Application Note

SSH (Secure Shell) - data

Version 1.1

Sollae Systems Co., Ltd.

http://www.ezTCP.com

Contents

1 Introduction

1.1 Terminology

- "ezTCP"
  ezTCP is the brand name of Sollae's products. It provides Internet connection to common serial communication devices.
- "host"
  A computer (or some network device – e.g. ezTCP) connected to the Internet (or local private network)
- "TCP/IP"
  TCP/IP is the set of communication protocols used for the Internet and private networks.

1.2 SSH (Secure Shell)

The Secure Shell (SSH) is a network protocol for providing a secure channel between two networked hosts. It is widely used for security in currently Internet environment and latest version of SSH is 2.0.

1.3 The ezTCP operation

The ezTCP has four operation mode called "ezTCP Mode" for TCP/IP communication like T2S(0), ATC(1), COD(2) and U2S(3). Each ezTCP Mode operates as below.

ezTCP Mode	TCP/IP
T2S(0)	TCP Server only
ATC(1)	TCP(both Server and Client)
COD(2)	TCP Client only
U2S(3)	UDP

1.4 SSH with the ezTCP

Originally SSH was designed as a replacement for exiting insecure remote shells, ex) TELNET. This application note introduces the SSH feature in ezTCP for data communication channel-not remote shells channel (refer to EZL-200F's application note for the SSH feature of originally purpose). The ezTCP guarantees the security of communications on Internet by supporting SSH 2.0. The products which support this feature are CSE-M32, CSE-M73, CSE-H20, CSE-H21 and CSE-H25.

2 Setting

2.1 Limitations

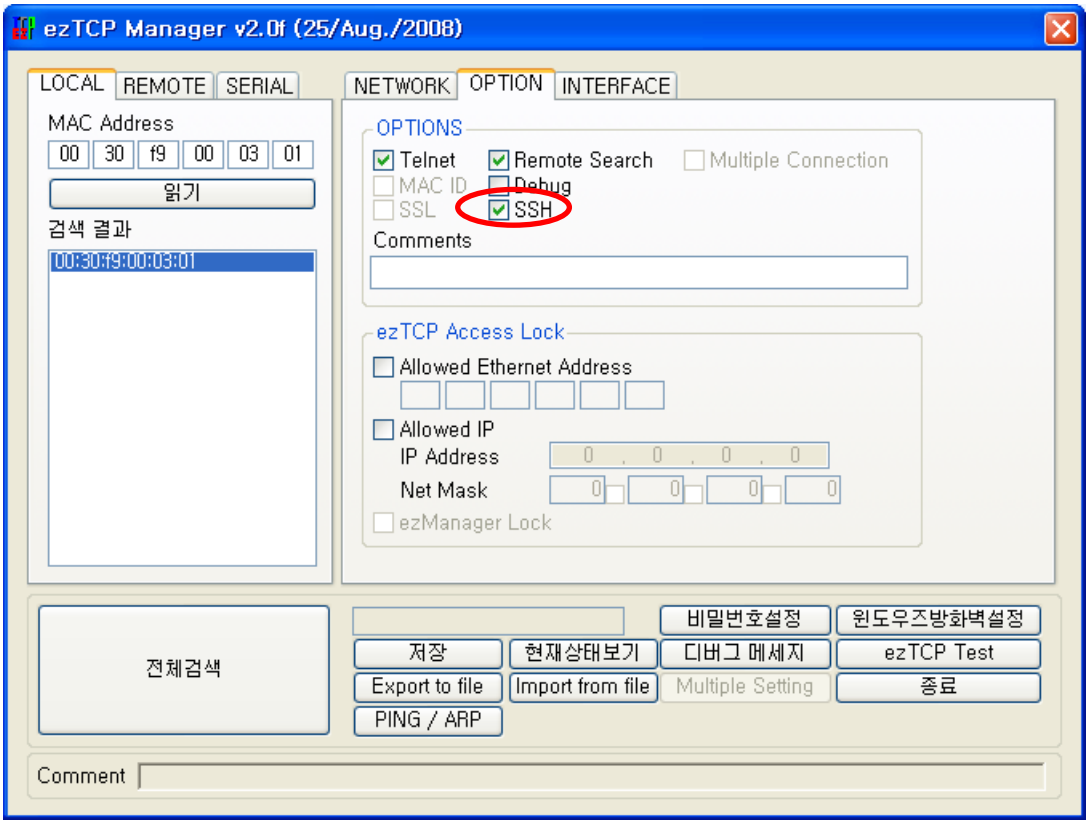
- Activate only in "T2S(0) – TCP Server" ezTCP Mode
- User cannot use below features
  SSL, Telnet COM Port Control Option
- Restrictions while using "SSH" feature by each products
  <CSE-M32, CSE-H20, CSE-H21>
  – COM2 serial port is disabled
  <CSE-M73, CSE-H25>
  – "Multi Monitoring" feature is disabled

2.2 Set up "SSH" feature

SSH function is only available in TCP server mode.

