

Application Note

SSH (Secure Shell) - data

Version 1.2

솔내시스템(주)

<http://www.sollae.co.kr>

목차

1	개요	- 2 -
1.1	SSH (Secure Shell)	- 2 -
1.2	ezTCP 적용.....	- 2 -
2	설정하기	- 3 -
2.1	설정하기 전에.....	- 3 -
2.2	SSH 기능 설정 하기.....	- 3 -
2.2.1	SSH 기능 활성화 - ezManager 설정	- 3 -
2.2.2	키 생성	- 4 -
3	사용 예	- 7 -
3.1	통신 준비.....	- 7 -
3.1.1	ezManager 확인.....	- 7 -
3.1.2	telnet 접속 확인	- 8 -
3.1.3	접속하기.....	- 9 -
3.2	통신 실험	- 12 -
3.2.1	Putty 터미널 확인.....	- 12 -
3.2.2	시리얼 터미널 확인.....	- 12 -
4	변경 이력	- 13 -

1 개요

1.1 SSH (Secure Shell)

SSH는 Secure Socket Shell이라고도 불리며 네트워크 장비 사이의 데이터 교환이 보안상 안전한 채널을 통해 이루어지도록 함으로서 원격 컴퓨터에 안전하게 액세스 할 수 있도록 만들어진 네트워크 프로토콜입니다. 현재 인터넷 환경에서 보안 유지에 널리 사용되고 있는 프로토콜이며 당사 제품은 SSH2 버전을 지원합니다.

1.2 ezTCP 적용

본래 SSH는 네트워크 관리자들이 각종 서버들을 원격지에서 제어하기 위해 기존의 Telnet을 대체하여 만들어진 프로토콜입니다. 기존 EZL Series 제품(예: EZL-200F)에는 이러한 목적에 맞게 적용되어 Telnet 대신 SSH 접속을 통해 ezTCP 제품의 장비 상태 점검, 환경변수 설정 등을 수행합니다.

본 문서는 이러한 SSH의 로그인 채널을 시리얼 포트를 통해 실제 오고 가는 데이터의 보안을 위해 사용하는 데이터 통신용 채널로의 SSH 사용에 대한 응용 문서이며 해당 제품은 CSE-M32, CSE-M73, CSE-H20, CSE-H21, CSE-H25 입니다.

시리얼 콘솔 포트가 있는 장비와 ezTCP를 시리얼로 연결하고 ezTCP에 리눅스 SSH 접속으로 연결하면 해당 콘솔 포트를 SSH 콘솔 포트로 사용이 가능합니다.

2 설정하기

2.1 설정하기 전에

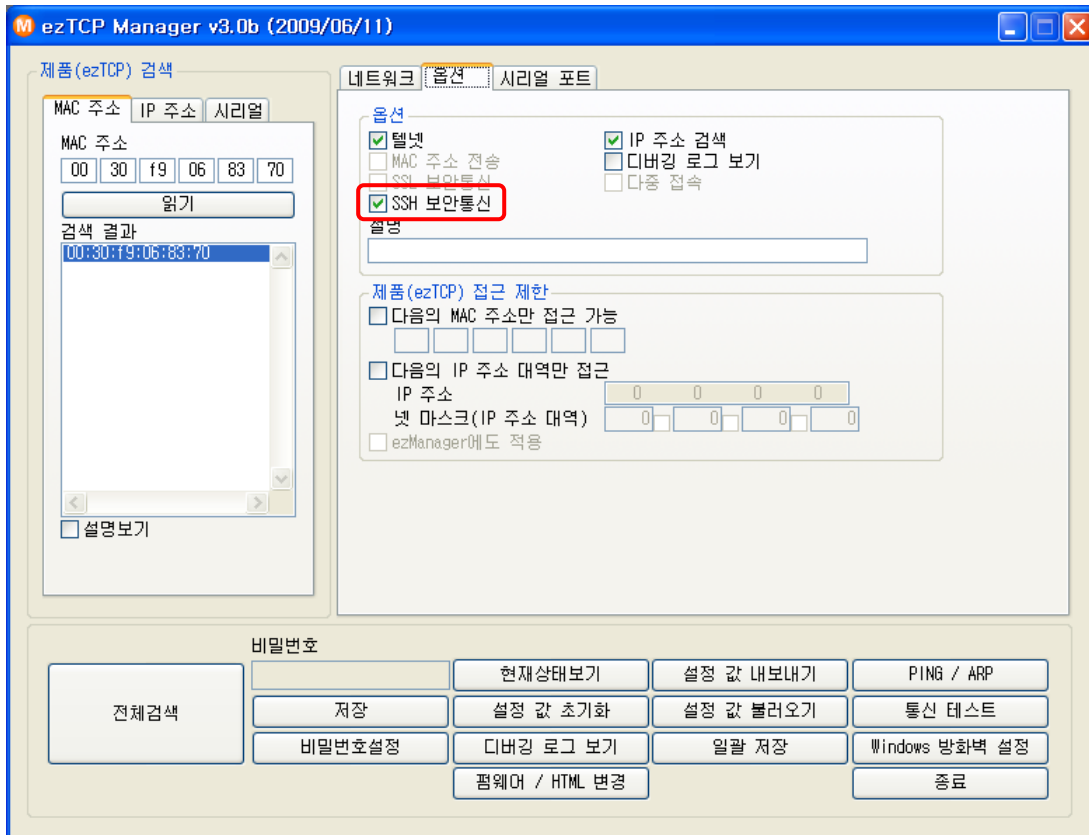
- ezTCP Mode T2S(0) – TCP Server 모드만 사용할 수 있습니다.
- SSH 기능 사용 중에 다음 기능을 사용할 수 없습니다.
SSL, Telnet COM Port Control Option
- SSH 기능 사용 중 각 제품별 제약 사항은 다음과 같습니다.
CSE-M32, CSE-H20, CSE-H21 –COM2 사용 불가
CSE-M73, CSE-H25 –멀티 모니터링 기능 사용 불가

