# Ethernet I/F Card

# IFBD-HE07/08 -BE07

# User's Manual

Rev. No. 3.00

Star Micronics Co., Ltd.

# Contents

# 1. GENERAL DESCRIPTION

This is an embedded network interface card (printer server) for STAR POS printers.*

* In this document, this product is called NIC (an acronym for network interface card).

## 1.1 Features

- Supports Star Micronics POS printers (including card readers and writers).
  See section 2.1 Model Names for details on supported printers.
  This product receives electric power from the printer, so there is no need to prepare a separate AC adapter.
- The physical layer conforms to IEEE802.3/3u (10BASE-T/100BASE-TX).
- Ethernet communication settings (10BASE-T/100BASE-TX, Full/Half Duplex) with the connected device are doen using Auto Negotiation.
- This can be used in a LAN (Local Area Network) environment.
- Communication protocols support TCP/IP (IPv4).
- Prints using LPR, Raw Socket Print (TCP #9100) and FTP protocols.
- This receives status information (ready status, causes of errors, and the like) issued from the printer and allows that information to be loaded onto a PC.
- Can be used simultaneously from multiple protocols.
  Raw Socket Print (#9100) also prints using multi-session.(*1)
  (Note *1) The factory default setting for multi-session for Raw Socket Print (#9100) differs between the old product IFBD-HE05/06/BE05 and this product IFBD-HE07/08/BE07.Be careful if you are switching from an old product.
  IFBD-HE05/06/BE05 (old product): Valid
  IFBD-HE07/08/BE07 (this product): Invalid
- The IP address for this product can be static or obtained by DHCP/BOOTP, RARP, ARP/Ping.
- Flash ROM is mounted on the board. Firmware updates are possible via FTP over a network.
- You can change this product and printer settings and monitor their states using device specific setting utilities, HTTP (WEB), TELNET, and FTP.
  Network settings that are set using HTTP (Web), Telnet, FTP for the IP address and #9100 multi-session are stored in the product's non-volatile memory.
- To be prepared for the unlikely event that the main firmware malfunctions for some reason, the boot loader of this product is provided a TFTP client function to allow you to download firmware from the server over the network for recovery of your firmware.
- Supports Star Micronics' Windows Printer Driver, OPOS Driver, JPOS Driver (Windows, Linux, and Mac), CUPS Driver (Linux, Mac)
- Supports the proprietary StarWebPRNT function from STAR MICRONICS CO., LTD. that allows direct printing from Web applications that support HTML 5. (IFBD-HE07X/08X/BE07X only)

## 1.2 Differences between IFBD-HE07/08/BE07 and IFBD-07X/08X/BE07X

IFBD-HE07/08/BE07 and IFBD-07X/08X/BE07X are different products. Some of these products support StarWebPRNT and some do not.

IFBD-HE07/08/BE07: StarWebPRNT not supported
IFBD-HE07X/08X/BE07X: StarWebPRNT supported

IFBD-HE07X/08X/BE07X is upwardly compatible with IFBD-HE07/08/BE07, and except for sections involving the StarWebPRNT function the specifications for IFBD-HE07/08/BE07 are covered by the specifications for IFBD-HE07X/08X/BE07X.

See "4. StarWebPRNT Function" for more details.

## 1.3 Main Settings At the Time of Shipment (Overview)

The main TCP/IP settings required to use this product are outlined below.

See section “3.3 Settings and Display Items” for a list of settings that are not listed here.

### 1.3.1 IP Parameter Factory Shipment Settings

| | |
|---|---|
| IP address | 0.0.0.0 |
| Sub-net Mask | 0.0.0.0 |
| Default Gateway | 0.0.0.0 |
| RARP Client | Valid |
| DHCP/BOOTP Client | Valid |

### 1.3.2 Log-in Password oo Administrator Right Setting At the Time of Factory Shipment

If product settings are changed, use either of the protocols of HTTP (WEB), TELNET, or FTP to log-in with an account having administrator rights for this product.
The following outlines administrator account information in HTTP (WEB), TELNET, and FTP.

| | |
|---|---|
| Administrator Account Name | “root” (required) |
| Password | “public” (required) |

* The password can be changed after logging in.

### 1.3.3 Log-in Password of User Right Setting At the Time of Factory Shipment

If only viewing this products settings or status information using TELNET or FTP, it is necessary to log-in with a user right account for this product. It is not necessary to log-in to view status information using HTTP (WEB).
The following outlines user right account information in TELNET and FTP.

| | |
|---|---|
| User Right Account Name | “user” (required) |
| Password | “guest” (required) |

However, for FTP, it is possible to log-in as anonymous (any account name and password).

* The password can be changed after logging in.

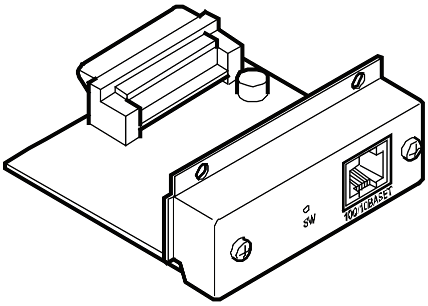
### 1.3.4 IP Address Setting

There are two ways to set this product’s IP address. They are the static method (fixed conditions) and dynamic (DHCP/BOOTP, RARP, and ARP/Ping).
See section 3.1.1 Setting the IP Address” for details on the process to acquire an IP address.
Static and dynamic settings cannot both be valid at the same time. For that reason, it is necessary to disable the dynamic settings (DHCP/BOOTP, RARP) to use static settings (a fixed IP address written to non-volatile memory).
Also, if the dynamic settings (DHCP/BOOTP) are valid, it is necessary to set all static settings (IP address, sub-net mask, and default gateway) to 0.0.0.0.
When using this product, take care that when setting using HTTP (WEB), FTP or TELNET, that both of these are not valid at the same time.
Acquired address information while operating can be checked by making a self-print when starting up the power.

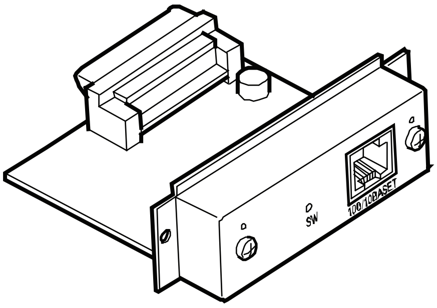
# 2. HARDWARE SPECIFICATIONS

## 2.1 Model Names

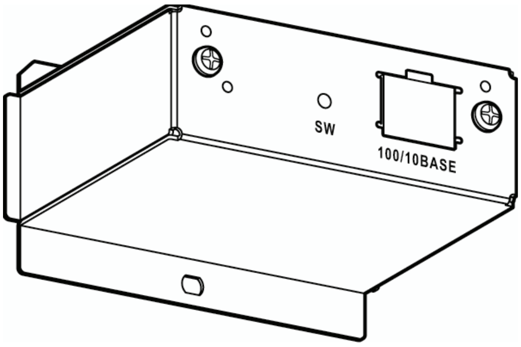
There are three models available. They differ in the bracket for mounting to the printer.
Models that support StarWebPRNT have an “X” at the end of the model names.



IFBD-HE07 / IFBD-HE07X



IFBD-HE08 / IFBD-HE08X

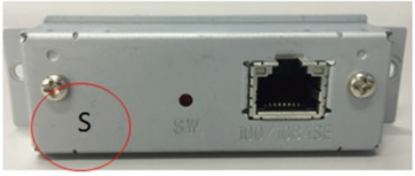


IFBD-BE07 / IFBD-BE07X

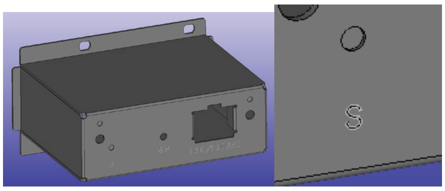
Products that support SSL/TLS have a "S" shape engraved on the NIC chassis. (F/W Ver4.0.0 and later supports SSL/TLS. However, products that do not have an engraved “S” shape, cannot support SSL/TLS even if the F/W is upgraded to Ver. 4.0.0 or later.)

The position of the engraved "S" shape

IFBD-HE



IFBD-BE



If this product has F/W Ver. 5.0.0 or later, there is an “M” shape engraved next to the above “S” shape.

The following shows example printers that comply with the product names.

| Product Model Name | Compatible Printer (Representative Examples) |
|---|---|
| IFBD-HE07 | TSP700II, TSP800II, TSP650(*1), TSP650II<br>TSP828L(*1), TUP500(*1), TCP300II(*1), TCP400(*1) |
| IFBD-HE08 | TSP1000(*1), SP700, SP500(*1), HSP7000(*1) |
| IFBD-BE07 | FVP10 |

The models indicated by (*1) are not supported by this product with F/W Ver. 5.0.0 or later.
See “5.2. Printer Firmware Support Table”, for details on the printers that support IFBD-HE07X/08X/BE07X.

Refer to each printer product specifications for details on models and mounting conditions.

## 2.2 Specifications

| | |
|---|---|
| Network I/F Unit: | IEEE802.3/3u<br>(10BASE-T Ethernet / 100BASE-TX Fast Ethernet) |
| LED: | Red x 1; Green x 1<br>Red: LINK/Activity<br>Green: 100BASE-TX<br>*Displays with flashing patterns when executing a special mode. |
| Switch for Settings: | Push Switch x 1<br>DIP SW (dipole) x 1<br>See sections 3.2.2 Push Switches and 3.2.3 DIP Switches for details on each specification. |
| PCB Dimensions: | 69 mm x 61 mm (Tolerance ± 0.5 mm)<br>t = 1.6 mm (Tolerance ± 0.2 mm) |
| Product Weight: | IFBD-HE07: Approximately 63 g<br>IFBD-HE08: Approximately 65 g<br>IFBD-BE07: Approximately 118 g<br>The weights above do not include packing materials or accessories. |
| Power Supply: | Operating Voltage 5V ±5%<br>Rated Current Consumption 500 mA Max. |

## 2.3 Ambient Conditions

| | |
|---|---|
| Ambient Storage Conditions: | Storage Temperature: -20˚C - +70˚C |
| | Storage Humidity: 20% - 90% (Must be no condensation) |
| Ambient Operating Conditions: | Operating Temperature: 0˚C - +55˚C |
| | Operating Humidity: 20% - 80% (Must be no condensation) |

## 2.4 Compatible Specifications

| | | |
|---|---|---|
| EMI | FCC | Part15 Class A |
| | VCCI | Class A |
| | EN55022 Class B | |

## 2.5 Connector Specifications

### 2.5.1 Network Interface (RJ45)

Manufacturer and Model Number
Hirose Electric Co., Ltd. TM11R-5M2-88-LP

Pin Number

| Pin Number | Signal Name | Direction | Remarks |
|---|---|---|---|
| 1 | TX+ | Output | |
| 2 | TX- | Output | |
| 3 | RX+ | Input | |
| 4-5 | NC | - | |
| 6 | RX- | Input | |
| 7-8 | NC | - | |

I/F card is the standard for direction.

The pin at the right toward the insertion side is pin 1.

## 2.6. Ethernet Communication Conditions

The communication link conditions with the connecting device of the Ethernet are determined by Auto Negotiation.

If this product is connected directly to an intelligent switch hub or intelligent hub, the physical link may take some time to become established.
In such cases, if set to get the IP address from a DHCP/BOOTP server, a timeout error could occur while waiting to get the address from DHCP/BOOTP, and it will fail to get the address. (Note 1) A workaround is to change the DIPSW1 to invalidate the timeout for getting the IP address. For details on how to set DIPSW 1, see section 3.2.3 DIP Switches.

Note 1: This issue sometimes can be overcome by setting up a normal hub (non-intelligent) between the product and intelligent switch.

## 2.7. Network Connection Cable

If the connecting device (hub, router or PC) does not support Auto MDI/MDI-X, be careful of the type of cable you use (straight or cross). Normally, when connecting to a hub or router (MDI-X), use a straight cable. For a PC (MDI), use a cross cable for connecting Peer-to-Peer.

Use the following cable standards.

| | |
|---|---|
| Cable Standard: | Category 5 or higher UTP cable |
| Cable Length: | 100 m or less |

# 3. FUNCTION SPECIFICATIONS

## 3.1 Scope of Communications Protocols

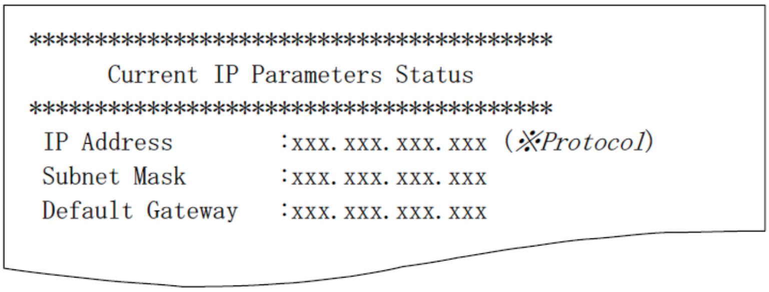
<TCP/IP>

| | |
|---|---|
| Network Layers | ARP, RARP, IP, ICMP |
| Transport Layers | TCP, UDP<br>TCP Keep-Alive Supported |
| Application Layers | DHCP, BOOTP<br>LPD (Printing)<br>Raw Socket Print (TCP Port 9100 Gets Printing/Printer Status)<br>Gets Printer Status (TCP Port 9101)<br>HTTP/HTTPS (Printer Status Display, Various Settings, StarWebPRNT (Note 1))<br>FTP (Gets printer status, various settings, prints, F/W updates)<br>Telnet (Gets printer status, various settings)<br>SDP (Star’s Genuine NIC Search Protocol)<br>TFTP (Recover Firmware)<br>Reset with authentication, gets settings information (TCP port 22222)<br>SNMP (supported by F/W Ver. 5.0.0 or later) |
| TCP/IP Specifications | IP version 4 (IPv4) |

Note 1: StarWebPRNT is only available for IFBD-HE07X/08X/BE07X. See “4. StarWebPRNT Function” for more details
F/W Ver4.0.0 and later supports HTTPS.

### 3.1.1 IP Address Setting

This product has a static (fixed condition) and dynamic (DHCP/BOOTP, RARP, and ARP/Ping) IP address. It is possible to specify a sub-net mask and default gateway with static and DHCP, BOOTP.
In the default settings, static is invalid and dynamic is valid.
The following pages describe how to acquire an IP address for each. See section 3.1.1.5 Address Acquisition Process Transition for details on each protocol transition state.
This product allows you to check the current IP parameter information while operating by a self-print when turning the power on.
This is output in the following format after running a self-print. See section 3.2.3 Self-print for details on running a self print.



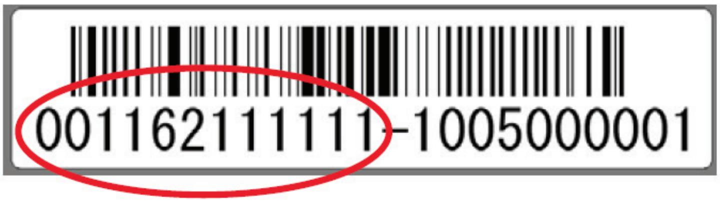
```
****************************************
      Current IP Parameters Status
****************************************
 IP Address        :xxx.xxx.xxx.xxx (※Protocol)
 Subnet Mask       :xxx.xxx.xxx.xxx
 Default Gateway   :xxx.xxx.xxx.xxx
```

* Protocol: The IP address acquisition protocol below is shown in the parentheses of the operating IP address line.

| | |
|---|---|
| (Static): | Static (Fixed address) |
| (DHCP): | Gets from DHCP server |
| (BOOTP): | Gets from BOOTP server |
| (RARP): | Gets from RARP server |
| (Didn’t obtain): | No IP address was acquired. |

You can find the MAC address to use in this section by using one of the following methods.
1. Execute a printer self-print (see section 3.2.5).
2. Check the first 12 characters in the barcode label affixed to the I/F card connector.

Example for when the MAC address is 00:11:62:11:11:11



### 3.1.1.1. Static

If the fixed IP address, sub-net mask, and default gateway are stored in non-volatile memory, the printer will always startup with the fixed conditions when the power is turned on. If started with fixed conditions, there is no DHCP/BOOTP, RARP request. ARP/Ping is also invalid. In default no fixed address is registered, so after dynamically acquiring one using either of the methods of DHCP, BOOTP, RARP, or ARP/Ping, described below, register the fixed address with the WEB, TELNET or FTP service.

### 3.1.1.2. DHCP, BOOTP

This product is set so that DHCP (Dynamic Host Configuration Protocol)/BOOTP (BOOT strap Protocol) is valid so you can acquire an IP address, sub-net mask, and default gateway from a DHCP or BOOTP server.
The default setting is DHCP, BOOTP: "enabled" A work-station running DHCP or BOOTP server over a LAN network is required for IP address settings using DHCP, BOOTP.

- The number of DHCP/BOOTP requests differs according to the DIPSW 1 settings on this product.
  DIPSW1 = OFF: This is issued three times 20 seconds after the TCP/IP startup. (Factory Default Setting)
  DIPSW1 = ON: Occurs unlimited times until the address is acquired.
- There is a partial compatibility of the DHCP Discover protocol with BOOTP Request, so both are handled as being the same.
  For example, if a BOOTP Replay is returned first to the DHCP Discover, the BOOTP acquired address is used.
- The DHCP, BOOTP Request is constantly broadcast with (255.255.255.255). However, only the DHCP Renew Request (extension request of the address usage period) is issued to the server that acquired that address.
- When the address information is acquired using DHCP, BOOTP, RARP and ARP/Ping are invalidated.
- The address acquired using DHCP, BOOTP is lost when the power is turned off without being written to the non-volatile memory.
- When acquiring an IP address from a DHCP server, the Subnet Mask is also acquired.
- When an IP address is acquired from a BOOTP server, the following Subnet Mask is used.
  [F/W Ver. 2.3.0 or older]
  The Subnet Mask is calculated automatically from the IP address.
  [F/W Ver. 3.0.0 or later]
  -When Subnet Mask (BOOT) = HE05 Emulation: The Subnet Mask is acquired from the BOOTP server. (Default settings)
  -When Subnet Mask (BOOT) = HE07 Emulation: The Subnet Mask is calculated automatically from the IP address.
  This setting can be changed by Telnet.

Settings: Register the combination of the IP address to be set, sub-net mask, default gateway and Mac address to the DHCP/BOOTP server and then turn on the printer power.

### 3.1.1.3. RARP

This product can obtain the IP address from the RARP server by setting the RARP (Reverse Address Resolution Protocol) to be valid. The default setting is RARP: "Valid"
A work-station running a RARP server over a LAN network is required for IP address settings using RARP.

- When using RARP, DIPSW1 on this product must be turned OFF.
- The RARP Request is issued once when 15 seconds have passed after the TCP/IP startup. However, if the IP address is obtained by the DHCP/BOOTP within 15 seconds, the RARP request is not generated.
- When the RARP address information is acquired using ARP/Ping is invalidated.
- You cannot get a subnet mask or default gateway from RARP servers.
- The address acquired using RARP is lost when the power is turned off without being written to the non-volatile memory.

Settings: Register the combination of the IP and MAC addresses to be set, to the RARP server, and then turn on the printer power.

### 3.1.1.4. ARP/Ping

Register the combination of the IP and MAC address of NIC to the ARP (Address Resolution Protocol) table on the PC and set the IP address using the Ping ARP by issuing a ping.

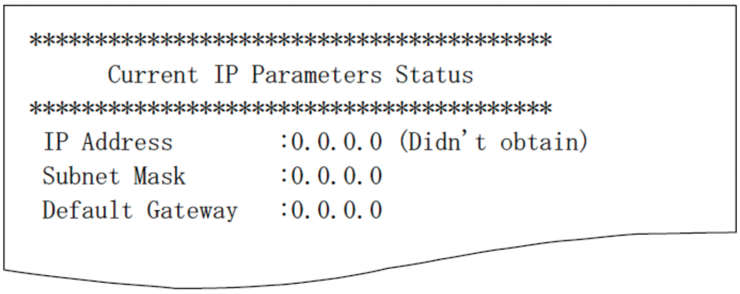
- When using RARP, DIPSW1 on this product must be turned OFF.
- Operations with an IP address set by ARP/Ping are possible only when the IP address is not acquired even with either of the methods of DHCP/BOOTP and RARP, when the Static address is not set.
- You cannot acquire a sub-net mask and default gateway with ARP/Ping.
- An address can be acquired using ARP/Ping only one time.
- The address acquired using ARP/Ping is lost when the power is turned off without being written to the non-volatile memory.

Setting examples are provided on the next page.

**Setting example using ARP/Ping**

This explanation assumes the MAC addres is 00:11:62:12:34:56, and the IP address is 192.168.10.2.

(1) Turn on the printer equipped with this product.
Wait for the printer to be ready for the ARP/Pping. (Normally, this is approximately 35 seconds.)
Or, execute a self-print on the printer and wait for the following to be printed.



```
****************************************
      Current IP Parameters Status
****************************************
 IP Address          :0.0.0.0 (Didn't obtain)
 Subnet Mask         :0.0.0.0
 Default Gateway     :0.0.0.0
```

(2) Avoid duplicating address by clearing the ARP table existing on the PC.

```
arp -d 192.168.10.2
arp -a
```

(3) Register the combination of IP and MAC addresses to the ARP table on the PC.
(For UNIX/Linux) Shell Input

```
arp -s 192.168.10.2 00:11:62:12:34:56
arp –a
```

(For Windows) Command Prompt Input

```
arp -s 192.168.10.2 00-11-62-12-34-56
arp –a
```

(4) Ping from the PC.

```
ping 192.168.10.2
```

(5) Check that there was an echo response to the specified address from NIC.
However, there is no echo response the first time because it is used only to acquire the IP address.
There is a response to the second and subsequent pings.

```
ping 192.168.10.2
 → No response (timeout)
ping 192.168.10.2
 → echo response
ping 192.168.10.2
 → echo response
ping 192.168.10.2
 → echo response
```

(6) Lastly, delete the ARP table registered at (3).
Always delete the table to avoid duplicating addresses.

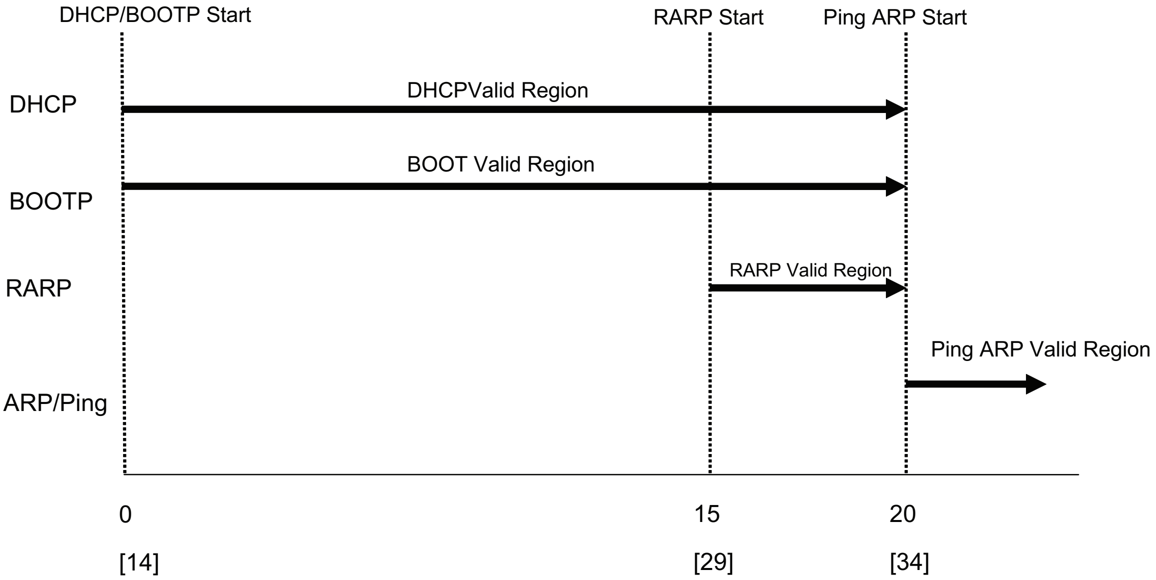
```
arp -d 192.168.10.2
arp -a
```

### 3.1.1.5 Transition of Processes in IP Address Acquisition

■ When Static is valid
If Static (fixed address) is set, startup always relies upon the Static condition (fixed address).
In such a case, DCHP/BOOTP, RARP, ARP/Ping become invalid, and startup does not occur.

■ When Static is invalid (default)
If Static (a fixed address) has not been, see the information below for details on the relationships (timing) for starting/stopping the server that provides the passing of time from the startup of the TCP/IP (*) and dynamic addresses. When the NIC setting is initialized, operations follow this timing.
Note that there is an error of approximately ±3 in the times disclosed below.
* There are approximately 14 seconds from the time the power is turned on to the startup of the TCP/IP.

<DIPSW1 = OFF (Default)>



→ Time after starting TCP/IP (seconds)

[Lower leve: Time after turning on the power (seconds)]

The first IP address acquired by either protocol becomes the NIC operating address, and all other protocols are invalid. The details are outlined below.

- The IP address acquired first by either DCHP and BOOTP in the time between 0 to 15 seconds is valid.
  When the IP address information is valid during that time, RARP and ARP/Ping do not start.
- The IP address acquired first by either DCHP, BOOTP, and RARP in the time between 15 and 20 seconds is valid.
  Addresses provided thereafter from another server are discarded.
  When the IP address information is valid during that time, ARP/Ping do not start.

<DIPSW1 = ON>
The DHCHP/BOOTP valid region is an infinite time after TCP/IP startup. If such cases, RARP, and ARP/Ping cannot be used.
If this product is connected directly to an intelligent switch or intelligent hub, the physical link may take some time to become established. In such cases, a timeout will occur while waiting to get the DHCP/BOOTP address, and it will fail to get the IP address. In such cases, set DIPSW1 = ON to ignore the IP address acquisition timeout.

### 3.1.2. LPR/LPD

The LPR protocol supported by the LPD of this product conforms to RFC1179 (partially unsupported). The list of logic printer names is handled as the queue name. LPR is an acronym for Line PRinter daemon protocol. It was originally a printing protocol prescribed as a UNIX printing system. Currently, it is supported as standard on Windows (NT and later).“LPR” is sometimes used as an execution file name of the LPR printing utility software.
The print server (Daemon) that supports LPR is called an LPD (Line Printer Daemon).
LPD uses TCP communication port 515.

- The reception buffer for print data is 1 M bytes (shared with Raw Socket Print).
- It does not support burner printing.
- Set to “lp” on the PC-port settings when specifying a queue name.
  Enable this if the LPR byte counter-added enable/disable can be selected.
- See section 5.3 Driver Support Table for details on support by Star Micronics’ drivers.
- If you are using a standard Windows TCP/IP printer port and a CUPS (UNIX, Linux, or Mac) driver, see section 5.3 Driver Support Table for important notes.
- Since there are additional instructions when using a Windows standard TCP/IP printer port or a CUPS (UNIX/ Linux, Mac) driver,See "5.3 Driver Support Table".

### 3.1.3. Raw Socket Print

This product supports Raw Socket Print communication for printing under the TCP/IP environment.
With Raw Socket Print, all data flowing during the TCP session is considered data handled between the printer and PC, and bidirectional data distribution is performed.
See the table below for TCP communications port specifications.

| Item | Specifications | Remarks |
|---|---|---|
| Communication Port Number | TCP #9100 | |
| Number of Simultaneous Connection Sessions | 1 or 8 | • Factory default setting is 1. |
| Data reception timeout | 0 (ignore), 30 seconds, 40 seconds, 60 seconds, 120 seconds, 180 seconds, 300 seconds | • Factory default setting is 0 (ignored).<br>• When there is a timeout, forcible disconnects connection. |

- The reception buffer for print data is 1 M bytes (shared with LPR).
- The maximum number of sessions received for port 9100 is set using NIC settings (9100 Multi Session). When set to "9100 Multi Session Enable," the maximum number of sessions for reception is 8; when set to "9100 Multi Session "Disable," the maximum number of sessions for reception is 1. When there are receptions for connection requests that exceed this number, a rejection packet (TCP Reset) is issued to the PC.

Note: Precautions regarding switching from old products IFBD-HE05/06/BE05
Be careful because the multi-session settings for Raw Socket Print (#9100) in the factory default settings are different.
Set the multi-session settings using HTTP (Web), Telnet, FTP.
We recommend setting to the same conditions when switching from an older product.
(For details, see section 5.3 Driver Support Table.)