2.2.1 Setting with ezManager

Set [SSH] checkbox in "OPTION" tab of ezManger.

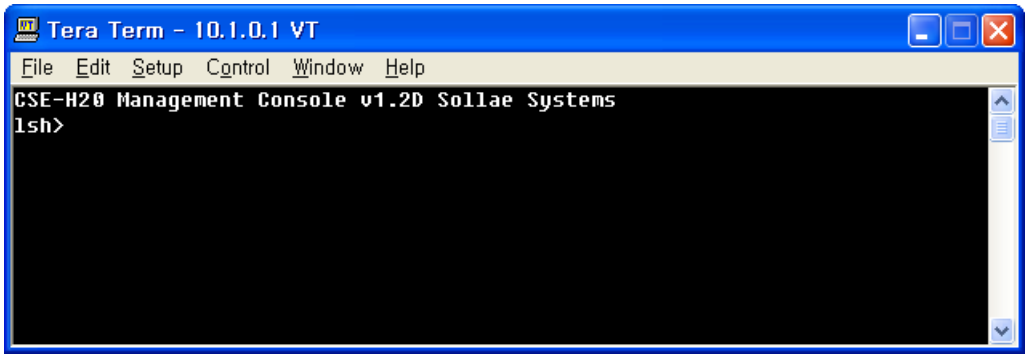


2.2.2 KEY generation

- The below is the telnet console command lists

Item	Command	Descriptions
RSA KEY	rsa keygen <key length>	Supporting KEY length 512/768/1024
	rsa key	Confirm generated RSA KEY
	rsa test	Check RSA KEY is correctly generated
DSA KEY	dsa keygen	Generate DSA KEY
	dsa key	Confirm generated DSA KEY
ID/PW	ssh id	Set up login ID & Password
Save	ssh save aa55cc33	Save the configuration of SSH related parameter

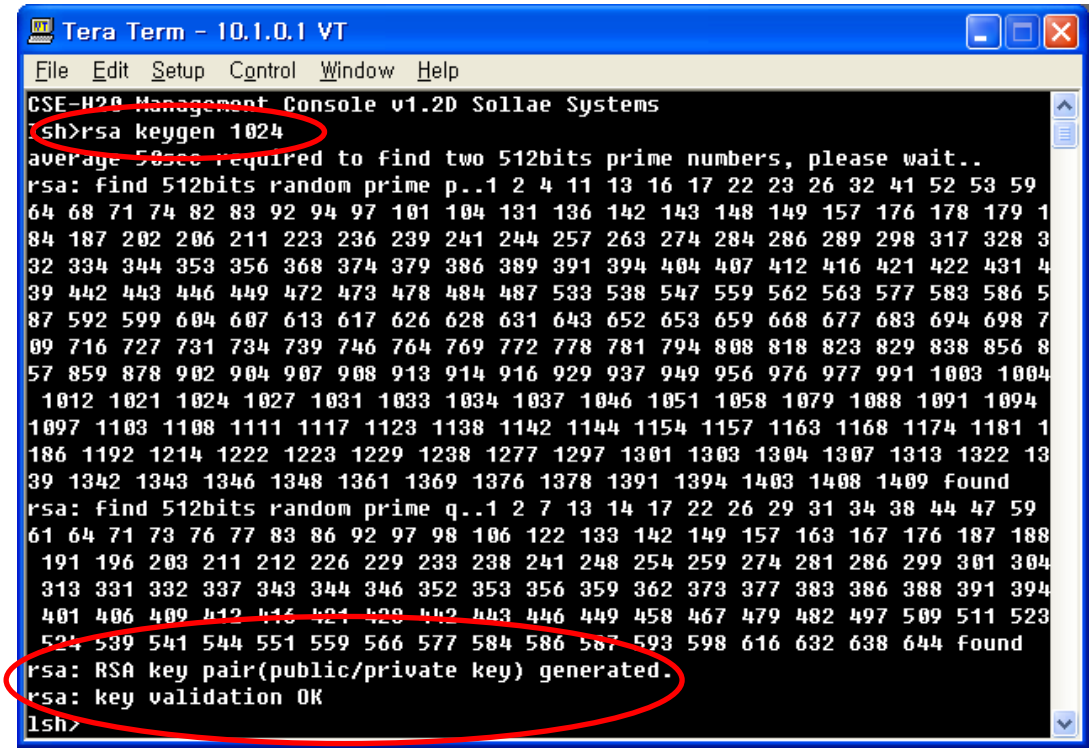
- Log in the telnet console of the ezTCP.



