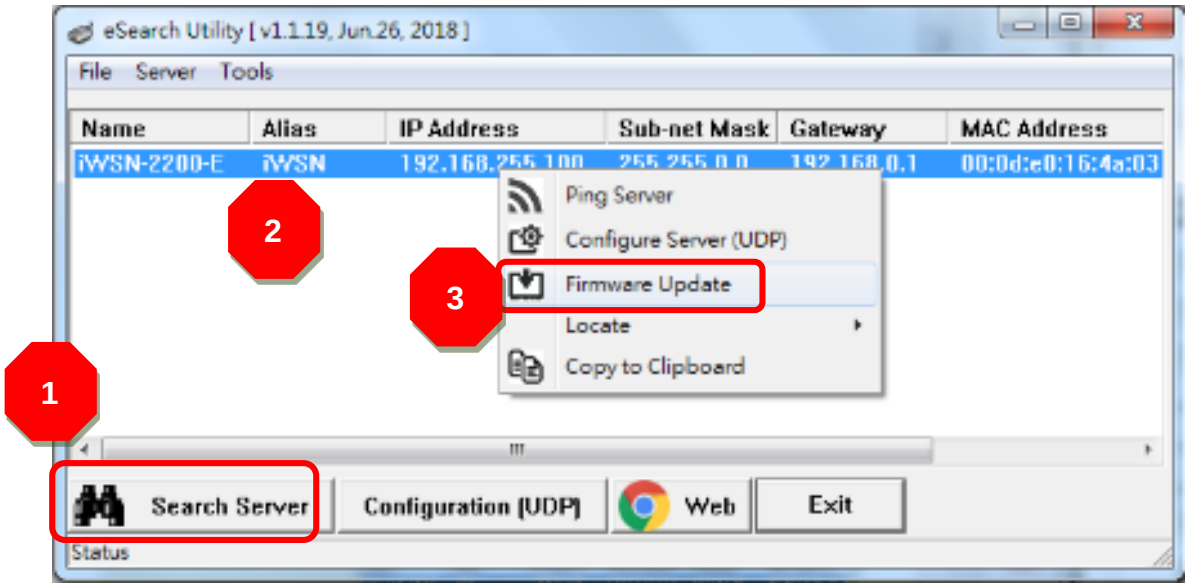


Follow the procedure described belowto update firmware of the module on the remote PC:

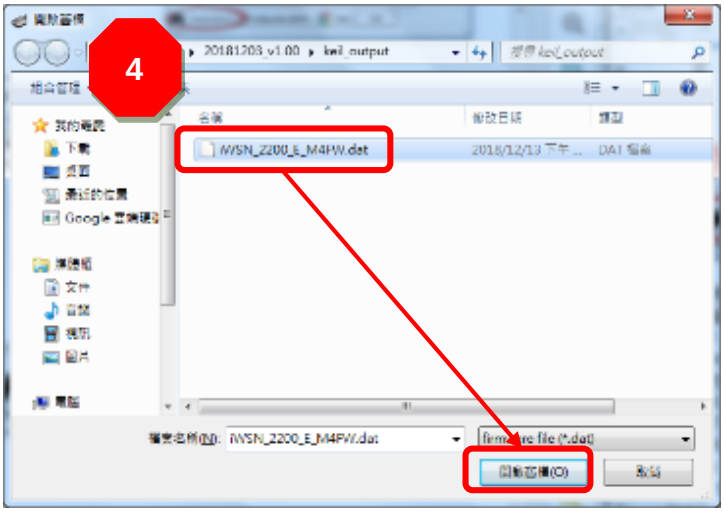
Step 1: In the eSearch Utility, click the **"Search Servers"** button to search for any modules connected to the network. (The network settings the module are described in Step 3 of Chapter1)

Step 2: Right click the name of the module to be updated.

Step 3: Select the **"Firmware Update"** item from the popup menu and the **"Open"** dialog box will be displayed.

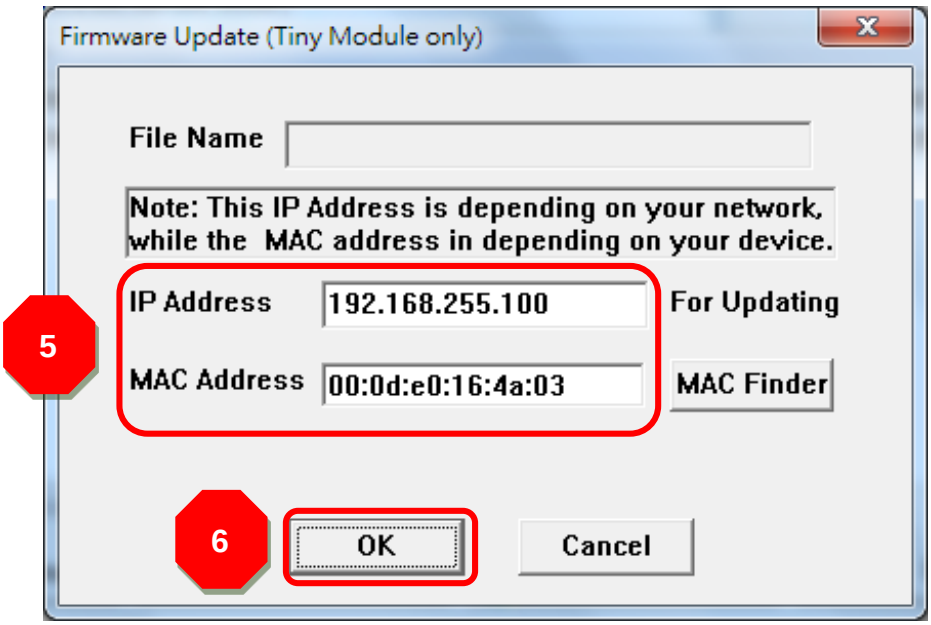


Step 4: In the **"Open"** dialog box, select the firmware file (iWSN_2200_E_M4FW.dat) that will be used to update the module and then click the **"Open"** button.