2.2 SSH 기능 설정 하기

SSH 기능은 TCP 서버 모드에서만 사용 가능합니다.

2.2.1 SSH 기능 활성화 – ezManager 설정

아래의 그림과 같이 [옵션] 탭의 [SSH 보안통신] 항목을 설정합니다.

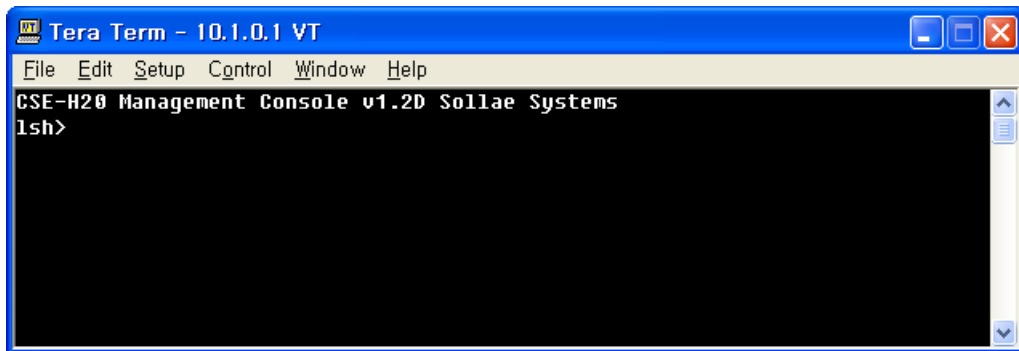


2.2.2 키 생성

- SSH와 관련된 telnet 명령어는 다음과 같습니다.

항목	명령어	설명
RSA KEY	rsa keygen <key length>	지원 KEY 길이 512/768/1024
	rsa key	생성된 RSA KEY 확인
	rsa test	생성된 RSA KEY 테스트
DSA KEY	dsa keygen	RSA KEY 생성 후 실행
	dsa key	생성된 DSA KEY 확인
ID/PW	ssh id	로그인 ID / PW 설정
설정 저장	ssh save aa55cc33	SSH 관련 설정 저장

- ezTCP의 텔넷 콘솔에 접속합니다.



- ☞ 제품에 비밀번호가 설정되어 있다면 텔넷 접속 시 비밀번호를 입력해야 합니다. 또한 펌웨어 버전 2.0A부터는 비밀번호가 설정되어 있지 않더라도 "sollae"를 입력해야 합니다.