#9100 Multi Session Factory Default Settings
• IFBD-HE05/06/BE05 (old product): Valid
• IFBD-HE07/08/BE07 (this product): Invalid

- When Multi Session is valid, and print data is received at the same time as multiple sessions are received from the PC, the session that first received the print data occupies the printer port, and print data of other sessions accumulates in the NIC reception buffer until the session is closed. Note that the session reception order and print output order do not always match.
- Data coming from the printer to the host computer is status information obtained from the printer.
  * See the printer's specifications manual for details on the contents of status information.
- Disconnection of the TCP session (TCP FIN, RST) is considered the end to one session.
  In that case, special communication procedures with the printer are not done. If special procedures are required, such as terminating printing, do so from the PC.
  If the RST packet is sent when the TCP session is disconnected from the PC side, some or all of the print data may be erased.
- You can automatically free a session that is unused while being connected, by setting the data reception data timeout 9100 Data Timeout. The data reception timeout can be set in 0, 30, 40, 60, 120, 180, 360 seconds.
  The settings can be made using WEB, Telnent and FTP, and the values are stored in the product's non-volatile memory.
  Factory default settings is 0 (timeout invalid).
- See section 5.3 Driver Support Table for details on support by Star Micronics' drivers.
- Since this protocol cannot be used when using a Windows standard TCP/IP printer port or a CUPS (UNIX/Linux, Mac) driver, specify LPR (LPD).
- For the user to create a socket communication program, see the communication procedures between the PC and printer, below.

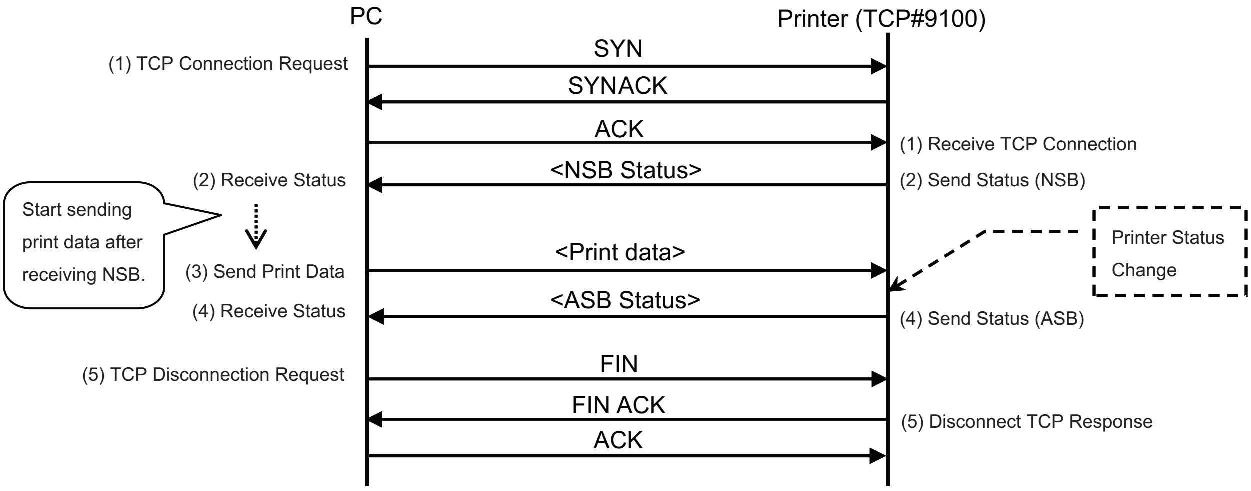
**Communication Procedures**

(1) Establish a TCP connection between the host and printer.
(2) When the NSB feature (*) is valid:
The PC sends and reads the status (NSB) sent by the printer. (Required)If the status data is not sent here, it is possible that the printer is not ready to receive the print data, so always do this.
(3) Send Print Data
(4) When the ASB feature (*1) is valid, receive the status because the printer sends the status to the PC when its status changes.
When the PC sends a status request command, receive because the status is returned for that command.
→ Repeat steps (3) and (4) until print data ends.
(5) Disconnect TCP connection from the host (Client) to the Printer (server).

Note: Before disconnecting the TCP connection with the printer, the PC must receive all of the status data sent from the printer.

Note: NSB feature: Sends status to PC when TCP#9100 is connected to the port
ASB feature: Sends automatic status to PC each time there is a change on the printer
See each printer's specifications manual and command specifications manuals for information related to valid/invalid settings of the NSB and ASB features.

Communication Chart Example (When NSB/ASB are valid)



Note: In the drawing, description of the <ACK> packet has been omitted.

### 3.1.4 Status Acquisition Feature

This product supports the printer status acquisition feature using TCP communications port 9101.
See the table below for TCP communications port specifications.

| Item | Specifications | Remarks |
|---|---|---|
| Communicatino Port Number | TCP #9101 | |
| Number of Simultaneous Connection Sessions | 8 | |
| Data reception timeout | 30 seconds | • When there is a timeout, forcible disconnects connection. |

When the following command and parameters are received from the computer, the printer status information (ASB) is returned.
If a command outside of the range is received, the connection is disconnected.

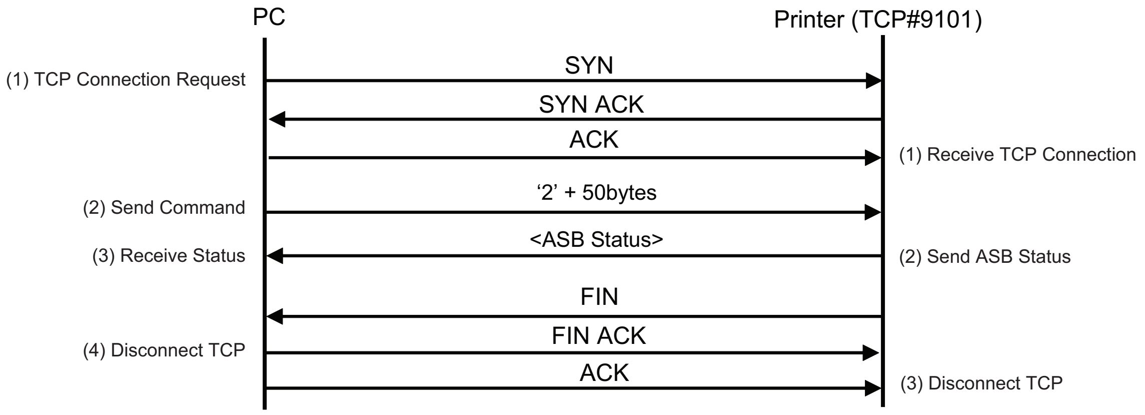
| Commands | Hexadecimal | Parameters |
|---|---|---|
| '2' | 32H | Any 50 bytes |

Procedures:
1) PC to printer
After connecting to TCP #9101, send the command and parameters, and wait for the response from the printer.
(For the parameters, we recommend 00H for all.
Data sending example:

32H 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

(2) Response printer to PC:
After the printer returns its status (ASB), it disconnects the connection.
When disconnected, the response from the computer cannot be confirmed.
See each printer's command specifications manual for details on the printer status information (ASB).
Data response example:
STAR Mode: 23H 86H 00 00 00 00 00 00 00 00 00

The following shows an example communication chart.



Note: In the drawing, some portions such as the <ACK> packet have been omitted.

## 3.1.5. Authentication Reset/Get Settings Information/TCP#9100 forced release

Use TCP communications port #22222 to send a command from the computer to perform an authentication reset and get settings information.
See the table below for TCP communications port specifications.

| Item | Specifications | Remarks |
|---|---|---|
| Communication Port Number | TCP #22222 | |
| Number of Simultaneous Connection Sessions | 4 | |
| Data reception timeout | 30 seconds | • When there is a timeout, forcible disconnects connection. |

The table below shows a list of supported commands.
If a command outside of the range is received, the connection is disconnected.

| Commands | Hexadecimal | Function | Automatic Disconnect |
|---|---|---|---|
| <FS> '0' [UserName] <NUL> [Password] <NUL> | 1CH, 30H, [UserName], 00H, [Password], 00H | Authentication Reset | Yes |
| <GS> '0' <NUL> | 1DH, 30H, 00H | Get NIC discovery data | Yes |
| <GS> '1' <NUL> | 1DH, 31H, 00H | Get printer status setting | Yes |
| <FS> '3' [Host Port Number] <NUL> | 1CH, 33H, [Host port Number] 00H | TCP#9100 forced release | Yes |

### 3.1.5.1. Authentication Reset Command

Code: <FS> '0' [User Name] <NUL> [Password] <NUL>

Hexadecimal: 1F 30 [User Name] 00 [Password] 00

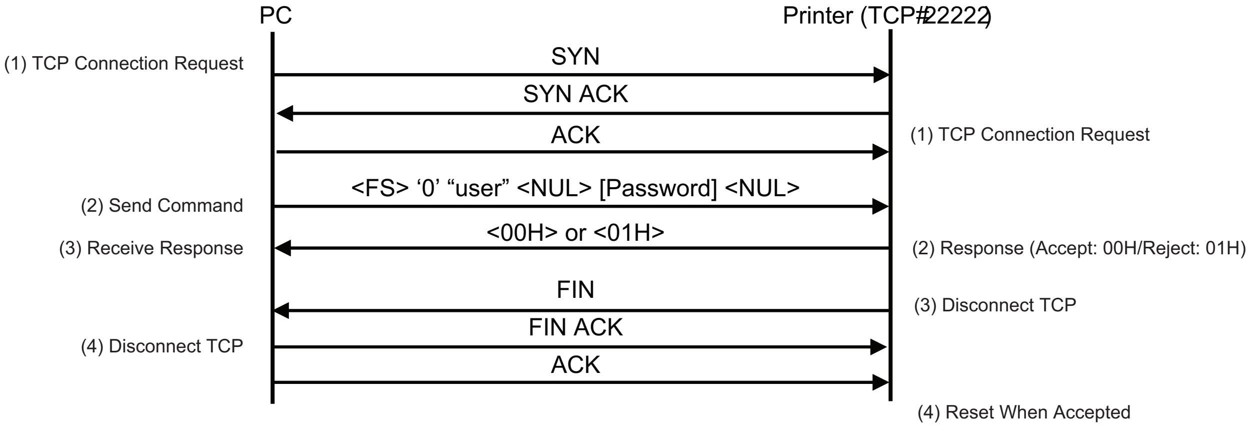
Parameter: User Name : "user" (Fixed)

Password: "guest" (When in default. Can be changed.)

Function: This command executes a forcible reset, regardless of the printer status. (online/error/printing/idling)
To run this feature, you need a user login name and password for user rights.
Use HTTP (WEB)/TELNET/FTP to change to any password to apply execution restrictions.

Reset Procedures:
1) PC to printer
After connecting to TCP #22222, send the command, and wait for the response from the printer.
(2) Response printer to PC
• When reset is authorized: After the printer resends 00H, the connection is cut (*2) and a reset is applied.
• When reset is rejected: After the printer resends 01H, the connection is cut (*2). No reset is executed.
(*2) Does not check for connection response on PC side.

The following shows an example communication chart.



Note: In the drawing, some portions such as the <ACK> packet have been omitted.

### 3.1.5.2. Setting Information Acquisition Command

Code <GS> '0' <NUL>

Hexadecimal 1D 30 00

Function This command will get the printer's NIC setting information (discovery data).
This command is used by Star Micronics drivers and tools.

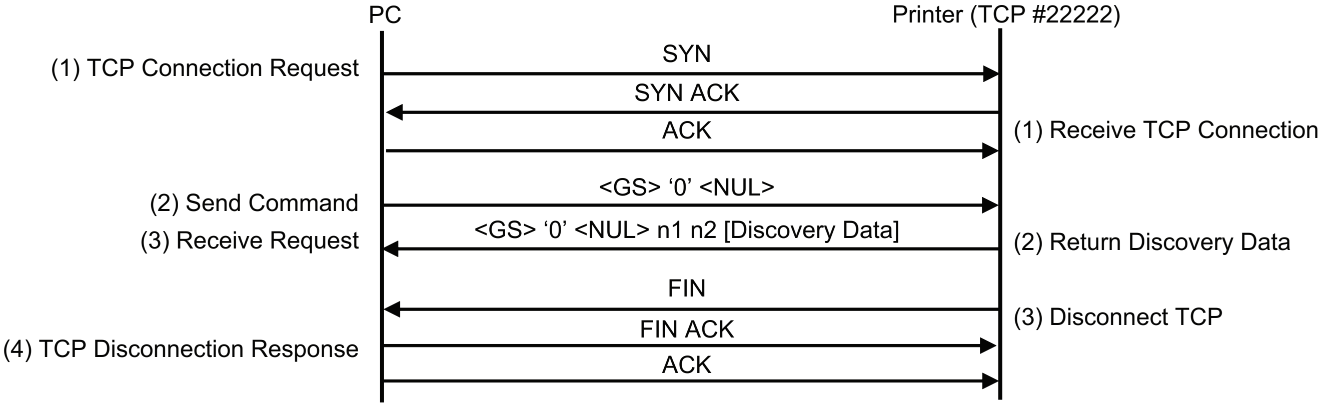
Procedures:
1) PC to printer
After connecting to TCP #22222, send the command, and wait for the response from the printer.
(2) Response printer to PC:
After the printer returns the NIC discovery data using the next response data format, it disconnects the connection. When disconnected, the response from the computer cannot be confirmed.

Format <GS> '0' <NUL> n1 n2 [Discovery data]

Hexadecimal 1D 30 00 n1 n2 [Discovery data]

Parameter n1, n2 : Discovery data data length (n1*256 + n2)

The following shows an example communication chart.


PC
Printer (TCP #22222)
(1) TCP Connection Request
SYN
SYN ACK
ACK
(1) Receive TCP Connection
(2) Send Command
<GS> '0' <NUL>
(3) Receive Request
<GS> '0' <NUL> n1 n2 [Discovery Data]
(2) Return Discovery Data
FIN
(3) Disconnect TCP
FIN ACK
(4) TCP Disconnection Response
ACK

Note: In the drawing, some portions such as the <ACK> packet have been omitted.

Code <GS> ‘1’ <NUL>

Hexadecimal 1D 31 00

Function This command will get the printer’s status setting information.
This command is used by Star Micronics drivers and tools.

Procedures:
1) PC to printer
After connecting to TCP #22222, send the command, and wait for the response from the printer.
(2) Response printer to PC:
After the printer returns the status setting information using the next response data format, it disconnects the connection.
When disconnected, the response from the computer cannot be confirmed.

Format <GS> ‘1’ <NUL> n1 n2 [P1] [P2] [P3] ...[Pn]

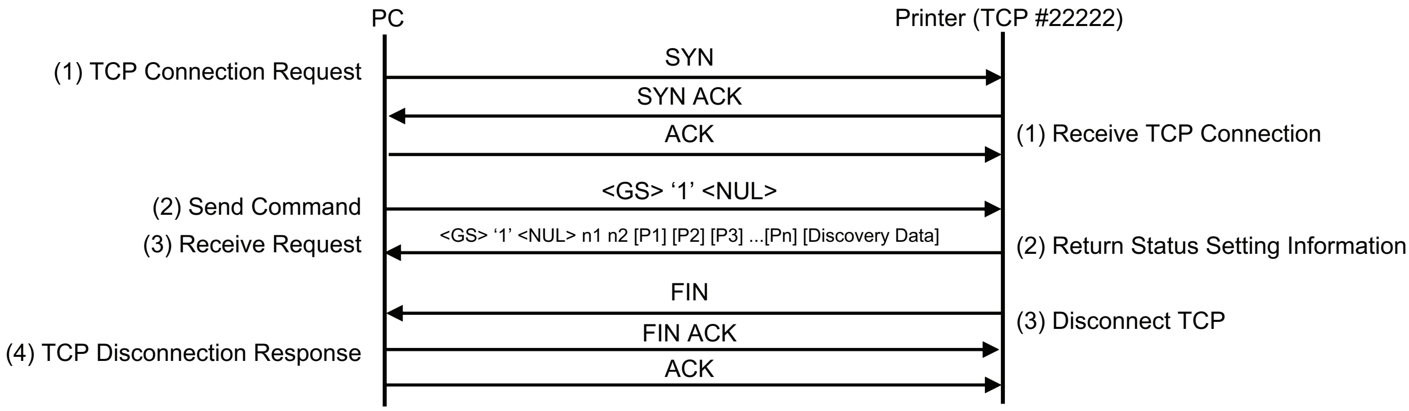
Hexadecimal 1D 31 00 n1 n2 [P1] [P2] [P3]...[Pn]

Parameter n1, n2 : Parameter [P1]-[Pn] data length (n1*256 + n2)

| Parameters | Item | Parameter Value | Hexadecimal | Contents |
|---|---|---|---|---|
| P1 | Status Format | ‘0’ | 30 H | Star ASB + Expanded Status |
| | | ‘1’ | 31 H | Only status |
| P2 | NSB Setting | ‘0’ | 30 H | Invalid |
| | | ‘1’ | 31 H | Valid |
| | ASB Setting | ‘0’ | 30 H | Invalid |
| | | ‘1’ | 31 H | Valid |

Return Example: Example: STAR Line mode, NSB=Valid, ASB=Valid
1DH 31H 00H 00H 03H 30H 31H 31H

The following shows an example communication chart.


PC
Printer (TCP #22222)
(1) TCP Connection Request
SYN
SYN ACK
ACK
(1) Receive TCP Connection
(2) Send Command
<GS> ‘1’ <NUL>
(3) Receive Request
<GS> ‘1’ <NUL> n1 n2 [P1] [P2] [P3] ...[Pn] [Discovery Data]
(2) Return Status Setting Information
FIN
(3) Disconnect TCP
FIN ACK
(4) TCP Disconnection Response
ACK

Note: In the drawing, some portions such as the <ACK> packet have been omitted.

### 3.1.5.3. TCP#9100 Forced Release

Release a specified host port number session from among connecting TCP#9100 sessions.

[Execution procedures]
As outlined in the following procedure, send a command from a PC to receive a response from the printer.
(1) Sending from PC to printer

| | |
|---|---|
| Format | <FS> ‘3’ [*Host Port Number*] <NUL> |
| Hexadecimal | 1C 33 [*Host Port Number*] 00 |
| Parameter | *Host Port Number*: The released host port number (2 byte data is specified in order of low-order byte to high-order byte.) |

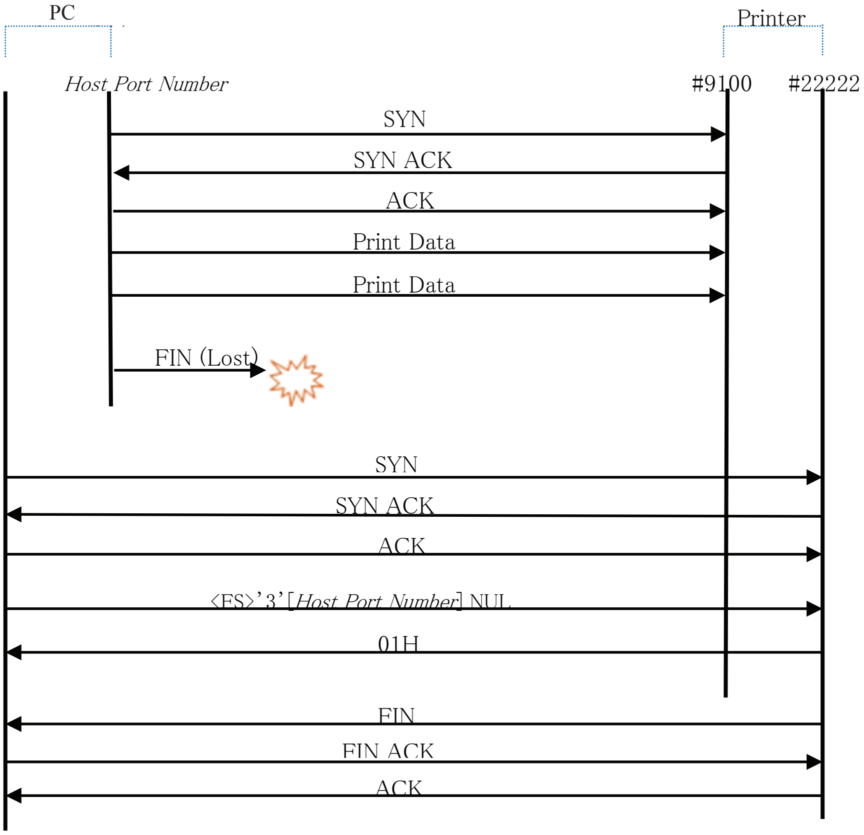
Command example:
Host Port Number = 256 (0100 hex): 1C 33H 00H 01H 00H
Host Port Number = 12300 (300C hex): 1C 33H 0CH 30H 00H
Host Port Number = 65530 (FFFA hex): 1C 33H FAH FFH 00H

(2) Response from printer to PC

- If there was no response when the session was connecting: The printer disconnects after responding 00H (*2)(*3).
- When releasing the session: The printer disconnects after responding 01H (*3).

(*2) It is mandatory to send this command from the same host device where the session was released that is connecting to TCP#9100. For a different device, the printer responds 00H and a forced release will not be executed.
(*3) This command does not confirm the PC's connection response.

The following shows an example communication chart.



Note: In the drawing, some portions such as the <ACK> packet have been omitted.

### 3.1.6. HTTP Server

This product has an HTTP (Hyper Text Transfer Protocol) server. By accessing from a web browser, you can change NIC settings, display network information, and monitor the printer status.
See section 3.3 Settings/Display Items for details on displaying information and settings.
Use TCP UDP communications port 80 for the HTTP server.
The StarWebPRNT function is available for IFBD-HE07X/08X/BE07X. By using the StarWebPRNT function, XML data can be printed via an HTTP server. See "4. StarWebPRNT Function" for more details.

- ➢ The HTTP version is HTTP 1.0.
- ➢ Maximum number of simultaneous connections is 1.
- ➢ User viewing homepage [Login Not Required]: http://IP Address/index.htm
  (Example) http://192.168.10.1/index.htm
- ➢ Administrator homepage [requires log-in]: http://IP Address/lindex.htm
  (Example) http://192.168.10.1/lindex.htm
- ➢ Veiwing and changing IP parameters, system settings, and passwords [Login Required]
  By specifying to execute the print settings when writing the settings, you can verify whether the setting contents were correctly written to the non-volatile memory. Also, if writing was successful, the printer will automatically be reset.
- ➢ Network information display [Login Not Required]
- ➢ Printer information display [Login Not Required]
  Printer status displays are updated automatically each time the settings are refreshed.

Accounts (user names, passwords) that can be accessed from a web browser are shown in the table below.
Items that can be viewed and set vary by the account.

| Account | User Name | Password | Target |
|---|---|---|---|
| User | Login Not Required | | General Users<br>(Only information display) |
| Root Users | "root" | "public"<br>• 1 to 31 characters of ASCII (Can be changed) | System administrator<br>(Information display and writing) |

For web settings using HTTP communication, the supported web browser versions are listed in the table below.
Operations are not guaranteed on earlier versions.

- F/W Ver. 4.X.X or earlier

| Web Browser | Windows | UNIX/Linux | Mac OS X |
|---|---|---|---|
| Mozilla Firefox 1.0 or higher | ○ | ○ | ○ |
| Netscape 7 or higher | ○ | ○ | ○ |
| Opera 8 or higher | ○ | ○ | ○ |
| Internet Explorer 4.0 or higher | ○ | | |

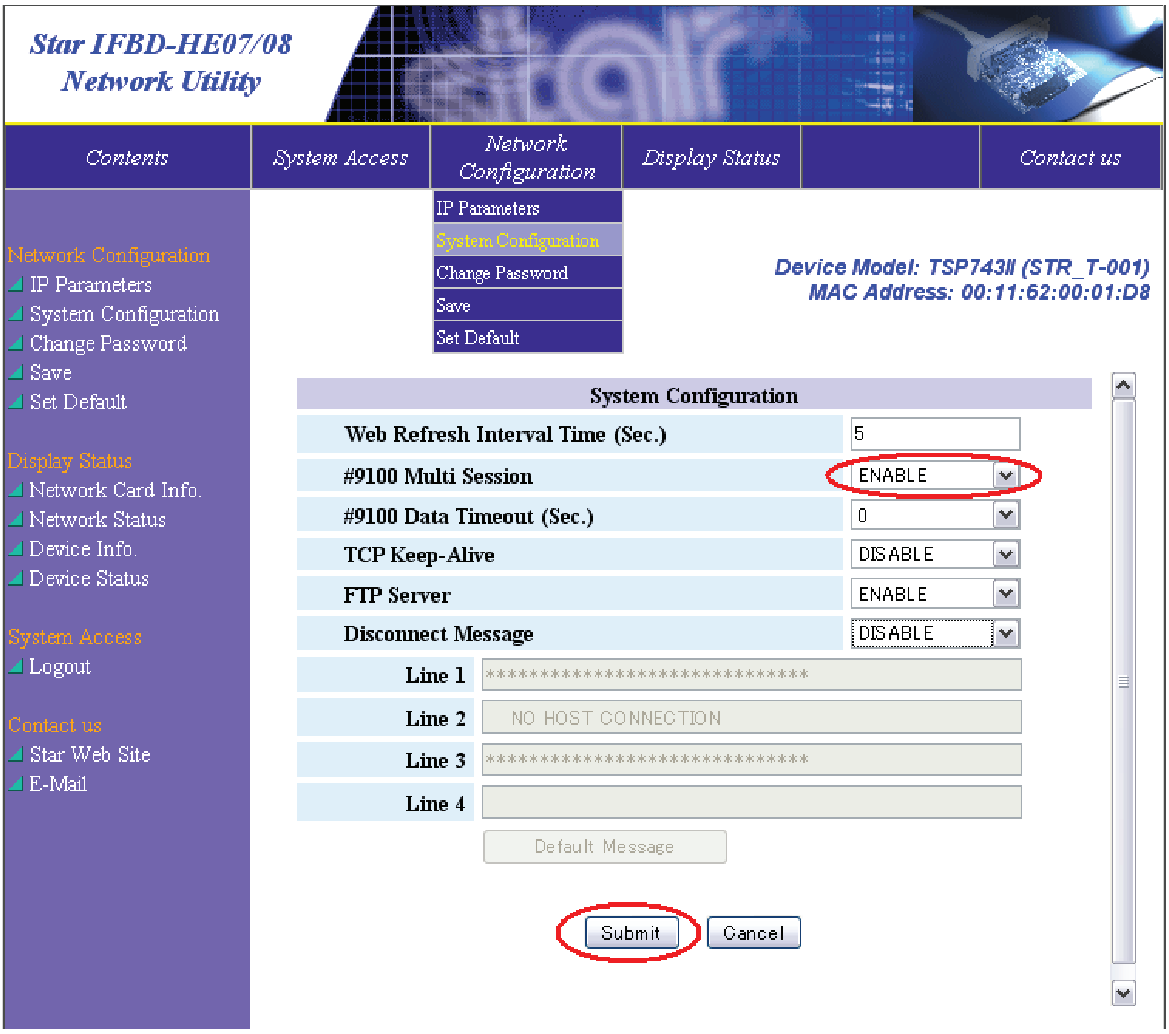
- Ver. 5.0.0 or later

| Web Browser | Windows | UNIX/Linux | Mac OS X |
|---|---|---|---|
| Mozilla Firefox | 3.5 ~ | 38 ~ | 3.6.21 ~ |
| Netscape | Not supported | Not supported | Not supported |
| Opera | 12.17 ~ | 12.16 ~ | 12.17 ~ |
| Internet Explorer | 8 ~ | | |
| Chrome | 4.0.2660 ~ | 48.0 ~ | 7.0 ~ |
| Safari | 5.1.7 ~ | | 4.0.2 ~ |

The following shows web browser settings.

- ➢ Java Script: Valid
- ➢ Style sheet: Valid
- ➢ Character Sizes, Display Magnification: Mid (Standard), 100% Display
- ➢ Inline frame: Valid (F/W Ver. 4.X.X or earlier only)

WEB execution example (Example of changing #9100 Multi-session from invalid to valid)
(1) Access: http:// 192.168.10.1/lindex.htm.
(2) User Name: Log-in as "root" Password: "public" (factory default setting).
(3) Click Network Configuration -> System Configuration.
In the screen below, select 9100 Multi Session: ENABLE. Then, click Submit.



