Projector/Monitor
Control Command
Authentication Flow Specifications

BDT180004
Revision1.1

Introduction

This manual describes the specifications related to the authentication flow in communicating with a projector or monitor made by NEC which supports the authentication function in sending or receiving a control command.
As the authentication function allows only pre-registered users (with user name and password) to communicate, the security level therefore improves.

The manual assumes a basic knowledge of projectors or monitors. For information about the connection between the projector or monitor and an external device, see the operation manual for the model being used.

Notes

1. The acts of disclosure, duplication, and modification of part or whole contents in this reference manual without permission are prohibited.
2. The contents of this reference manual are subject to change without notice.
3. Great care has been taken in the preparation of this reference manual; however, should you notice any questionable points, errors or omissions, please contact us. See the User's Manual of the model you use to find the contact details.
4. Notwithstanding article 3. NEC will not be responsible for any claims on loss of profit or other matters deemed to result from using this reference manual.

Contents

Projector/Monitor Control Command Authentication Flow Specifications................................1

Introduction 2

Contents.. 3

1. **Authentication flow...4**

1.1 Overview... 4

1.2 Sequence diagram 5

1.3 Details.. 6

2. **Example of authentication flow..7**

3. **Revision History...8**

1. Authentication flow

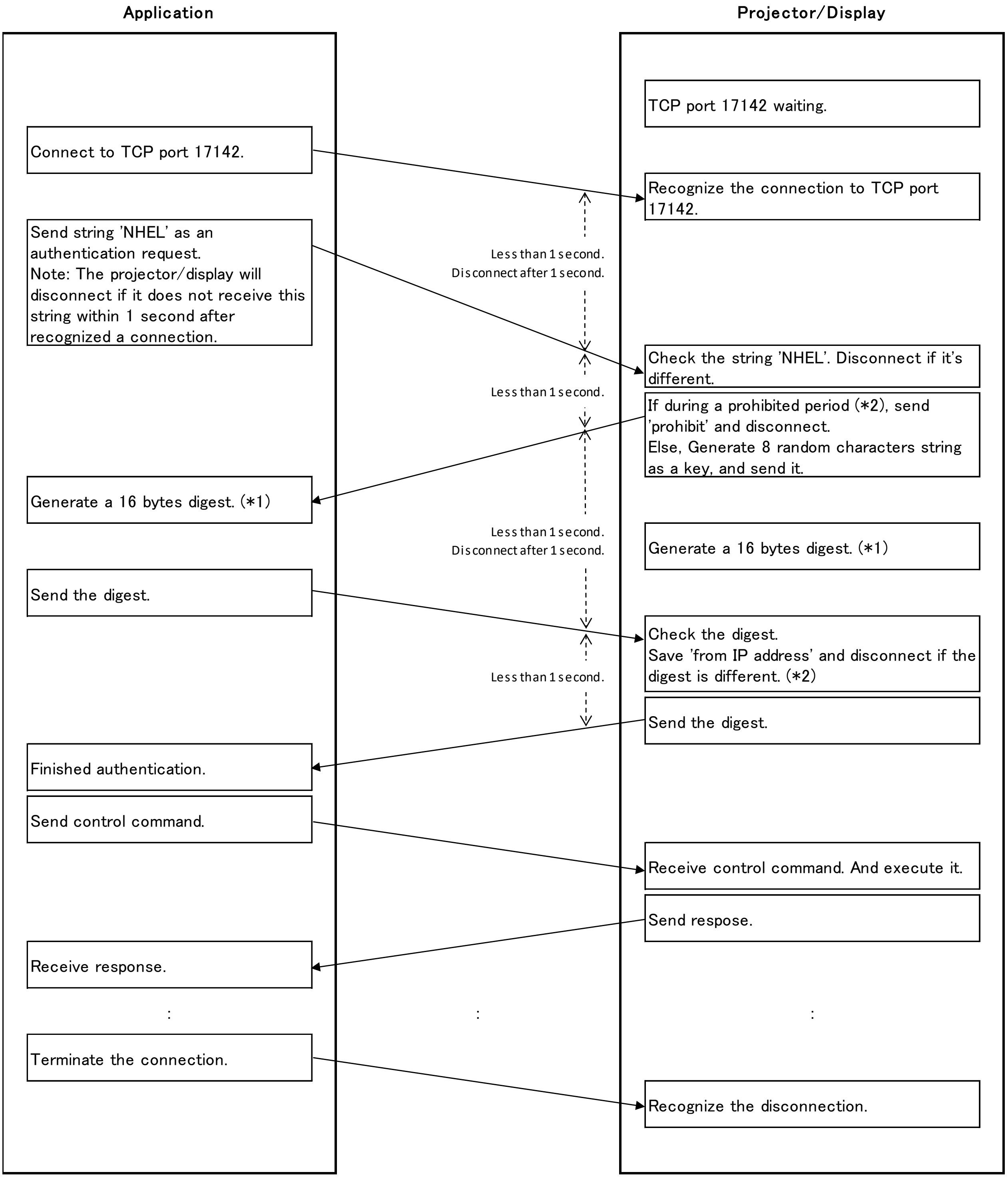
1.1 Overview

When the authentication function is enabled in the projector or monitor, it is necessary to carry out the authentication process in order to control the projector or monitor using control commands. The authentication flow is carried out when a connection is established using a combination of user name and password.