☞ ***Entering a password is required if you set a password to your product. Starting with firmware version 2.0A, you need to enter "sollae" without setting a password.***

- RSA KEY generation

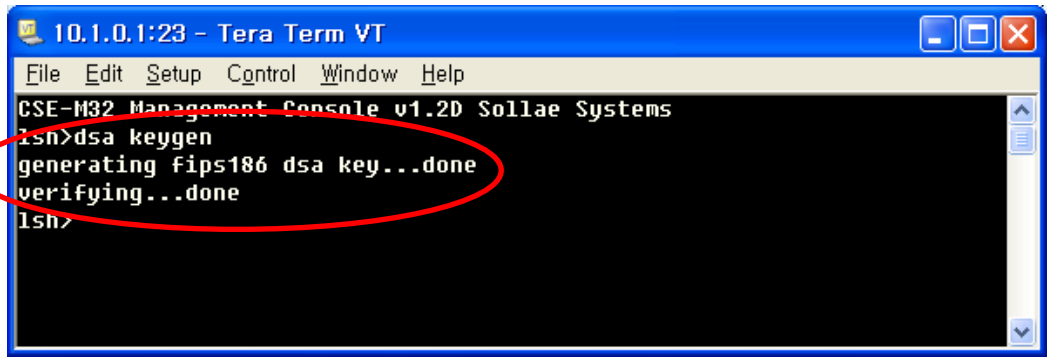
  Generate RSA KEY first than DSA KEY. The ezTCP supports 512, 768 and 1024 bytes KEY length. In accordance with the KEY length, KEY generation may take a number of minutes. Longer KEY length provides more secure communications and takes longer time for KEY generation. For example, 1024-bit KEY length may take about 1 minute on average. The command form is "rsa keygen <key length>" as shown below.



This RSA KEY can check if it is correctly generated by "rsa test" command. The present generated RSA KEY can confirm by "rsa key" command.

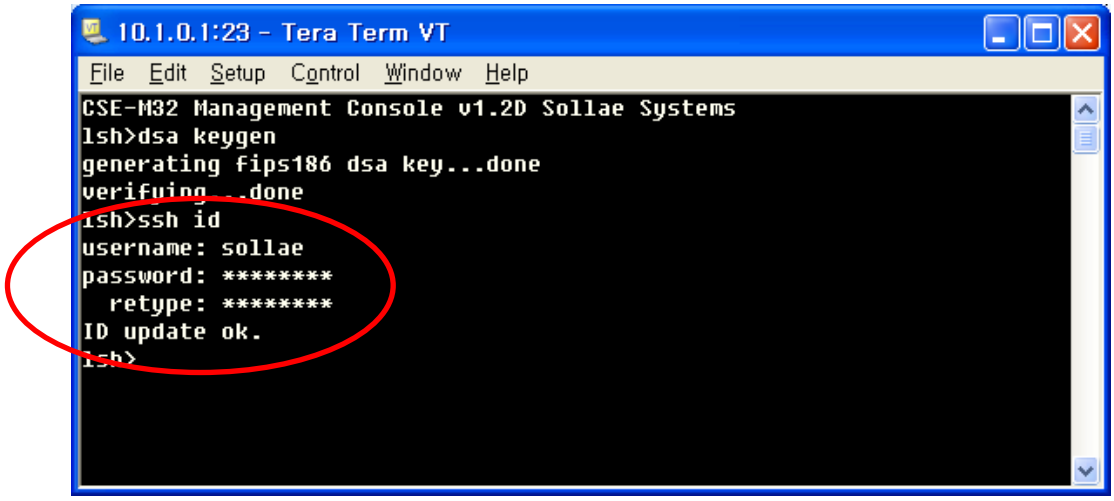
- DSA KEY generation

  If RSA KEY is generated successfully, generate DSA KEY by "dsa keygen" command. The KEY length filed doesn't need. The present generated DSA KEY can confirm by "dsa key" command.



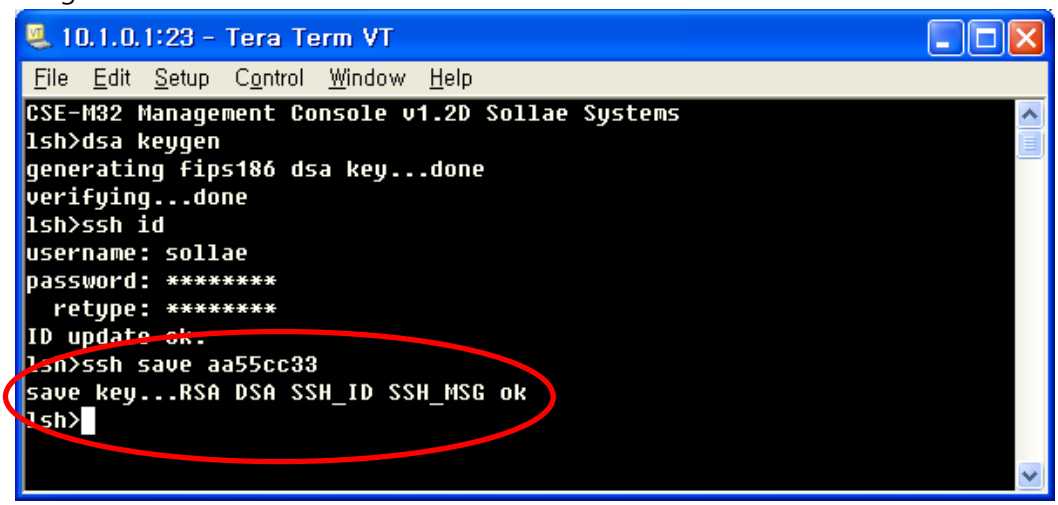
- Set up login ID and password

  Set up ID and password by "ssh id" command for "SSH" login.