- RSA KEY 생성

RSA KEY를 먼저 생성합니다. KEY 길이는 512, 768, 1024 바이트를 지원하며 생성할 때 그 크기에 따라 수분이 걸릴 수도 있으며 KEY가 길면 길수록 시간이 길어집니다. 1024 바이트의 KEY는 평균 1분 정도 소요됩니다. 명령어 형식은 다음 화면과 같이 'rsa keygen <key length>'의 형식으로 입력하십시오.

```

Tera Term - 10.1.0.1 VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
1sh>rsa keygen 1024
average 50sec required to find two 512bits prime numbers, please wait..
rsa: find 512bits random prime p..1 2 4 11 13 16 17 22 23 26 32 41 52 53 59
64 68 71 74 82 83 92 94 97 101 104 131 136 142 143 148 149 157 176 178 179 1
84 187 202 206 211 223 236 239 241 244 257 263 274 284 286 289 298 317 328 3
32 334 344 353 356 368 374 379 386 389 391 394 404 407 412 416 421 422 431 4
39 442 443 446 449 472 473 478 484 487 533 538 547 559 562 563 577 583 586 5
87 592 599 604 607 613 617 626 628 631 643 652 653 659 668 677 683 694 698 7
09 716 727 731 734 739 746 764 769 772 778 781 794 808 818 823 829 838 856 8
57 859 878 902 904 907 908 913 914 916 929 937 949 956 976 977 991 1003 1004
1012 1021 1024 1027 1031 1033 1034 1037 1046 1051 1058 1079 1088 1091 1094
1097 1103 1108 1111 1117 1123 1138 1142 1144 1154 1157 1163 1168 1174 1181 1
186 1192 1214 1222 1223 1229 1238 1277 1297 1301 1303 1304 1307 1313 1322 13
39 1342 1343 1346 1348 1361 1369 1376 1378 1391 1394 1403 1408 1409 found
rsa: find 512bits random prime q..1 2 7 13 14 17 22 26 29 31 34 38 44 47 59
61 64 71 73 76 77 83 86 92 97 98 106 122 133 142 149 157 163 167 176 187 188
191 196 203 211 212 226 229 233 238 241 248 254 259 274 281 286 299 301 304
313 331 332 337 343 344 346 352 353 356 359 362 373 377 383 386 388 391 394
401 406 409 412 416 421 428 442 443 446 449 458 467 479 482 497 509 511 523
524 537 541 544 551 559 566 577 584 586 587 593 598 616 632 638 644 found
rsa: RSA key pair(public/private key) generated.
rsa: key validation OK
1sh>
  
```

생성된 RSA KEY는 'rsa test' 명령어를 통해 정상적으로 생성되었는지 테스트가 가능하며 현재 제품의 RSA KEY는 'rsa key' 명령어를 통해 확인이 가능합니다.

- DSA KEY 생성

RSA KEY가 정상적으로 생성되었으면 'dsa keygen' 명령어를 통해 DSA KEY를 생성하십시오.

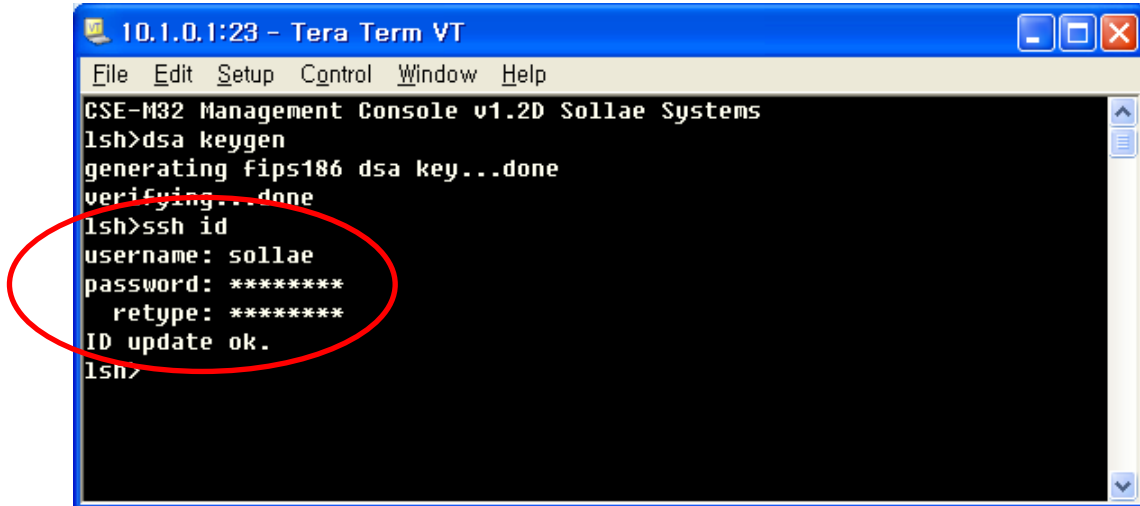
```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
1sh>dsa keygen
generating fips186 dsa key...done
verifying...done
1sh>
  
```

현재 생성된 DSA KEY는 'dsa key' 명령어를 통해 확인이 가능합니다.

- 로그인 ID / PW 설정

SSH 로그인을 위한 ID와 비밀번호를 'ssh id' 명령어를 통해 설정하십시오.