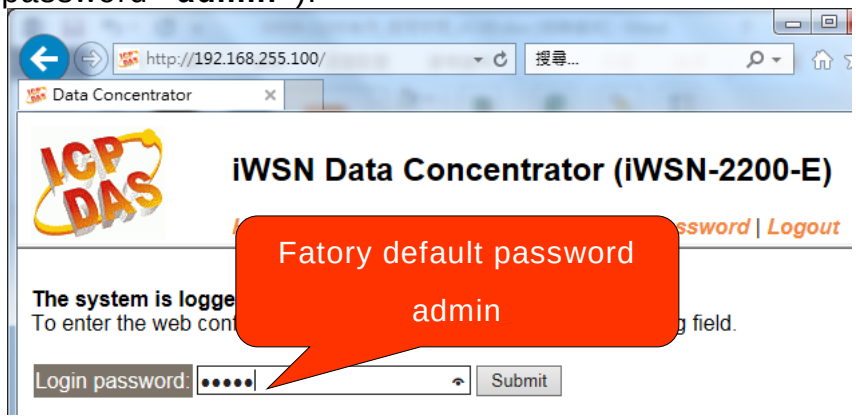
Step 5: Assign a valid IP Address (can be different with the current IP) and the factory-default MAC Address for the module. If this IP addressis invalid (e.g. IP Address: 0.0.0.0) or a user-defined MAC addressis assigned. Refer to note 2 and note 3 for more details.

Step 6: Click the **"OK"** button.



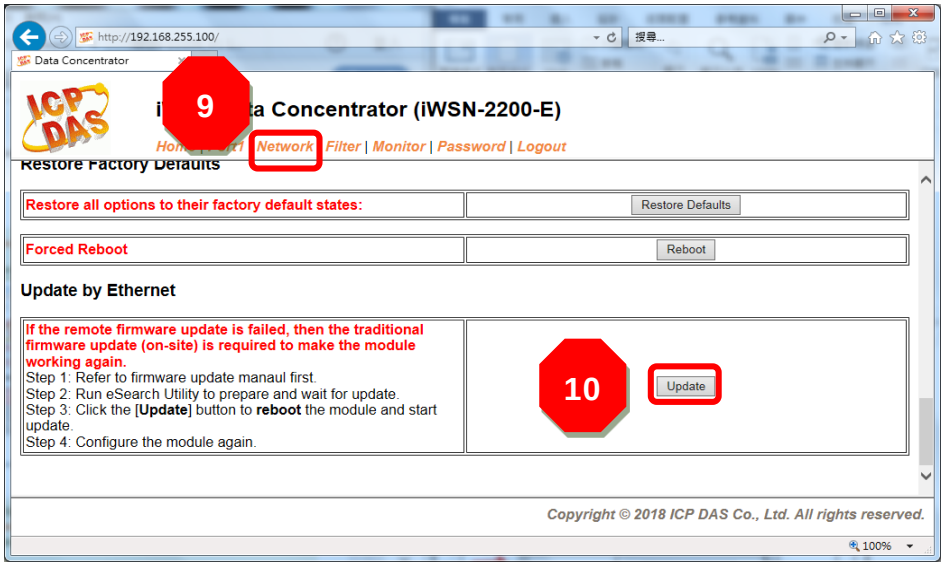
Step 7: You are now ready to update the firmware. A Command Prompt windows will be displayed the progress of the update.

Step 8: Open a web browser such as Internet Explorer or Firefox and enter the URL for the module in the address bar of the browser and log in to the web configuration pages (use the default password **"admin"**).



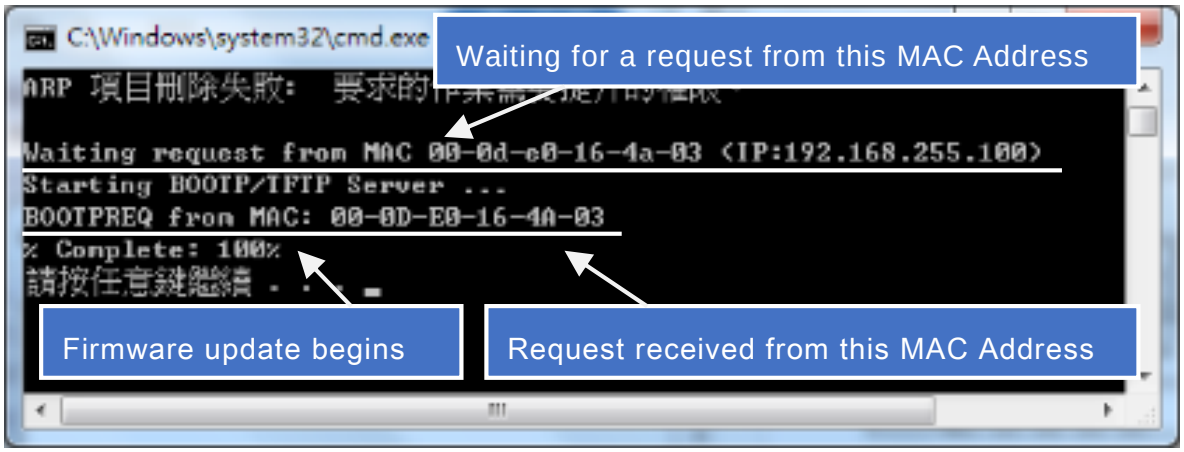
Step 9: Click the **"NetworkSetting"** tab to displaythe Network Settings page.