- Save the configuration

  The user has to save the RSA KEY, DSA KEY and ID/PW to the flash memory of ezTCP for using "SSH" feature. The command form is "ssh save aa55cc33".



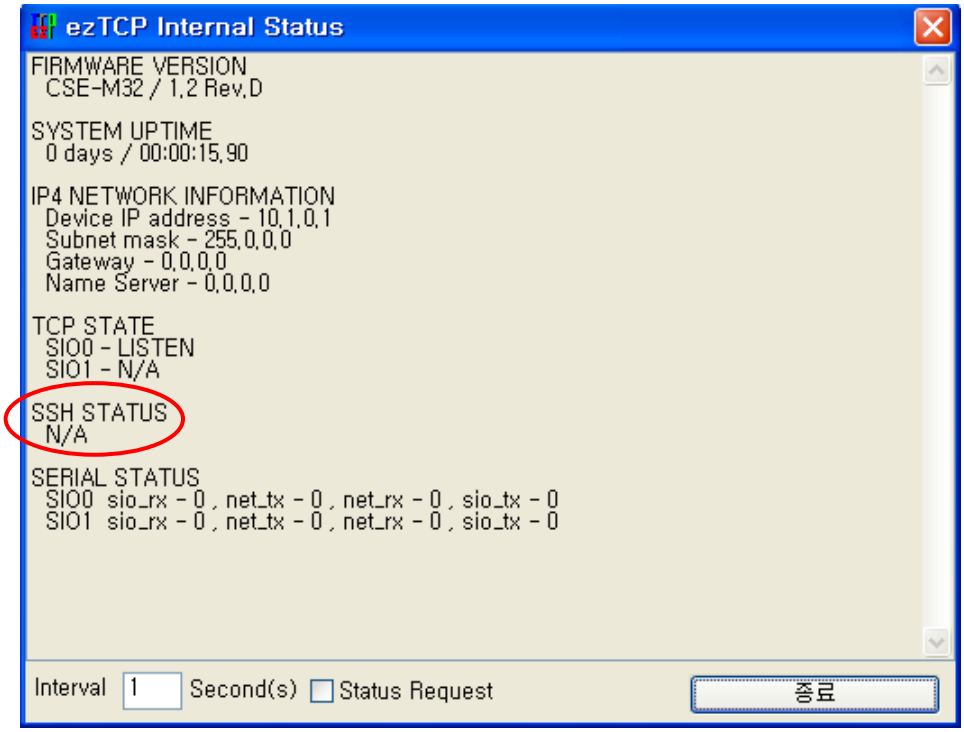
3 Example of use

This section describes how to communicate with ezTCP which is enabled "SSH" feature.