Device Model: TSP743II (STR_T-001)
MAC Address: 00:11:62:00:01:D8

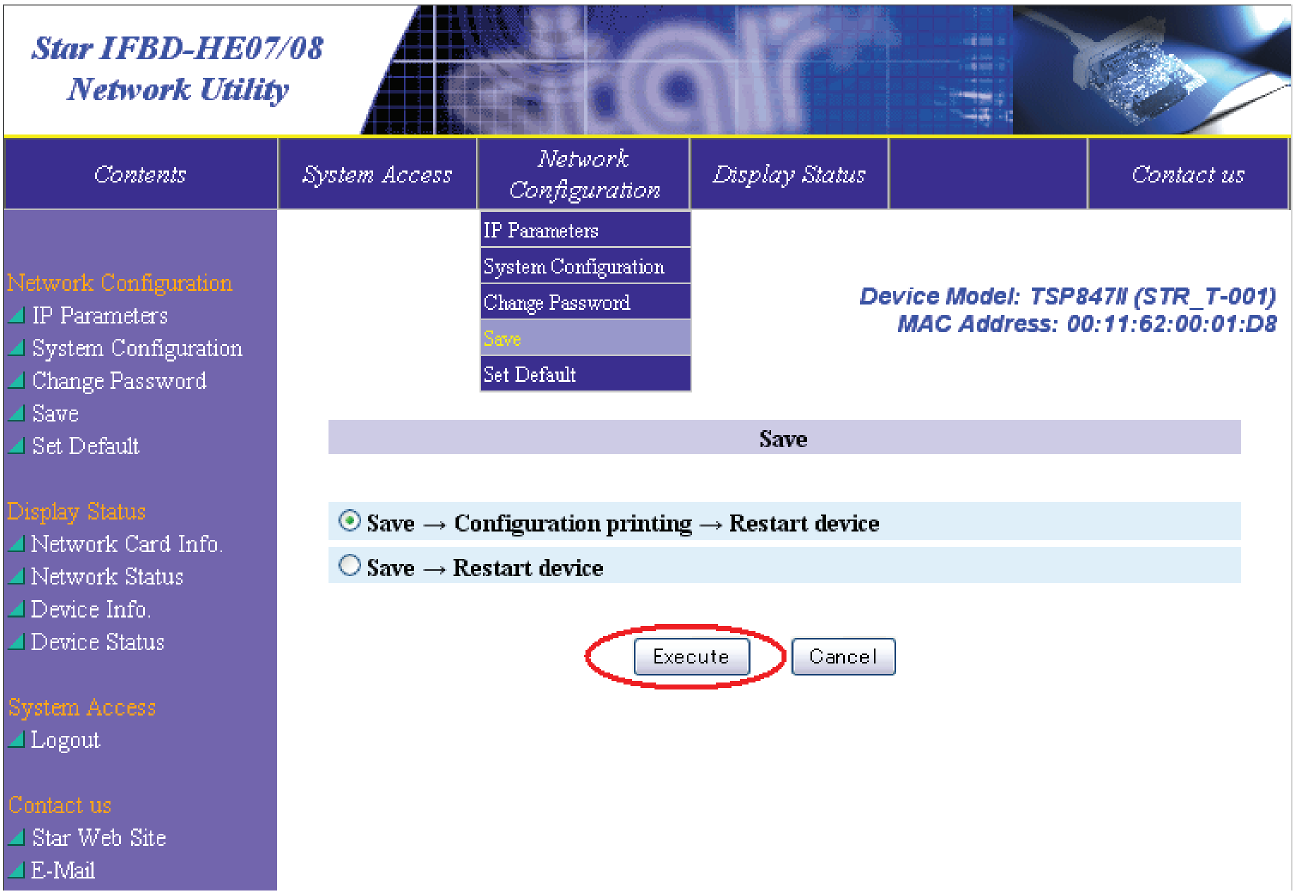
System Configuration

| | |
|---|---|
| Web Refresh Interval Time (Sec.) | 5 |
| #9100 Multi Session | ENABLE |
| #9100 Data Timeout (Sec.) | 0 |
| TCP Keep-Alive | DISABLE |
| FTP Server | ENABLE |
| Disconnect Message | DISABLE |
| Line 1 | ****************************** |
| Line 2 | NO HOST CONNECTION |
| Line 3 | ****************************** |
| Line 4 | |

(4) Click Network Configuration -> Save.
Select any of the following, the click Execute:

- Save → Configuration Printing → Restart device
- Save → Restart device

(After the set print is output, when you select, Configuration Printing) Wait for the printer to reset.



Device Model: TSP847II (STR_T-001)
MAC Address: 00:11:62:00:01:D8

**Save**

● Save → Configuration printing → Restart device

○ Save → Restart device

### 3.1.7. TELNET Server

The TELNET (TELecommunication NETwork) of this product allows you to change NIC settings, network network displays, and to monitor the printer status. See section 3.3 Settings/Display Items for details on displaying information. Use TCP UDP communications port 23 for the TELNET server.

- ➢ The maximum number of sessions that can be connected simultaneously with TELNET is 8.
- ➢ By specifying to execute the print settings when writing the settings, you can verify whether the setting contents were correctly written to the non-volatile memory. Also, if writing was successful, the printer will automatically be reset.

An account has multiple accounts at login. The user names and passwords are as follows.
Items that can be viewed and set vary by the account.

| Account | User Name | Password | Target |
|---|---|---|---|
| User | "user" | "guest"<br>• 1 to 31 characters of ASCII (Can be changed) | General Users<br>(Only information display) |
| Root Users | "root" | "public"<br>• 1 to 31 characters of ASCII (Can be changed) | System administrator<br>(Information display and writing) |

(1) TELNET command execution example (Ex.: Changing a fixed IP address)
The following is an input example of the Windows command prompt. UNIX/Linux shell input is the same.
(Assumed Condition) • Printer IP address acquired by DHCP is 192.168.10.3
• The Pritner IP address to be set is 192.168.10.1; subnet mask is 255.255.255.0.

```
D;¥>telnet 192.168.10.3                     ← telnet connection


Welcome to IFBD-HE07/08 TELNET Utility.
Copyright(C) 2005 Star Micronics co., Ltd.

<< Connected Device >>
   Device Model: TSP700II (STR_T-001)
   NIC Product : IFBD-HE07/08
   MAC Address : 00:11:62:12:34:56

login: root                                 ← Enter user name
Password: ******                            ← Enter password (Default:  public)
Hello root

=== Main Menu ===
  1) IP Parameters Configuration
  2) System Configuration
  3) Change Password
 96) Display Status
 97) Reset Settings to Defaults
 98) Save & Restart
 99) Quit

Enter Selection: 1                          ← Select the IP parameter setting

=== IP Parameters Menu ===
  1) Static
       IP Address      : 0.0.0.0
       Subnet Mask     : 0.0.0.0
       Default Gateway: 0.0.0.0
  2) Dynamic
       DHCP/BOOTP      : ENABLE
       RARP            : ENABLE
 99) Back to Main Menu

Enter Selection: 1                          ← Select the Static setting

=== Static IP Address ===
  1) IP Address      : 0.0.0.0
  2) Subnet Mask     : 0.0.0.0
  3) Default Gateway: 0.0.0.0
 99) Back to IP Address Menu

Enter Selection: 1                          ← Select the IP address setting
Enter IP address(x.x.x.x) : 192.168.10.1                 ← Enter the fixed IP address

OK> New IP address <192.168.10.1> is accepted.

=== Static IP Address ===
  1) IP Address      : 192.168.10.1
  2) Subnet Mask     : 0.0.0.0
  3) Default Gateway: 0.0.0.0
 99) Back to IP Address Menu

Enter Selection: 2                                        ← Select the subnet mask setting

Enter subnet mask(x.x.x.x) : 255.255.255.0               ←Enter the fixed subnet mask

OK> New subnet mask <255.255.255.0> is accepted.

=== Static IP Address ===
  1) IP Address      : 192.168.10.1
  2) Subnet Mask     : 255.255.255.0
  3) Default Gateway : 0.0.0.0
 99) Back to IP Address Menu
                                                          ← Return to the previous menu
Enter Selection: 99
                                                          ← telnet connection
=== IP Parameters Menu ===
  1) Static
        IP Address      : 192.168.10.1
        Subnet Mask     : 255.255.255.0
        Default Gateway: 0.0.0.0
  2) Dynamic
        DHCP/BOOTP      : DISABLE
        RARP            : DISABLE
 99) Back to Main Menu

Enter Selection: 99                                       ← Return to the main menu

=== Main Menu ===
  1) IP Parameters Configuration
  2) System Configuration
  3) Change Password
 96) Display Status
 97) Reset Settings to Defaults
 98) Save & Restart
 99) Quit

Enter Selection: 98                                       ← Store the settings and select restar

=== Save to NVRAM & Restart NIC Menu ===
  1) Save & Configuration printing & Restart device
  2) Save & Restart device
  4) Exit without saving
 99) Back to Main Menu

Enter Selection: 1                                        ← Store and print setings and run restart

The configuration data is being written in memory.
(Don't turn off power the device.)                        ← Wait for the settings to be printed
OK> Configuration succeeded!                              ← Wait for pinter to restart
```

(2) TELNET execution example (Example of changing #9100 Multi-session from invalid to valid)

The following is an input example of the Windows command prompt. UNIX/Linux shell input is the same.

(Assumed Conditions) Printer IP address = 192.168.10.1

```
D;¥>telnet 192.168.10.1                                 ← telnet connection

Welcome to IFBD-HE07/08 TELNET Utility.
Copyright(C) 2005 Star Micronics co., Ltd.

<< Connected Device >>
    Device Model: TSP700II (STR_T-001)
    NIC Product : IFBD-HE07/08
    MAC Address : 00:11:62:12:34:56

login: root                                             ← Enter user name
Password: ******                                        ←Enter password (Default:  public)
Hello root

=== Main Menu ===
  1) IP Parameters Configuration
  2) System Configuration
  3) Change Password
 96) Display Status
 97) Reset Settings to Defaults
 98) Save & Restart
 99) Quit

Enter Selection: 2                                      ← Select System Configuration

=== System Configuration Menu ===
  1) Web Refresh Interval Time (Sec.) : 5
  2) #9100 Multi Session              : DISABLE
  3) #9100 Data Timeout (Sec.)        : 0
  4) TCP Keep-Alive                   : DISABLE
  5) FTP Server                       : ENABLE
  6) Disconnect Message               : ENABLE
 99) Back to Main Menu

Enter Selection: 2                                      ← Select #9100 Mutli Session

=== #9100 Multi Session ===
  1) ENABLE
  2) DISABLE
 99) no change

Enter Selection: 1                                      ← Select ENABLE


OK> 9100 Multi Session <ENABLE> is accepted.

=== System Configuration Menu ===
  1) Web Refresh Interval Time (Sec.) : 5
  2) #9100 Multi Session              : ENABLE
  3) #9100 Data Timeout (Sec.)        : 0
  4) TCP Keep-Alive                   : DISABLE
  5) FTP Server                       : ENABLE
  6) Disconnect Message               : ENABLE
 99) Back to Main Menu

Enter Selection: 99                                     ← Return to the main men

=== Main Menu ===
  1) IP Parameters Configuration
  2) System Configuration
  3) Change Password
 96) Display Status
 97) Reset Settings to Defaults
 98) Save & Restart
 99) Quit

Enter Selection: 98                                     ← Store the settings and select restart

=== Save to NVRAM & Restart NIC Menu ===
  1) Save & Configuration printing & Restart device
  2) Save & Restart device
  4) Exit without saving
 99) Back to Main Menu

Enter Selection: 1                                      ← Store and print settings and run restart

The configuration data is being written in memory.
(Don't turn off power the device.)                      ← Wait for the settings to be printed
OK> Configuration succeeded!                            ← Wait for pinter to restart
```

### 3.1.8. FTP Server

You can make NIC settings, get the status, print and overwrite NIC firmware by uploading or downloading files to any specified directory using the product’s FTP (File Transfer Protocol) server.See section 3.3 Settings/Display Items for details on displaying information.
For control, the FTP server uses TCP • UDP communication port 21; for data transfers, it uses TCP communication port 20.

- ➢ The FTP server is set to valid in the factory default settings, but you can invalidate it using HTTP (Web), Telnet and FTP.
  Use HTTP (Web) or Telnet to return it to valid.
- ➢ The maximum number of sessions that can be connected simultaneously with FTP is 8. However, for details on FTP printing (writing to the /lp/ directory), the number of sessions that can be printed simultaneously is 1. Also, when simultaneously writing data from a multiple of sessions, and the first received session occupies more than one minute, the writing request of subsequently connected sessions will be rejected.
- ➢ It is necessary to specify ASCII (Type A) or Binary (Type I) for files as the transfer modes, but the mode differences depend on the client without processing on this product.  Data is transferred as is in the Binary mode, but 0Ahex is converted to 0Dhex + 0Ahex for transfer in the ASCII mode. For that reason, to avoid mistakenly specifying this mode, this product should be set to Binary mode to transfer all files.
- ➢ Supports both Active and Passive modes, so you can send data over a firewall.Transfer throughput is less efficient in Passive mode.
- ➢ Anonymous log in
  If you login with a user name or password that is not registered, you can login with general user rights.
  When logging in as anonymous, the user name and password must be within 31 characters.
  In this case, the password is omitted.
- ➢ When accessing an FTP server from a PC, do so using an FTP client software (CUI version, command direct input) of a standard OS.
- ➢ If there is no access from the FTP client for 15 minutes, the FTP server will forcibly disconnect the connection.

There are multiple accounts that require logging in for operations. The user names and passwords are as follows.

| Account | User Name | Password | Target |
|---|---|---|---|
| User | “user” | “guest”<br>• 1 to 31 characters of ASCII (Can be changed) | General Users<br>(Only information display) |
| Root Users | “root” | “public”<br>• 1 to 31 characters of ASCII (Can be changed) | System administrator<br>(Information display and writing) |

The directory displayed by FTP and the file configuration and functions are shown on the next page.

Directory, File Configuration and Functions

| Directory | Filename Note 2 | Extension Restriction Note 3 | Transfer Mode Note 4 | Account Limit Note 1 | | |
|---|---|---|---|---|---|---|
| | | | | user | root | Function |
| / | | | | - | - | None (Root directory) |
| /lp/ | printdat.prn | No | Binary | W | W | Print Output to Printer<br>→ See “3.1.8.1 FTP Printing” |
| /net_config/ | netconf.ini | “.ini” | Binary or ASCII | R | R/W | Reads and updates network settings<br>→ See section 3.1.8.2 NIC Settings |
| /status/ | netstas.txt | - | Binary or ASCII | R | R | Reads operation information of operating network |
| | nicver.txt | - | Binary or ASCII | R | R | Reads network card version information |
| | prnstas.txt | - | Binary or ASCII | R | R | Read printer status (hexadecimal dump display) |
| | deviceid.txt | - | Binary or ASCII | R | R | Read Printer Device ID |
| /firmware/ | NIC_MAIN.bin | “.bin” | Binary | - | W | NIC Main F/W Update<br>→ See “3.1.8.3 F/W Update” |
| /freespace/ | - | No | Binary or ASCII | R | R/W | Free space |

Note 1. Account Limit
R: Read Only; W: Write Only; R/W: Read/Write; -: No Function

Note 2. Filenames
Filenames should be less than 32 characters, including the extension. There are no restrictions to filenames to write, except for the extension. Usable characters are limited to English numbers and alphabet. (“A”to”Z”, “a”to”z”, “0”to”9”)

Note 3. File Extension Restrictions
When an extension restriction is specified, the filename specified, other than the specified extensions, is rejected.
There is no concept of extension in UNIX/Linux and Mac OS X, but this restriction is applied to the final four characters of the filename.

Note 4: Transfer mode
Files can be transferred by Binary alone, or ASCII can be specified. However, specify always Binary mode to prevent specification mistakes.

Note 5: Observe the following restrictions for the total size for files and number of files that can be uploaded to the free space.
• Total File Size: Max. 640 K bytes
• Total Number of Files: Max. 10
Also, do not place an executable file in this directory.

Example FTP Command Execution
This is an example of input in a Windows command prompt. UNIX/Linux shell input is the same.
This is an example execution of acquiring a printer status file.
The file list display (dir command (on UNIX/Linux, it is the ls command)) is in UNIX compatible format (including version display).

(Assumed Conditions) Printer IP address = 192.168.10.1

```
D:¥>ftp 192.168.10.1                                    ← Connect to FTP

Connected to 192.168.10.1.
220 Star IFBD-HE07/08 FTP Server.
User (192.168.10.1:(none)): root                        ← Enter user name
331 User root OK, send password.
Password:                                               ← Enter password (Default:  public)
230 Password OK.

ftp> dir
200 PORT command Ok.
150 File Listing Follows in ASCII mode
d-w--w--w- 1 noone group1 76     Jan 01 00:00 lp
drw-rw-rw- 1 noone group1 76     Jan 01 00:00 net_config
d-w--w--w- 1 noone group1 76     Jan 01 00:00 firmware
dr--r--r-- 1 noone group1 304    Jan 01 00:00 status
drw-rw-rw- 1 noone group1 0      Jan 01 00:00 freespace
226 Transfer complete.
ftp: 285 bytes received in 0.22Seconds 1.30Kbytes/sec.

ftp> cd status                                          ← Move to status directory
250 Directory is changed

ftp> pwd                                                ← Current directory position display
257 "/status" is current directory

ftp> ls                                                 ← File list
200 PORT command Ok.
150 File Listing Follows in ASCII mode
prnstas.txt
netstas.txt
deviceid.txt
nicver.txt
226 Transfer complete.
ftp: 52 bytes received in 0.20Seconds 0.26Kbytes/sec.

ftp> bin                                                ← Specify binary transfer mode
200 Type set to I.

ftp> get prnstas.txt                                    ← Get the prnstas.txt fi
200 PORT command Ok.
150 About to open data connection.
226 Transfer complete.
ftp: 239 bytes received in 0.20Seconds 1.18Kbytes/sec.

ftp> cd /                                               ← Move to root directory
250 Directory is changed

ftp> quit                                               ← Quit FTP
221 Goodbye.

D:¥>
```

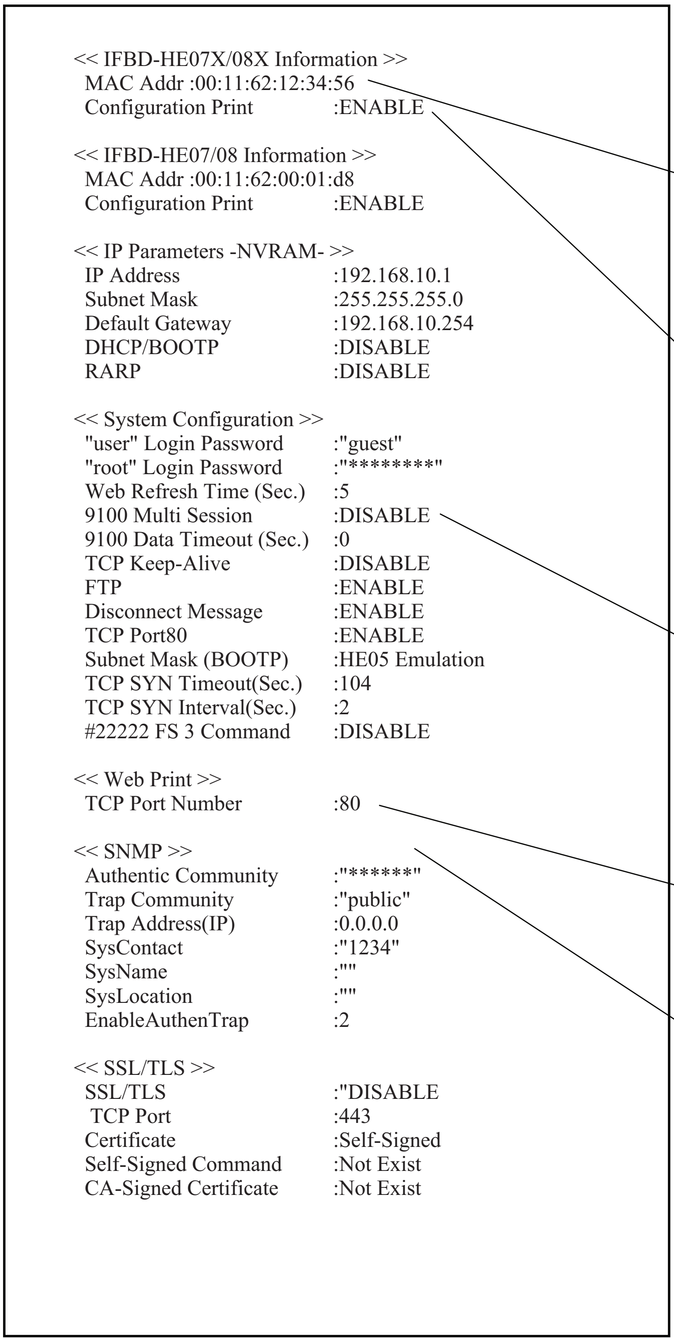
### 3.1.8.1. FTP Printing

When writing data to the \lp\ directory, it is transferred to the printer as print data.

### 3.1.8.2. NIC Setting

Login to the FTP server from an FTP client to view the settings by reading the setting file in the \net_config\ directory. Also, by uploading the setting file to the same directory, you can store the settings in the non-volatile memory.
The extensions of filenames uploaded from the FTP client are changed to “$$$” prior to writing to NVRAM, and the files are saved as mid-way files. When updating is successful, the mid-way files are deleted, but if the format of the setting contents is incorrect or the writing to the non-volatile memory is erroneous and the writing fails, the files will remain without being deleted (extension “$$$”) Also, if writing ends normally, the printer will automatically be reset. If the “Configuration Print” item is “Enable” the reset will be applied when the settings print is ended.

Setting Example: Example of F/W Ver. 5.0.0, Star WebPRNT model (netconf.ini)



```
<< IFBD-HE07X/08X Information >>
 MAC Addr :00:11:62:12:34:56
 Configuration Print          :ENABLE

<< IFBD-HE07/08 Information >>
 MAC Addr :00:11:62:00:01:d8
 Configuration Print          :ENABLE

<< IP Parameters -NVRAM- >>
 IP Address                   :192.168.10.1
 Subnet Mask                  :255.255.255.0
 Default Gateway              :192.168.10.254
 DHCP/BOOTP                   :DISABLE
 RARP                         :DISABLE

<< System Configuration >>
 "user" Login Password        :"guest"
 "root" Login Password        :"********"
 Web Refresh Time (Sec.)      :5
 9100 Multi Session           :DISABLE
 9100 Data Timeout (Sec.)     :0
 TCP Keep-Alive               :DISABLE
 FTP                          :ENABLE
 Disconnect Message           :ENABLE
 TCP Port80                   :ENABLE
 Subnet Mask (BOOTP)          :HE05 Emulation
 TCP SYN Timeout(Sec.)        :104
 TCP SYN Interval(Sec.)       :2
 #22222 FS 3 Command          :DISABLE

<< Web Print >>
 TCP Port Number              :80

<< SNMP >>
 Authentic Community          :"******"
 Trap Community               :"public"
 Trap Address(IP)             :0.0.0.0
 SysContact                   :"1234"
 SysName                      :""
 SysLocation                  :""
 EnableAuthenTrap             :2

<< SSL/TLS >>
 SSL/TLS                      :"DISABLE
  TCP Port                    :443
 Certificate                  :Self-Signed
 Self-Signed Command          :Not Exist
 CA-Signed Certificate        :Not Exist
```

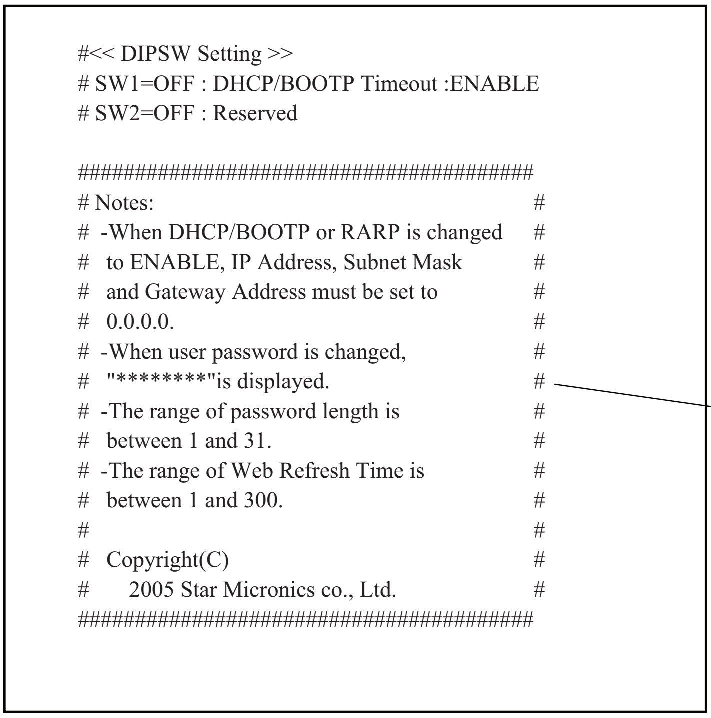
The loaded NIC MAC information is used for the MAC Address item, but when uploaded, the MAC information field is ignored. Therefore, when you use a loaded setting file to upload to NIC, you do not need to change this field.

When you specify Enable for the Configuration Print item, you can print the settings to verify that they have been loaded to the non-volatile memory.

The factory default setting for 9100 Multi-session is different from the old product.
Factory Default Settings
IFBD-HE05/06/BE05 (old product): ENABLE
IFBD-HE07/08/BE07 (this product): DISABLE

The Web Print setting items are for the Star WebPRNT model only.

The SNMP setting items are for F/W Ver. 5.0.0 or later only.



```
#<< DIPSW Setting >>
# SW1=OFF : DHCP/BOOTP Timeout :ENABLE
# SW2=OFF : Reserved

##########################################
# Notes:                                 #
#  -When DHCP/BOOTP or RARP is changed   #
#   to ENABLE, IP Address, Subnet Mask   #
#   and Gateway Address must be set to   #
#   0.0.0.0.                             #
#  -When user password is changed,       #
#   "********"is displayed.              #
#  -The range of password length is      #
#   between 1 and 31.                    #
#  -The range of Web Refresh Time is     #
#   between 1 and 300.                   #
#                                        #
#   Copyright(C)                         #
#       2005 Star Micronics co., Ltd.    #
##########################################
```

The lines beginning with a # (sharp) are comment lines.

File Format Rules

- Setting line format is “Item Name”: “Setting Value” The separator (delimiter) is a single-byte English character “:” (colon)
- Only ASCII characters can be used in this file.
- Uploads are rejected for the follwoing.
  • When an item name that does not exist is specified, or there are insufficient number of setting items
  • When the setting value input is out of range
  • When the input for Static value and Dynamic value has a standard violation in the IP parameter setting field. (See the Notes Field)
- Lines beginning with “#” are skipped as comment lines.

### 3.1.8.3. F/W Update

Log in to this product using FTP to update the NIC firmware (F/W) by uploading the version upgrade binary data to the \firmware\ directory.

- ➢ When uploading F/W data, the FTP server calculates the CRC value of the F/W data and checks that it has been transferred correctly. If the firmware is not correctly transferred, cancel the upload.
- ➢ When all data has been confirmed to be correctly received, start writing to the Flash ROM. If writing to the Flash ROM ends normally, the printer will automatically be reset.
  Writing takes several minutes. Absolutely never turn off the power or apply a reset prior to final reset being applied. If terminated partway, the Flash ROM data will be damanged, and later it may not start up.

The following describes the procedures to update the F/W of this product using FTP.
For Windows, start the command prompt, then following the directions below. For UNIX/Linux, do the same operations on the shell execution screen.

(Assumed Conditions) Printer IP address = 192.168.10.1
Assumes the main F/W data (”HE7_V100(NIC_MAIN).bin”) for the for this product is in the current directory D:/ when FTP is executed on the computer.

```
D:¥>ftp 192.168.10.1                          ← Connect to FTP

Connected to 192.168.10.1.
220 Star IFBD-HE07/08 FTP Server.
User (192.168.10.1:(none)): root              ← Enter the user name
331 User root OK, send password.
Password:                                     ← Enter the password (Default:  public)
230 Password OK.

ftp> cd firmware                              ← Move to the firmware directory
250 Directory is changed

ftp> pwd                                      ← Current directory position display
257 "/firmware" is current directory

ftp> bin                                      ← Specify binary transfer mode
200 Type set to I.

ftp> put HE7_V100(NIC_MAIN).bin               ← Write the firmware file
200 PORT command Ok.
150 About to open data connection.
226 Transfer complete.
ftp: 693286 bytes received in 4.30Seconds 161.34Kbytes/sec.
                                              ← Wait here for the printer to restart
ftp> quit                                     ← Quit FTP

D:¥
```

Precautions for F/W update compatibility

The following restrictions on F/W update apply to the subject F/W versions.