Step 10: Click the **"Update"** button in the **"RemoteFirmwareUpdate"** section to start the update.



Step 11: Confirm that the two MAC addresses (factory-default) listed in the Command Prompt window, **“Waiting request from MAC x.x.x.x”** and **“BOOTPREQ from MAC: x.x.x.x”**, are the same, as indicated in the image below. If these addresses do not match, the update cannot proceed. Refer to note4 below for more details.

Step 12: Once the update is complete (i.e., when the progess indicator reaches 100%), close the Command Prompt window.

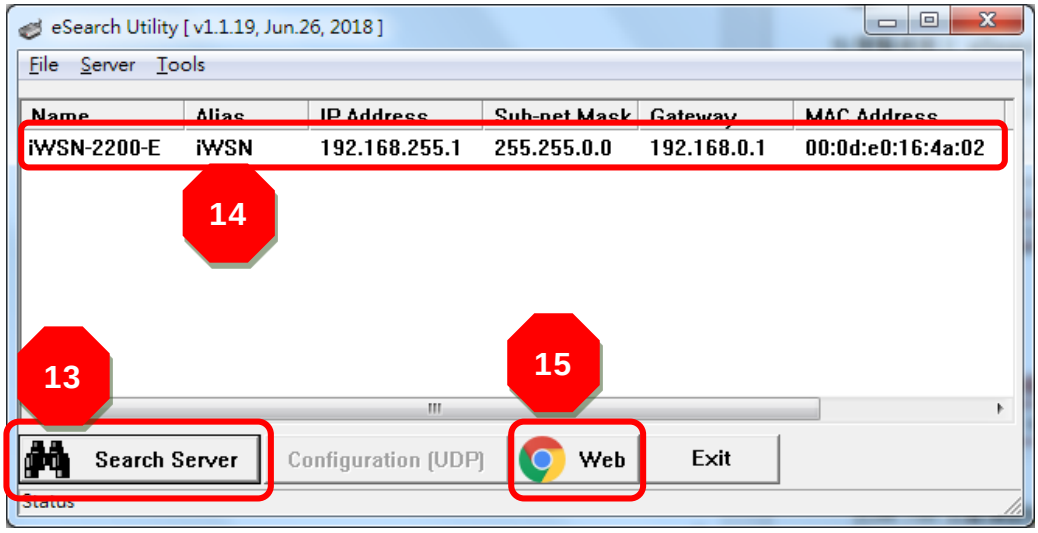


Note: If the Remote Firmware Update methodfails, please refer to Section 3.1 Firmware update in BOOT mode (local operation) to restore the module.

Step 13: In the eSearch Utility, search for the module again to verify thatit is functioning correctly. Note that the network settings for the module may need to be reconfigured after updating the firmware. Refer to Step 3 in Chpater1 above for more details.

