atop
Technologies

Atop Technologies, Inc.

Industrial Smart Secure Layer-2 Switch

User Manual
V1.4
June 21th, 2018

Series covered by this manual:
EHG2408

* The user interface on these products may be slightly different from the one shown on this user manual

> **This PDF Document contains internal hyperlinks for ease of navigation.**
> For example, click on any item listed in the **Table of Contents** to go to that page.

Published by:

Important Announcement

The information contained in this document is the property of ATOP Technologies, Inc., and is supplied for the sole purpose of operation and maintenance of ATOP Technologies, Inc., products.

No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of ATOP `Technologies, Inc.,

Offenders will be held liable for damages and prosecution.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.

Suggestions for improvement are welcome. All other product's names referenced herein are registered trademarks of their respective companies.

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help users manage the switch and use its software, a background in general theory is a must, when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atop.com.tw.

Warranty Period

Atop technology provides a limited 5-year warranty for unmanaged Ethernet switches.

Documentation Control

Author:	Saowanee Saewong
Revision:	1.4
Revision History:	TFTP
Creation Date:	1 September 2017
Last Revision Date:	27 June 2018
Product Reference:	Industrial Layer-2 Unmanaged Secure Switch EHG2408 series
Document Status:	Released

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Introduction to Industrial Smart Switch

ATOP's EHG (<u>E</u>thernet Switching <u>H</u>ub Full <u>G</u>igabit, or Fast <u>E</u>thernet Switching <u>H</u>ub) 24XX series are product lines of powerful industrial switch which are referred to as Open Systems Interconnection (OSI) Layer 2 bridging devices.

ATOP's switch is also an industrial switch and not a typical commercial switch. A commercial switch simply works in a comfortable office environment. However, an industrial switch is designed to perform in harsh industrial environments, i.e., extreme temperature, high humidity, dusty air, potential high impact, or the presence of potentially high static charges. Atop's unmanaged switch works fine even in these environments.

ATOP's switch supports essential IEEE standard protocols. This switch is excellent for keeping systems running smoothly, reliable for preventing system damage or losses, and friendly to all levels of users. The goal of this innovative product is to bring users an easy network management experience with robustness.

This device also embeds advanced encryption protocols in order to have the link on 2 Gigabit ports to be encrypted through 802.1AE MACsec Protocol. This protocol, working on Layer-2, encrypts hop-to-hop the data flow through a dedicated hardware that guarantees ultra-low-latency and throughput up to 98% with large packet sizes. The throughput can't achieve a theoretical 100% of non-encrypted because of the fact that MACsec headers make the packet longer.

Note:
Throughout the manual, the symbol * indicates that more detailed information of the subject will be provided at the end of this manual or as a footnote.

1.2 Software Features

ATOP's Industrial Layer-2 Smart Secure Switches come with essential network protocols and software features. These protocol and software features allow the network administrator to implement security and reliability into their network with ease. These features enable Atop's switches to be used in safety applications, and factory and process automation. The followings are the list of protocols and software features.

- User Interfaces
    - Web browser
- Dynamic Host Configuration Protocol (DHCP) Client
- Security
    - Media Access Control Security (MACSec) or IEEE 802.1AE standard
- Layer-2 Switching
- Trivial File Transfer Protocol (TFTP) client for firmware resetting

2 Configuring with a Web Browser

Chapter 2 explains how to access the industrial smart switch for the first time by using the web browser.
The web browser allows users to access the switch over the Internet or the Ethernet LAN which has a user-friendly interface.

2.1 Web-based Management Basics

Users can access the smart secure switch easily using their web browsers (Internet Explorer 8 or 11, Firefox 44, Chrome 48 or later versions are recommended). We will proceed to use a web browser to introduce the smart switch's functions.

2.1.1 Default Factory Settings

Below is a list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the switch has an IP address in the same subnet and the subnet mask is the same. Table 2.1 summarizes the default IP setting for EHG2408 series.

> IP Address: 10.0.50.1
> Subnet Mask: 255.255.0.0
> Default Gateway: 0.0.0.0
> User Name: admin
> Password: default

Table 2.1 Default Setting for IP Network on EHG2408 Series

Model Name	Default IP Setting			
	IP	Netmask	Gateway	Default DNS
EHG2408	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0
EHG2408-2SFP	10.0.50.1	255.255.0.0	0.0.0.0	0.0.0.0

2.1.2   Login Process and Main Window Interface

Before users can access the configuration, they have to log in. This can simply be done in two steps.