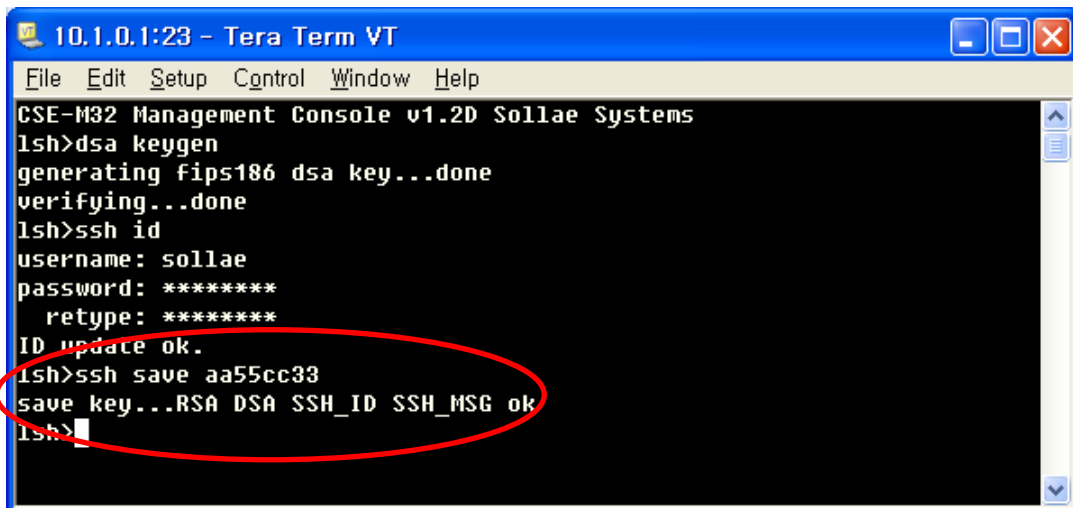


```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
lsh>dsa keygen
generating fips186 dsa key...done
verifying...done
lsh>ssh id
username: sollae
password: *****
retype: *****
ID update ok.
lsh>
  
```

- 설정사항 저장

SSH 보안 통신을 위해 생성된 RSA KEY, DSA KEY와 ID/PW를 제품의 비휘발성 메모리에 저장해야 합니다. 명령어는 'ssh save aa55cc33'입니다.



```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE-M32 Management Console v1.2D Sollae Systems
lsh>dsa keygen
generating fips186 dsa key...done
verifying...done
lsh>ssh id
username: sollae
password: *****
retype: *****
ID update ok.
lsh>ssh save aa55cc33
save key...RSA DSA SSH_ID SSH_MSG ok
lsh>
  