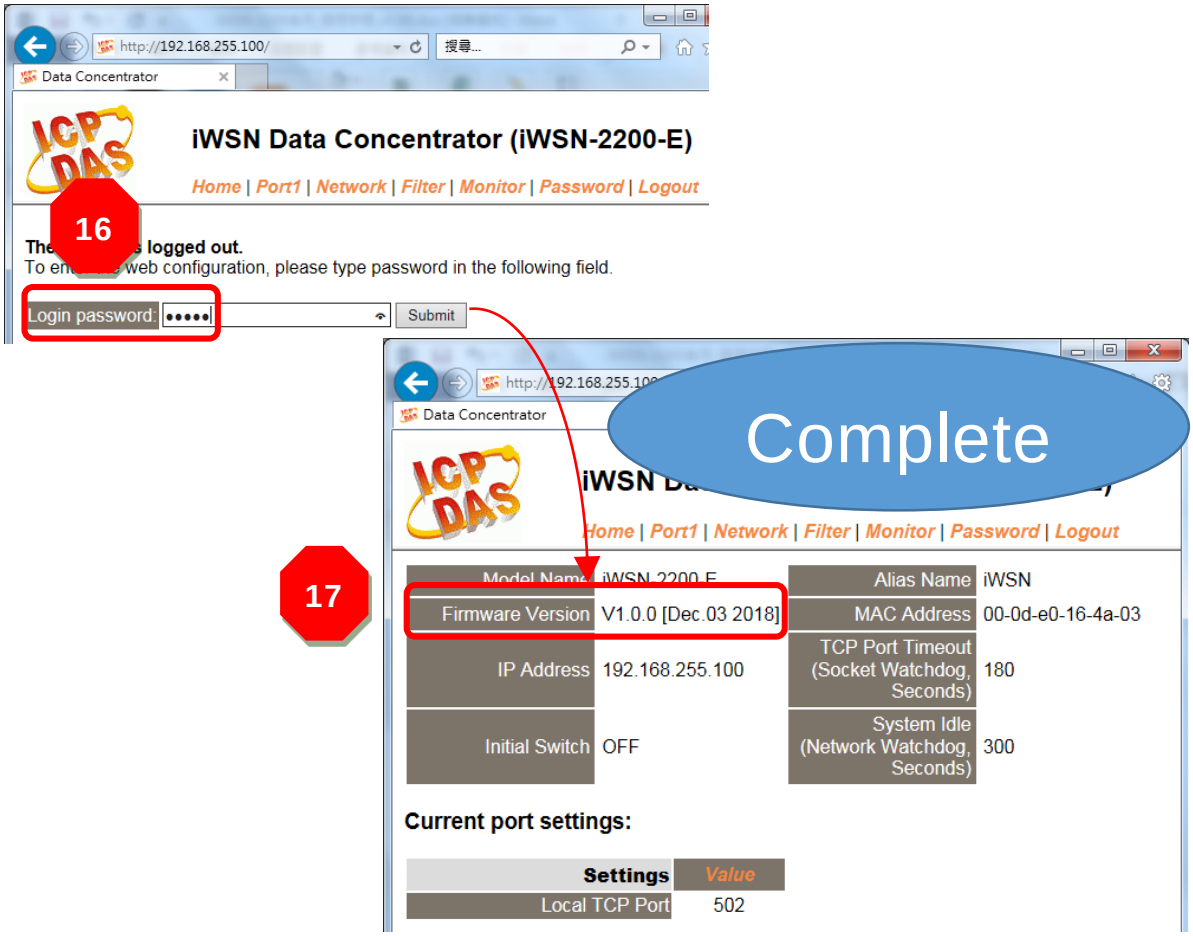
Step 14: Click the name of the moduleto highlight it.

Step 15: Click the **"Web"** button and the default web browser will be opened.



Step 16: Login to the web configuration pages for the module (use the default password **"admin"**).

Step 17: Verify that the version and date details for the firmware are correct.

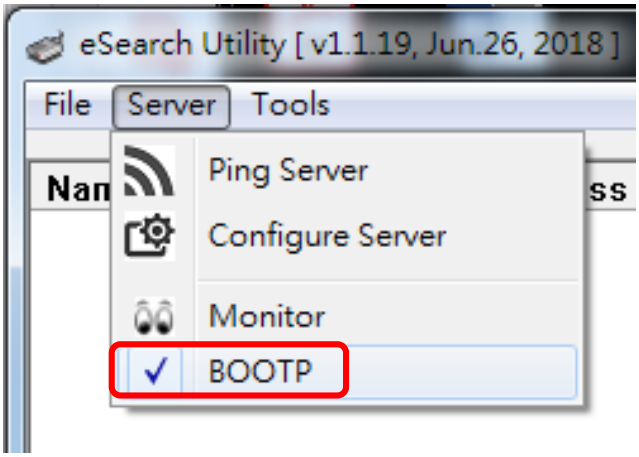


3. Troubleshooting

3.1. Firmware update in BOOTP mode

If the module is not functioning correctly (e.g.there isno response to the searchrequest, orifthe system LED is always displayed as either offor on), please download a newimage of the firmware from the ICPDAS websiteand then update the firmware for the module usingthe following procedure.

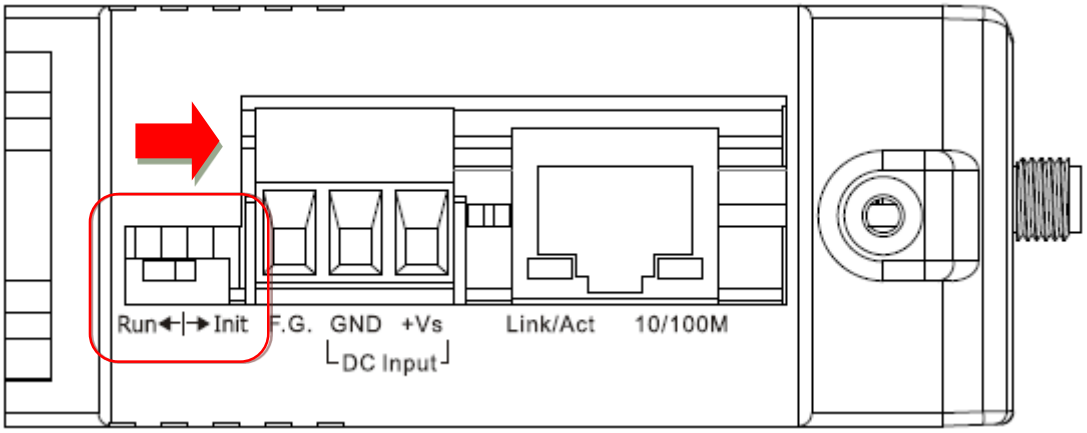
Step 1: In the eSearch Utility, select the **"BOOTP"** item from the **"Server"** menu. A check mark should be displayed next to the item after it has been selected.