1.   Launch a web browser.
2.   Type in the switch IP address (e.g. http://10.0.50.1), as shown in Figure 2.1).
       Note: After pressing the Enter key, the login page will be shown. User has to input the default password which is set to "default".
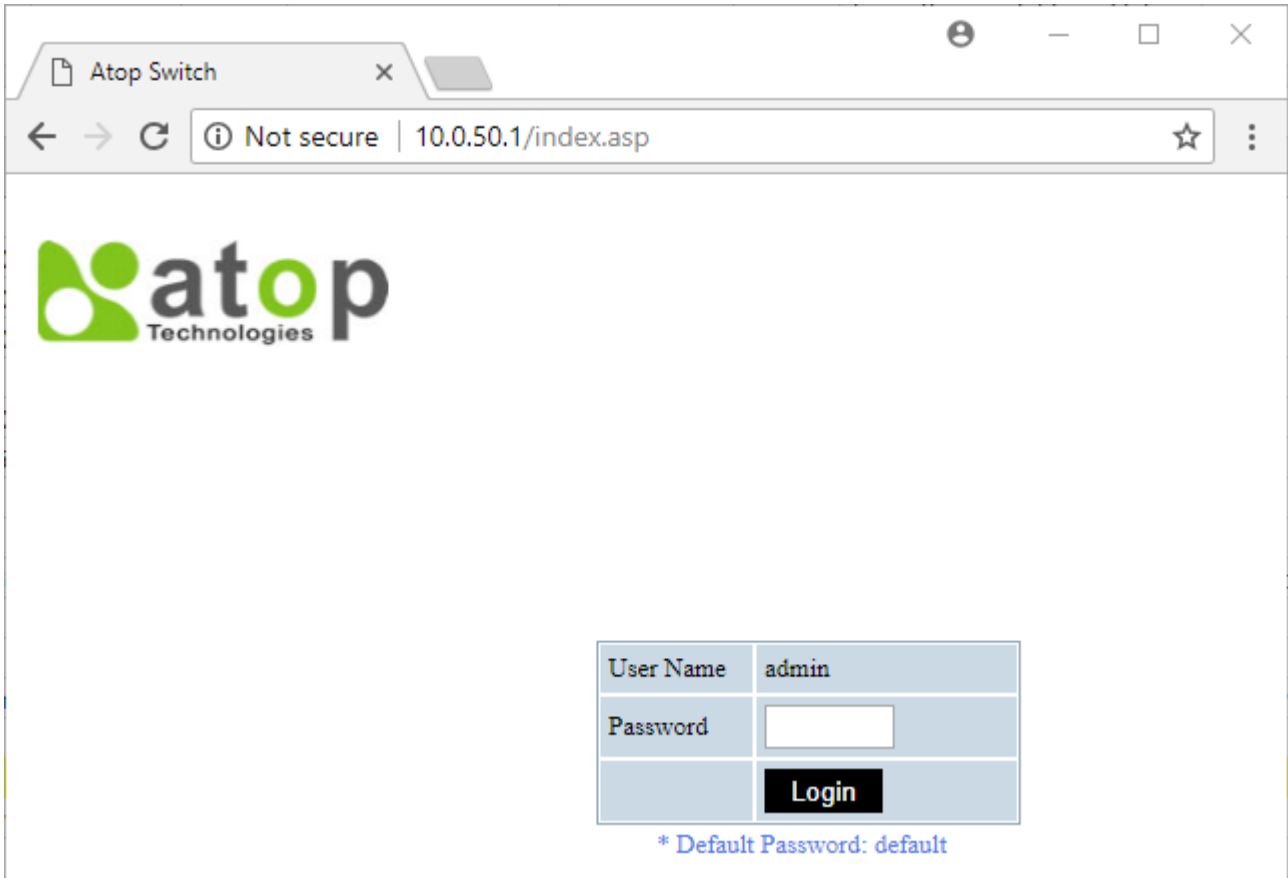
Figure 2.1 IP Address for Web-based Setting

After the login process, the main interface will show up for EHG2408 and EHG2408-2SFP, as shown in Figure 2.2 and Figure 2.3, respectively. The main menu (left side of the screen) provides the links at the top-level links of the menu hierarchy and by clicking on each item it allows lower-level links to be displayed. Note that the difference between EHG2408 and EHG2408-2SFP is that the EHG2408-2SFP will have **Port Setting** menu for its optical fiber slots.

System Info
System Setting
Password
IP Setting
Static SAK Setting
Firmware Upgrade
Reset to Default
Reboot System

System Info

Model Name	EHG2408
MAC Address	00:60:E9:21:29:B9
Firmware Version	1.13-svn91
Kernel Version	1.13-svn91
IP Address	10.0.50.1
Default Gateway	0.0.0.0
Subnet Mask	255.255.0.0

Figure 2.2 Default Web Interface of EHG2408

System Info
System Setting
Password
IP Setting
Port Setting
Static SAK Setting
Firmware Upgrade
Reset to Default
Reboot System

System Info

Model Name	EHG2408-2SFP
MAC Address	00:60:E9:21:29:28
Firmware Version	1.13-svn91
Kernel Version	1.13-svn91
IP Address	10.0.50.1
Default Gateway	0.0.0.0
Subnet Mask	255.255.0.0

Figure 2.3 Default Web Interface of EHG2408-2SFP

2.2 System Information

To help users become familiar with the device, the **System Information** or **System Info** section provides important details of the ATOP's industrial smart secure switch. This is also the main welcome screen once the user has logged in. The details make it easier to identify different switches connected to the network. The user can check various information such as the **Model Name**, **MAC Address**, **Firmware Version**, **Kernel Version**, **IP Address**, **Default Gateway** and **Subnet Mask**. Figure 2.4 depicts an example of System Information of EHG2408. Table 2.2 summarizes the description of each field of system information.