```

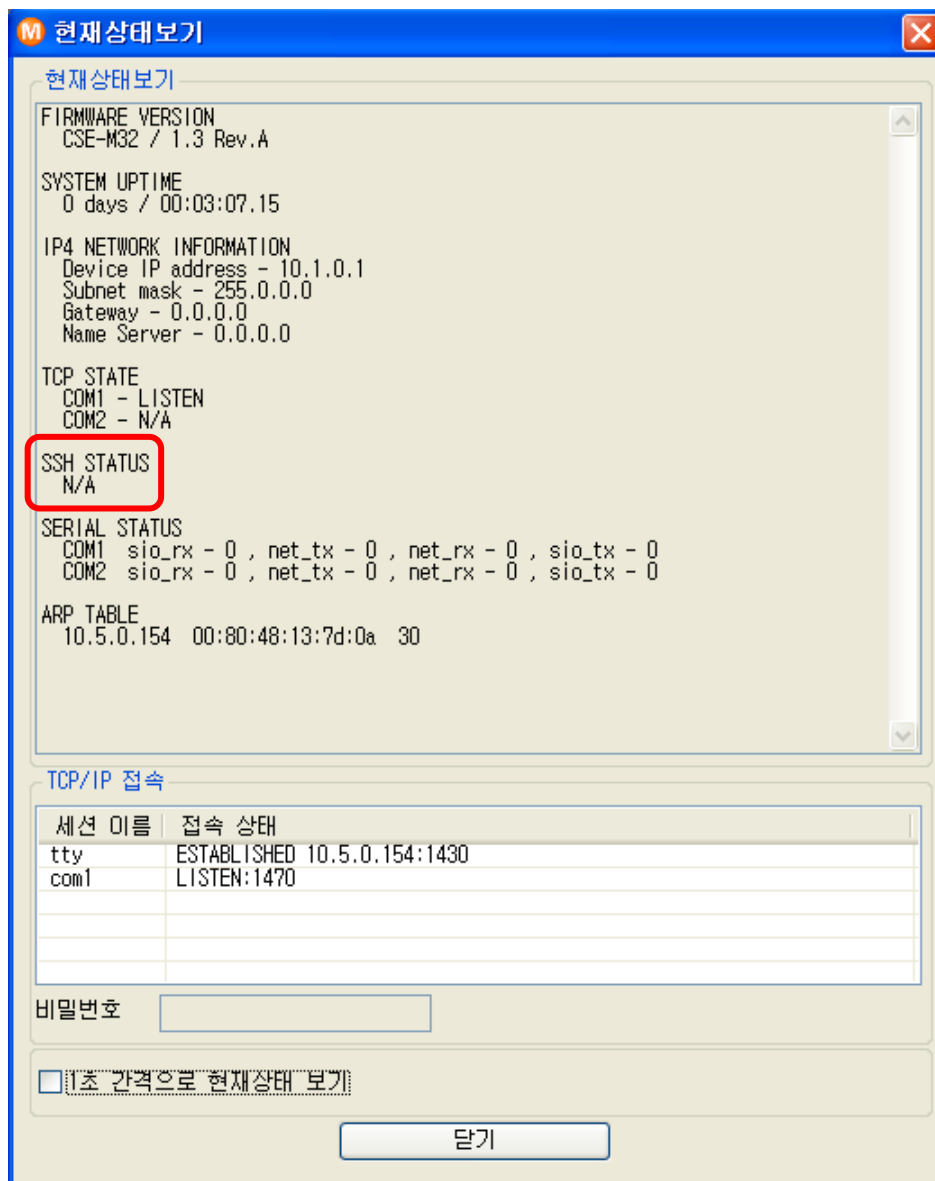
3 사용 예

SSH 서버로 동작하는 제품에 SSH 클라이언트 프로그램으로 설정된 사용자 ID와 PW 입력을 통해 로그인 후 시리얼 장비와 데이터 통신을 합니다.

3.1 통신 준비

3.1.1 ezManager 확인

ezManager에서 [현재상태보기] 버튼을 눌러 현재 상태를 확인합니다.



위 그림과 같이 SSH STATUS 항목이 나타나는지 확인하십시오.

3.1.2 telnet 접속 확인

제품의 텔넷 콘솔에 접속해 RSA KEY, DSA KEY와 사용자 ID/PW를 확인합니다. 관련 명령어는 'rsa key', 'dsa key', 'ssh id'입니다. 'ssh id' 명령어 입력하면 사용자 ID/PW가 출력되고 (PW는 '*'로 표현됩니다.) 새로운 사용자 ID를 요구합니다. 이 때 엔터를 입력하면 현재 설정 값 확인 후 종료가 되며 사용자 ID/PW를 분실했을 때는 새로운 사용자 ID/PW를 입력하면 됩니다. 사용자 ID/PW를 새로 입력한 후에는 반드시 'ssh save aa55cc33' 명령어를 통해 현재 설정을 저장해야 합니다.

```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
CSE-M02 Management Console v1.2D Sollae Systems
1sh>rsa key
RSA public modulus: 512 bits
+ bc:e4:43:92:50:d6:00:fd:e3:ad:4d:8b:20:1c:f0:82
+ 0a:7f:0f:cc:cc:62:ba:be:d1:e9:03:c3:be:8d:6a:33
+ 49:b6:a6:77:cc:07:ff:a3:31:65:a9:2f:ff:70:66:77
+ e0:a6:07:01:43:42:2c:4d:f2:ec:bf:9a:6b:51:b6:97
RSA public exponent: 24 bits
+ 01:00:01
1sh>dsa key
DSA public prime P: 1024 bits
+ e2:18:9f:b9:ea:48:04:b8:5d:ce:94:d2:fb:08:f5:50
+ 8c:52:0b:7d:dc:ee:50:90:49:09:e9:a9:3c:1d:ae:b6
+ 9e:e2:cf:46:d0:2b:7d:db:43:05:f4:61:21:a8:1a:4d
+ 1e:4e:fd:44:87:2a:dd:58:9e:de:33:64:8d:e6:48:70
+ e7:b8:e2:33:99:00:20:e3:92:2b:01:dd:00:62:70:b3
+ 88:51:91:84:c1:5b:2a:93:08:b3:93:b4:89:68:4d:d6
+ 34:51:e7:45:53:c1:57:2f:6e:32:49:52:b8:1c:0d:a3
+ 8a:db:ea:00:3b:a6:4b:bd:f4:30:7b:24:ae:80:ab:b7
DSA public sub prime Q: 160 bits
+ e8:d4:e3:5b:e1:ee:5e:5a:d9:64:03:91:28:06:f9:51
+ 38:0c:8b:7d
DSA public base G: 1024 bits
+ a4:e4:de:58:0d:d6:e4:3e:5e:04:0f:a1:1a:91:07:5f
+ 1d:55:ac:02:68:dd:d0:24:da:87:2c:8e:5c:29:5e:14
+ 0b:44:f6:ba:27:22:04:da:74:ea:85:ac:ef:14:30:fc
+ 61:e4:e1:bf:fe:7d:02:79:8f:61:2a:55:96:78:99:65
+ c6:d0:fa:e0:06:fa:bf:40:5d:a1:61:5a:a8:5c:96:c6
+ 09:6e:28:36:40:b8:4e:f9:7f:20:59:09:a2:0a:d2:36
+ d6:8f:0a:a7:b9:f1:d9:cf:15:61:5d:c7:c4:fc:d7:8c
+ 4a:f0:94:a3:99:49:9d:76:41:c9:96:fb:50:11:31:d3
1sh>ssh id
sollae : *****
username :
1sh>