User name	ASCII 1 - 16 characters (ASCII code: 0x20 - 0x7e)
Password	ASCII 1 - 16 characters (ASCII code: 0x20 - 0x7e)

See the User’s Manual (“Authentication Settings” etc.) of the model you are using for details on how to set the authentication function of the projector or monitor.

1.2 Sequence diagram



Application

Projector/Display

TCP port 17142 waiting.

Connect to TCP port 17142.

Recognize the connection to TCP port 17142.

Send string 'NHEL' as an authentication request.
Note: The projector/display will disconnect if it does not receive this string within 1 second after recognized a connection.

Less than 1 second.
Disconnect after 1 second.

Check the string 'NHEL'. Disconnect if it's different.

Less than 1 second.

If during a prohibited period (*2), send 'prohibit' and disconnect.
Else, Generate 8 random characters string as a key, and send it.

Generate a 16 bytes digest. (*1)

Less than 1 second.
Disconnect after 1 second.

Generate a 16 bytes digest. (*1)

Send the digest.

Check the digest.
Save 'from IP address' and disconnect if the digest is different. (*2)

Less than 1 second.

Send the digest.

Finished authentication.

Send control command.

Receive control command. And execute it.

Send respose.

Receive response.

:

Terminate the connection.

Recognize the disconnection.

(*1)

MD5 of "'key' + ';' + 'user' + ';' + 'password'"

ex.) key = '238a76cf', user = 'Admin', password = 'Password'

MD5 = '3d6ae16b690b148c3160f458a4d4e5a7'

Digest = 0x3d, 0x6a, 0xe1, 0x6b, 0x69, 0x0b, 0x14, 0x8c, 0x31, 0x60, 0xf4, 0x58, 0xa4, 0xd4, 0xe5, 0xa7

(*2)

When the digest sent from the same IP address made a mistake 5 times, an authentication prohibited period is set for 5 minutes.
The cumulative number of the times will be cleared 5 minutes later.
It will also be cleared when receiving a right digest.

1.3 Details

The authentication procedure is as follows.

① Connect to the TCP 17142 port on the projector or monitor from the application.

② Establish a connection with the projector or monitor.

③ Send the character string “NHEL” as an authentication request from the application.

- Send within 1 second after the connection is established.
- After 1 second, the connection will be disconnected from the projector or monitor

④ Check the character string received in the projector or monitor and if the character string is different from “NHEL”, disconnect the connection.

⑤ Send a random character string of 8 characters as a key from the projector or monitor within 1 second after ④.

- During the connection prohibited period, send the character string “prohibit” and disconnect the connection.
- If a different digest is received consecutively for 5 times from the same IP address, the connection is disconnected and connection will be prohibited for 5 minutes.
- The number of times that a different digest is received is cleared after 5 minutes. It is also cleared when authentication is completed.

⑥ Generate a 16-byte digest from the “user name”, “password” and “key” in both the application and the projector or monitor.

- See (*1) in the “1-2. Sequence Diagram” for details.

⑦ Send the digest generated in ⑥ from the application.

⑧ The projector or monitor will compare the digest generated in ⑥ and the digest received in ⑦.

- If they do not match, save the IP address of the transmission source and disconnect the connection.
- Count the cumulative number of times that a different digest was received from the same IP address for 5 minutes.

⑨ If the result in ⑧ matches, the projector or monitor will send the digest generated in ⑥ within 1 second after ⑧.

- Clear the cumulative number of times that a different digest was received from the same IP address.

⑩ The authentication flow ends upon receiving the digest generated in ⑥ from the projector or monitor.

⑪ Hereinafter, the same control command as in the case the authentication is not used will be sent and received.

2. Example of authentication flow

An example of the authentication flow is described here when the user name and password are as follows.

[NOTE] Circled numbers conform to the numbers in “1.2 Sequence Diagram”.

User name	Admin
Password	Password

③→④: Authentication request

Character code (Hexadecimal)	4e	48	45	4c
Character	N	H	E	L

⑤→⑥: Random character string (key)

Character code (Hexadecimal)	32	33	38	61	37	36	63	66
Character	2	3	8	a	7	6	c	f

⑦→⑧: Digest

Hexa−decimal	3d	6a	e1	6b	69	0b	14	8c	31	60	f4	58	a4	d4	e5	a7

⑨→⑩: Digest

Hexa−decimal	3d	6a	e1	6b	69	0b	14	8c	31	60	f4	58	a4	d4	e5	a7

3. Revision History

Revision	Date	Description
1.0	October 25, 2018	First version
1.1	July 17, 2019	Errata correction Contents of *1 in “1.2 Sequence diagram” Contents of Digest in “2. Example of authentication flow”