Figure 2.4 Details of System Info Webpage

Table 2.2 Descriptions of the Basic information

Label	Description
Model Name	The device's complete model name
MAC Address	The MAC address of the device
Firmware Version	The current firmware version of the device
Kernel Version	The current kernel version of the device
IP Address	The IP address to login into the configuration page of the device
Default Gateway	The current setting of the default gateway
Subnet Mask	The subnet mask for identified the network address of the device

2.3   System Setting

Users can assign device's details to Atop's switch in this section. By entering unique and relevant system information such as device name, this information can help identify one specific switch among all other devices in the network. Please click on the "**Update**" button to update the information on the switch. Figure 2.5 shows **Device Information Setting** page of an **EHG2408** smart secure switch model. Table 2.3 summarizes the device information setting descriptions and corresponding default factory settings.

Figure 2.5 Details of System Setting Webpage

Table 2.3 Description of the System Setting

Label	Description	Factory Default
Device Name	Specifies a particular role or application of different switches. The name entered here will also be shown in Atop's Device Management Utility. Max. 63 Char.	(Model name)

2.4 Password

Password **"default"** is set for the device when it is manufactured. Users can modify the device's password to ensure overall system security. The password can be updated in this page as shown in Figure 2.6. The password must be entered twice in **Password** and **Confirmed Password** textboxes before a change to confirm its correctness. Please click on the "**Update**" button to update the password information on the switch.

Table 2.4 summarizes the description of each field.

Figure 2.6 Password Setting Webpage

Table 2.4 Descriptions of Password Setting

Label	Description	Factory Default
Password	Password to log-in with maximum length of 15 characters.	Default
Confirmed Password	Re-type the password. This has to be exactly the same as the password entered in the above field with maximum length of 15 characters.	Default

2.5 IP Setting

In this section, users may modify network settings of Internet Protocol version 4 (IPv4) for the smart secure switch.

The **IP Setting** webpage is depicted in Figure 2.7. Inside the **Local Login Setting** box, the user can enable Dynamic Host Configuration Protocol (DHCP) client inside the switch by checking the **DHCP** box so that the switch can obtain IP address' setting automatically from a DHCP server available on the user's local network. If the DHCP is enabled, the rest of the fields will be disabled. Note that the user should consult your local network administrator for information about the availability of DHCP server. If the user prefers a static IP setting, then the user can proceed to enter the **IP Address**, **Subnet Mask**, **Gateway**, and the **Primary DNS**. If the user set gateway or DNS on this page, the smart secure switch will not use the gateway or the DNS from DHCP server. After entering the desired information, please click **Update** button to change the IP Setting.

Figure 2.7 IP Setting under IP Setting Webpage

The description of each field and its default value in IP Setting webpage are summarized in Table 2.5.

Table 2.5 Descriptions of IP Settings

Label	Description	Factory Default
DHCP	By checking this box, an IP address and related fields will be automatically assigned. Otherwise, users can set up the static IP address and related fields manually.	Uncheck
Static IP Address	Display current IP address. Users can also set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display current Subnet Mask or users can set a new subnet mask in this field	255.255.0.0
Gateway	Show current Gateway or set a new IP address for the Gateway	0.0.0.0
Primary DNS	Set the primary DNS' IP address to be used by your	NULL

2.6   Port Setting

Note that this menu is only available in EHG2408-2SFP model only.

EHG2408-2SFP model supports two 1000BASE-X fiber optics SFP (small form-factor pluggable) slots on the box, which are Port 7 and Port 8. Therefore, this menu will allow the user to set the data rate or communication speed on each of the port as shown in Figure 2.8. The user can select either 1000Mbps (1Gbps) or 100 Mbps from the drop-down list under the Speed column. After finishing a change on the speed setting, please click on the **Update** button.

Figure 2.8 Port Setting Webpage

2.7   Static SAK Setting

EHG2408 series support advanced security features that allow traffic encryption and high throughput. MACsec or Media Access Control Security is a security standard specified by IEEE also called IEEE 802.1AE. This IEEE MAC security standard provides connectionless user data confidentiality, frame data integrity, and data origin authenticity. MACsec can establish point-to-point security on Ethernet links between directly connected nodes. ATOP's secure smart switches support this security feature and can be used to transparently secure an IEEE 802 LAN connection to a peer device (such as another switch) that also supports the MACsec.