```

3.1.3 접속하기

SSH 기능이 활성화된 ezTCP와 통신을 하려면 상대 호스트에 SSH를 지원하는 클라이언트가 있어야 합니다. 본 절에서는 상용 무료 SSH 클라이언트 Putty 프로그램을 이용한 접속 테스트 과정을 소개하겠습니다.

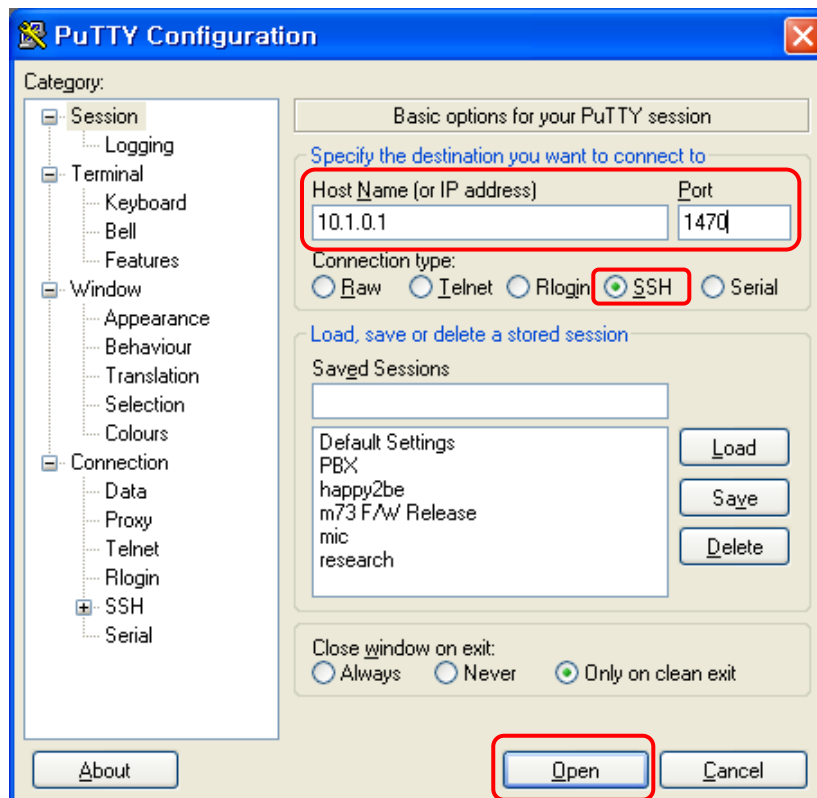
- 설정 전 확인 사항

제품의 IP 주소와 Port 번호는 ezTCP가 설치된 환경에 맞게 설정해야 합니다. 이해를 돕기 위해 제품의 IP는 공장 출하 값 그대로 가정하고 설정사항을 확인해 주십시오.

	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

- Putty 설정사항

다음의 Putty 초기화면에서 표시된 부분과 같이 ezTCP 제품의 Local IP Address와 Local Port 번호를 입력하십시오.



입력 후 위 그림과 같이 Connection type이 SSH인지 확인하고 Open 버튼을 누르십시오.