- When using a product with I/F card F/W that is Ver. 4.X.X or earlier
  Upgrade to F/W Ver. 5.0.0 or later is not possible. Use Ver. 4.X.X or earlier F/W.
- When using a product with I/F card F/W that is Ver. 5.0.0 or later
  Downgrade to F/W Ver. 4.X.X or earlier is not possible. Use Ver. 5.0.0 or later F/W.

Checking the version of the I/F card that is used

- Turn on the power while pressing and holding the Feed switch on the printer unit and check the self-test print information. (For details about the contents of self-test print, refer to section 3.2.5 “Self-test Print”.)
- To check the version from the PCB chassis appearance, refer to section 2.1 “Model Names”.

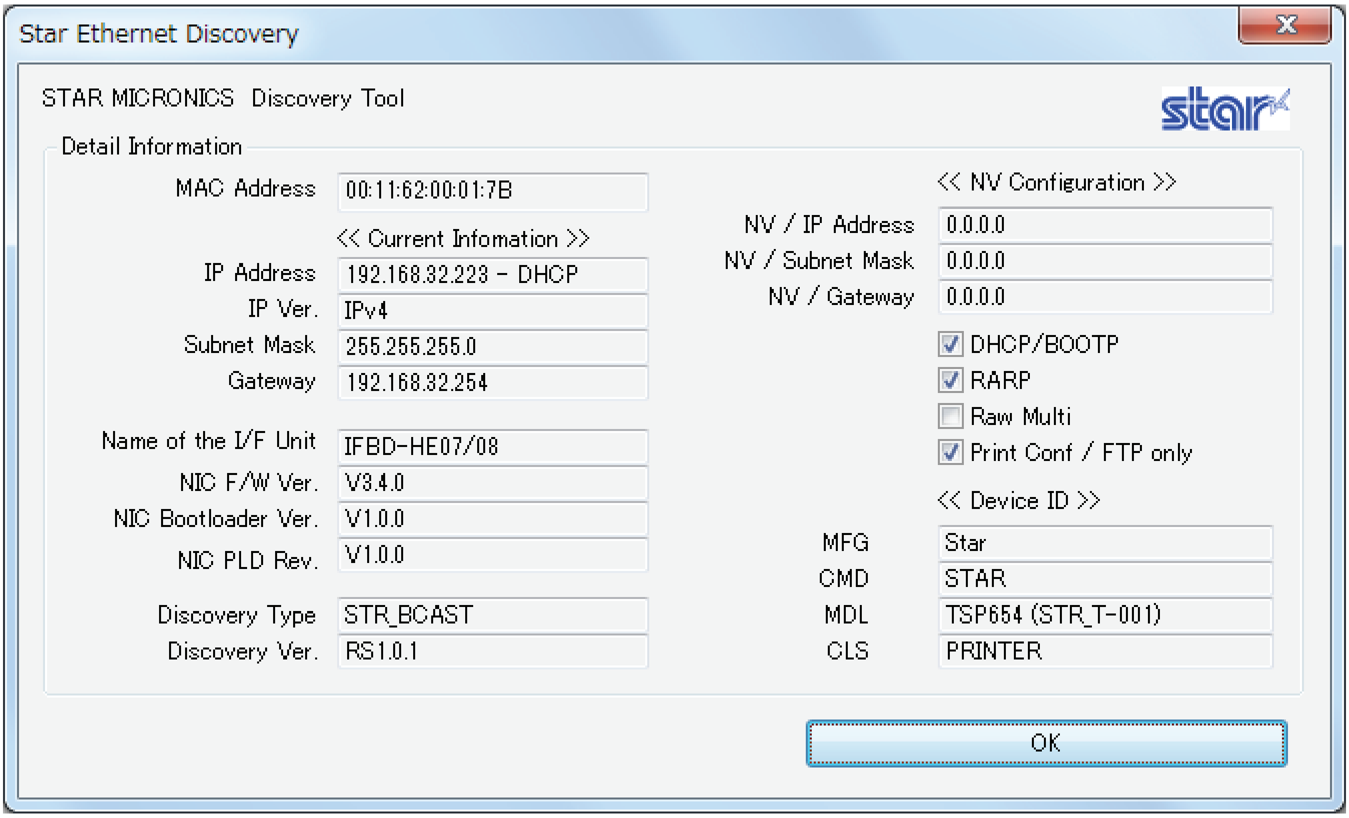
### 3.1.9. Discovery

This product has a Star genuine NIC search protocol SDP (Star Discovery Protocol).
SDP uses UDP communication port 22222.
SDP is used to search the product over LAN using application software such as a setting utility program.

The following is an example.
The Name of I/F Unit field is different this product (IFBD-HE07/08/BE07) and the old products (IFBD-HE05/06/BE05).

- Name of I/F Unit: "IFBD-HE05/06"
- Name of I/F Unit: "IFBD-HE07/08"

(Ex.) Detailed display example of search results using a discovery tool (OS: Windows 7)



Star Ethernet Discovery

STAR MICRONICS Discovery Tool

Detail Information

| | |
|---|---|
| MAC Address | 00:11:62:00:01:7B |
| | << Current Infomation >> |
| IP Address | 192.168.32.223 - DHCP |
| IP Ver. | IPv4 |
| Subnet Mask | 255.255.255.0 |
| Gateway | 192.168.32.254 |
| Name of the I/F Unit | IFBD-HE07/08 |
| NIC F/W Ver. | V3.4.0 |
| NIC Bootloader Ver. | V1.0.0 |
| NIC PLD Rev. | V1.0.0 |
| Discovery Type | STR_BCAST |
| Discovery Ver. | RS1.0.1 |

| | |
|---|---|
| | << NV Configuration >> |
| NV / IP Address | 0.0.0.0 |
| NV / Subnet Mask | 0.0.0.0 |
| NV / Gateway | 0.0.0.0 |

☑ DHCP/BOOTP
☑ RARP
□ Raw Multi
☑ Print Conf / FTP only

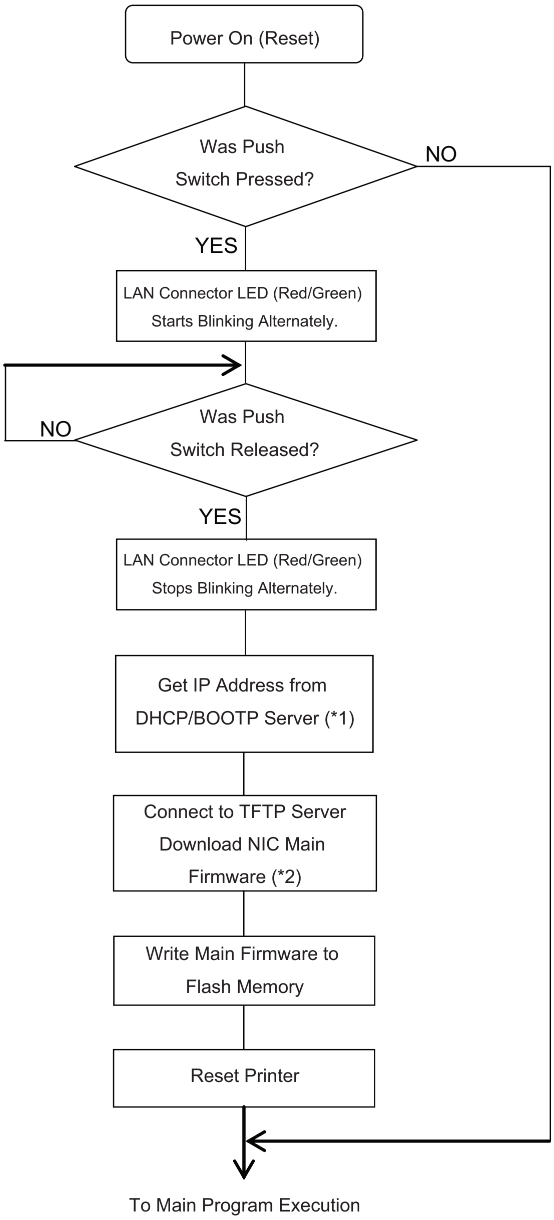
| | |
|---|---|
| | << Device ID >> |
| MFG | Star |
| CMD | STAR |
| MDL | TSP654 (STR_T-001) |
| CLS | PRINTER |

### 3.1.10. TFTP Client

When the printer power is turned on while you hold down the push switch, the TFTP (Trivial File Transfer Protocol) client stored in the boot loader is started up.

The TFTP client automatically downloads the main program from the TFTP server over the LAN, and writes to the Flash ROM on the NIC board. When writing ends normally, the printer will automatically be reset and will startup normally.

The following flowchart shows the series of operations.


Power On (Reset)
Was Push Switch Pressed?
NO
YES
LAN Connector LED (Red/Green) Starts Blinking Alternately.
NO
Was Push Switch Released?
YES
LAN Connector LED (Red/Green) Stops Blinking Alternately.
Get IP Address from DHCP/BOOTP Server (*1)
Connect to TFTP Server Download NIC Main Firmware (*2)
Write Main Firmware to Flash Memory
Reset Printer
To Main Program Execution

*1 It is necessary to startup the TFTP and DHCP/BOOTP servers on the same machine.

*2: The NIC main firmware filename downloaded from TFTP must be “NIC_MAIN.bin.”Even if the version is different, the firmware must be the same name as when downloading using TFTP. ((Ex.:) You can change “HE7_V100(NIC_Main).bin” to “NIC_MAIN.bin.”)

Note: This TFTP client function is used for emergency recovery when the F/W main firmware has been damaged. Use the FTP server function for ordinary F/W updates. (See section 3.1.6 FTP Server.)

### 3.1.11. TCP Keep-Alive

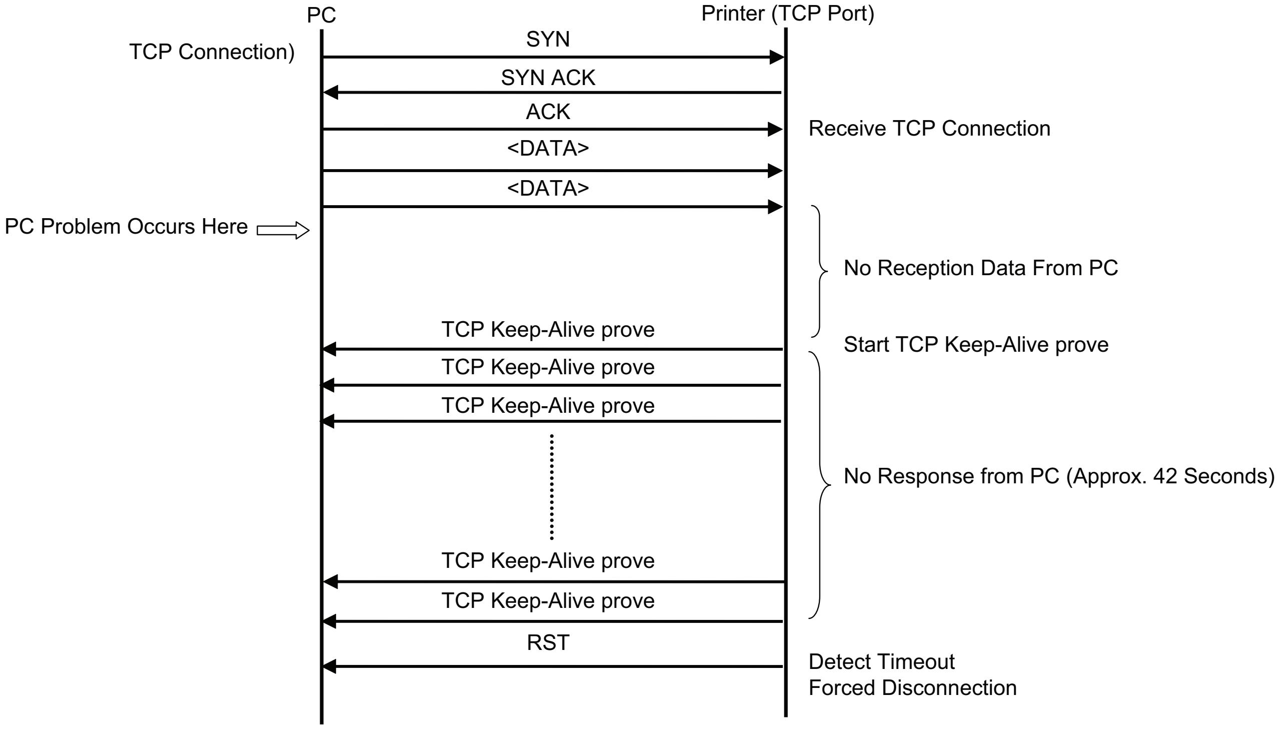
This product supports TCP Keep-Alive.
If TCP Keep-Alive is valid, TCP Keep-Alive operations are performed under the following conditions on the computer.

| Item | Value | Factory Default | Remarks |
|---|---|---|---|
| Setting | ENABLE/DISABLE | DISABLE | |
| Disconnection timeout time | Approx. 42 seconds | | Note 1 |

Note 1: If there is no response for this time from the computer, the printer forcibly disconnects the connection (RST).

- ➢ This feature is applied to all TCP/IP communications ports.
- ➢ This feature is unrelated to the TCP#9100 data reception timeout.

The following is an example communication chart.



Note: In the drawing, description of the <ACK> packet has been omitted.

### 3.1.12. SNMP

This function supports F/W Ver. 5.0.0 or later.
The SNMP of this product includes a SNMP agent that operates using UDP/IP.
Various information about this product and the printer can be managed with the SNMP manager.

It is compatible with SNMPv1, and supports MIB-II (RFC1213) and HostResource-MIB (RFC1514).
Read privilege is granted to community name "public", and the character string registered in "Authentic Community" in the product settings is handled as the write privilege.
However if no character string is set in "Authentic Community", write privilege is granted to community name "public".

* Restrictions
sysContact, sysName, and sysLocation are limited to a maximum of 78 (1-byte) characters.
ifAdminStatus and ifOperStatus are read-only and 1 is always returned as the read value.

An explanation of the MIB supported by this product is listed in the table below.

MIB-II (RFC1213)

| Name | Description |
|---|---|
| sysDescr | ASCII character string containing the device name, version, and other information |
| sysObjectID | Object ID indicating the product identification number |
| sysUpTime | Elapsed time after starting up (units: 10 msec) |
| sysContact | ASCII character string containing the administrator name and contact information |
| sysName | ASCII character string containing the device manager domain name and other information |
| sysLocation | ASCII character string indicating the physical location where the device is installed |
| sysServices | Value indicating the device protocol level service |
| ifNumber | Device network interface number |
| ifIndex | Interface identification number |
| ifDescr | ASCII character string indicating information associated with the interface |
| ifType | Physical layer and link protocol interface type |
| ifMtu | Maximum transmittable datagram size |
| ifSpeed | Interface transmission speed [bit/sec] |
| ifPhysAddress | Interface physical address |
| ifAdminStatus | Interface administration status |
| ifOperStatus | Interface operating status |
| ifLastChange | sysUpTime value at the time when the interface operating status was last changed |
| ifInOctets | Number of bytes received by the interface |
| ifInUcastPkts | Number of subnet work unicast packets received and delivered to a higher layer |
| ifInNUcastPkts | Number of broadcast or multicast packets received and delivered to a higher layer |
| ifInDiscards | Number of normal received packets that were discarded due to full buffer or other reason |
| ifInErrors | Number of received error packets |
| ifInUnknownProtos | Number of received packets that were discarded because of an invalid or unsupported protocol |
| ifOutOctets | Total number of transmitted bytes |
| ifOutUcastPkts | Number of packets that a higher-level protocol requested unicast transmission of |

| Name | Description |
|---|---|
| ifOutNUcastPkts | Number of packets that a higher-level protocol requested broadcast or multicast transmission of |
| ifOutDiscards | Number of packets that were discarded and not transmitted due to full buffer or other reason |
| ifOutErrors | Number of packets that were not transmitted due to error |
| ifOutQLen | Length of the output queue (number of packets) |
| ifSpecific | MIB-defined object ID unique to the interface media that is being used |
| atIfIndex | Value that identifies the interface related to this translation entry (=ifIndex) |
| atPhysAddress | Media-dependent physical address |
| atNetAddress | Network address (IP address) corresponding to the physical address |
| ipForwarding | Indication of whether or not there is a function for forwarding IP datagrams received at the IP gateway to other destinations<br>(1:Forwarding 2:NotForwarding) |
| ipDefaultTTL | Default value of IP datagram header TTL |
| ipInReceives | Total number of received IP datagrams |
| ipInHdrErrors | Number of datagrams discarded due to IP header error |
| ipInAddrErrors | Number of datagrams discarded due to problem with the IP header destination address |
| ipForwDatagrams | Number of IP datagrams forwarded to the final destination |
| ipInUnknownProtos | Number of IP datagrams intended for own node that were discarded due to unknown or unsupported protocol |
| ipInDiscards | Number of datagrams discarded due to buffer space or other internal problem |
| ipInDelivers | Number of datagrams delivered to IP user protocols (higher-level protocols including ICMP) |
| ipOutRequests.0 | Number of IP datagram transmission requests executed by local IP user protocols |
| ipOutDiscards | Number of IP datagrams that were discarded and not transmitted due to insufficient buffer or other reason |
| ipOutNoRoutes | Number of IP datagrams discarded because no route to the destination could be found when transmitting |
| ipReasmTimeout | Maximum value of receiving wait time for all IP datagrams when fragmented IP datagrams are received and reassembled |
| ipReasmReqds | Number of received fragmented IP datagrams necessary to reassemble the entity |
| ipReasmOKs | Number of received fragment IP datagrams that were successfully reassembled |
| ipReasmFails | Number of received fragment IP datagrams where reassembly failed |
| ipFragOKs | Number of datagrams that were successfully fragmented for this entity |
| ipFragFails | Number of datagrams that could not be fragmented and were discarded for this entity |
| ipFragCreates | Number of fragment IP datagrams that were generated as a result of fragmentation for this entity |
| ipAdEntAddr | IP address which is associated with the address information |
| ipAdEntIfIndex | Interface identification number corresponding to this IP address |
| ipAdEntNetMask | Subnet mask value associated with this IP address |
| ipAdEntBcastAddr | Value of the least significant bit in the IP broadcast address used for broadcast sent on the interface of the IP address |
| ipAdEntReasmMaxSize | Maximum IP datagram size that can be reassembled for the entity from the received fragment IP datagrams |

| Name | Description |
|---|---|
| ipRouteDest | Destination IP address of this route (0.0.0.0 = Default route) |
| ipRouteIfIndex | Interface identification number for transmitting to the next destination host on this route (= ifIndex) |
| IpRouteMetric | Primary routing metric for this route (-1 = Not used) |
| ipRouteNextHop | IP address of next hop on this route |
| IpRouteType | Route types (1: None of the following, 2: Invalid route, 3: Direct connection, 4: Indirect connection) |
| IpRouteProto | Routing mechanism by which this route was learned |
| IpRouteAge | Elapsed time after this route was last confirmed as a normal route [sec] |
| IpRouteMask | Value which performs logical AND before comparison with ipRouteDest or the destination address |
| ipRouteInfo | MIB definition number for routing protocol used for this route |
| ipNetToMediaIfIndex | Interface identification number for this entry (=ifIndex) |
| ipNetToMediaPhysAddress | Media-dependent physical address |
| ipNetToMediaNetAddress | IP address corresponding to the physical address of this entry |
| ipNetToMediaType | Address conversion method (1: None of the following, 2: Invalid value, 3: Dynamic conversion, 4: Static conversion) |
| icmpInMsgs | Total number of received ICMP |
| icmpInErrors | Number of received ICMP messages that were discarded due to checksum error or other ICMP specification error |
| icmpInDestUnreachs | Number of ICMP destination-unreachable messages received |
| icmpInTimeExcds | Number of ICMP time-exceeded messages received |
| icmpInParmProbs | Number of ICMP parameter-problem messages received |
| icmpInSrcQuenchs | Number of ICMP source-quench messages received |
| icmpInRedirects | Number of ICMP redirect messages received |
| icmpInEchos | Number of ICMP echo-request messages received |
| icmpInEchoReps | Number of ICMP echo-reply messages received |
| icmpInTimestamps | Number of ICMP timestamp-request messages received |
| icmpInTimestampReps | Number of ICMP timestamp-reply messages received |
| icmpInAddrMasks | Number of ICMP address mask request messages received |
| icmpInAddrMaskReps | Number of ICMP address mask reply messages received |
| icmpOutMsgs | Total number of ICMP messages transmitted |
| icmpOutErrors | Number of ICMP messages that were discarded and not transmitted due to full buffer or other reason at time of ICMP transmission |
| icmpOutDestUnreachs | Number of ICMP destination-unreachable messages transmitted |
| icmpOutTimeExcds | Number of ICMP time-exceeded messages transmitted |
| icmpOutParmProbs | Number of ICMP parameter-problem messages transmitted |
| icmpOutSrcQuenchs | Number of ICMP source-quench messages transmitted |
| icmpOutRedirects | Number of ICMP redirect messages transmitted |
| icmpOutEchos | Number of ICMP echo-request messages transmitted |
| icmpOutEchoReps | Number of ICMP echo-reply messages transmitted |
| icmpOutTimestamps | Number of ICMP timestamp-request messages transmitted |
| icmpOutTimestampReps | Number of ICMP timestamp-reply messages transmitted |
| icmpOutAddrMasks | Number of ICMP address mask request messages transmitted |
| icmpOutAddrMaskReps | Number of ICMP address mask reply messages transmitted |

| Name | Description |
|---|---|
| tcpRtoAlgorithm | Algorithm that decides the resend timeout value for TCP connection (1: None of the following, 2: Fixed value, 3: MIL-STD-1778, 4: Van Jacobson's algorithm) |
| tcpRtoMin | Minimum TCP protocol resend timeout value (units: 10 msec) |
| tcpRtoMax | Maximum TCP protocol resend timeout value (units: 10 msec) |
| tcpMaxConn | Maximum number of TCP connections |
| tcpActiveOpens | Number of times that TCP connections were actively opened |
| tcpPassiveOpens | Number of times that TCP connections were passively opened |
| tcpAttemptFails | Number of times that TCP connections failed |
| tcpEstabResets | Number of times that TCP connections were reset |
| tcpCurrEstab | Number of TCM connections with status ESTABLISHED or CLOSE-WAIT |
| tcpInSegs | Number of received TCP segments |
| tcpOutSegs | Number of transmitted TCP segments |
| tcpRetransSegs | Number of resent TCP segments |
| tcpConnState | Status of this TCP connection<br>(1:Closed 2;Listen 3:SynSent 4:SynReceived 5:Established 6:FinWait1 7:FinWait2 8:CloseWait 9:LastAck 10:Closing 11:TimeWait 12:DeleteTCB) |
| tcpConnState | Status of this TCP connection |
| tcpConnLocalAddress | Local IP address of this TCP connection |
| tcpConnLocalPort | Local port number of this TCP connection |
| tcpConnRemAddress | Remote IP address of this TCP connection |
| tcpConnRemPort | Remote connection port of this TCP connection |
| tcpInErrs | Number of received error segments (TCP checksum error, etc.) |
| tcpOutRsts | Number of times that TCP connections were reset |
| udpInDatagrams | Total number of UDP datagrams delivered to UDP users |
| udpNoPorts | Number of received UDP datagrams destined for ports that are not open |
| udpInErrors | Number of received UDP datagrams which were discarded due to a problem with the destination port application |
| udpOutDatagrams | Number of transmitted UDP datagrams |
| udpLocalAddress | Local address of UDP receiving standby port (0.0.0.0: no designated receiving address) |
| udpLocalPort | Receiving wait local port number |

| Name | Description |
|---|---|
| snmpInPkts | Total number of SNMP messages received from the transport service |
| snmpOutPkts | Total number of SNMP message transmission requests sent to the transport layer |
| snmpInBadVersions | Total number of received SNMP messages that were for an unsupported version |
| snmpInBadCommunityNames | Total number of received SNMP messages with an invalid community name |
| snmpInBadCommunityUses | Number of received SNMP messages that indicated an operation which is not permitted by that community |
| snmpInASNParseErrs | Number of errors in ASN.1 or BER format detected while decoding received SNMP messages |
| snmpInTooBigs | Number of received SNMP/PDU with error status "TooBig" |
| snmpInNoSuchNames | Number of received SNMP/PDU with error status "NoSuchName" |
| snmpInBadValues | Number of received SNMP/PDU with error status "BadValue" |
| snmpInReadOnlys | Number of received SNMP/PDU with error status "ReadOnly" |
| snmpInGenErrs | Number of received SNMP/PDU with error status "GenErr" |
| snmpInTotalReqVars | Number of MIB objects read successfully as a result of Get-Request and Get-NextRequest PDUs |
| snmpInTotalSetVars | Number of MIB objects changed successfully as a result of receiving Set-Request |
| snmpInGetRequests | Number of received SNMP Get-Request PDUs |
| snmpInGetNexts | Number of received SNMP Get-NextRequest PDUs |
| snmpInSetRequests | Number of received SNMP Set-Request PDUs |
| snmpInGetResponses | Number of received SNMP Get-Response PDUs |
| snmpInTraps | Number of received SNMP trap PDUs |
| snmpOutTooBigs | Number of transmitted PDUs with designated error status "TooBig" |
| snmpOutNoSuchNames | Number of transmitted PDUs with designated error status "NoSuchName" |
| snmpOutBadValues | Number of transmitted PDUs with designated error status "BadValue" |
| snmpOutGenErrs | Number of transmitted PDUs with designated error status "GenErr" |
| snmpOutGetRequests | Number of transmitted SNMP Get-Request PDUs |
| snmpOutGetNexts | Number of transmitted SNMP Get-NextRequest PDUs |
| snmpOutSetRequests | Number of transmitted SNMP Set-Request PDUs |
| snmpOutGetResponses | Number of transmitted SNMP Get-Response PDUs |
| snmpOutTraps | Number of transmitted SNMP trap PDUs |
| snmpEnableAuthenTraps | Control of authentication-failure trap generation<br>(1: Generate traps, 2: Do not generate traps) |

Host Resource-MIB(RFC1514)

| Name | Description |
|---|---|
| hrDeviceIndex | Characteristic value assigned to the connected device |
| hrDeviceType | Connected device type |
| hrDeviceDescr | Character string describing the connected device |
| hrDeviceID | Connected device product ID |
| hrDeviceStatus | Connected device status<br>(1:Unknown 2:Running 3:Warning 4:Testing 5:Down) |
| hrDeviceErrors | Number of times errors were generated by the connected device |
| hrPrinterStatus | Connected printer status<br>(1:Idle 2:Printing 3:Warmup) |
| hrPrinterDetectedErrorState | Connected printer error status<br>(0:LowPaper 1:NoPaper 2:LowToner 3:NoToner 4:DoorOpen 5:Jammed 6:Offline 7:ServiceRequested) |

### 3.1.12.1. SNMP Configuration Parameters

The following parameters can be set from web configuration or Telnet.
These values can also be checked at self-test print.

| Name | Setting range | Default value |
|---|---|---|
| Authentic Community | Max. 15 characters (ASCII) | "public" |
| Trap Community | Max. 15 characters (ASCII, Japanese OK) | "public" |
| Trap Address (IP) | 0.0.0.0 - 255.255.255.255 | 0.0.0.0 |
| SysContact | Max. 78 characters (ASCII, Japanese OK) | None |
| SysName | Max. 78 characters (ASCII, Japanese OK) | None |
| SysLocation | Max. 78 characters (ASCII, Japanese OK) | None |
| EnableAuthenTrap | 1 or 2 | 2 |

### 3.1.12.2. Trap Issue Events

When the EnableAuthenTrap setting for this product is ENABLE,
then this product issues traps to the SNMP manager (trap notification address) when the following 3 events occur.

[Trap issue events]

1. When product was started up
   [Generic trap type = 0(Cold Start)]

2. When printer status changed (IEEE1284 port status monitor)
   [Generic trap type = 6(Enterprise Specific)]

3. When access by an invalid committee name occurred
   [Generic trap type = 4(Authentication Failure)]

## 3.2 Other Specifications

### 3.2.1. Operating Time

There are approximately 14 seconds from the time the power is turned on to the startup of the TCP/IP (start of IP address acquisition).
It takes approximately 18 seconds before the TCP/IP services (HTTP, TELNET, FTP, LPD, Raw Socket Print) can be used after turning on the power.