MACsec defines two terms called secure channel and connectivity association when setting up a secure communication between two switches. A secure channel in MACsec is unidirectional and used for transmitting (outbound traffic) or receiving (inbound traffic) data. A connectivity association when MACsec is enabled consists of two secure channels: one for inbound traffic and one for outbound traffic.

The point-to-point links can be secured by MACsec after matching security keys are exchanged and verified between the ports on two different secure switches. There are two modes for setting up the static security keys: Secure Association Key (SAK) and Connectivity Association Key (CAK). Note that EHG2408 only supports SAK mode.

1. **Static Association Key (SAK):**

   The static secure association key (SAK) security mode is when the user manually configured the same static secure association key (SAK) on both sides of a connection. There is no key server in this mode and the key must be matched on the ports of both switches. This can be viewed as setting up two secure channels within a connectivity association. It is suggested to have a periodic manual key update in order to prevent the key to be broken by brute-force attack.

2. **Connectivity Association Key (CAK):**

   The static connectivity association key (CAK) security mode is when the user configured a pre-shared key which consists of a connectivity association name (CKN) and a connectivity association key (CAK), which will be used to randomly generate a secure association key (SAK) later. The MACsec Key Agreement (MKA) protocol (defined in IEEE 802.1x standard) is responsible for maintaining MACsec on the link and chooses which switch on the link will become the key server. The key server then automatically creates a SAK that is shared with the other switch, and that SAK is used to secure the traffic between the link. The key server will periodically create and share a fresh SAK over the link for secure key changing. It is suggested to have a periodic manual key update in order to prevent the key to be broken by brute-force attack.

2.7.1   Static SAK

Static secure association key (SAK) setting webpage is shown in Figure 2.9. To enable secure association mode on secure MACsec switch's port(s), first select **one or multiple ports** from the list under the Ports. Then, check the **Enabled** box. Then, enter the **Secure Channel Identifier (SCI)** with a 16-digit hexadecimal number (i.e., 0,1,2,…,a,b,c,d,e,f) and enter the **Secure Association Key (SAK)** with a 32-digit hexadecimal number. Finally, click on the **Add/Modify** button to add the setting to the table below.

The selected port(s) will use the given static **SAK** as the secure key to secure all the traffic. If any two switches have the same SCI and SAK, they can securely communicate. If there is any non-secured traffic that uses incorrect SCI and SAK, the traffic will be dropped by the ingress port of the switch. The description of the static SAK setting fields are summarized in Table 2.6.

To disable the SAK setting for any of the port(s), simply select the desired port(s) from the list and uncheck the Enabled box. Then click on the **Add/Modify** button. This will update the status of the setting in the table below the Figure 2.9.

Note that the static SAK mode and the static CAK mode are mutually exclusive mode. Each port can only be enabled in one of the two modes at a time. However, EHG2408 only supports the SAK mode.

Figure 2.9 Static SAK Setting Webpage

Table 2.6 Description of Static SAK Setting Webpage

Label	Description	Factory Default
Port	Set specific ports to be configured.	Option
Enabled	Check the box to enable static secure association key (SAK) mode for the selected port(s)	Unchecked
SCI	Secure Channel Identifier (SCI) is a 16-digit hexadecimal number. Note that if the user did not configure all digits of SCI, all remaining digits will be auto-configured to 0s.	0
SAK	Secure Association Key (SAK) is a 32-digit hexadecimal number. Note that if the user did not configure all digits of SAK, all remaining digits will be auto-configured to 0s.	0

2.8   Firmware Upgrade

The users can update the device firmware via web interface as shown in Figure 2.10. To update the firmware, the users can download a new firmware from Atop's website and save it in a local computer. Then, the users can click **Browse…** button and choose the firmware file that is already downloaded. The switch's firmware typically has a ".dld" extension such as EHG240X-K113A113.dld. After that, the users can click **Upload** button and wait for the update process to be done.

Note: please make sure that the switch is plug-in all the time during the firmware upgrade.
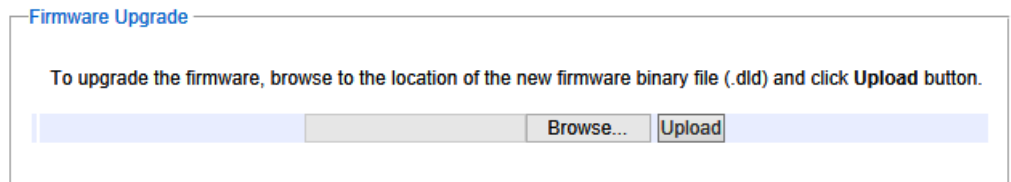
Figure 2.10 Firmware Update Webpage