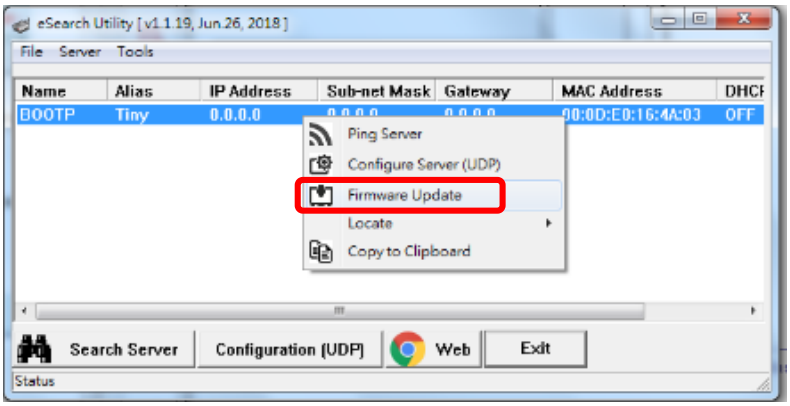
Step 2: Set the **"Init Switch"** to the **"Init Mode"** position.

Step 3: Power-on and reboot the module and then click the **"SearchServers"** button to search for the module at the same time.

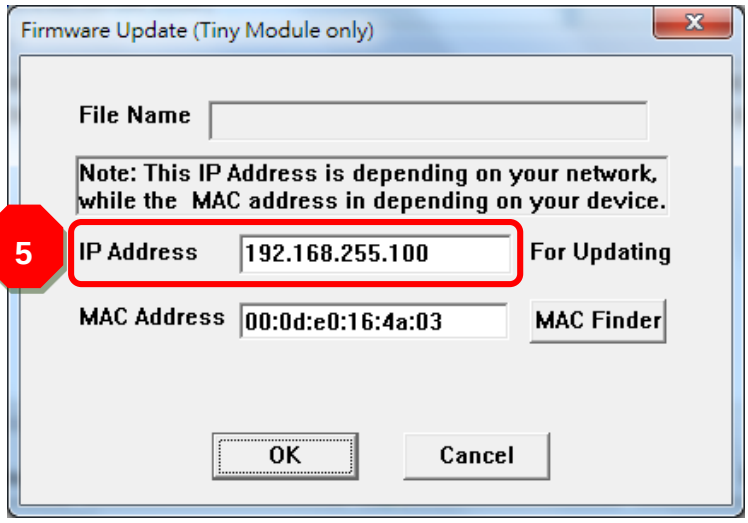
Note: the module sends BOOTP messages about 5 seconds when booting in Init Mode.If this step is not successful, reboot the module and execute the search again.



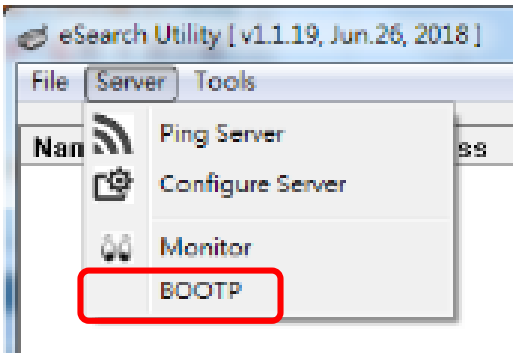
Step 4: Right click on the name **"BOOTP"** and then select the **"Firmware Update"** item from the popup menu.



Step 5: Refer to Steps 4 to 17 in **"Chapter 2-Firmware Update Procedure"** to complete the update process. Note, the module will response with no IP address in the BOOTP mode. User has to assign a valid IP manually in step 5.



Step 6: After updating the firmware, disable BOOTP mode from the eSearch utility. By selecting **"BOOTP"** item from the **"Server"** menu.



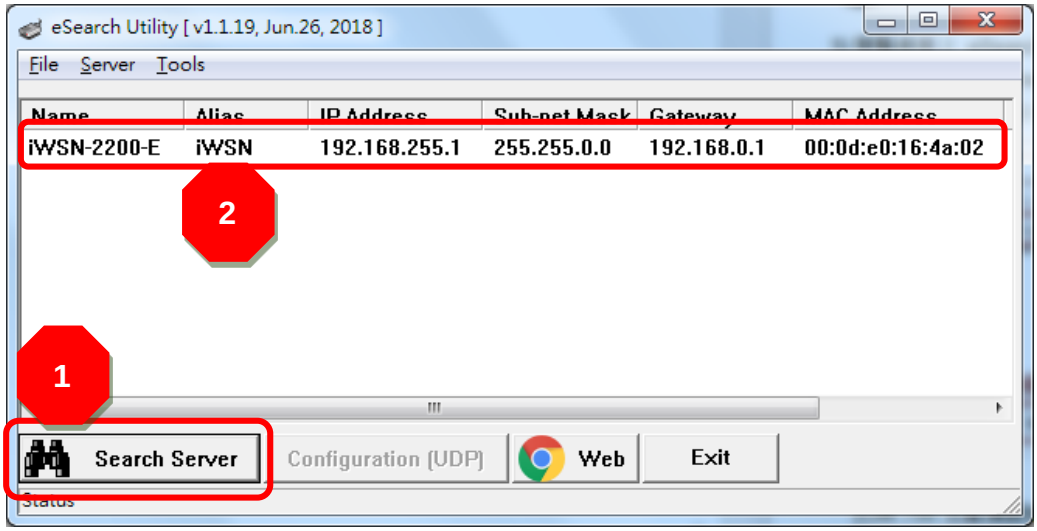
3.2. How to update Firmware when the Different Network Segment for IP Address of the tGW-700 and Host PC.