**Note: When acquiring the IP address by Dynamice (DHCP/BOOTP, RARP), this time may lengthen depending on the server response time.**

### 3.2.2. Push Switch

While the TCP/IP is operating (the power has been turned on, and it is within the elapse time described in section 3.2.1 Startup Time), if the push switch is continued to be held down, the LED display pattern will change according to the times shown below.
When the switch is released, the product will enter each special mode.

Special Mode

| Phase | SW Pressing Time | LAN Connector<br>LED Blinking Pattern | | Special Mode |
|---|---|---|---|---|
| | | Green | Red | |
| 1 | 1 second to less than 5 seconds | Blinking | Blinking | NIC setting initialize mode (*2) |
| 2 | 5 second to less than 9 seconds | Extinguished | Blinking | Reserved (Undefined) |
| 3 | 9 second to less than 13 seconds | Blinking | Extinguished | Reserved (Undefined) |
| | Over 13 seconds (*1) | | | |

**Note 1. When Phase 3 is exceeded, press the switch for 1 second to return to Phase 1.**

**Note 2. Execution procedures for the NIC setting initialize mode**

1. After entering this mode, press the push switch once and release it.
The LED display will be “Green = Extinguished; Red = Extinguished” and the initializing of the NIC settings in the non-volatile memory will begin.

2. If the initialization is successful, the printer will automatically be reset.
Do not turn off the power or apply a reset until this reset has been applied.
Also, if the NIC setting initialization fails, the LED display will be “Green = Extinguished; Red = Lit” and all operations will stop.
If so, turn the power off.

**Note: When turning the power on, a different mode (automatic firmware update function using TFTP client) will startup that is different to the above functions, for the operations when turning the power on with the push switch pressed. For details, see section 3.1.8 TFTP Client.**

### 3.2.3. DIP Switches

DIP switches are loaded when the power is turned on or when the printer is reset. Therefore, when you change the settings, enable them by turning the printer on again, or by executing a printer reset.Turn the power off before changing the PCB and interface type.

| DIP switch | Feature | ON | OFF |
|---|---|---|---|
| DIPSW1 | Sets IP address acquisition timeout | No timeout | 20 seconds (factory default setting) |
| DIPSW2 | Reserved (Fixed at off) | - | - |

DIPSW1

Sets the timeout time when getting the address from a DHCP/BOOTP server. The factory default setting (when set to off) is 20 seconds.

When set to on, there is no timeout.

If this product is connected directly to an intelligent switch or intelligent hub, the physical link may take some time to become established. As a result, a timeout will occur while waiting to get the DHCP/BOOTP address, and it will fail to get the IP address. In such cases, set DIPSW1 = ON to have no IP address acquisition timeout.

DIPSW2

Presently unused. A feature will be added in the future. This should always be off.

### 3.2.4. LED

There is a red and a green LED equipped on the network interface connector (LAN connector RJ45).
These function as outlined below under normal operating conditions.

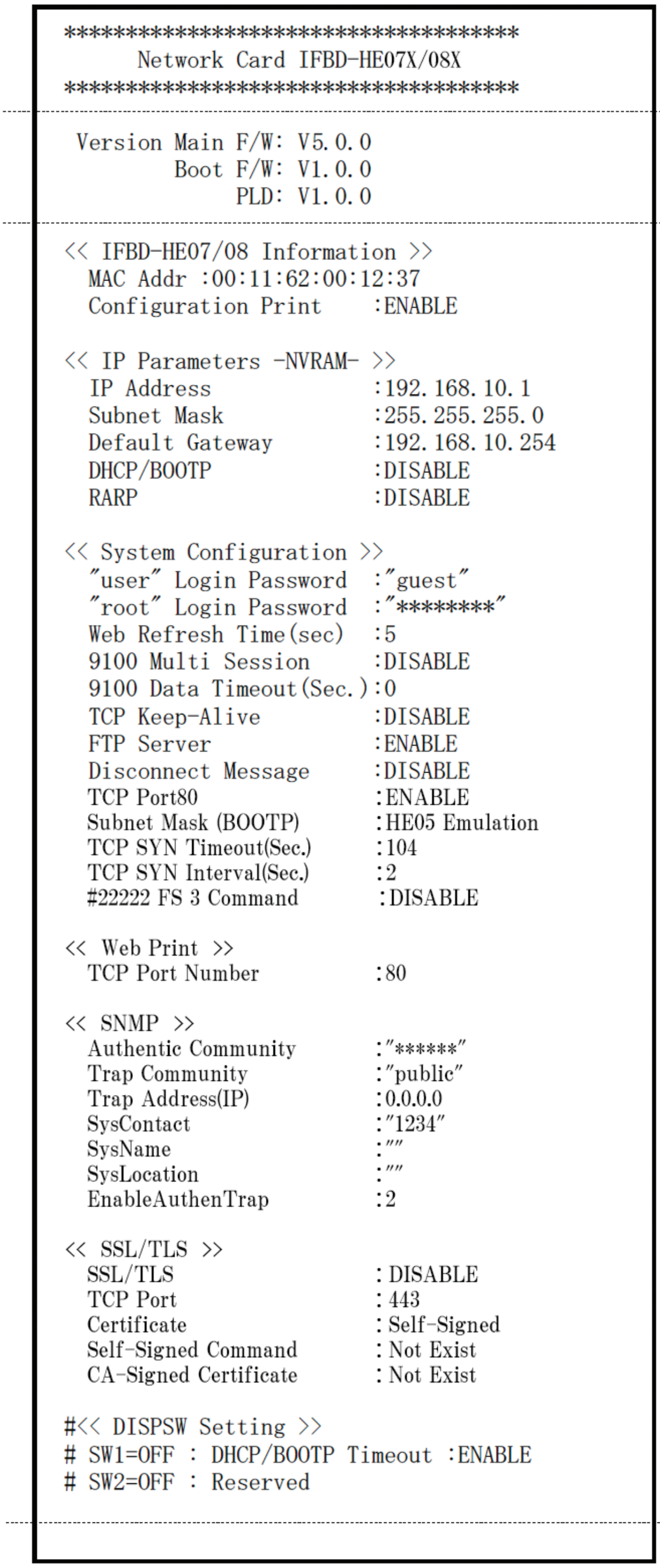
| | |
|---|---|
| Red (LINK/Activity): | A link has been established between the port and the connected device. Communications are ready at both devices. |
| Green (100M): | Lights when the port is operating at 100 Mbps. |

For others, the flashing pattern changes according to the pressing of the push switch.
For details, see sections 3.1.10 TFTP Client and 3.2.2 Push Switch.

### 3.2.5. Self-test Print

If this product executes a printer self-print, the following is printed after the printer setting print.
Finally, for the IP parameter information during operation, it is not possible when conducting a self-print by command from the PC.

Self-test Print Example (For F/W Ver. 5.0.0 and StarWebPRNT model)

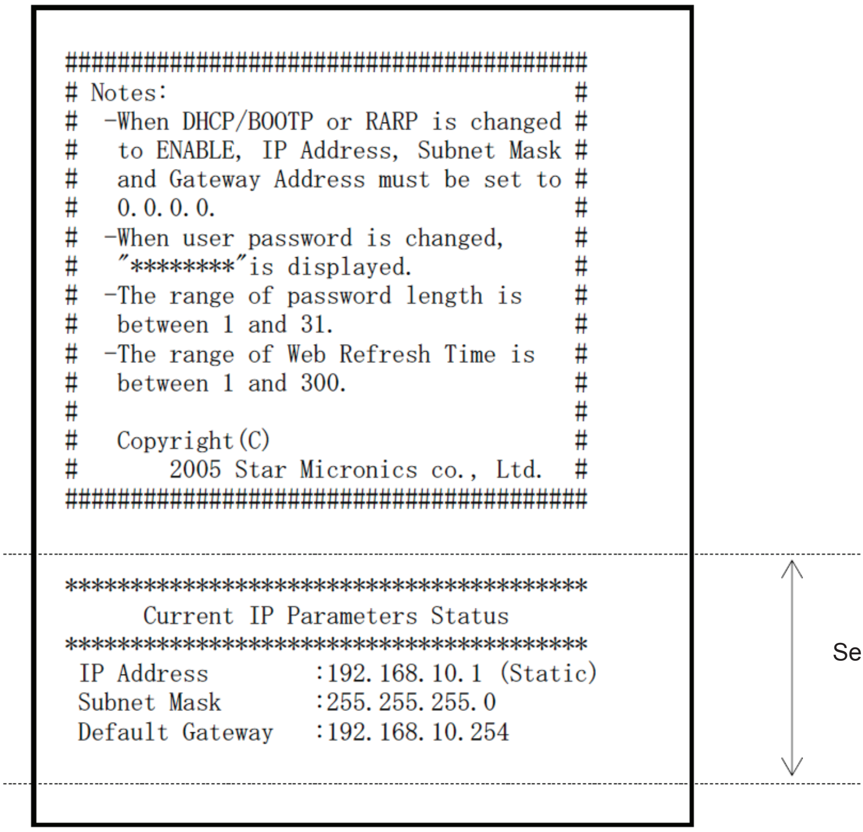


```
*************************************
      Network Card IFBD-HE07X/08X
*************************************

 Version Main F/W: V5.0.0
         Boot F/W: V1.0.0
              PLD: V1.0.0

<< IFBD-HE07/08 Information >>
  MAC Addr :00:11:62:00:12:37
  Configuration Print     :ENABLE

<< IP Parameters -NVRAM- >>
  IP Address              :192.168.10.1
  Subnet Mask             :255.255.255.0
  Default Gateway         :192.168.10.254
  DHCP/BOOTP              :DISABLE
  RARP                    :DISABLE

<< System Configuration >>
  "user" Login Password   :"guest"
  "root" Login Password   :"********"
  Web Refresh Time(sec)   :5
  9100 Multi Session      :DISABLE
  9100 Data Timeout(Sec.):0
  TCP Keep-Alive          :DISABLE
  FTP Server              :ENABLE
  Disconnect Message      :DISABLE
  TCP Port80              :ENABLE
  Subnet Mask (BOOTP)     :HE05 Emulation
  TCP SYN Timeout(Sec.)   :104
  TCP SYN Interval(Sec.)  :2
  #22222 FS 3 Command     :DISABLE

<< Web Print >>
  TCP Port Number         :80

<< SNMP >>
  Authentic Community     :"******"
  Trap Community          :"public"
  Trap Address(IP)        :0.0.0.0
  SysContact              :"1234"
  SysName                 :""
  SysLocation             :""
  EnableAuthenTrap        :2

<< SSL/TLS >>
  SSL/TLS                 : DISABLE
  TCP Port                : 443
  Certificate             : Self-Signed
  Self-Signed Command     : Not Exist
  CA-Signed Certificate   : Not Exist

#<< DISPSW Setting >>
# SW1=OFF : DHCP/BOOTP Timeout :ENABLE
# SW2=OFF : Reserved
```

Version Information (Main, Boot Load, PLD)

NIC Setting Information
(Same as the *netconf.ini" File)

* The Web Print setting items are for models which support Star WebPRNT only.
* The SNMP setting items are for F/W Ver. 5.0.0 or later only.



```
#########################################
# Notes:                                #
#  -When DHCP/BOOTP or RARP is changed #
#   to ENABLE, IP Address, Subnet Mask #
#   and Gateway Address must be set to #
#   0.0.0.0.                            #
#  -When user password is changed,      #
#   "********"is displayed.             #
#  -The range of password length is     #
#   between 1 and 31.                   #
#  -The range of Web Refresh Time is    #
#   between 1 and 300.                  #
#                                       #
#   Copyright(C)                        #
#       2005 Star Micronics co., Ltd.   #
#########################################

*****************************************
      Current IP Parameters Status
*****************************************
 IP Address          :192.168.10.1 (Static)
 Subnet Mask         :255.255.255.0
 Default Gateway     :192.168.10.254
```

Select IP Parameter While Running

### 3.2.6. Broken Link Detection

TCP/IP communications on this product informs the operator when printing is not possible. Therefore, it supports the broken link detection feature.

There are two broken links that can be detected.
1 Physical link down
Indicates either of the following states.
- Time from powering on the printer until the Ethernet link is established (TCP/IP startup)
- Error status because Ethernet link detected to be down because the LAN cable was disconnected between the printer and HUB.

Chattering removal conditions when connecting and disconnecting the LAN cable are shown below.
- When LAN cable is disconnected (link down judgment): 4 seconds
- When LAN cable is inserted (link established judgment): 2 seconds

2 IP address lost
Indicates either of the following states.
- Time from TCP/IP startup until IP address is obtained.
- Error status when failed to get IP address.

When a broken link is detected, the following operations are requested to the printer.
IP address lost takes priority over physical link down.
Also, actual operations for LED display and printing warnings must be supported by the printer.
(For details, see section 5.2 Printer Firmware Support Table and each printer's product specifications manual.)
When this happens, check the LAN cable connection and the IP address settings for the communication path, and then restart the printer.

- LED Display

LED blinking on the printer operation panel inform the operator of the physical link down and IP address lost.
However, the LED type and blinking cycles depend on the printer's specifications.

Example display on TSP700II/TSP800II
(1) Physical link down
POWER LED (green) and ERROR LED (orange) blink slowly (on=2 seconds, off = 2 seconds).
(2) IP address lost
POWER LED (green) and ERROR LED (orange) blink quickly (on=0.125 seconds, off = 0.125 seconds).

Network communications are ready when both (1) and (2) are removed (blinking stops).
You cannot invalidate this operation.

- Warning print

When physical link down or IP address lost (error when it fails to get the IP address) is detected, this sends warning print data to the printer to inform the operator that a problem has occurred.
Reception data before and after this operation executes is not guaranteed.

This feature can be made valid or invalid using HTTP (Web), Telnet, and FTP. Use HTTP (Web) to register the warning print data. The setting is stored on the product's non-volatile memory.

Warning print settings specifications

| Item | | Range | Factory Default |
|---|---|---|---|
| Operation setting | | ENABLE/DISABLE | DISABLE |
| Warning data | Character Types | ASCII (20H-7FH) | ***********************************<br>NO HOST CONNECTION<br>*********************************** |
| | Number of lines | 1-4 lines | |
| | Character Count | Max. 80 characters/line, 4 lines total:<br>Up to 320 characters. | |

## 3.3 Settings/Display Items

The following describes the types of information that can be set and displayed by HTTP (WEB), TELNET, FTP.

### 3.3.1. IP Parameter Settings

The following table shows the Static (fixed address) and Dynamic (dynamic address acquisition) items of the IP address that can be stored in the non-volatile memory.

| Category | Setting Items | Input Range | Initial Value (Factory Default) |
|---|---|---|---|
| Static | IP Address | 0.0.0.0 - 255.255.255.254 | 0.0.0.0 |
| | Subnet Mask | 0.0.0.0 - 255.255.255.255 | 0.0.0.0 |
| | Default Gateway | 0.0.0.0 - 255.255.255.255 | 0.0.0.0 |
| Dynamic | DHCP, BOOTP | ENABLE/DISABLE | ENABLE |
| | RARP | ENABLE/DISABLE | ENABLE |

**Note: If setting Static to anything other than 0.0.0.0, set all Dynamic to DISABLE.**
**If setting Dynamic to ENABLE, set all Static to 0.0.0.0.**

### 3.3.2. System Settings

The following shows the NIC system setting items.
These settings are stored in the non-volatile memory on the product’s card.

| Setting Items | Input Range | Initial Value (Factory Default) |
|---|---|---|
| “user” Login Password (Note 1) | • 1-31 characters<br>• ASCII characters<br>• Upper case/lower case sensitive | “guest” |
| “root” Login Password | • 1-31 characters<br>• ASCII characters<br>• Upper case/lower case sensitive | “public” |
| Web Page Refresh Interval Time (sec.) | 1 - 300 | 5 |
| 9100 Multi Session | ENABLE/DISABLE | DISABLE (Note 2) |
| 9100 Data Timeout (Sec.) | 0, 30, 40, 60, 120, 180, 360 | 0 |
| TCP Keep-Alive | ENABLE/DISABLE | DISABLE |
| FTP Server | ENABLE/DISABLE | ENABLE |
| Disconnect Message | ENABLE/DISABLE | DISABLE |
| (Warning data Note 3) | Line1<br>Line2<br>Line3<br>Line4<br><br>Default Message (Note 4) | |
| TCP Port80 (Note 5) | ENABLE/DISABLE | ENABLE |
| Subnet Mask(BOOTP) (Note 6) | HE05 Emulation / HE07 Emulation | HE05 Emulation |
| TCP SYN Timeout (Sec.) (Note 7) | 1 ～ 300 | 104 |
| TCP SYN Interval (Sec.) (Note 7) | 1 ～ 300 | 2 |
| #22222 FS 3 Command (Note 8) | ENABLE/DISABLE | DISABLE |

**Note 1: The “user” login password is displayed with the default value (“guest”), but if changed to other than the default, it is camouflaged with “********.”**

**Note 2: The factory default settings for 9100 Multi-session are different for the old (IFBD-HE05/06/BE05) and new products (IFBD-HE07/08/BE07).**

**IFBD-HE05/06/BE05 (old product): ENABLE**
**IFBD-HE07/08/BE07 (this product): DISABLE**

**Note 3: Warning data registration is done only on HTTP (Web).**

**Note 4: When Disconnect Message = ENABLE, press Default Message to display the next data in Line 1 – Line 4 fields.**

**Line 1: ******************************

**Line 2: NO HOST CONNECTION**

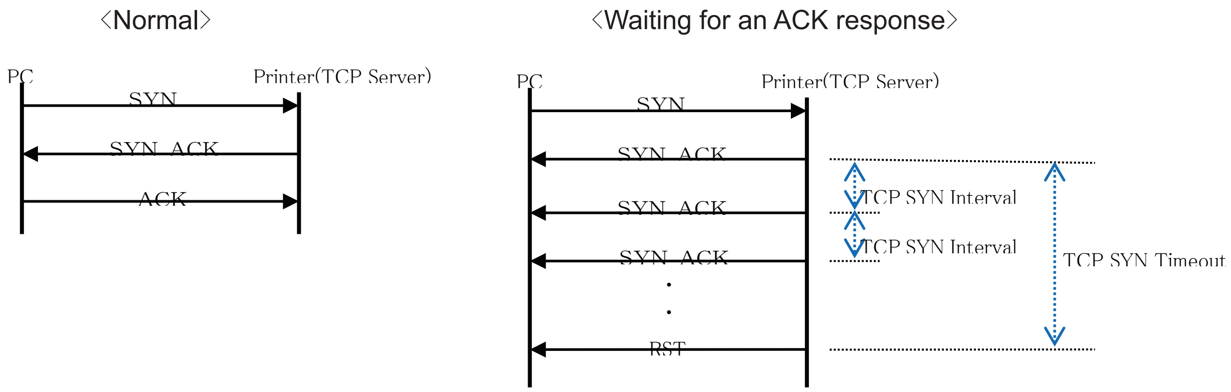
**Line 3: ******************************

**Line 4:**

**Note 5: The TCP Port80 setting is only available for Telnet. Supported by Ver 2.3.0 and later.**

**Note 6: This setting is only available for Telnet. Supported by Ver 3.0.0 and later.**

**Note 7: TCP SYN Timeout/Interval specifies the SYN ACK output retry conditions if there is no ACK response from the host (PC) to the SYN ACK from the server (this NIC) when the TCP connection is accepted (SYN receiving). Supported by Ver 3.3.0 and later.**



**Note 8: This setting is only available for Telnet and FTP. Supported by Ver 3.4.0 and later.**

### 3.3.3. WebPrint Settings (IFBD-HE07X/08X/BE07X only)

StarWebPRNT Function is set up.
This setting is stored in the product’s non-volatile memory.
See “4. StarWebPRNT Function” for more details.

| Setting Items | Input Range(Note 1) | Initial Value (Factory Default) |
|---|---|---|
| TCP Port Number | • 1-65535 | 80 |

**Note 1: Port numbers that are also used by other services cannot be used. “Well-known” ports are not recommended.**

### 3.3.4. SNMP Settings

Configure the settings for SNMP. This setting is for web and Telnet only. It is supported beginning from F/W Ver. 5.0.0 or later. Refer to section 3.1.12.1 “SNMP configuration parameters”.

### 3.3.5. SSL/TLS Settings

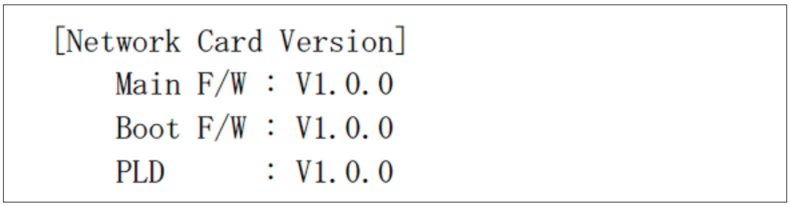
Configure the settings for SSL/TLS. This setting is only available for WEB sites. Supported by Ver 4.0.0 and later.

| Selected Items | Setting Items | Input Range | Default Value (Factory Default) |
|---|---|---|---|
| SSL/TLS Setting | SSL/TLS | ENABLE/DISABLE | DISABLE |
| | TCP Port | Optional | 443 |
| | Certificate | Self-Signed/CA Signed | Self-Signed |
| Create Self-Signed Certifacate | | | - |
| Import CA-Signed Certificate | | | - |

### 3.3.6. Network Card Information Display

Displays the NIC main firmware version, boot loader version and PLD revision.

Display Example

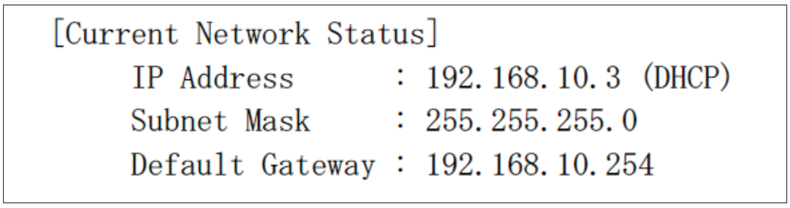


```
[Network Card Version]
    Main F/W : V1.0.0
    Boot F/W : V1.0.0
    PLD      : V1.0.0
```

### 3.3.7. Current IP Parameter Status Display

Displays the operating IP address. An address acquisition prototocl is input in the IP address parentheses.

Display Example

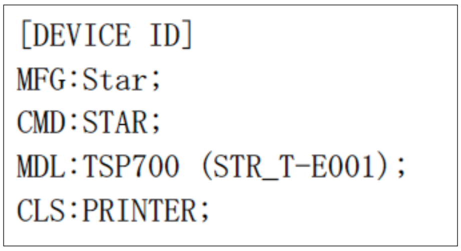


```
  [Current Network Status]
       IP Address      : 192.168.10.3 (DHCP)
       Subnet Mask     : 255.255.255.0
       Default Gateway : 192.168.10.254
```

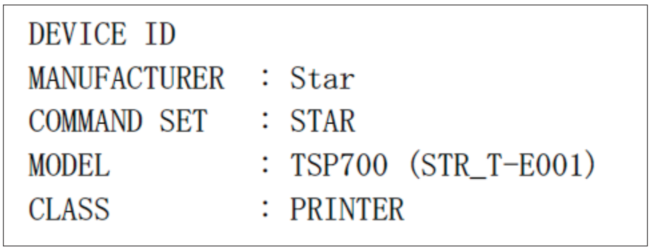
### 3.3.8. Printer Device ID Display

Displays the printer device ID.  Format conforms to IEEE1284.

Display Exampel 1 (TELNET, FTP)  Display Example 2 (Web)



```
[DEVICE ID]
MFG:Star;
CMD:STAR;
MDL:TSP700 (STR_T-E001);
CLS:PRINTER;
```

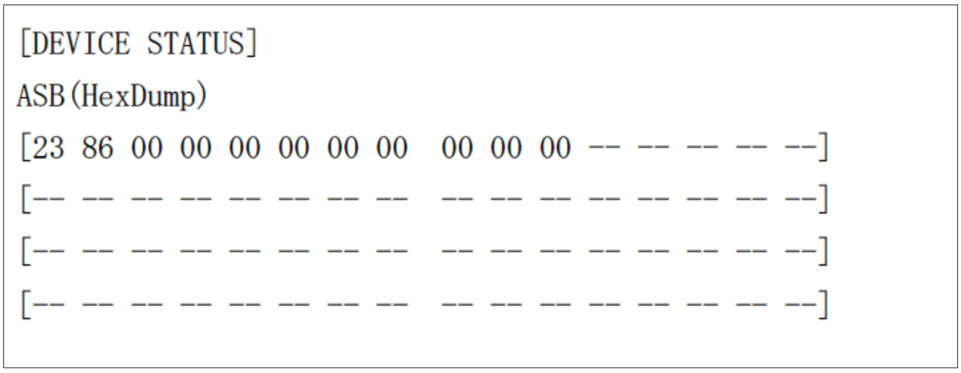


```
DEVICE ID
MANUFACTURER  : Star
COMMAND SET   : STAR
MODEL         : TSP700 (STR_T-E001)
CLASS         : PRINTER
```

### 3.3.9. Printer Status Display

• The printer automatic status is displayed in a hexadecimal dump by HTTP (WEB), TELNET, and FTP.

Display Example



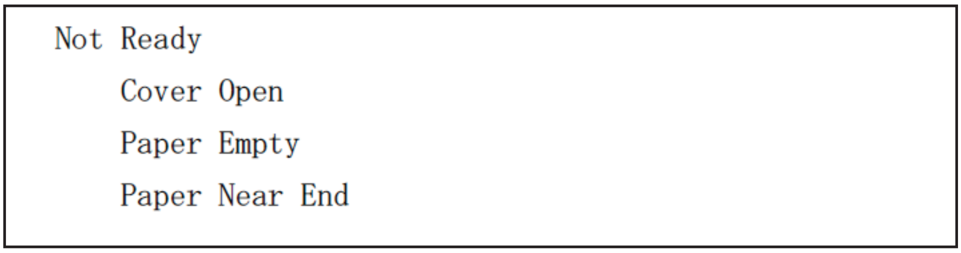
```
[DEVICE STATUS]
ASB(HexDump)
[23 86 00 00 00 00 00 00  00 00 00 -- -- -- -- --]
[-- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --]
[-- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --]
[-- -- -- -- -- -- -- --  -- -- -- -- -- -- -- --]
```

• Other status details of the hexadecimal dump display are displayed by HTTP (WEB).

The displayable status information is shown below.
* See the printer's specifications manual for details on status specifications.

| Status Information | Display | Status |
|---|---|---|
| Ready | | Idling |
| Not Ready | | Error status |
| Not Ready Causes | Cover Open | Cover open |
| | Paper Empty | Paper out |
| | Paper Near End | Paper near-end |
| | Paper Size Error (Black Mark/ Label Error) | Black mark error (models that support BM)/ label size error (models that support labels) |
| | Auto Cutter Error | Auto-cutter Error |
| | Presenter Paper Jam Error | Paper jam at presenter |
| | Mechanical Error | Mechanical Error |
| | High Temperature Detection | High temperature stop |
| | Non-recoverable Errors | Non-recoverable Error |

Display Example



```
 Not Ready
     Cover Open
     Paper Empty
     Paper Near End
```

# 4. Star WebPRNT FUNCTION (IFBD-HE07X/08X/BE07X)

## 4.1 General description

The StarWebPRNT function can perform printer control operations (printing, cash draw driving etc.) over a network from a network device equipped with a Web browser. This function performs printer control operations by sending XML data to an Ethernet I/F card from a Web application without using operating system print applications or printer drivers.
StarWebPRNT is only available for IFBD-HE07X/08X/BE07X.

Main Features
Native applications for all operating systems are unnecessary allowing for easy printing
Simple configuration and easy maintenance
The application can be placed in the cloud

## 4.2 Specification

<Communication specification>

| | |
|---|---|
| TCP/IP version | : TCP/IP v4 |
| Communication Protocol | : HTTP/HTTPS(*) |
| Data format | : XML<br>REST format supported |
| Start communication session | : Start from device. |
| End communication session | : End from IFBD-HE07X/08X/BE07X. |
| Communication port number | : Optional (Default setting HTTP:TCP Port80, HTTPS:TCP Port443)(*)<br>Can be changed by Telnet, FTP, or Web settings. See “3.3 Settings/Display Items”. |
| Character Code | : ASCII, Code Page(On European and U.S. models)<br>UTF-8(Kanji model)(Correspondence is required of the printer side. ) |

Black Mark: Supported *

* F/W Ver4.0.0 or later supports HTTPS and Black Mark.

See “5.2 Supported Printer Firmware” for details on the supported models and firmware for the main printer unit.