2.9   Reset to Default

When the switch is not working properly, the users can reset it back to the original factory default setting by clicking on the **Reset** button as shown in Figure 2.11. A pop-up window will show up during the resetting process as shown in Figure 2.12. When the switch is restarted, the web browser will be redirected to the login web page as depicted in Figure 2.2. Note that there is no physical reset button on the front panel of the box; therefore, the user will have to either using the Reset button in this menu or using the TFTP procedure described in Section 2.9.1 to reset the device to factory default setting.
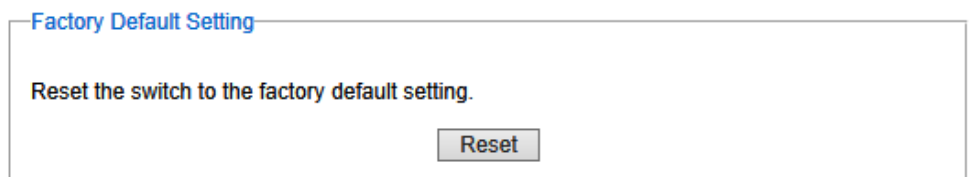

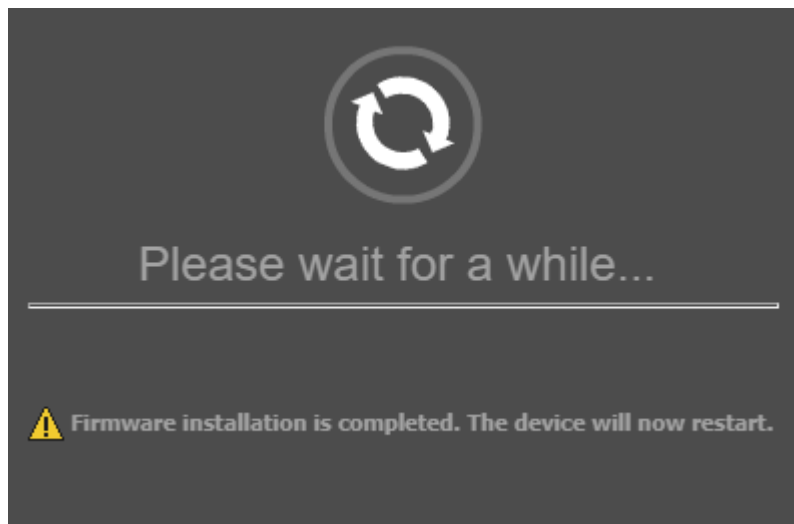Figure 2.11 Factory Default Setting Webpage

Figure 2.12 Pop-up window during the resetting process

2.9.1   *TFTP Factory Default Setting*

EHG2408 series also provide alternative method for factory default setting. This feature can be achieved by setting up a Trivial File Transfer Protocol (TFTP) server. Note that the user need to install a TFTP application such as tftpd64 (https://bitbucket.org/phjounin/tftp64) on the PC that will be used to configure the switch. This TFTP server must be available and connected on the same local area network (LAN) as the EHG2408 switch, i.e. the PC that is installed this tftpd64 must be on the same LAN as the EHG2408. The EHG2408 will use a default IP address of 192.168.195.252 as a TFTP client while the TFTP Server will use a default IP address of 192.168.195.253. Note that default TFTP Address and its related parameters are summarized in Table 2.7.

Table 2.7 Default TFTP's Parameters

Model Name	Default TFTP		
	IP	Netmask	Gateway
EHG2408	192.168.195.252	255.255.255.0	192.168.195.254
EHG2408-2SFP	192.168.195.252	255.255.255.0	192.168.195.254

To perform automatic factory default setting, please follow these steps:

1. On the industrial smart secure switch, using the IP Setting menu as described in Section 0 to change the IP Address of the switch to 192.168.195.252 and set the Subnet Mask to 255.255.255.0. Note you will need to re-login to the switch via the web browser by entering the password after the changes.