3.1 Confirm setting

3.1.1 Confirm setting with ezManager

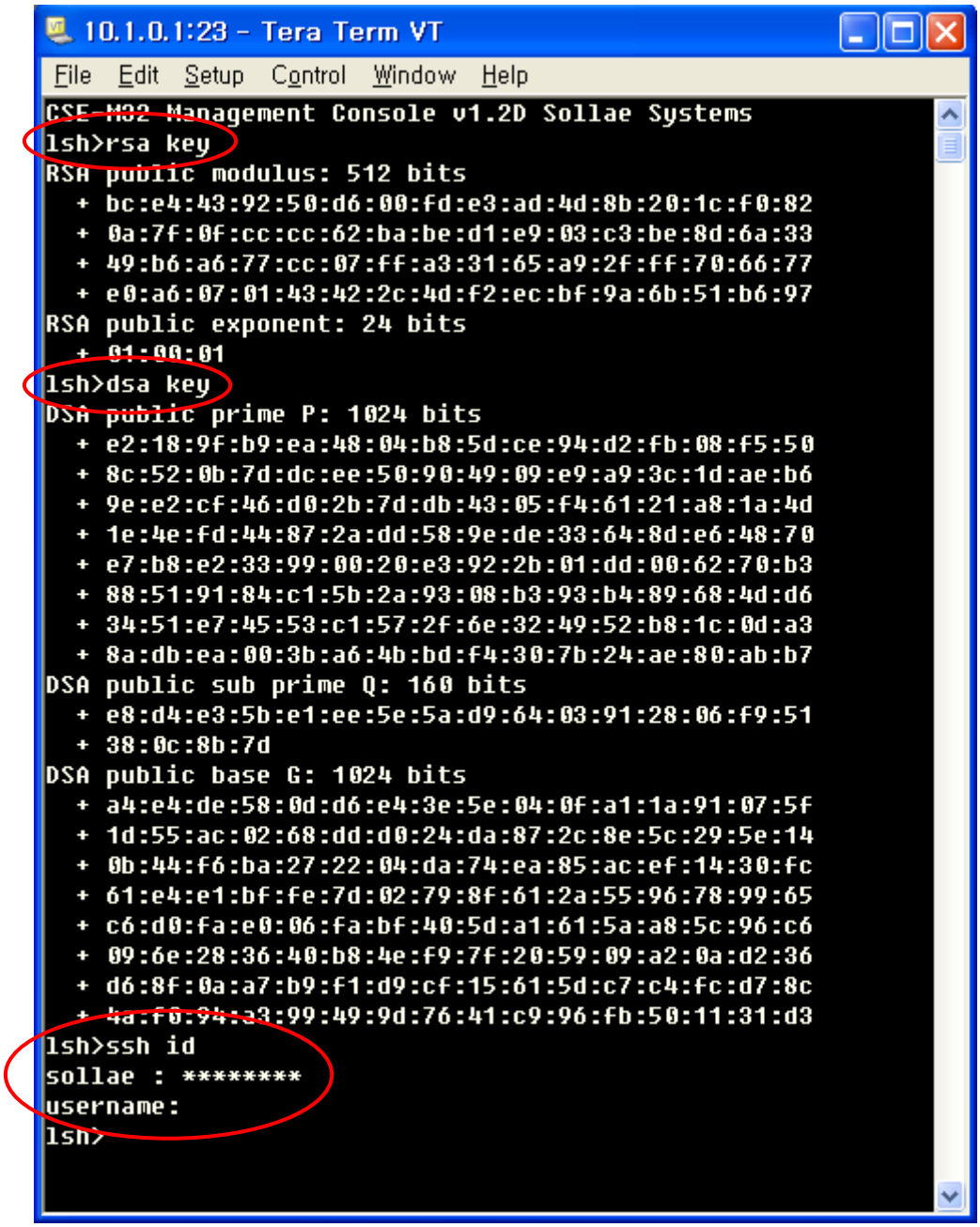
Click the [STATUS] button of ezManger.



Check if there is "SSL STATUS" as shown above.

3.1.2 Confirm setting with telnet console

After log in telnet console of ezTCP, check RSA KEY, DSA KEY and user ID/PW. The related command is "rsa key", "dsa key" and "ssh id". When user ID/PW lost, user can make new user ID/PW by "ssh id" command. After ezTCP receive "ssh id" command, ezTCP print currently user ID/PW (PW is printed in '*' symbols) and request new user ID. If user doesn't want to change currently user ID/PW, just type <Enter>. After changing user ID/PW, user must save the currently configuration by "ssh save aa55cc33" command.



3.1.3 Connecting to the ezTCP

To communicate with the ezTCP enabled the SSH feature remote host must support SSH client operation. Confirm SSH feature by using "Putty, freeware" support SSH client.