<About the StarWebPRNT SDK>
Star provides an SDK for use when creating a Web application that uses this function to perform printer control.
The SDK contains JavaScript and HTML samples that perform XML document creation and communication control between a device and a printer etc.
See the “Star WebPRNT User’s Manual” on the Star homepage for the SDK and the XML element specifications.

Operating environment
-Web browser:  HTML 5 support

In accordance with SSL/TLS support, tests were carried out by checking compatibility with F/W Ver4.0.0.
The validated compatibility results tested by Star Micronics Co., Ltd. are shown in the following table. (Results of F/W Ver4.0.0 as of Dec. 2015)

〈Conditions of the operation check〉

- Star WebPRNT SDK operation
  Printing and status acquisition work normally. A security error does not appear on the web browser.
- Web configuration operation of NIC
  Changing the settings operate normally. A security error does not appear on the web browser.
  All results of the operation tests must be OK with both SSL/TLS Enable/Disable.

[Windows environment]

| WEB browser | Windows7 | Windows8.1 | Windows10 |
|---|---|---|---|
| Firefox (Ver:41.0.1) | OK | OK | OK |
| Safari (Ver:5.1.7) | OK | OK | OK |
| Chrome (Ver:45.0.2454.85) | OK | OK | OK |
| Internet Explorer11 (Ver:11.0.9600.18015) | OK | OK | OK |
| Microsoft Edge (Ver:20.10240.16384) | OK | OK | OK (*1) |

*1) You may need to register the printer's IP address as a "Trusted site" in the web browser settings.

[Mac environment]

| WEB browser | OS X V10.10.3 |
|---|---|
| Firefox (Ver:40.0.0.3) | OK |
| Safari (Ver8.0.8) | OK |
| Chrome (Ver:43.0.2357.130) | OK |

[iOS environment]

| WEB browser | iOS 8.2 | iOS 9.02 |
|---|---|---|
| Safari (Ver5.1.7) | OK | OK |

[Android environment]

| WEB browser | Andriod 4.4.2 | Android 6.0 |
|---|---|---|
| Firefox (Ver:40.0.0.3) | OK | - |
| Chrome (Ver:45.0.2454.94) | OK | OK |

-: Unconfirmed device

* 2017.8.16: Added information
When performing SSL/TLS communication with Chrome Ver. 58 or later, F/W Ver. 4.1.0 or later, or F/W Ver. 5.0.0 or later, is required.

# 5. SSL/TLS COMMUNICATIONS

## 5.1. General Description

This NIC can encrypt communication (HTTPS) using SSL (Socket Security Layer)/TLS (Transport Layer Security).

## 5.2. Specifications

<Communication specifications>
SSL/TLS version: TLS1.2 (SSL3.3)
Application protocol: HTTPS (Server Authentication)
TCP communication pot number: Optional (factory default setting: 443)
Certificate: Self-signed certificate or CA-signed certificate
Encryption algorithm: AES 128/256, RC4
Hash algorithm: SHA-256, SHA-1, MD5

Factory default setting is SSL/TLS=Disable. You need to enable them in the Web settings.
Regarding the certificate required to authenticate with the client's device, register either a self-signed certificate or a CA-signed certificate.
You can check the basic settings (SSL/TTL Enable/Disable, the TCP communication port number, certificate selection, and whether it is necessary or unnecessary to register a certificate) by self-print.

To use this function, F/W Ver.4.0.0 and later must be installed on this NIC, and it must be a model with "S" shape engraved on the chassis of the NIC at the time of shipment from the factory.
For the position of the engraved "S" shape, see "2.1 Model Names" in "2. HARDWARE SPECIFICATIONS".
The "S" shape indicates that the product has been shipped with a private key required for using SSL communication.

### 5.2.1. Self-signed Certificates

Creating and signing a server certificate on the web settings screen of the NIC printer unit. You can register the certificate easily because you are not required to install an application.
The input items on the “Self-Signed Certificate” screen of the web settings are shown in the following table.

Input items when creating a certificate

| Variable name | Max length of string | *[Example]* | Default value |
|---|---|---|---|
| Country Name (2 letter code) | 2 | *JP* | (Blank) |
| State or Province Name | 128 | *Shizuoka city* | (Blank) |
| Locally Name (eg, city) | 128 | *Shimizu-ku, Nanatshushinya* | (Blank) |
| Organization Name (eg, company) | 128 | *Star Micronics Co., ltd.* | (Blank) |
| Organization Unit Name (eg, section) | 128 | *Software Section* | (Blank) |
| Domain (IP Address) | 128 | *192.168.1.175* | (Blank) |
| Expiration Date (eg, YYYY/MM/DD) | 2015.01.01 ～ 2049.12.31 | *2020/12/31* | (Blank) |

- To register a certificate in the web browser, click [Create Self-Signed Certificate] and then click [Download].
- You can delete a certificate file by clicking [Delete]after clicking [Create Self-Signed Certificate]. To delete a self-signed certificate, you need to disable SSL/TLS beforehand.
- Enter the expiration date of the certificate in the "Expiration Date" field. You can specify an expiration date up to "2064.12.31". However, the web browser will misinterpret the expiration date as 1950 or later, and cause an error when specifying a date from 2050 or later. Consequently the maximum date is fixed at "2049.12.31".
  The valid period start date is fixed at “2015.01.01” with F/W Ver.4.0.0. With F/W Ver.4.1.0 or later and Ver. 5.0.0 or later, the start date is the date of creation.
  In addition, the minimum date for the expiration date is fixed at "2015.01.01".
- Once the certificate has been registered, it cannot be deleted by initializing NIC. To delete the certificate, click [Create Self-Signed Certificate] and then click [Delete] on the SSL/TLS settings screen.
- The minimum required items for creating a certificate are the "Domain" and "Expiration Date", but we recommend you input information for all items.
- With F/W Ver. 4.1.0 and Ver. 5.0.0 or later, the Subject Alt Name (SAN) item is generated based on the value input for Domain (IP Address).

An example procedure for creating and signing a self-signed certificate is described in "7.1 Example procedures for registration of SSL certificate" in appendix 2.

### 5.2.2. CA-signed Certificates

You can import a server certificate created externally and signed by CA (Certification Authority) and a private key to the printer NIC.

〈Server certificate specification〉
• Encoding type:  Base64 (filename extension = PEM)
• Types of the certification file: PKCS #1
• Key length (F/W Ver.4.X.X or earlier): RSA 1024bit
•  Key length (F/W Ver.5.0.0 and later): RSA 2048bit or 1024bit

- The CA above is required to register as a "Trusted Root Certification Authorities" in the web browser.
- You can delete the certificate registered to the NIC by clicking [Delete] after selecting [Import CA-Signed Certificate]. However, the [Delete] button is disabled unless a CA-signed certificate and a CA-signed private key are registered.
- Once the certificate has been registered, it cannot be deleted by initializing the NIC. To delete the certificate, click [Import CA-Signed Certificate] and then click [Delete] on the SSL/TLS settings screen.

An example procedure for importing a CA-signed certificate to NIC is indicated in "7.1 Example procedures for registration of SSL certificate" in appendix 2.

## 5.2.3. Operation Tested Environment

### 5.2.3.1. About the Operation Tested Environment

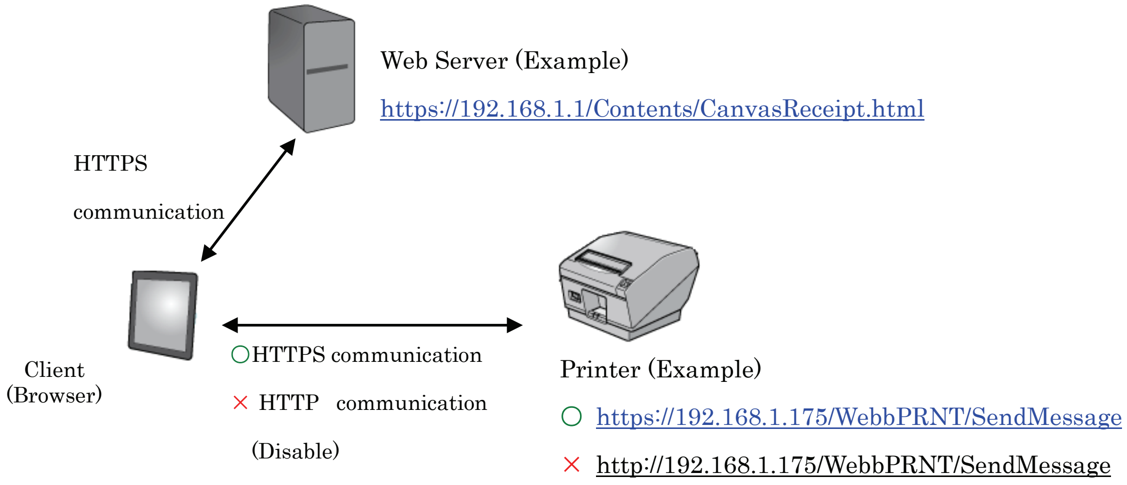
Depending on the device, operating system, type and version of your web browser, the operation of SSL/TLS communication (HTTPS) may differ.
For a list of validated compatibility results tested by Star Micronics Co., Ltd., see "4.2 Specification" in 4. StarWebPRNT FUNCTION (IFBD-HE07X/08X/BE07X).
If you operate the device using an operating environment not recorded in this table, this function may not work normally and a failure may occur such as an error appearing in the web browser.

### 5.2.3.2. HTTP/HTTPS Mixed Environments

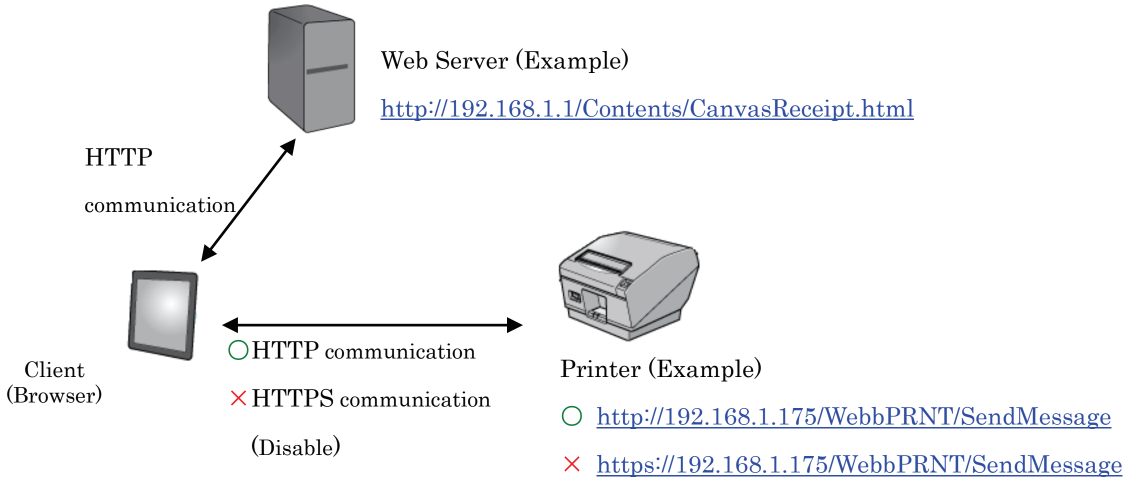
Security communication (HTTPS) and no security communication (HTTP) cannot be mixed in the WebPRNT application due to security specifications of the client's web browser.

For this reason, match the security level between the web server's URL for storing web contents and the printer's URL when you use WebPRNT as shown below. For example, if the printer's IP address begins with "https://", the web server's IP address also must begin with "https://".
Operating environments that mix security levels are referred to as "Cross Scheme" or "Mix Content".

<Web Server: For HTTPS communication>


Web Server (Example)
https://192.168.1.1/Contents/CanvasReceipt.html
HTTPS
communication
Client
(Browser)
○HTTPS communication
× HTTP communication
(Disable)
Printer (Example)
○ https://192.168.1.175/WebbPRNT/SendMessage
× http://192.168.1.175/WebbPRNT/SendMessage

<Web Server: For HTTP communication>


Web Server (Example)
http://192.168.1.1/Contents/CanvasReceipt.html
HTTP
communication
Client
(Browser)
○HTTP communication
×HTTPS communication
(Disable)
Printer (Example)
○ http://192.168.1.175/WebbPRNT/SendMessage
× https://192.168.1.175/WebbPRNT/SendMessage

### 5.2.3.3. Precautions when Using Google Chrome Ver. 58 or Later

Beginning with Ver. 58, Google Chrome requires Subject Alt Name (SAN) as a certificate item. Therefore when using Chrome Ver. 58 or later to perform SSL/TLS communication with this product, the following precautions must be observed.

(1) When using self-signed certificates
When Chrome Ver. 58 or later is used, it is necessary to create and sign a self-signed certificates with a product that has F/W Ver. 4.1.0 or later or F/W 5.0.0 or later.

(2) When using CA-signed certificates
When Chrome Ver. 58 or later is used, the externally created CA-certificates must contain the Subject Alt Name (SAN) item. When this product has F/W Ver. 4.1.0 or later or F/W Ver. 5.0.0 or later, it is necessary to import a CA certificate that includes the SAN item into this product.

# 6. APPENDIX 1

## 6.1 New (IFBD-HE07/08/BE07) and Old Product (IFBD-HE05/06/BE05) Comparison List

| Feature | Specifications, Protocols | This product IFBD-HE07/08/BE07 | Old product IFBD-HE05/06/BE05 |
|---|---|---|---|
| Temporary IP Address Setting | ARP/Ping | ○ | ○ |
| Dynamic IP Address Acquisition | DHCP/BOOTP, RARP | ○ | ○ |
| DHCP/BOOTP Timeout Setting | DIPSW1 Setting | ○ (DIPSW1 = OFF: Valid (Factory Default Setting/ ON = Invalid) | x (Fixed at Valid) |
| NIC Search on LAN | SDP (UDP#22222) | ○ Name of I/F Unit: IFBD-HE07/08) | ○ Name of I/F Unit: “IFBD-HE05/06”) |
| NIC Self-print | | ○ | ○ |
| Print | TCP#9100/LPR/FTP | ○ | ○ |
| Status Acquisition (#9100) | TCP#9100 | ○ | ○ |
| Status Acquisition (#9101) | TCP#9101 | ○ | × |
| ASB/NSB Settings | TCP#9100 | ○ | × (V1.0.1)/○ (V1.1.0 + Printer Support) |
| ESCPOS Status Support | TCP#9100, HTTP(WEB)/Telnet/FTP | ○ | × (V1.0.1)/○ (V1.1.0 + Printer Support) |
| IP Address Setting | HTTP(WEB)/Telnet/FTP | ○ | ○ |
| Web Refresh Time Setting | HTTP(WEB)/Telnet/FTP | ○ | ○ |
| #9100 Multi-session Setting (Dynamic) | HTTP(WEB)/Telnet/FTP, (TCP#9100) | ○ (Factory Default Setting: Multi Session = Invalid) | ○ (Factory Default Setting: Multi Session = Valid) |
| #9100 Data Timeout Setting, (Operation) | HTTP(WEB)/Telnet/FTP, (TCP#9100) | ○ | × |
| TCP Keep-Alive Setting, (Operation) | HTTP(WEB)/Telnet/FTP, (TCP Port) | ○ | × |
| FTP Server Valid/Invalid Settings | HTTP(WEB)/Telnet/FTP | ○ | × |
| Broken Link Detection Support (LED Blinking Operation) | | ○ (See section 5.2 Printer Firmware Support Table) | × |
| Broken Link Detection Support (Warning Print Operation) | | ○ (See section 5.2 Printer Firmware Support Table) | × |
| Broken Link Warning Print Settings | HTTP(WEB)/Telnet/FTP | ○ | × |
| Broken Link Warning Data Registration | HTTP(WEB) | ○ | × |
| TCP Port80 Valid/Invalid Settings | Telnet | ○ (V2.3.0) | × |
| Authentication Reset | TCP#22222 (<FS>’0’) | ○ | ×(V1.0.1) / ○(V1.1.0) |
| Setting Information Acquisition (NIC Discvoer Information) | TCP#22222 (<GS>’0’) | ○ | × |
| Setting Information Acquisition (Printer Status Setting) | TCP#22222 (<GS>’1’) | ○ | × |
| StarWebPRNT Function | HTTP | ○ (IFBD-HE07X/08X/BE07X only) | × |
| SSL/TLS communication | HTTPS | ○(V4.0.0) | × |
| SNMP agent functions | SNMP | ○ (V5.0.0 or later) | × |

○: Supported; ×: Not supported

## 6.2 Printer Firmware Support Table

Can be used with the F/W versions shown in the table below. (As of August 16, 2017)

| Model | Supports IFBD-HE07/08/BE07 | | Supports IFBD-HE07X/08X/BE07X | | Supports Broken Link Detection (LED Blinking Operation, Warnign Print Operation) |
|---|---|---|---|---|---|
| | Boot | Main | Boot | Main | |
| TSP800II | Ver1.0 | Ver1.2 | × | × | ○ |
| FVP10 | Ver1.0 | Ver1.3 | Ver1.0(Note1) | Ver1.3(Note1)<br>Ver1.5(Note2) | ○ |
| SP500(Note3) | Ver4.0 | Ver4.0 | × | × | × |
| SP700 | Ver2.0 | Ver3.0 | × | Ver3.3(Note2) | ○ |
| TSP700II | Ver2.0 | Ver3.0 | Ver2.0(Note1) | Ver3.0(Note1)<br>Ver4.1(Note2) | ○ |
| TSP650(Note3) | Ver2.0 | Ver3.0 | × | × | ○ |
| TSP650II | Ver1.0 | Ver1.0 | Ver1.0(Note1) | Ver1.0(Note1)<br>Ver1.2(Note2) | ○ |
| TUP500(Note3) | Ver2.0 | Ver3.0 | × | × | ○ |
| TSP1000(Note3) | Ver4.0 | Ver3.0 | × | × | × |
| TSP828L(Note3) | Ver2.0 | Ver2.0 | × | × | × |
| HSP7000(Note3) | Ver2.1 | Ver5.0 | × | × | ○ |
| TCP300II(Note3) | - | Ver3.0 | × | × | × |
| TCP400(Note3) | - | Ver3.0 | × | × | × |

○: Supported; ×: Not supported

**Note 1:** **Only European and U.S. models**

**Note 2:** **European and U.S. models(As UTF-8 is not supported), kanji models (As UTF-8 is supported)**

**Note 3:** **Models indicated by (*3) are not supported by this product with F/W Ver. 5.0.0 and later. Use the product with F/W Ver. 4.X.X or earlier.**

## 6.3 Driver Support Table

Drivers support table for IFBD-HE07/08/BE07. (As of August 16, 2017)

### 6.3.1. Small Model Printers

#### 6.3.1.1. Star PRNT Inteligence CD (Multi-model support CD)

| Model | StarPRNT Inteligence Ver1.1 (Note 2) | | |
|---|---|---|---|
| | Printer Driver | OPOS Ver1.13.2 or later | StarIO Ver1.2.2 or later |
| TSP800II | ○ | ○ (Note 1) | ○ |
| FVP10 | ○ | ○ (Note 1) | ○ |
| TSP700II | ○ | ○ | ○ |
| TSP650 (Note 5)(Note6) | ○ | ○ | ○ |
| SP500(Note6) | ○ | ○ | ○ |
| SP700 | ○ | ○ | ○ |
| TUP500 (Note 3)(Note6) | ○ | ○ | ○ |
| TSP650II (Note 4) | ○ | ○ | ○ |

Note1：With Star PRNT Inteligence CD, supports IFBD-HE07/08/BE07 from Ver. 1.1.

Note2: You can search for printers that do not have an IP address in environments that do not pass through a DHCP server, using a combination of IFBD-HE07/HE08/BE07 Ver. 2.2.0 or later and StarPRNT Intelligence Ver2.0 or later. For earlier versions, you cannot search for printers that do not have an IP address in environments that do not pass through a DHCP server. Select “Help - Cannot find printer”, and then follow the steps to setup a temporary IP address.

Note3: StarPRNT Intelligence Ver. 1.4 or later supports TUP500.

Note4: StarPRNT Intelligence Ver. 2.0 or later supports TUP650II.

Note5: StarPRNT Intelligence Ver. 2.0 or later does not support TSP650. Use StarPRNT Intelligence Ver. 1.5 with TSP650.

Note6: The models indicated with *6 are not supported by this product with F/W Ver.5.0.0 or later. Use the product with F/W Ver. 4.X.X or earlier.

### 6.3.1.2. Star Printer Driver CD or Driver Pacakge (Stand-alone model support CD)

| Model | Version | Printer Driver Stand-alone | Settings Utility Note 4 | Remarks |
|---|---|---|---|---|
| TSP650 *5 | CD Ver 1.0 | ○ *3 | × *1 | |
| TSP700II | CD Ver 1.1 | ○ *3 | × *1 | |
| SP700 | CD Ver 1.1 | ○ *3 | × *1 | |
| HSP7000 *5 | CD Ver 2.0 | ○ *3 | Δ *2 | Revision patch: HSP7000_Config_ValueAdd_Update_for_HE08_20100521.zip |
| TUP500 *5 | Ver 1.0 | ○ *3 | Δ *2 | Revision patch: TUP500_Config_ValueAdd_Update_for_HE07_20100521.zip |

Note *1 The Search for Printer on LAN feature of the settings utility does not recognize IFBD-HE07/08/BE07. You cannot use the setting utility.
→ Supported using Star PRNT Inteligence CD Ver. 1.1. (However, VPE is not supported by Star PRNT Inteligence CD. )

Note *2 We provide a revision patch to support IFBD-HE07/08/BE07. Even after applying the patch, in ESC/POS mode, the virtual serial nport will not operate.
To use OPOS, you must change the #9100 Multi-session setting for IFBD-HE07/08/BE07 to Valid.
To change settings, see sections 3.1.6 HTTP Server, 3.1.7 TELNET Server, and 3.1.8 FTP Server.
If you use Windows Vista or 7 in an environment that does not go through a DHCP server, you cannot search for printers that have not been set with an IP address.In such cases, set the IP address on the printer after reading Guidelines for Using an Ethernet Environment in the printer’s software manual.

Note *3 To use the printer driver as a stand-alone, you must manually set the IP address. Set the IP address on the printer after reading Guidelines for Using an Ethernet Environment in the printer’s software manual.

Note *4 The setting utility is for Windows XP, Vista (32 bit) and 7 (32 bit). Windows 64 bit OS is not supported.

Note *5 The printer indicated by *5 is not supported by this product with Ver.5.0.0 or later. Use the product with Ver. 4.X.X or earlier.

### 6.3.1.3. OPOS Driver (Web Release)

- Supported with OPOS ver 1.13.2 or later.
- To use OPOS version 1.13.1 or earlier, you must change the #9100 Multi-session setting for IFBD-HE07/08/BE07 to Valid.

To change settings, see sections 3.1.6 HTTP Server, 3.1.7 TELNET Server, and 3.1.8 FTP Server.

### 6.3.1.4. CUPS Driver (Web Release)

| | |
|---|---|
| • Linux Version: | Supported after Ver. 3.1.1. |
| • Mac Version: | Supported after Ver. 3.1.1. |

- To use the CUPS driver, specify LPD (LPR) for the print port.

### 6.3.1.5. JavaPOS Driver (Web Release)

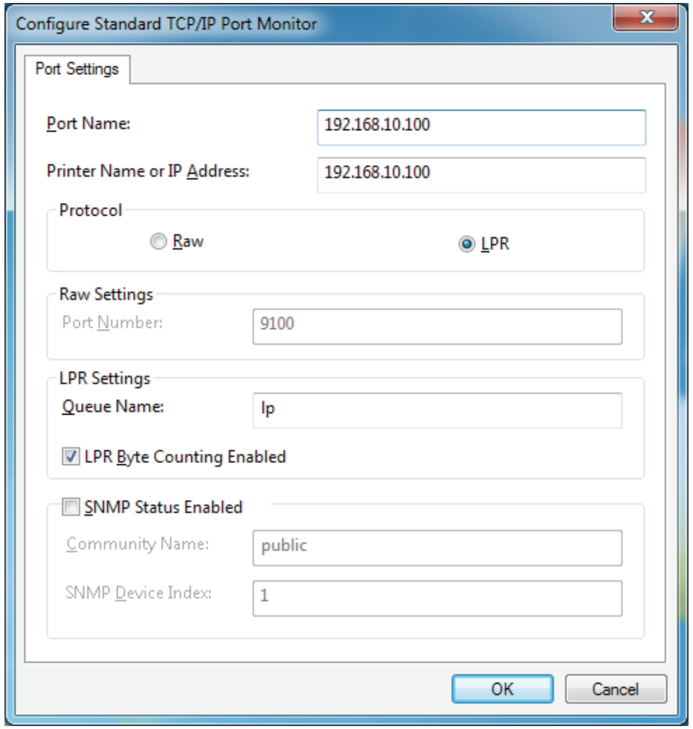
- Supported with JavaPOS Driver Ver. 1.9.13 or later, or Star PRNT Inteligence CD Ver. 1.2. or later.

### 6.3.1.6. When Using a Standard Windows TCP/IP Printer Port

If, for printing, you are using a standard TCP/IP printer port with a printer driver that is not listed in 6.3.1.1. or 6.3.1.2. above, select LPR.
The following example shows how to configure the settings in Windows 7.

The port monitor LPR settings are below. Always specify the queue name.
- Queue name: lp
- Apply a check mark to “Enable LPR Byte Counter”

(Reference Example 1) Example of Port Monitor Setting Screen (For Windows 7)



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: 192.168.10.100

Printer Name or IP Address: 192.168.10.100

Protocol
○ Raw ● LPR

Raw Settings
Port Number: 9100

LPR Settings
Queue Name: lp

☑ LPR Byte Counting Enabled

☐ SNMP Status Enabled
Community Name: public
SNMP Device Index: 1

## 6.3.2. Card Reader/Writer

This product with F/W Ver.5.0.0 and later does not support card reader/writer products. Use the product with Ver. 4.X.X or earlier.

| Model | VisualCardOCX1.9.0 | Setup StarNIC V3.0 |
|---|---|---|
| TCP300II | Δ Note*1 | ○ Note*2 |
| TCP400 | Δ Note*1 | ○ Note*2 |

**Note*1 You must change the #9100 Multi-session setting for IFBD-HE07/08/BE07 to Valid.**
**To change settings, see sections 3.1.6 HTTP Server, 3.1.7 TELNET Server, and 3.1.8 FTP Server.**

**Note*2 Uses Windows XP, Vista, 7, 8 and 8.1.**

## 6.3.3. How to Set the IP Address

| OS | Setting Tool | Remarks |
|---|---|---|
| Windows | Printer Connection Wizard<br>(6.3.1.1 StarPRNT Inteligence CD) | • You can search for printers that do not have an IP address in environments that do not pass through a DHCP server, using a combination of IFBD-HE07/HE08/BE07 Ver. 2.2.0 or later and StarPRNT Intelligence Ver2.0 or later. For earlier versions, you cannot search for printers that do not have an IP address in environments that do not pass through a DHCP server. Select "Help - Cannot find printer", and then follow the steps to setup a temporary IP address. |
| | Star Setting Utility<br>(6.3.1.2 Star Printer Driver CD) | • If you use Windows Vista or 7 in an environment that does not go through a DHCP server, you cannot search for printers that have not been set with an IP address.In such cases, set the TCP/IP address on the printer after reading Guidelines for Using an Ethernet Environment in the printer's software manual.<br>• Uses Windows XP, Vista (32 bit) and 7 (32 bit). Windows 64 bit OS is not supported. |
| | Setup StarNIC V3.0 | • If you use Windows Vista, 7, 8 or 8.1 in an environment that does not go through a DHCP server, IFBD-HE07, HE08 or BE07 with Ver2.1.0 or earlier cannot search for printers that have not been set with an IP address. In such cases, set the TCP/IP address on the printer after reading Guidelines for Using an Ethernet Environment in the printer's software manual.<br>• Uses Windows XP, Vista, 7, 8 and 8.1. |
| LInux | - | See the driver manual. |
| Mac | - | See the driver manual. |

## 6.4 Comparison List of F/W Ver.5.0.0 or Later and Ver. 4.X.X or Earlier

| Function | Specification, protocol, etc. | F/W Ver.5.0.0 or later | F/W Ver. 4.X.X or earlier |
|---|---|---|---|
| SSL/TLS communication | Key length for CA-signed certificates | RSA 2048bit or 1024bit | RSA 1024bit |
| SNMP agent functions | SNMP | Supported | Not supported |
| F/W update | FTP, TFTP | Cannot downgrade to F/W Ver. 4.X.X or earlier. | Cannot upgrade to F/W Ver.5.0.0 or later. |
| Web settings | HTTP | Refer to P3-14 “Table of supported web browser versions”. | |
| Browser settings for web display | Inline frame setting | Setting not necessary | Must be enabled. |
| Identification of new/old products | Mark on PCB chassis | Has “M” mark. | No “M” mark. |
| | Indication of the F/W version on the individual packing boxes (optional parts) | “V5.0.0” or later | “V4.X.X” or earlier |
| Printer models that can be used | | Refer to section 6.2 “Printer Firmware Support Table”.<br>Refer to section 6.3 “Driver Support Table”. | |

# 7. APPENDIX 2

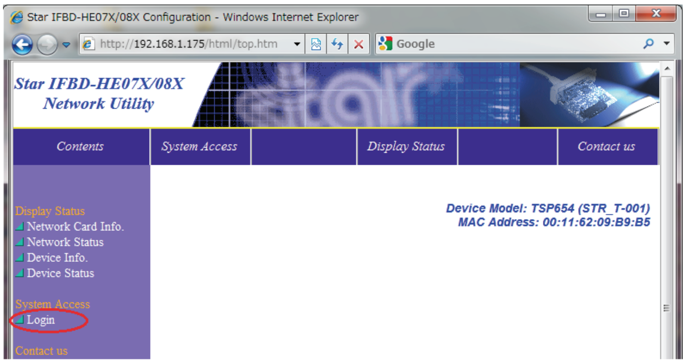
## 7.1. Example procedures for registration of SSL/TLS certificates

To use SSL/TLS communications (HTTPS), you must configure settings for the use of either a self-signed certificate or CA-signed certificate beforehand.
The following shows each procedure.