2. On the PC with Windows Operating System, set the new IPv4 address for Ethernet Interface as 192.168.195.253 and Subnet Mask as 255.255.255.0 by going to the Internet Protocol Version 4 (TCP/IPv4) Properties. Note on Windows 10 OS, please select Settings → Network & Internet → Ethernet → Change adapter options. On previous version of Windows OS, go to Control Panel → Network and Internet → Network Connections. Then select the Ethernet icon as depicted in Figure 2.13 and right click on it and then select the Properties. A new window for Ethernet Properties will pop-up as shown in Figure 2.14. Next select **Internet Protocol Version 4 (TCP/IPv4)** from the list of items. Then click on the **Properties** button to bring up another pop-up window as shown in Figure 2.15. Fill in the information as shown in Figure 2.15. Note that you will also need to temporary disable the Windows Defender Firewall (or any other firewall software on the PC) to allow the tftp connection between the PC and the EHG2408 switch. Alternatively, you may allow only the TFTP Server apps to communicate through Windows Firewall. On Windows 10, you can disable the firewall by going through Settings → Windows Security → Firewall & network protection.
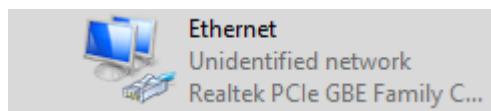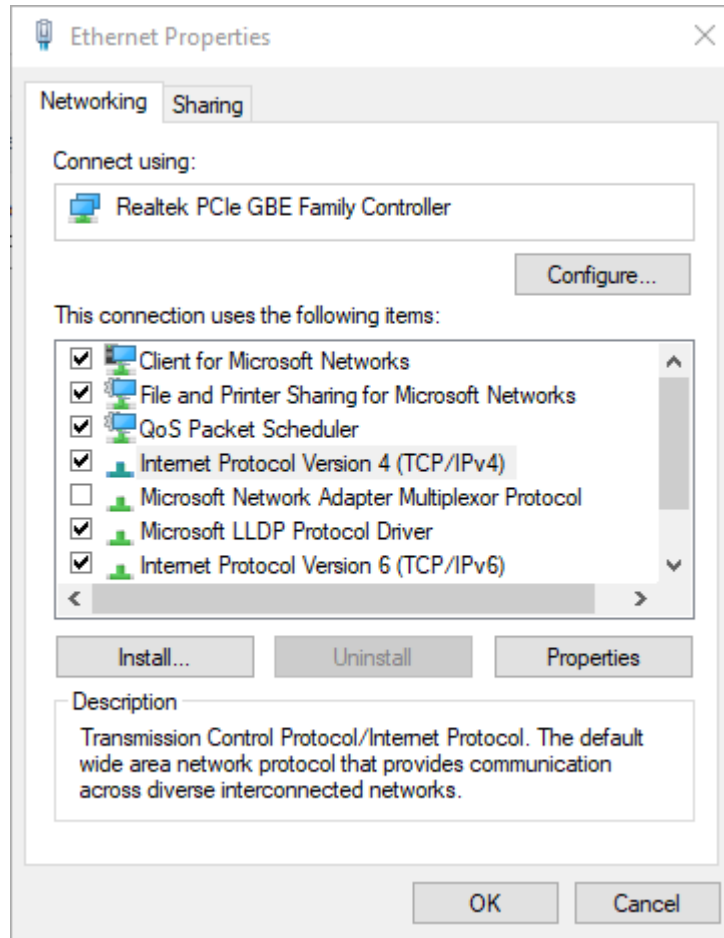