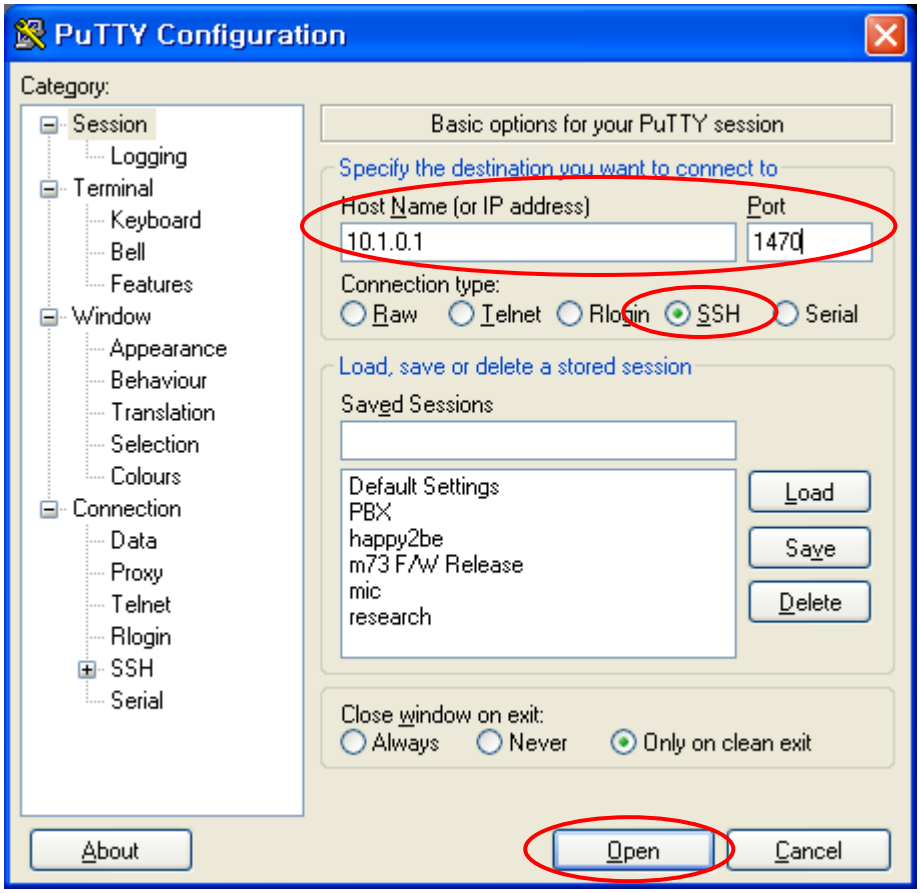
- Confirm basic parameter of ezTCP

  Check the basic configuration of ezTCP as show below.

	PC	CSE-M32, CSE-H20, CSE-H21, CSE-M73, CSE-H25
Local IP Address	10.1.0.2	10.1.0.1
Subnet Mask	255.0.0.0	255.0.0.0
Local Port	-	1470
ezTCP Mode	-	T2S(0) – TCP Server

- Setting Putty

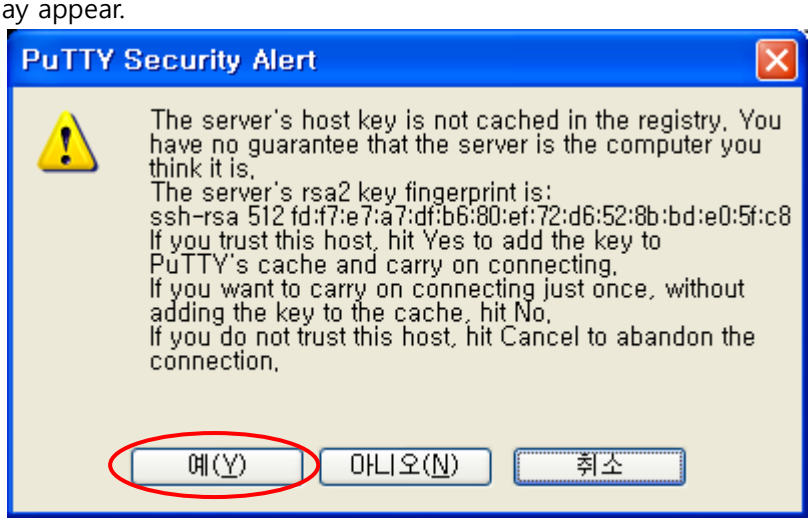
  Set up the [Host Name] and [Port] respectively 'Local IP Address' and 'Local Port' of ezTCP as shown below.



Check the [Connection type] whether it is [SSH] then click [Open] button.

- Check KEY value of SSH Server(ezTCP)

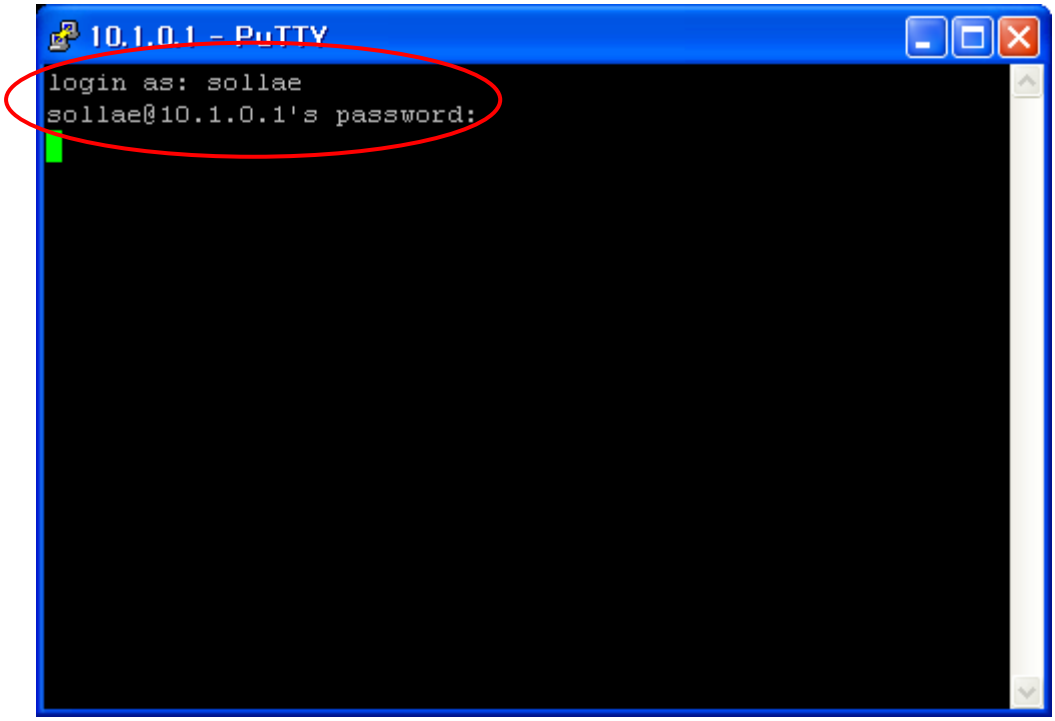
  When user connect to ezTCP which is enabled "SSH" feature, pop up window like the below may appear.