- 서버 키 확인

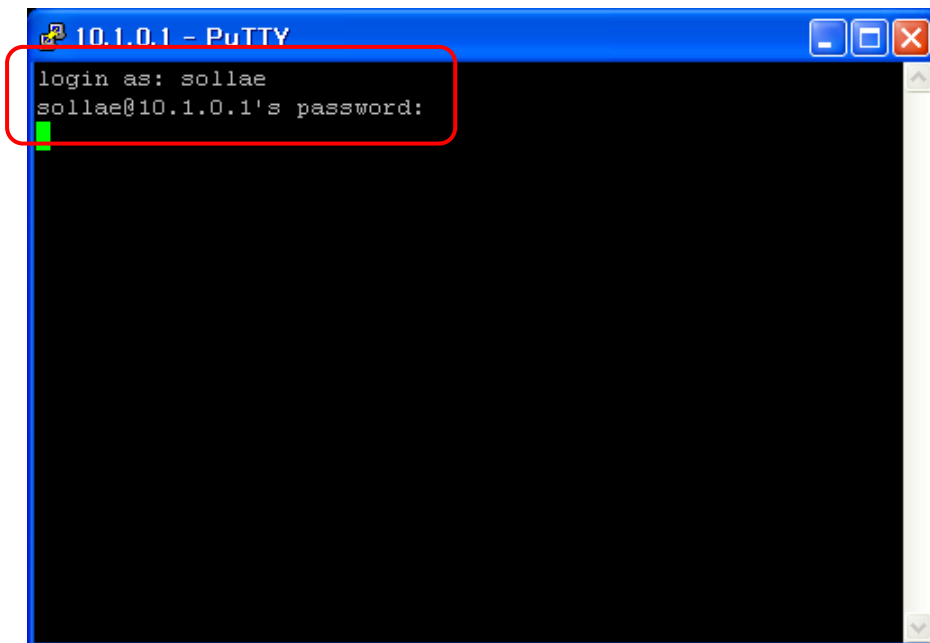
ezTCP 제품의 SSH 기능 활성화 후 처음으로 접속할 때 다음과 같은 화면이 나타납니다.



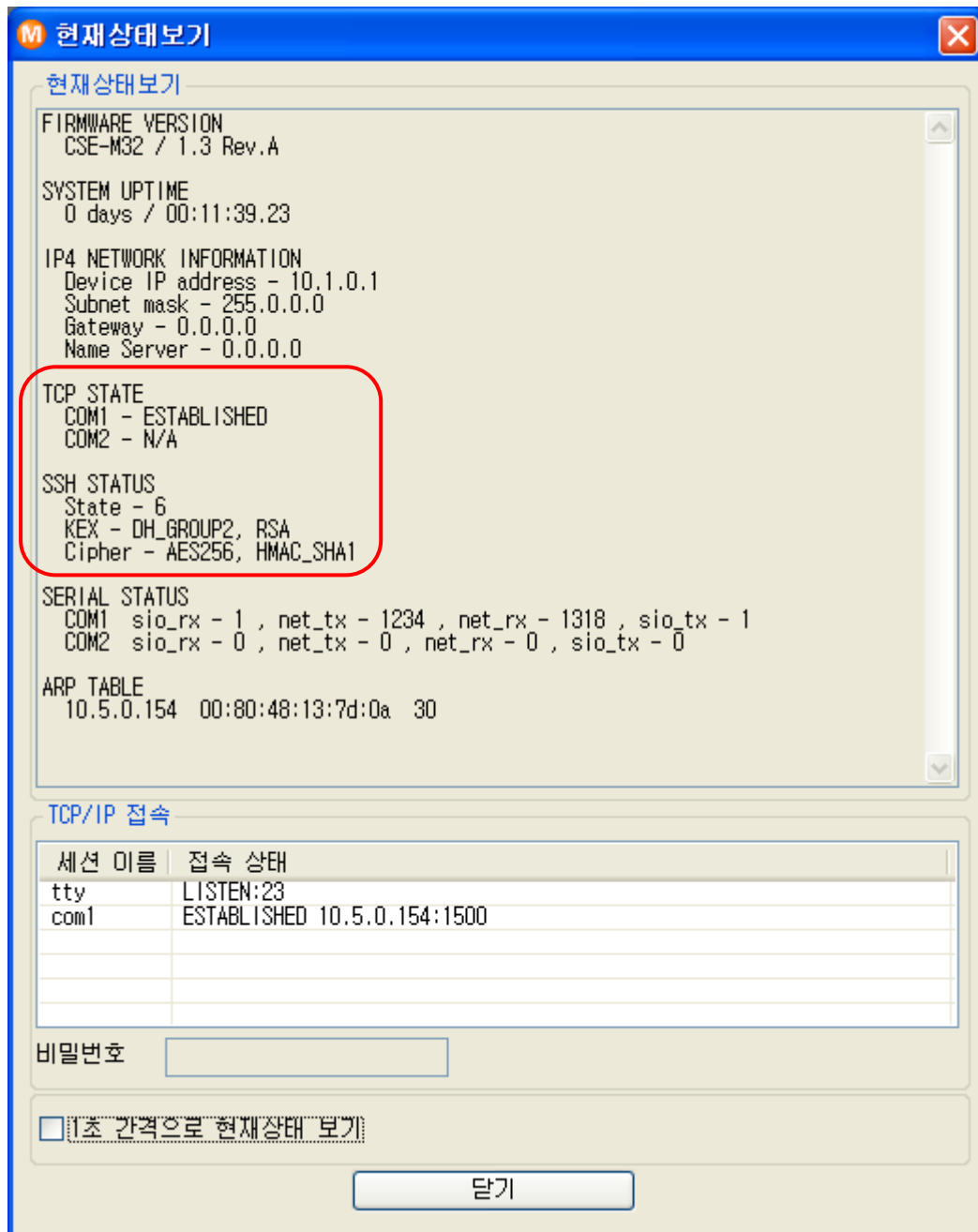
ezTCP 제품의 키 정보 값이 한번도 저장된 적이 없을 때 나오는 화면으로 최초 접속할 때 나타나며 '예(Y)' 버튼을 누르고 다음으로 진행하십시오. 한번 키 값이 저장되면 추후 다시 저장 여부를 묻지 않습니다. 단 ezTCP 제품의 키 값을 변경하면 그 후 최초 접속할 때마다 새로운 키 값을 저장해야 됩니다.