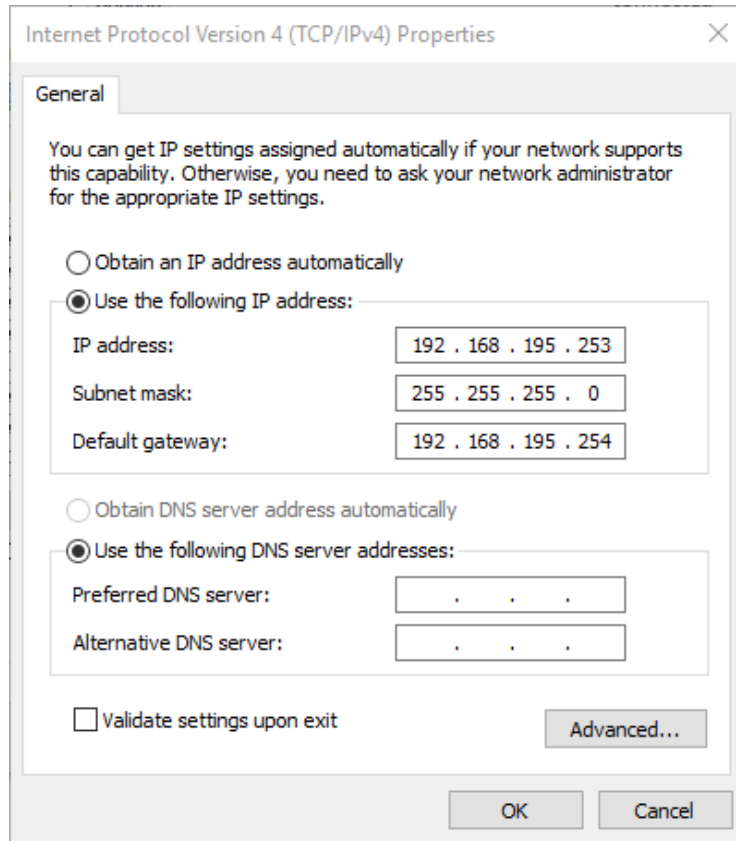Figure 2.13 Ethernet Icon

Figure 2.14 Ethernet Properties

Figure 2.15 Internet Protocol Version 4 (TCP/IPv4) Properties

3. Open the TFTP Server (such as tftpd64) as shown in and set the Current Directory to C:\ or any directory of your choice.
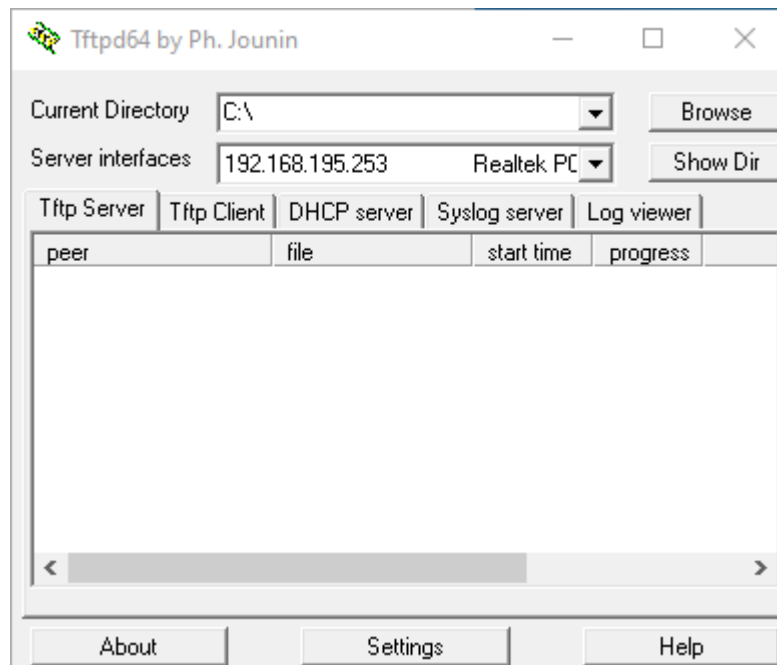

Figure 2.16 Tftpd64 Main Window

4. Create a text file using any text editor (such as notepad) and name it as "testerase.txt". Then enter the MAC address of the EHG2408 device in the text file as shown in Figure 2.17. Note that you can find the MAC address of the device on the label on the case.
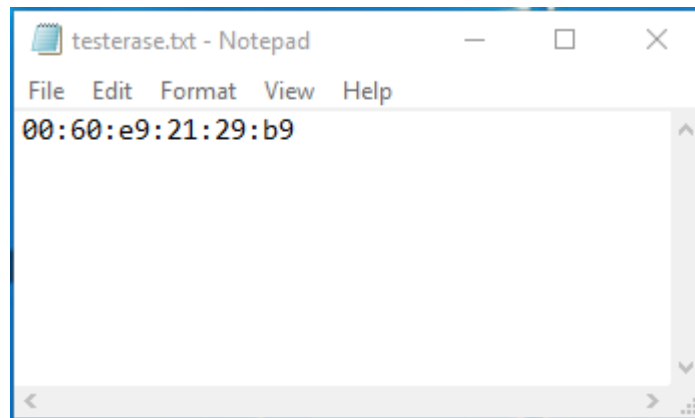

Figure 2.17 testerase.txt file

5. Save the text file under the C:\ directory or any directory of your choice.
6. Reboot the EHG2408 device by going to the Reboot System menu as described in Section 0 and the EHG2408 will execute the factory default setting. Note that the TFTP window will indicate the TFTP's progress as shown in.
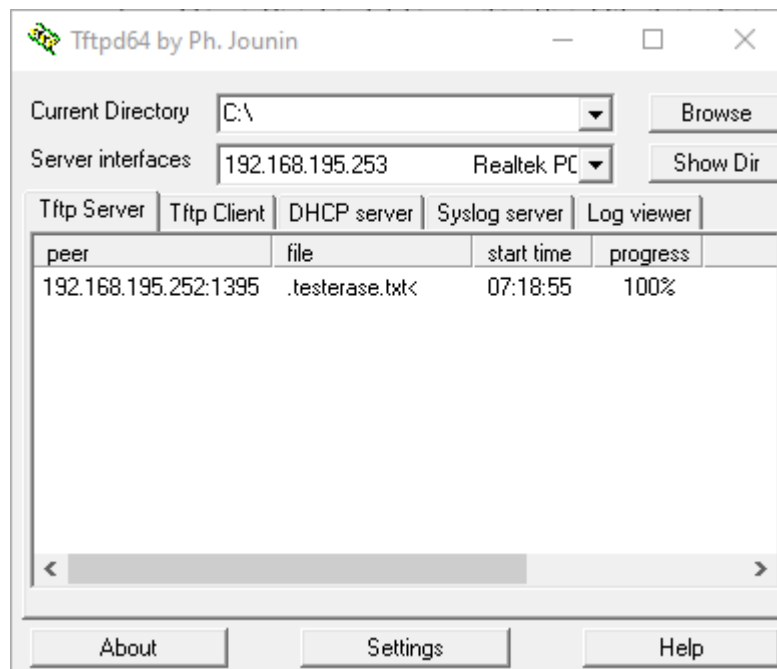
Figure 2.18 TFTP's progress during the factory default setting

7. After the EHG2408 is rebooted, it will be reset back to its original factory default settings. Note that the default IP address of EHG2408 will be restored to 10.0.50.1. Therefore, you will need to change the PC's IP address back to an address in the same subnetwork such as 10.0.50.100 in order to use the web browser to login to the EHG2408 again. Moreover, it is recommended that you turn the Windows firewall back on to ensure the security of your PC after finishing the factory default setting.