For example, the first time to get the module, the factory default IP address is 192.168.255.1, but the host PC IP address is 10.0.8.31, refer to the following two methods to update firmware.

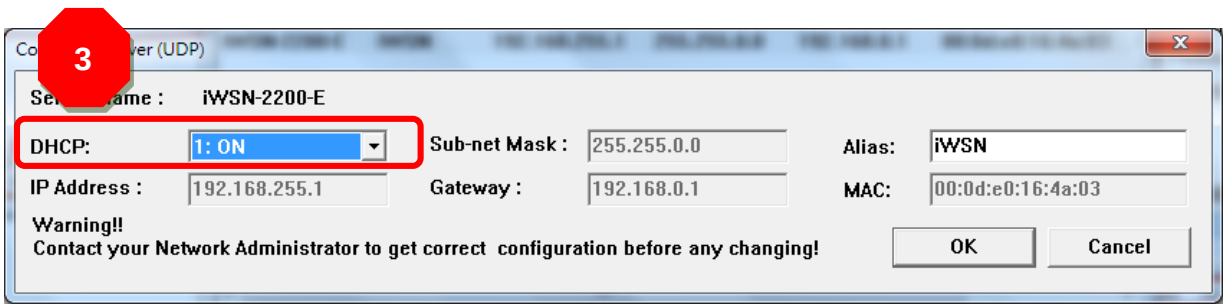
Method 1: Using**"Dynamic Host Configuration Protocol (DHCP)"**to automatically assigns an IP address to module. Follow the procedure described below:

Step 1: Run the eSearch Utility to search for any modules to the network

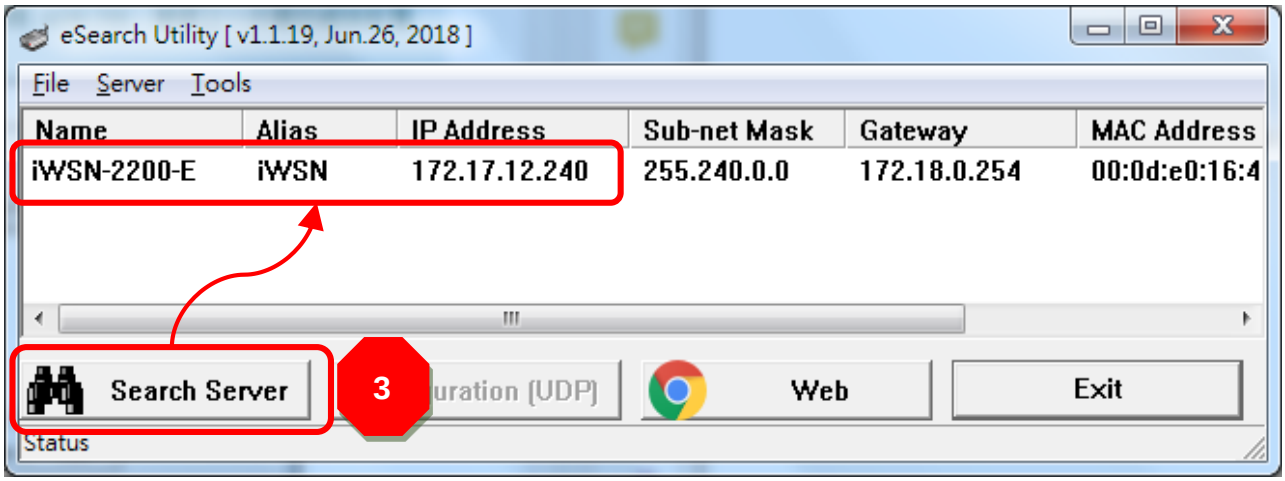
Step 2: Double click the name of module to open the **"Configure Server (UDP)"** dialog box.



Step 3: Select the **"1: ON"** option from the **"DHCP:"** drop-down menu and click the **"OK"** button.



Step 4: Wait 2 seconds and then click the **"Search Servers"** button again to ensure the module is working well with new configuration.