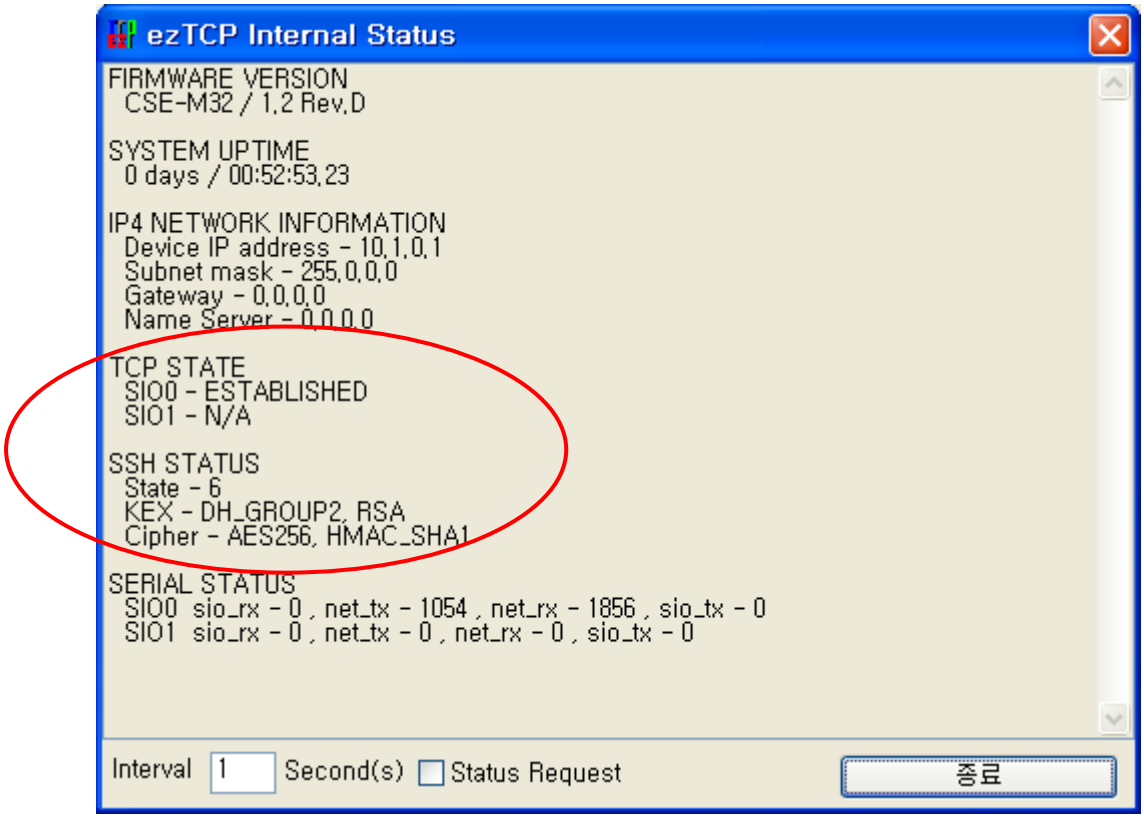
  When and if the SSH server's key is not cached in SSH client, the SSH client ask whether it save the server's key. After saving the server's key once, the SSH client doesn't ask it again. If user change the key of ezTCP the SSH client will ask it again.

- Login

  The below is first screen right after connect to the ezTCP. The ezTCP request user ID/PW, enter pre-configured ID and Password.



- Confirm TCP connection
  Click the [STATUS] button of ezManager.



User can confirm "TCP STATE" / "SIO0 – ESTABLISHED" and "SSH STATUS" / "State – 6", "Cipher – AES_256, HMAC_SHA1".