2.10 Reboot System

A simple reboot function is provided in this webpage requiring only one single click on the **Reboot** button as shown in Figure 2.19.

Figure 2.19 Reboot Webpage

3 Glossary

Term	Description
802.1	A working group of IEEE standards dealing with Local Area Network.
802.1p	Provide mechanism for implementing Quality of Service (QoS) at the Media Access Control Level (MAC).
802.1x	IEEE standard for port-based Network-Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
Broadcast	Broadcast packets to all stations of a local network.
Client	Device that use services provided by other participants in the network.
DES	**D**ata **E**ncryption **S**tandard is a block cipher that uses shared secret encryption. It's based on a symmetric-key algorithm that uses a 56-bit key.
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol allows a computer to be configured automatically, eliminating the need for intervention by a network administrator. It also prevents two computers from being configured with the same IP address automatically. There are two versions of DHCP; one for IPv4 and one for IPv6.
DNS	**D**omain **N**ame **S**ystem is a hierarchical naming system built for any computers or resources connected to the Internet. It maps domain names into the numerical identifiers. For example, the domain name www.google.com is translated into the address 74.125.153.104.
EAP	**E**xtensible **A**uthentication **P**rotocol is an authentication framework widely used by IEEE.
Ethernet	In star-formed physical transport medium, all stations can send data simultaneously. Collisions are detected and corrected through network protocols.
Gateway	Provide access to other network components on the OSI layer model. Packets which are not going to a local partner are sent to the gateway. The gateway takes care of communication with the remote network.
IEEE	Institute of Electrical and Electronics Engineers
IGMP	**I**nternet **G**roup **M**anagement **P**rotocol is used on IPv4 networks for establishing multicast group memberships.
IP	Internet Protocol
IPv4	**I**nternet **P**rotocol **v**ersion **4** is the fourth revision of the Internet Protocol. Together with IPv6, it is the core of internet network. It uses 32-bit addresses, which means there are only 2^32 possible unique addresses. Because of this limitation, an IPv4 addresses became scarce resource. This has stimulated the development of IPv6, which is still in its early stage of development.
LAN	Local Area Network is the network that connects devices in a limited geographical area such as company or computer lab.

MAC	Media Access Control is a sub-layer of the Data Link Layer specified in the OSI model. It provides addressing and channel access control mechanisms to allow network nodes to communicate within a LAN.
MAC Address	A unique identifier assigned to network interfaces for communications on a network segment. It is formed according to the rules of numbering name space managed by IEEE.
MD5	Message-Digest algorithm 5 is a widely used cryptographic which has a function with a 128-bit hash value.
Multicast	This type of transmission sends messages from one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. Also, networks that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverges points, multicast packets will be copied and forwarded. This method can manage high volume of traffic with different destinations while using network bandwidth efficiently.
OSI Model	**O**pen **S**ystem **I**nterconnection mode is a way of sub-dividing a communication system into smaller parts called layers. A layer is a collection of conceptually similar functions that provide services to the layer above it and receives services from the layer below it.
QoS	Quality of Service
RADIUS	**R**emote **A**uthentication **D**ial **In** **U**ser **S**ervice is an authentication and monitoring protocol on the application level for authentication, integrity protection and accounting for network access.
Server	Devices that provide services over the network.
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol (**SMTP**) is an internet standard for email transmission across IP network.
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol is a protocol for managing devices on IP networks. It exposes management data in the form of variables on the managed systems, which describe the system configuration.

atop
Technologies

Atop Technologies, Inc.

www.atoponline.com
www.atop.com.tw

TAIWAN HEADQUARTER:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231

ATOP INDIA OFFICE:

Abhishek Srivastava
Head of India Sales
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-80-4920-6363
E-mail: Abhishek.S@atop.in

ATOP INDONESIA BRANCH:

Jopson Li
Branch Director
Wisma Lampung Jl.
No. 40, Tomang Raya
Jakarta Barat, 11430, Indonesia
Tel. +62-857-105957755
E-mail : jopsonli@atop.com.tw

ATOP EMEA OFFICE:

Bhaskar Kailas (BK)
Vice President (Business Development)
Atop Communication Solution(P) Ltd.
No. 22, Kensington Terrace,
Kensington Rd,
Bangalore, 560008, India
Tel: +91-988-0788-559
E-mail: Bhaskar.k@atop.in

ATOP AMERICAs OFFICE:

Venke Char
Sr. Vice President & Head of Business
11811 North Tatum Blvd, Suite 3031
Phoenix, AZ 85028,
United States
Tel: +1-602-953-7669
E-mail: venke@atop.in