- 로그인 하기

다음은 접속 후 첫 화면입니다. 사용자 ID/PW를 요구하며 이 때 미리 설정된 ID/PW를 순서대로 입력하십시오.



- TCP 접속 확인
ezManager에서 [현재상태보기] 버튼을 눌러 현재 상태를 확인합니다.



위 그림과 같이 TCP STATE 항목의 [COM1 - ESTABLISHED], SSH STATUS 항목의 [State - 6], [Cipher - AES_256, HMAC_SHA1] 이 나타나고 통신 준비가 완료된 것을 확인할 수 있습니다.

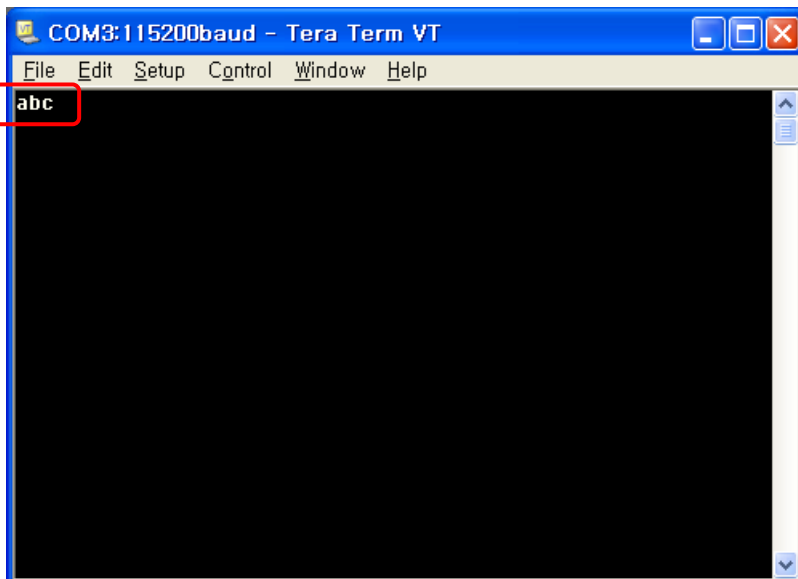
3.2 통신 실험

SSH 접속 후 ezTCP 제품의 시리얼 포트를 터미널로 오픈하여 양방향으로 데이터가 오고 가는지 확인하십시오. 시리얼 터미널 창에 "123"이라는 데이터를 보내면 Putty 터미널에 "123"이 나타나고, 반대로 Putty 터미널 창에 "abc" 데이터를 보내면 시리얼 터미널 창에 "abc" 데이터가 나타납니다. 이 때 오고 가는 데이터는 암호화되어서 송신 및 수신되므로 일반 통신 모드 때와는 달리 안전하며 높은 보안이 요구되는 환경에서 사용에 적합합니다.

3.2.1 Putty 터미널 확인



3.2.2 시리얼 터미널 확인



4 변경 이력

날짜	버전	설명	작성자
2008.09.04	1.0	○ 최초 배포	-
2009.08.03	1.1	○ 일부 용어, 그림 및 내용 오류 수정 ○ 지원 제품 CSE-H25 추가	-
2016.04.07	1.2	○ 텔넷 접속 관련 안내문구 추가	이 인