### 7.1.1. Using a self-signed certificate

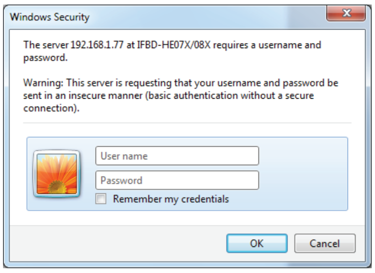
1. Create a certificate in NIC

Access the printer's IP address (in this procedures: http://192.168.1.175), and then log in as root privileges.



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

Enter the following user ID and password, and then click [OK]. User name: "root", password: "public" (factory default setting)



The server 192.168.1.77 at IFBD-HE07X/08X requires a username and password.

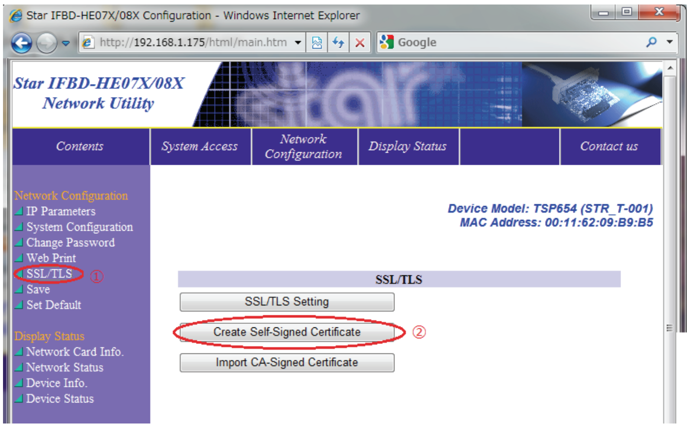
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name

Password

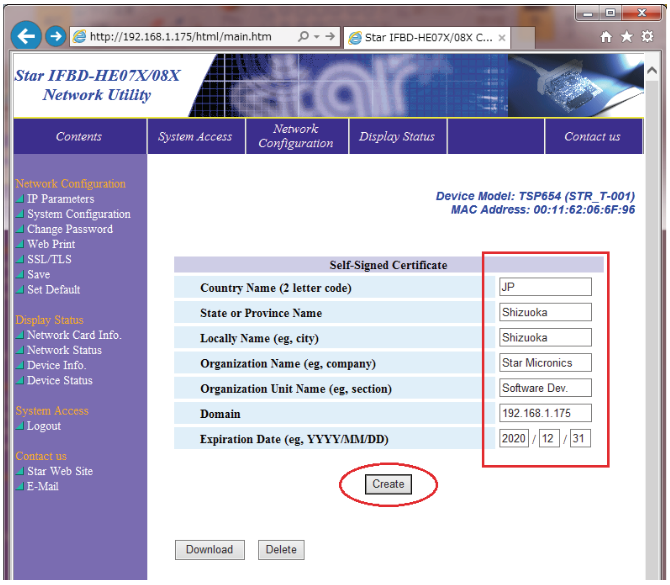
□ Remember my credentials

Click [SSL/TLS].
Click [Create Self-Signed Certificate].



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

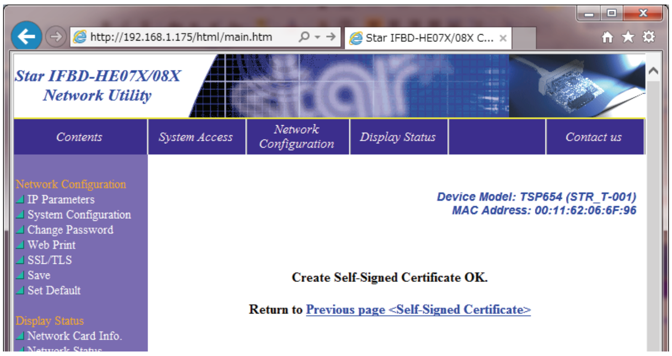
After entering each item in the "Self-Signed Certificate" fields and clicking [Create], a certificate is created in NIC.
For the "Domain", enter the printer's IP address (the static value). * The following value is an example.



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

| Self-Signed Certificate | |
|---|---|
| Country Name (2 letter code) | JP |
| State or Province Name | Shizuoka |
| Locally Name (eg, city) | Shizuoka |
| Organization Name (eg, company) | Star Micronics |
| Organization Unit Name (eg, section) | Software Dev. |
| Domain | 192.168.1.175 |
| Expiration Date (eg, YYYY/MM/DD) | 2020 / 12 / 31 |

The following screen appears when you successfully create a certificate.



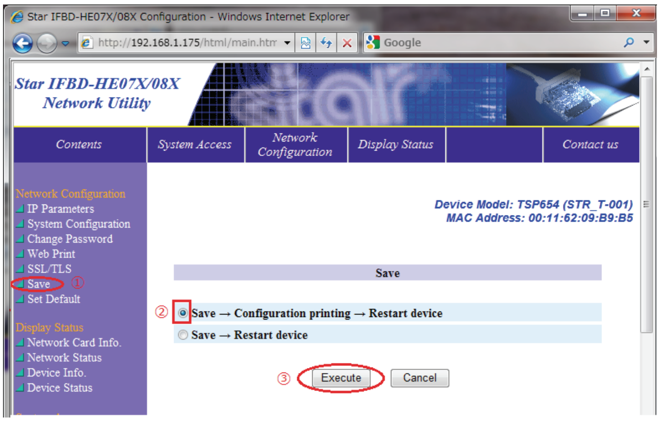
Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

Create Self-Signed Certificate OK.

Return to Previous page <Self-Signed Certificate>

2. Enable the self-signed certificate in NIC

Click [SSL/TLS].
Click [SSL/TLS Setting].



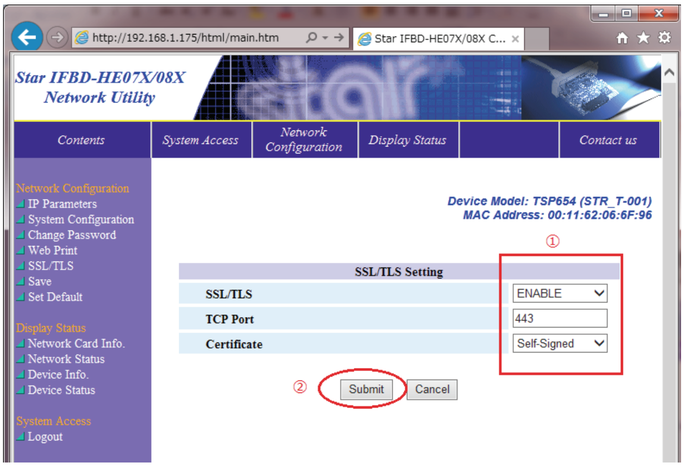
Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

Save

● Save → Configuration printing → Restart device

○ Save → Restart device

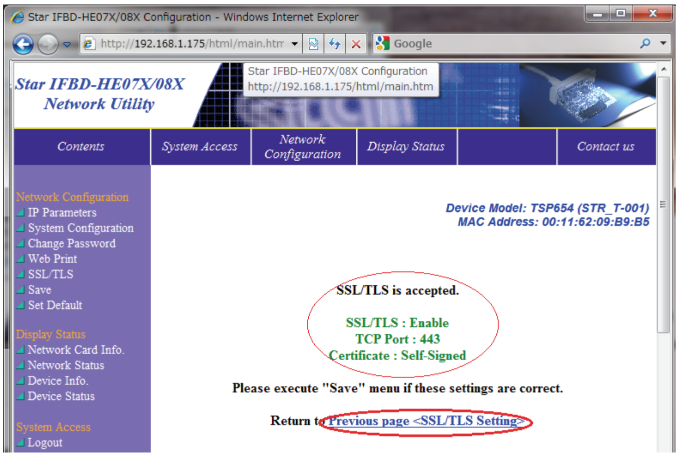
Select [ENABLE] in the "SSL/TLS" drop-down list and [Self-Signed] in the "Certificate" drop-down list, and then click [Submit].



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

| SSL/TLS Setting | |
|---|---|
| SSL/TLS | ENABLE |
| TCP Port | 443 |
| Certificate | Self-Signed |

The following information is displayed. Check that the following information matches the information on the screen. SSL/TLS: ENABLE, Certificate:  Self-Signed.



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

SSL/TLS is accepted.

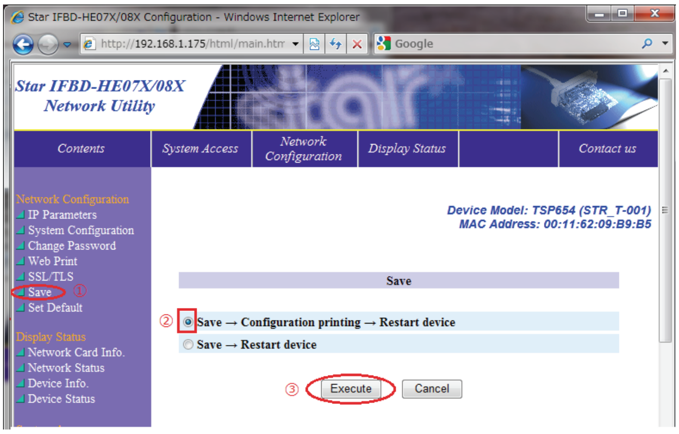
SSL/TLS : Enable
TCP Port : 443
Certificate : Self-Signed

Please execute "Save" menu if these settings are correct.

Return to Previous page <SSL/TLS Setting>

Click [Save]. On the save screen select "Save → Configuration printing → Restart device", and then click [Execute].
The printer prints the settings information. Check that the settings are the same as shown below.

- SSL/TLS: ENABLE
- Self-Signed Certifcate: Exist
- Certifiate: Self-Signed



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

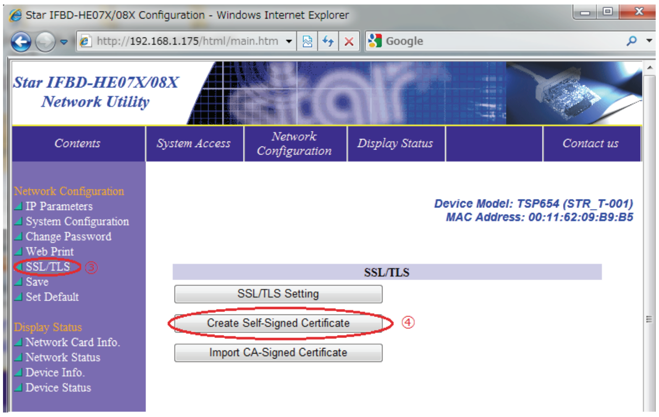
Save

● Save → Configuration printing → Restart device
○ Save → Restart device

The procedures for creating the NIC self-signed certificate are completed.

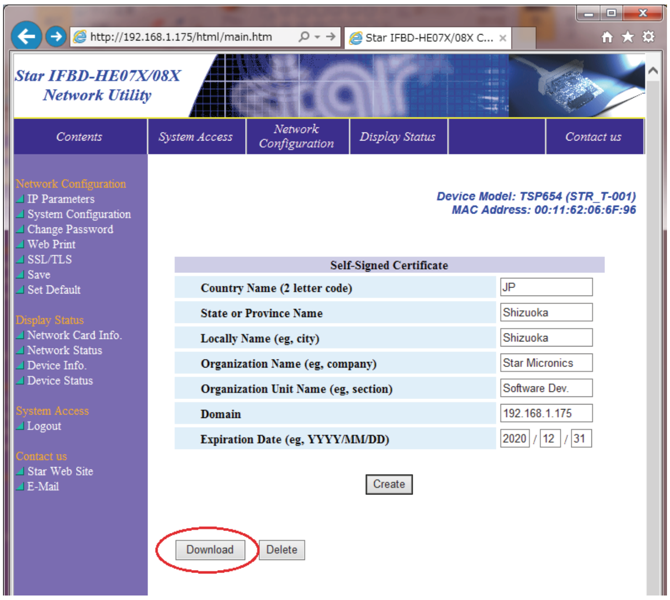
3. Import a certificate to the web browser
Import the created certificate in NIC to the web browser of the client's device.

■ For a Windows device (Windows 7)
Click [SSL/TLS].
Click [Create Self-Signed Certificate].



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

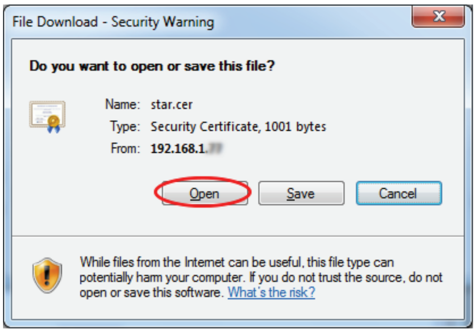
Click [Download] and save a certificate file (name is optional) to any place in Windows.
(In this procedures, save this file as "star.cer".)



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

| Self-Signed Certificate | |
|---|---|
| Country Name (2 letter code) | JP |
| State or Province Name | Shizuoka |
| Locally Name (eg, city) | Shizuoka |
| Organization Name (eg, company) | Star Micronics |
| Organization Unit Name (eg, section) | Software Dev. |
| Domain | 192.168.1.175 |
| Expiration Date (eg, YYYY/MM/DD) | 2020 / 12 / 31 |

On the client device, double click the saved certificate file and click [Open].

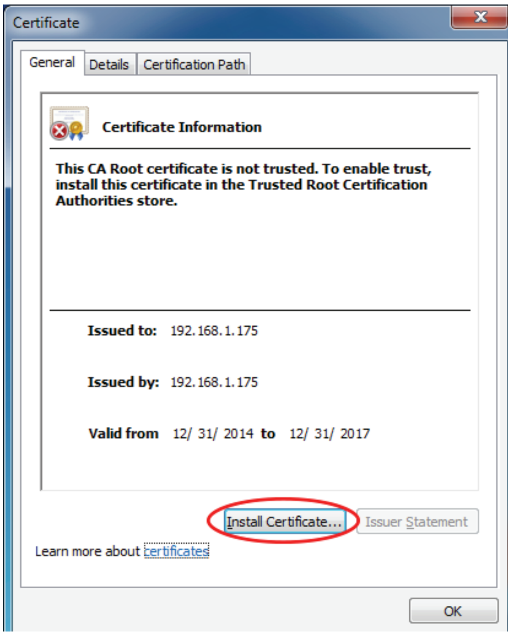


Do you want to open or save this file?

Name: star.cer
Type: Security Certificate, 1001 bytes
From: 192.168.1.

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Click [Install Certificate].



Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

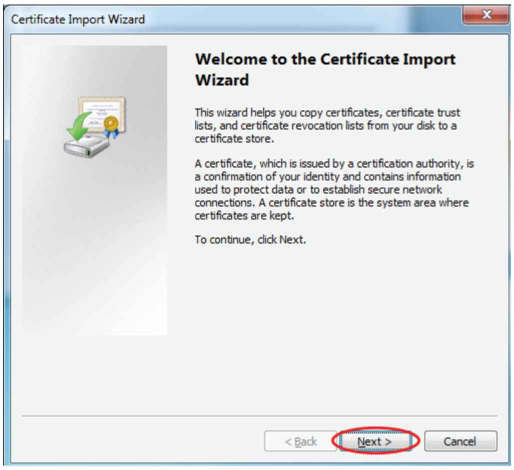
Issued to: 192.168.1.175

Issued by: 192.168.1.175

Valid from 12/ 31/ 2014 to 12/ 31/ 2017

Learn more about certificates

Click [Next].



Certificate Import Wizard

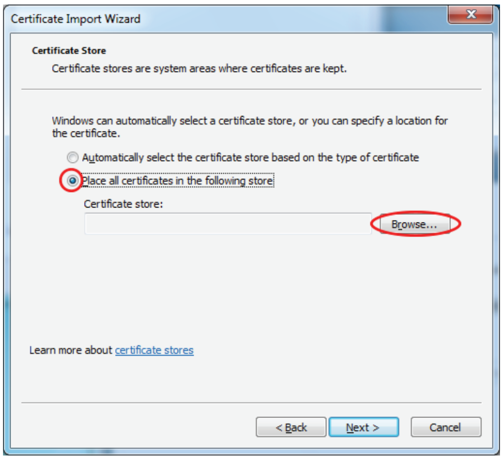
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Select "Place all certificates in the following store" and click [Browse].



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

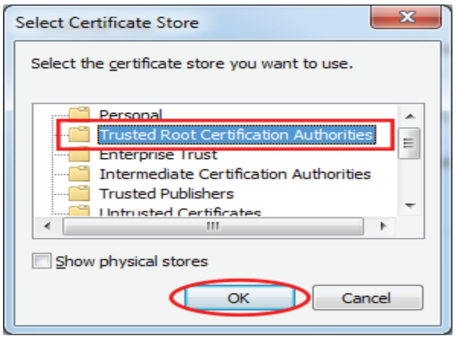
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Learn more about certificate stores

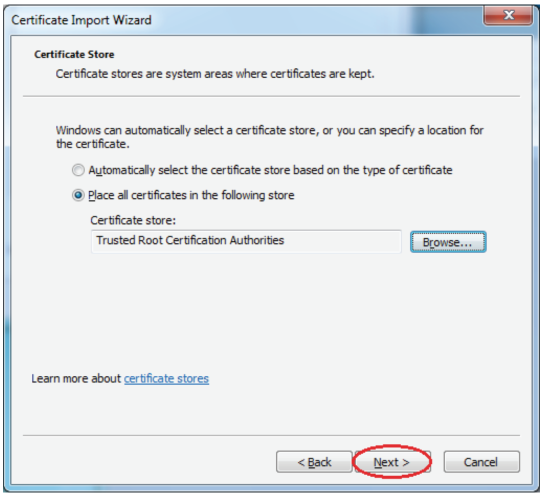
Select a "Trusted Root Certification Authorities" and click [OK].



Select Certificate Store

Select the certificate store you want to use.

Click [Next].



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

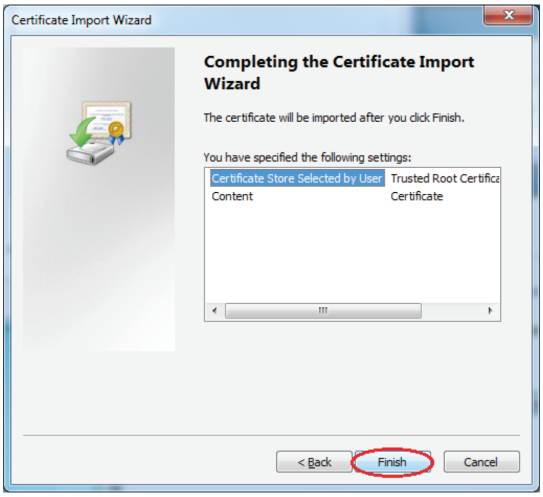
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

Click [Finish].



Certificate Import Wizard

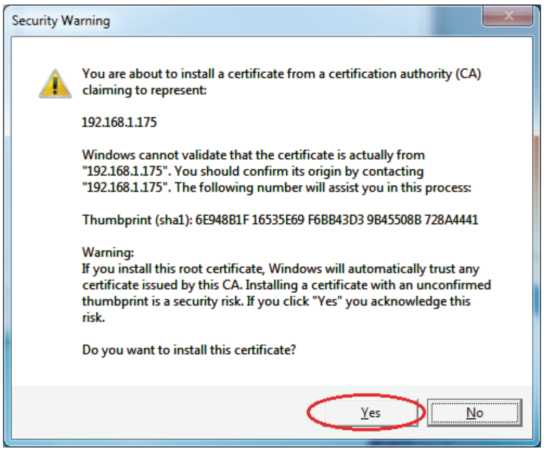
**Completing the Certificate Import Wizard**

The certificate will be imported after you click Finish.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected by User | Trusted Root Certifica |
| Content | Certificate |

Click [Yes] when the following message appears.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

192.168.1.175

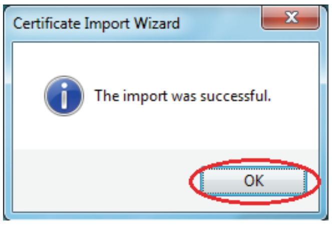
Windows cannot validate that the certificate is actually from "192.168.1.175". You should confirm its origin by contacting "192.168.1.175". The following number will assist you in this process:

Thumbprint (sha1): 6E948B1F 16535E69 F6BB43D3 9B45508B 728A4441

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

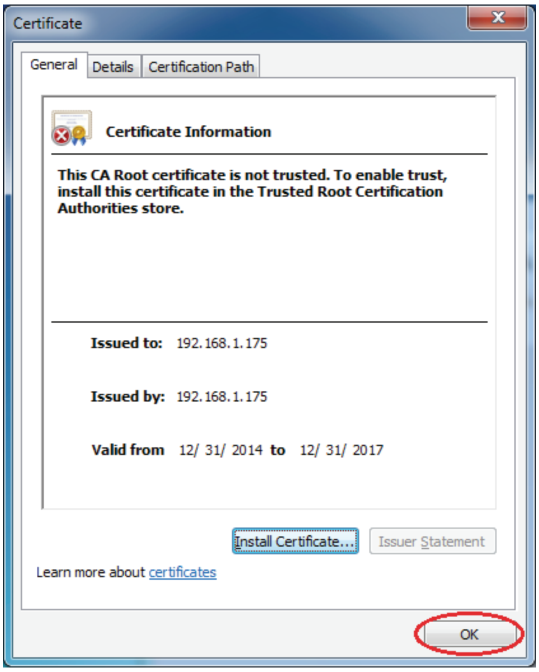
Click [OK].



Certificate Import Wizard

The import was successful.

Click [OK] and close. The procedure is complete.



Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

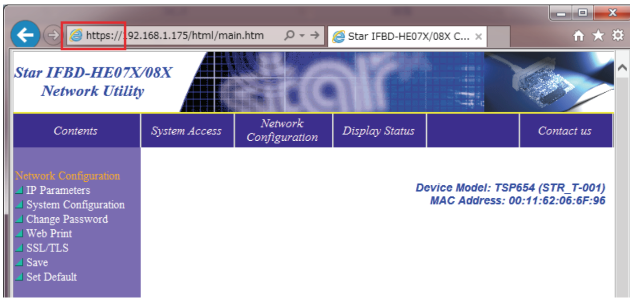
Issued to: 192.168.1.175

Issued by: 192.168.1.175

Valid from 12/ 31/ 2014 to 12/ 31/ 2017

Learn more about certificates

Turn on the printer's power again, and check that the printer's web screen displays normally by entering an address beginning with "https://".



https://192.168.1.175/html/main.htm

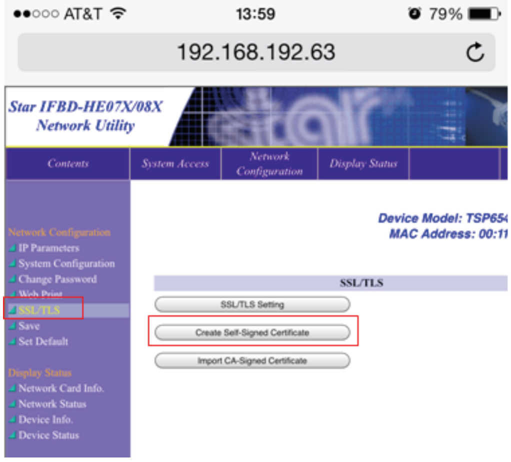
Star IFBD-HE07X/08X Network Utility

Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

However, depending on the client device environment, you may need to add the address as a "Trusted Sites".
(In fact, such a case has been reported when using a combination of Windows 10 and Microsoft Edge.)
→ See "7.1.3 Additional information".

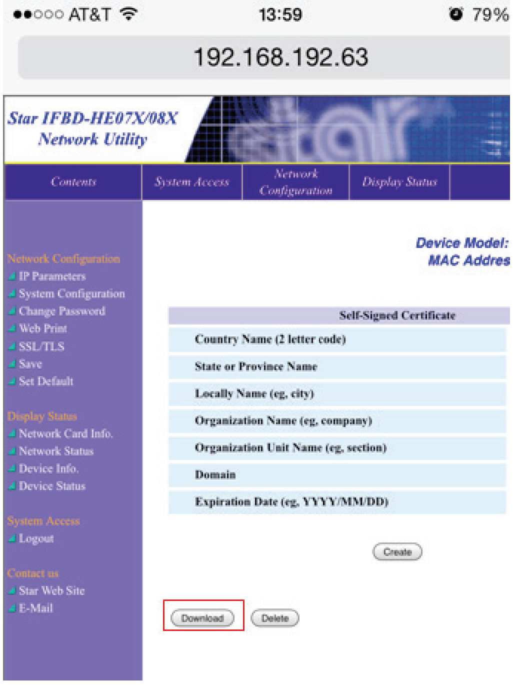
［References］
When importing a certificate file to the web browser on Windows 8 or Windows 10, you must activate certificate manager, "certmgr.msc" in Windows administrative tools, and then perform the following procedure.
• Select "Trusted Root Certification Authorities" and then [Certificate].
• Select [All tasks] and then [Import] from the "Operation Menu".
• Import a self-singed certificate in accordance with the import certificate wizard.
• Make sure you import the certificate by referring to "Trusted Root Certification Authorities" and then [Certificate].

■ For iOS devices
Access the printer's IP address (in this procedure: http://192.168.192.63) on Safari, and log in as root privileges.
Select "SSL/TLS", and then select [Create Self-Signed Certificate].
* With an iOS device, use Safari because certificate download is not permitted when a browser other than Safari is used.



Device Model: TSP654
MAC Address: 00:11

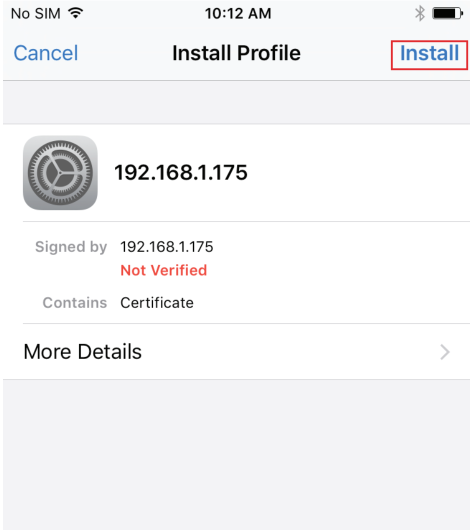
(1) Select [Download].



Device Model:
MAC Addres

Self-Signed Certificate
Country Name (2 letter code)
State or Province Name
Locally Name (eg, city)
Organization Name (eg, company)
Organization Unit Name (eg, section)
Domain
Expiration Date (eg, YYYY/MM/DD)

Select [Install] when the following screen appears.