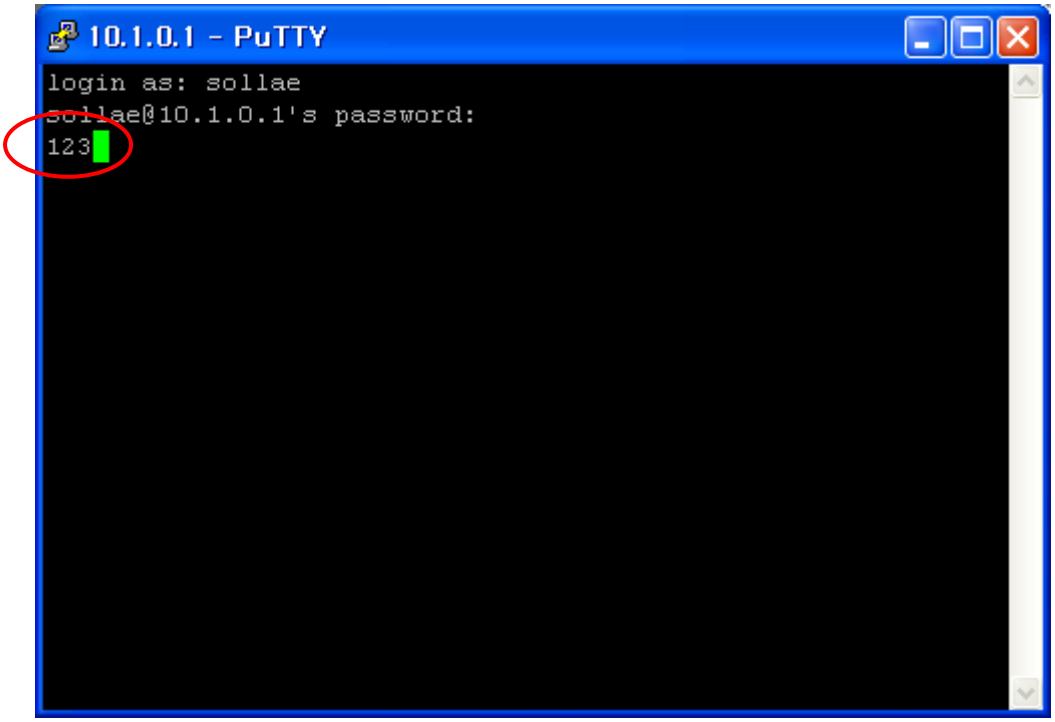
3.2 Communication test

After SSH connection succeeds, connect the serial port of PC to ezTCP's serial port. And check communication between client host PC and ezTCP.

Open serial port of PC and enter "123" on that Serial terminal, then this data-"123"- will appear on the Putty terminal. By contrast, enter "abc" on the Putty terminal and then this data- "abc"- will appear on the Serial terminal.

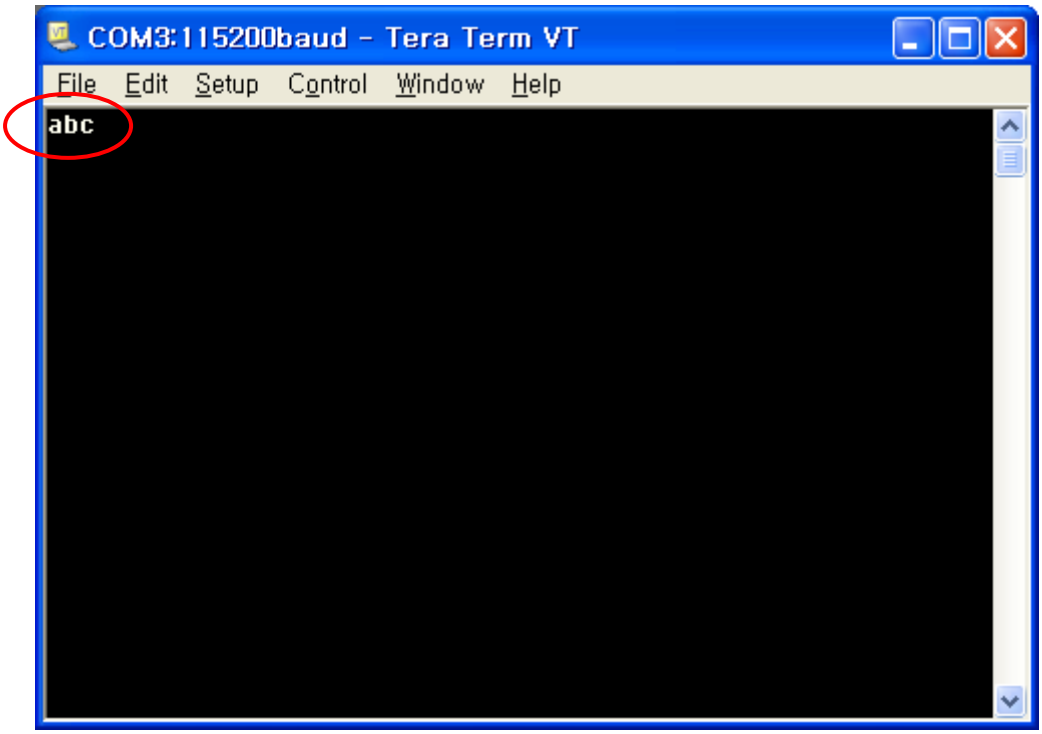
3.2.1 Putty terminal

Received data – "123" from serial port of ezTCP



3.2.2 Serial terminal

Received data – "abc" from putty terminal of client host



4 Revision History

Date	Version	Comments	Author
2008.10.23	1.0	○ Initial Release	-
2016.04.07	1.1	○ Add CSE-H25 on product list ○ Add an explanation about TELNET login	Roy LEE