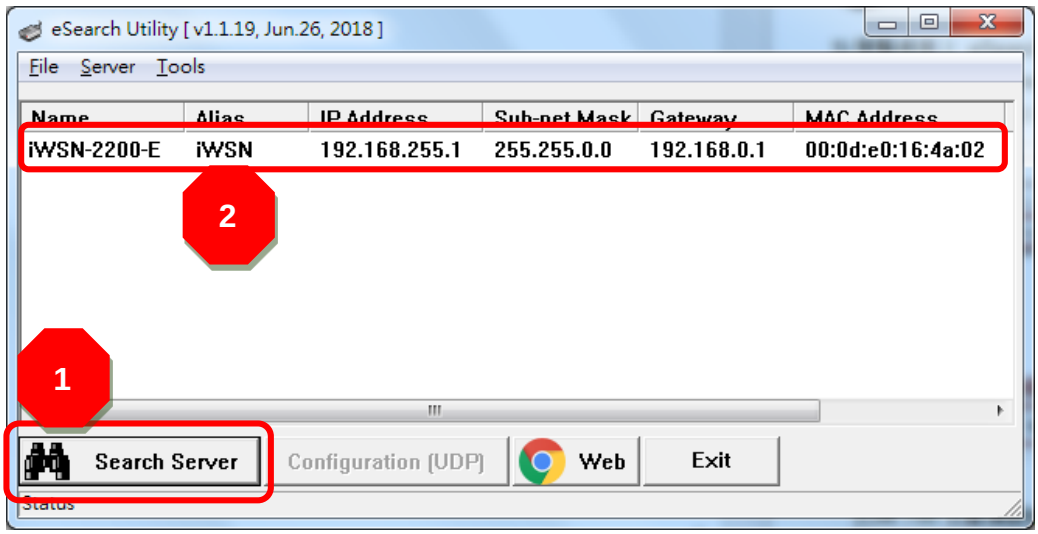


Step 5: Refer to **"Chapter 2-Firmware Update Procedure"** for details of how to complete the update process.

Method 2: Using**"Manual configuration"** to assigns an IP address to module. Follow the procedure described below:

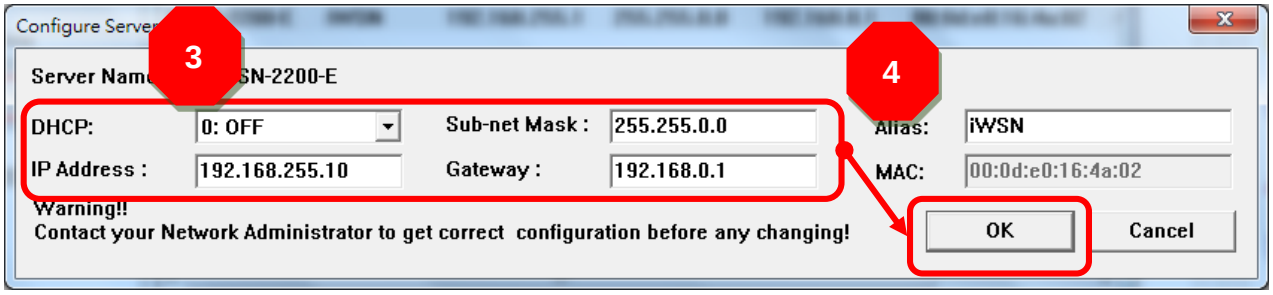
Step 1: Run the eSearch Utility to search for any modules to the network.

Step 2: Double click the name of module to open the **"Configure Server (UDP)"** dialog box.

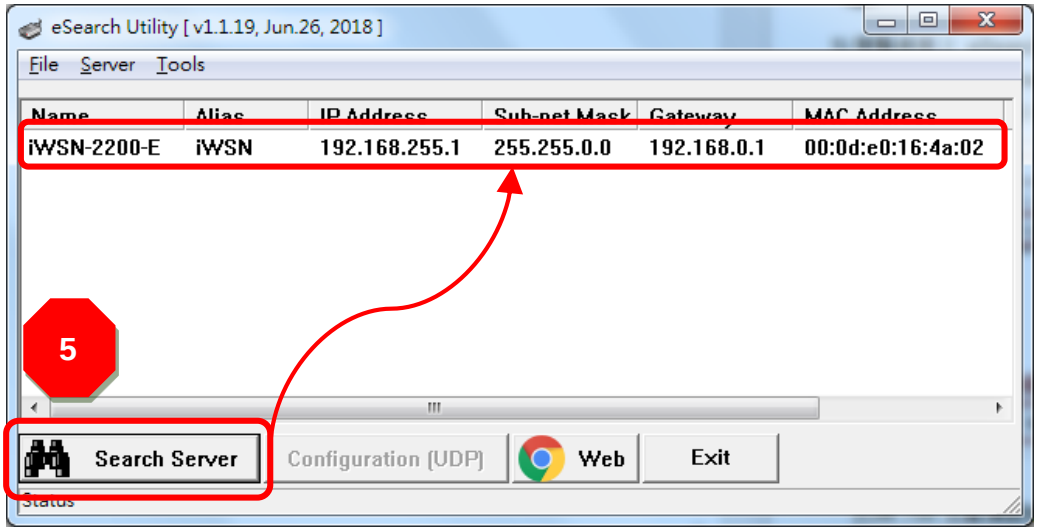


Step 3: Select the **“0: OFF”** option from the **“DHCP:”** drop-down menu.

Step 4: Contact your Network Administrator to obtain a correct network configuration (such as IPAddress/Sub-net Mask/Gateway). Enter the network settingsand click the **“OK”** button.



Step 5: Wait 2 seconds and then click the **“Search Servers”** button again to ensure the module is working well with new configuration.



Step 6: Refer to **“Chapter 2-Firmware Update Procedure”** for details of how to complete the update process.

4. Additional Information

The code contained in the boot loader, which isused to update the firmware image, is not part of the firmware it-self. This means that, the firmware can still be updated even if the built-in firmwarehas been corruptedor does not exist. If the firmware update fails, simply executethe update procedures again in BOOTP mode, as described in Chapter 3, and the update should be successful.

The module obtains the IP address assigned by the user and retrieves thefirmware image through the utility program. Note: that when updating the firmware, the module uses the factory-default MAC address rather than any user-defined MAC addresses. The module has a built-in flash protection feature that prevents any modification to the firmware stored in the flash memory, before attempting to update the firmware, the "**Init Switch**" should be set to the "**Init**" position and then the module can be **powered-on and rebooted** to disable the flash protection. Since the flash memory then becomes writable, the firmware can be updated via the Ethernet network.

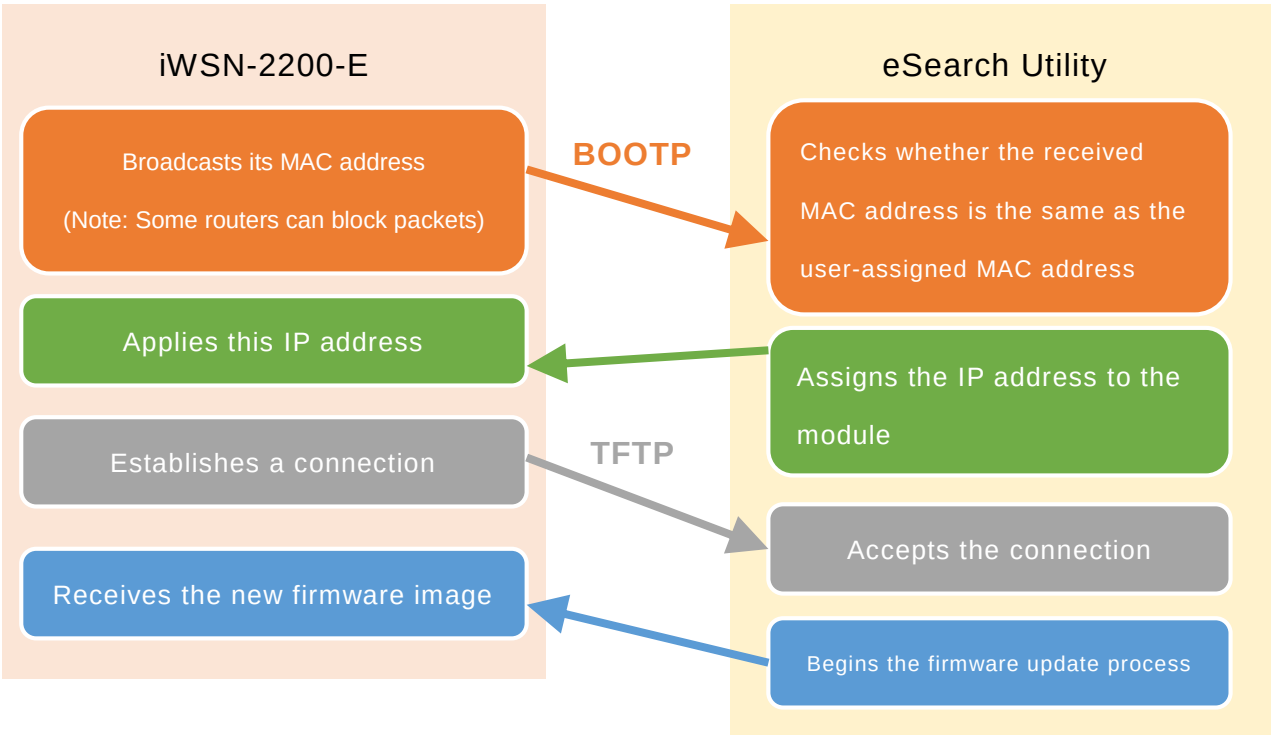
Mode	Flash Protection	Firmware Update	Configuration
Init	No	Yes	Factory-default
Run	Yes	No	User-defined

Note:

Note 1: If the IP address settings do not work correctly (e.g.there is no response to a ping command), please contact your network administrator to obtain a valid IP address for the module.
Note 2: If the settings displayed in the IP address field of the firmware update window is incorrect or invalid (e.g. IP address: 0.0.0.0), then a valid IP address must be manually specified for the module in order to process the update operation. Please contact your network administrator toobtain avalid IP address before proceeding.
Note 3: When updating the firmware, the factory-default MAC address is used rather than the user-defined MAC address. Thus, the MAC address (user-defined) displayed in the firmware update window may not be the one required. If this is the case, the

factory-default MAC address should be manually entered into the MAC Address field, or restore theMAC address to the factory-defaultsettings via the web configuration pages.

Note 4: The **"BOOTPREQ from MAC: xx-xx-xx-xx-xx-xx"** message indicates there is a module with the factory-default MAC address "xx-xx…"that is asking for the firmware to be updated. The update process will not begin if you assign a user-defined MAC address in the firmware update window, since the addresses do not match. If this situation occurs, repeat the update procedure and manually enter the factory-default MAC address in the firmware update window, as described in **Step 5**. The firmware update procedure is illustrated in the figure below.



Note 5: BOOTP (Bootstrap Protocol) is defined in RFC-951 and usesUDP ports67 and 68.

Note 6: ◦ TFTP (Trivial File Transfer Protocol) is defined in RFC-1350 and uses UDP port 69.