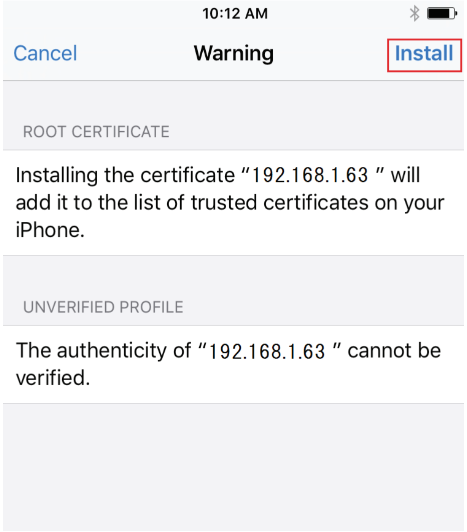


192.168.1.175

Signed by 192.168.1.175
Not Verified

Contains Certificate

Select [Install] when the following screen appears.



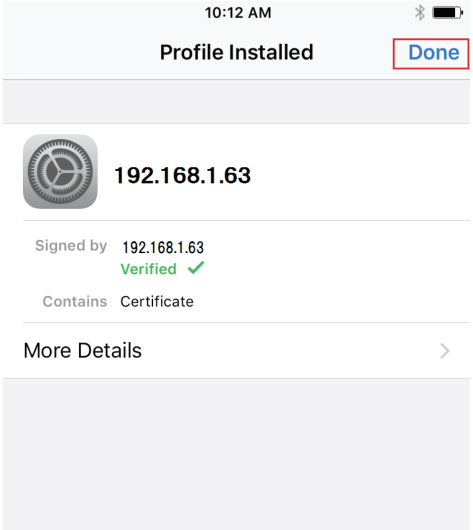
ROOT CERTIFICATE

Installing the certificate "192.168.1.63 " will add it to the list of trusted certificates on your iPhone.

UNVERIFIED PROFILE

The authenticity of "192.168.1.63 " cannot be verified.

Installation is complete when the following screen appears. Tap [Done].



192.168.1.63

Signed by 192.168.1.63
Verified ✓

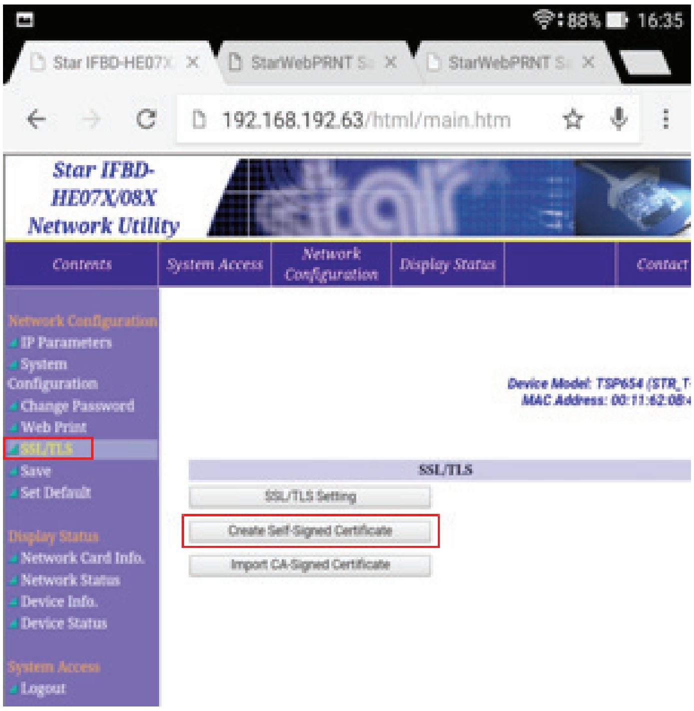
Contains Certificate

Turn on the printer's power again, and check that the printer's web screen displays normally by entering an address beginning with "https://".
When using iOS 10.3 or later, additional settings on the iOS side are required. Therefore, also refer to section 7.1.4 "Required settings when registering certificates with iOS 10.3 or later".

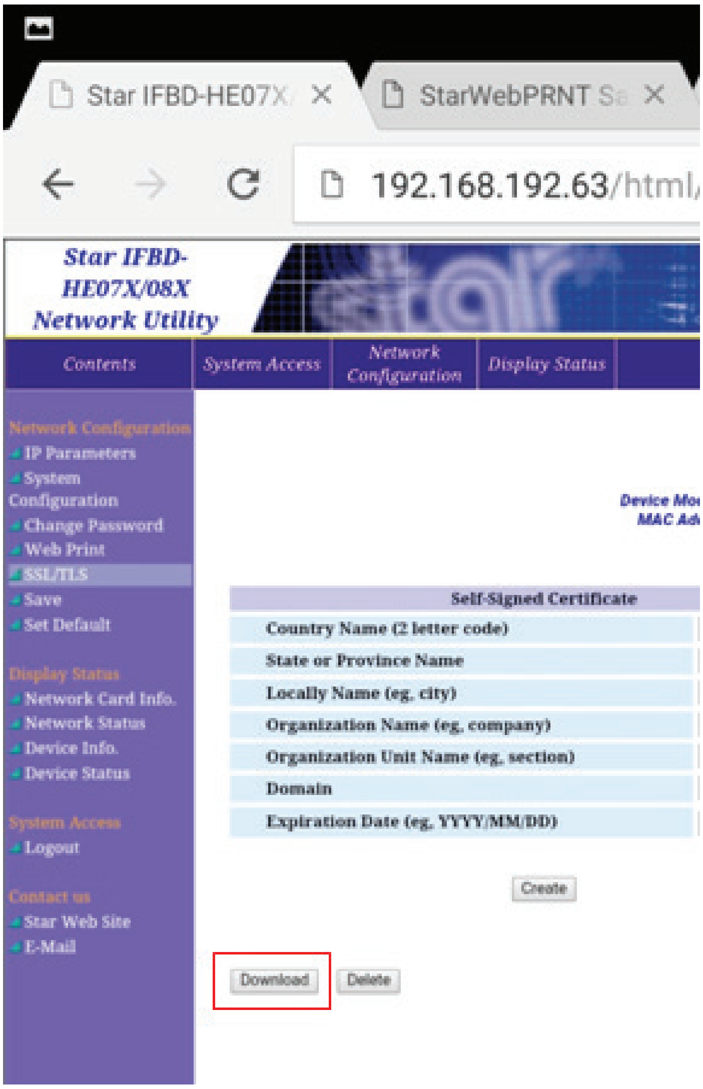
■ For Android

Go to the printer's IP address (in this procedures: http://192.168.192.63) on Chrome, and log in as Root Privileges.

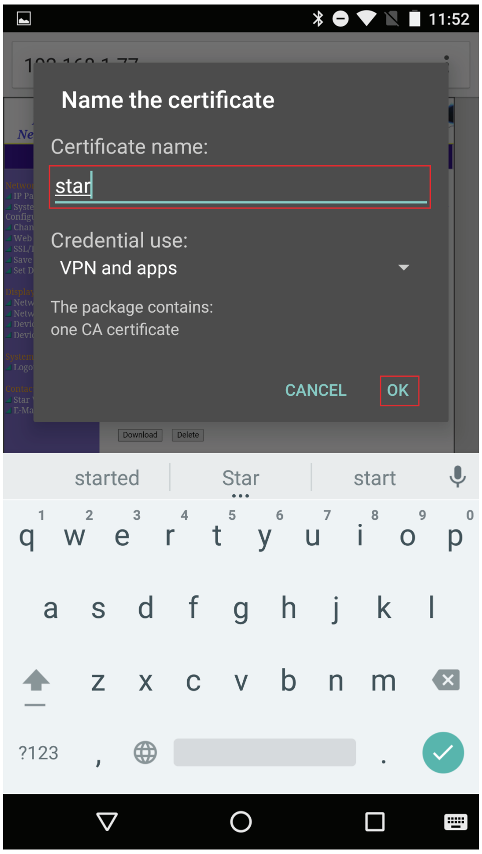
Select "SSL/TLS", and then select [Create Self-Signed Certificate].



Select [Download].



When the name of the certificate is required, enter any name (in this procedure: "star") and tap [OK].



Name the certificate

Certificate name:

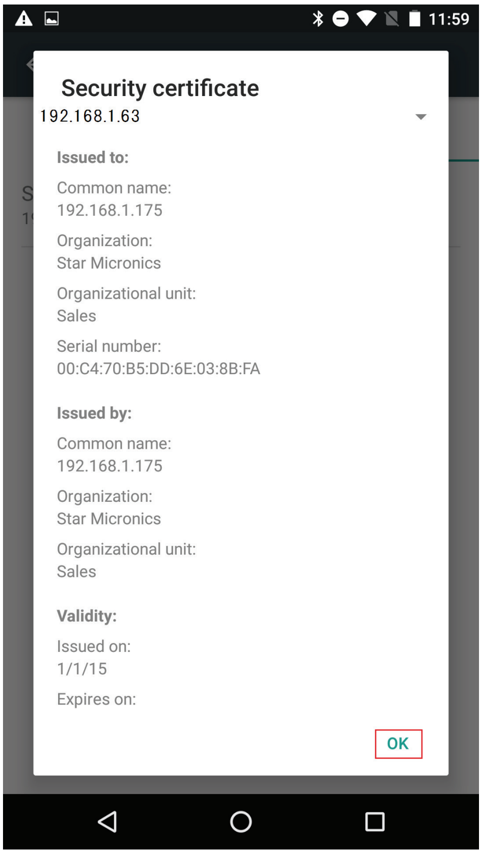
star

Credential use:

VPN and apps

The package contains:
one CA certificate

Installation is complete when the contents of the certificate appear. Tap [OK].



Security certificate

192.168.1.63

Issued to:

Common name:
192.168.1.175

Organization:
Star Micronics

Organizational unit:
Sales

Serial number:
00:C4:70:B5:DD:6E:03:8B:FA

Issued by:

Common name:
192.168.1.175

Organization:
Star Micronics

Organizational unit:
Sales

Validity:

Issued on:
1/1/15

Expires on:

Turn on the printer's power again, and check that the printer's web screen displays normally by entering an address beginning with "https://".

## 7.1.2. Using CA-signed Certificates

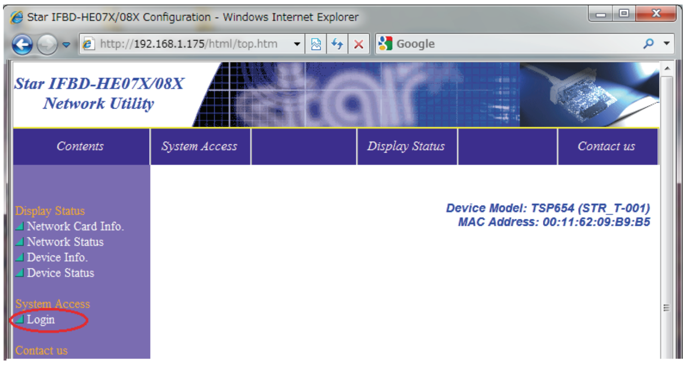
Import a server certificate created externally and signed by CA and a private key to the printer's NIC.
For the browser, you must register the CA (Certificate Authority) as a "Trusted Root Certification Authorities".

1. Prepare the server certificate and private key
Prepare a server certificate file signed by an external Certificate Authority and a private key file beforehand.

- Encoding type:  Base64 (the file extension is PEM)
- Types of certificate file: PKCS #1
- Key length: RSA 1024bit (F/W Ver. 4.X.X)
- Key length: RSA 2048bit (F/W Ver. 5.0.0 or later)

2. Import a server certificate and a private key to NIC
Access the LAN interface from the web browser. The following is an example from Internet Explorer on Windows 7.

Access the printer's IP address (in this procedure: http://192.168.1.175), and then log in as root privileges.

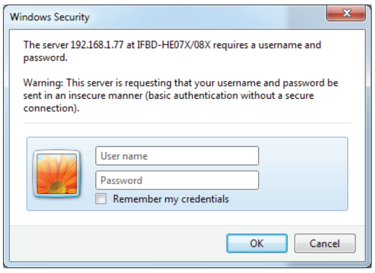


Star IFBD-HE07X/08X Configuration - Windows Internet Explorer

http://192.168.1.175/html/top.htm

Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

Enter the following user ID and password, and then click [OK]. User name: "root", password: "public" (factory default setting)

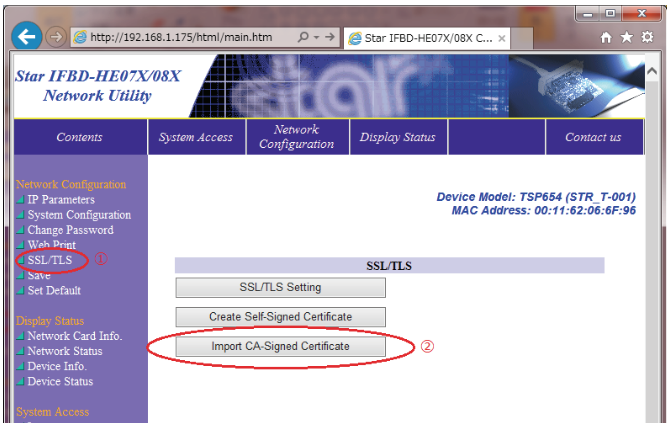


Windows Security

The server 192.168.1.77 at IFBD-HE07X/08X requires a username and password.

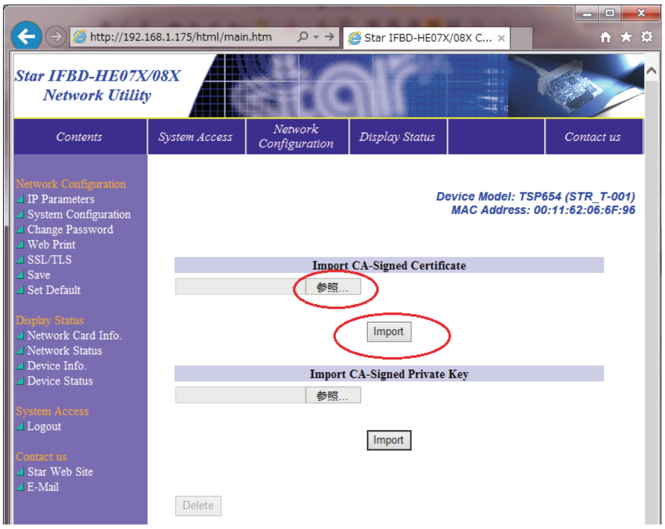
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

Click [SSL/TLS].
Click [Import CA-Signed Certificate].



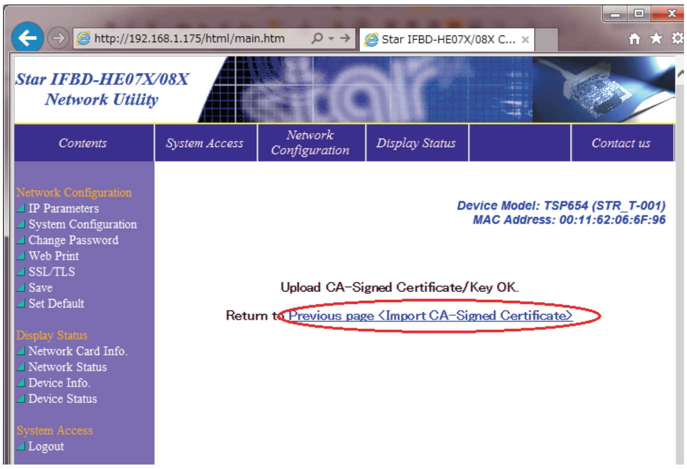
Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

Click [Browse] in the "Import CA-Signed Certificate" column. Select the certificate file to import from the client device's file dialog, and then click [Import].



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

The following screen appears when importing has been successful. Return to the previous page by clicking "Return to Previous page".

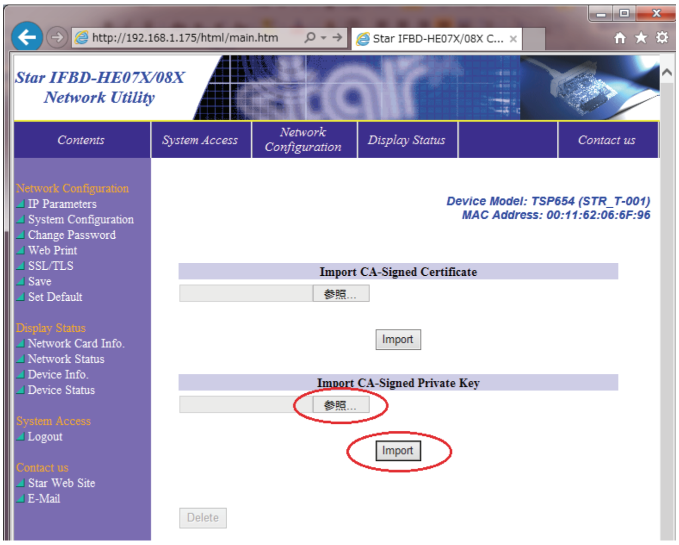


Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

Upload CA-Signed Certificate/Key OK.

Return to Previous page <Import CA-Signed Certificate>

Click [Browse] in the "Import CA-Signed Private Key" column. Select the desired private key file from the client device's  file dialog, and then click [Import].

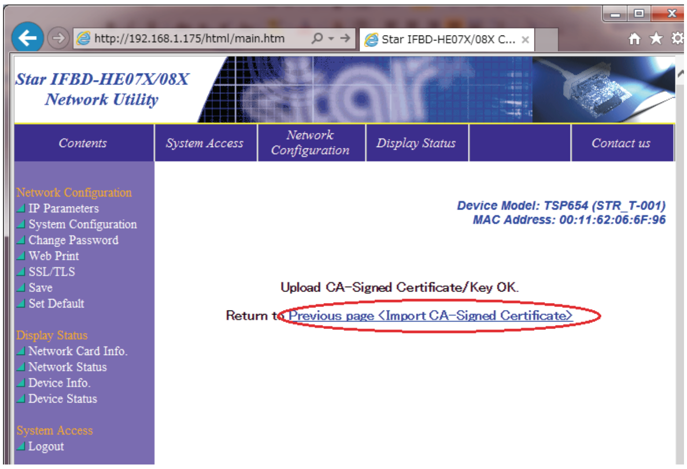


Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

Import CA-Signed Certificate

Import CA-Signed Private Key

The following screen appears when importing has been successful.



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

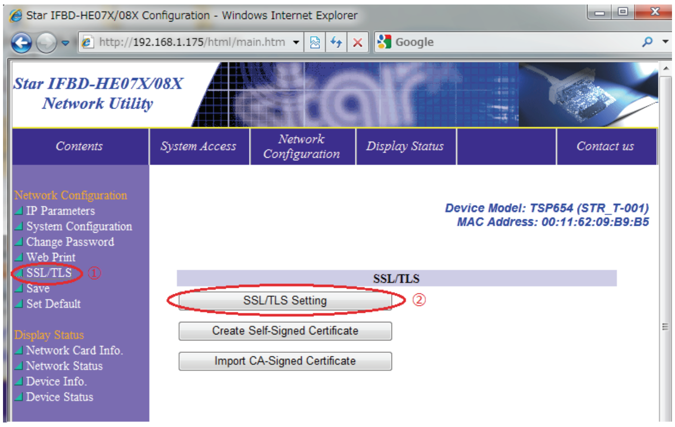
Upload CA-Signed Certificate/Key OK.

Return to Previous page <Import CA-Signed Certificate>

The procedure is complete.

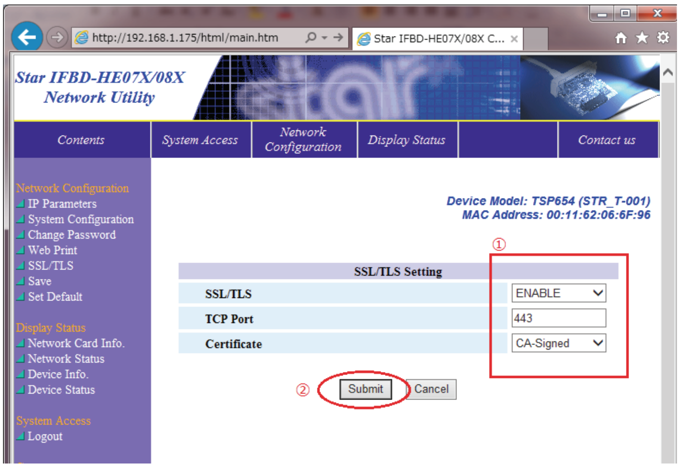
3. Enable SSL/TLS settings on NIC

Click [SSL/TLS].
Click [SSL/TLS Setting].



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

Select [Enable] from the "SSL/TLS" drop-down list and [CA-Signed] from the "Certificate" drop-down list.  Click [Submit].

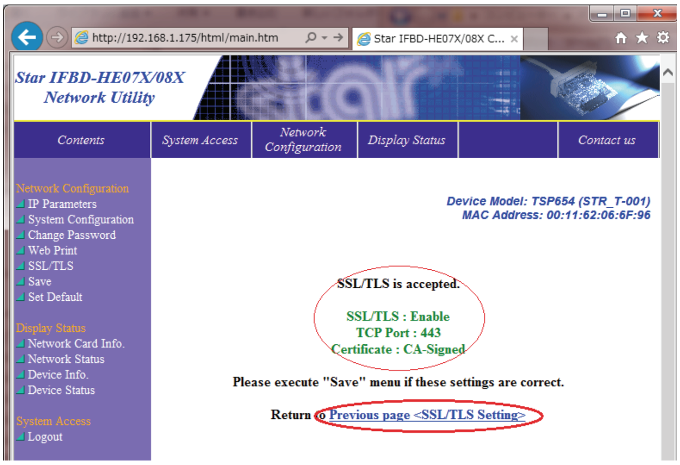


Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

SSL/TLS Setting

| | |
|---|---|
| SSL/TLS | ENABLE |
| TCP Port | 443 |
| Certificate | CA-Signed |

The following information is displayed. Check that the following information matches the information on the screen. "SSL/TLS: ENABLE", "Certificate:  CA-Signed"



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

SSL/TLS is accepted.

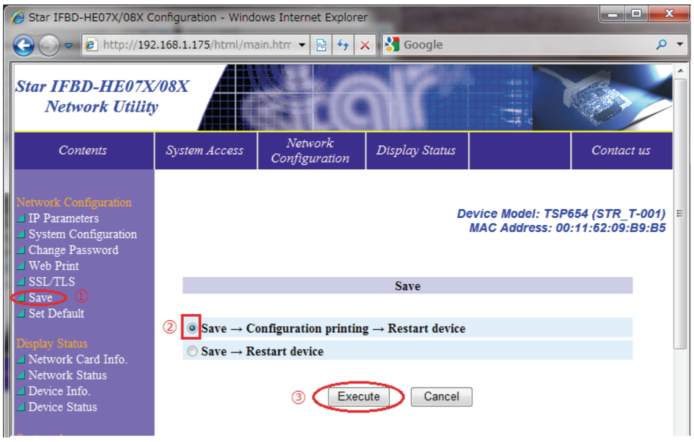
SSL/TLS : Enable
TCP Port : 443
Certificate : CA-Signed

Please execute "Save" menu if these settings are correct.

Return to Previous page <SSL/TLS Setting>

Click [Save], select "Save → Configuration printing → Restart device" on the save screen, and then click [Execute].
The printer prints the settings information. Check that the settings are the same as shown below.

• SSL/TLS: ENABLE
• CA-Signed Certifcate: Exist
• Certifiate: CA-Signed



Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:09:B9:B5

Save

② ● Save → Configuration printing → Restart device
○ Save → Restart device

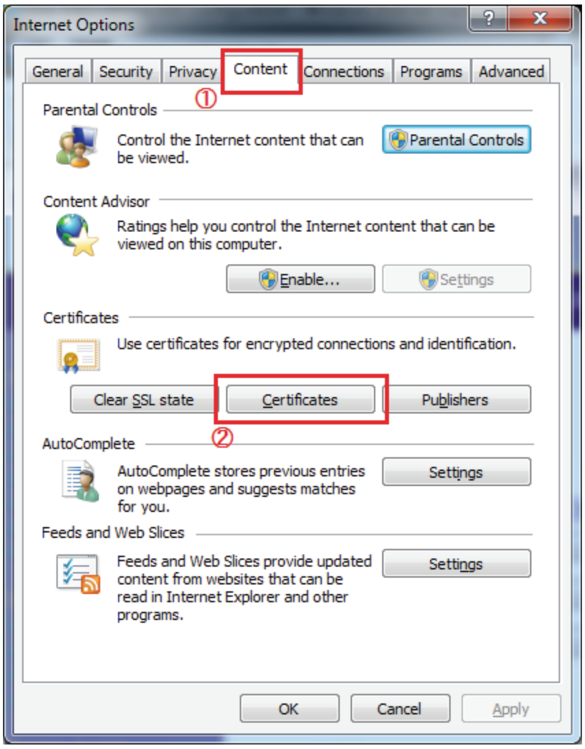
③ Execute   Cancel

Importing a server certificate and a private key to NIC is complete.

4. Registering in the web browser
Register the server certificate signed by a Certificate Authority (CA) in the web browser of the client device as a "Trusted Root Certification Authorities".
(You may not need to do this procedure if you have already registered.)

■ For a Windows device (Windows 7)

Open the Internet Options screen on the web browser.
Select the "Content" tab, and then click [Certificates].



Control the Internet content that can be viewed.

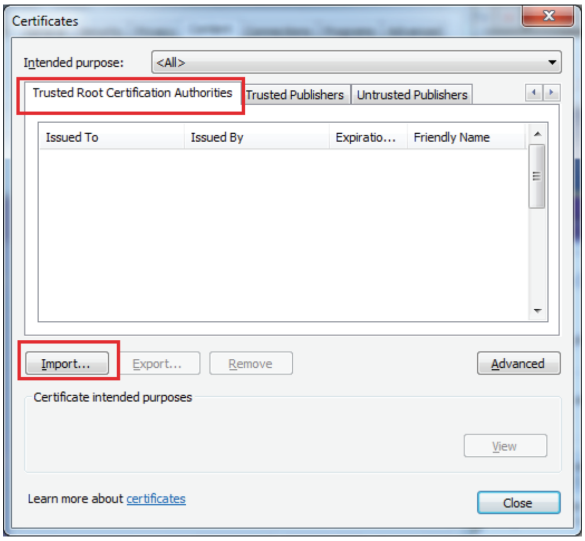
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

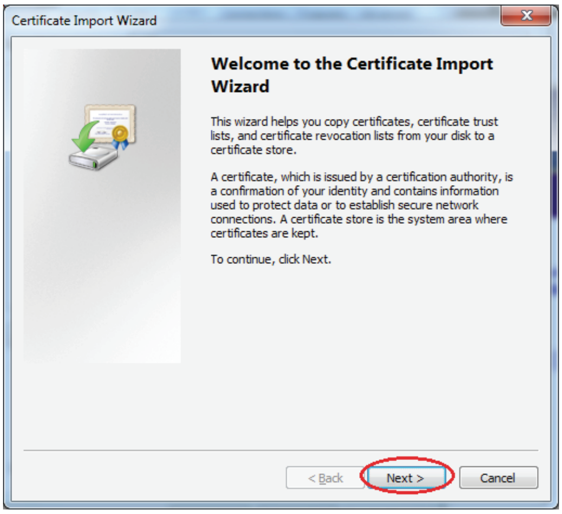
Select the "Trusted Root Certification Authorities" tab, and then click [Import...].



Intended purpose: <All>

Learn more about certificates

Click [Next].



Certificate Import Wizard

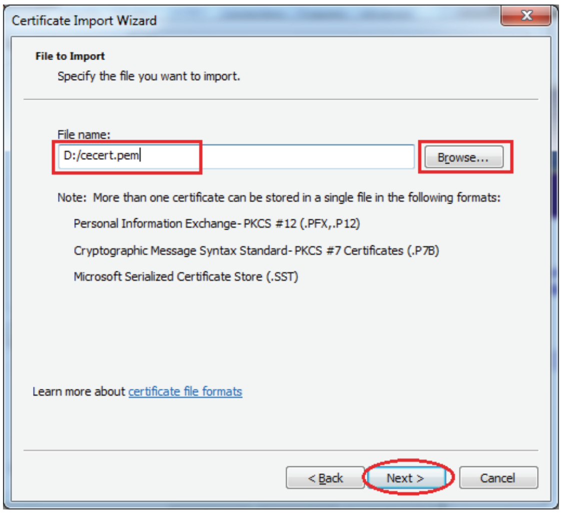
**Welcome to the Certificate Import Wizard**

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Click [Browse...], specify the Certificate Authority's certificate file signed on the server certificate (in this procedure: "cecert.pem"), and then click [Next].



Certificate Import Wizard

**File to Import**

Specify the file you want to import.

File name: D:/cecert.pem

Note: More than one certificate can be stored in a single file in the following formats:

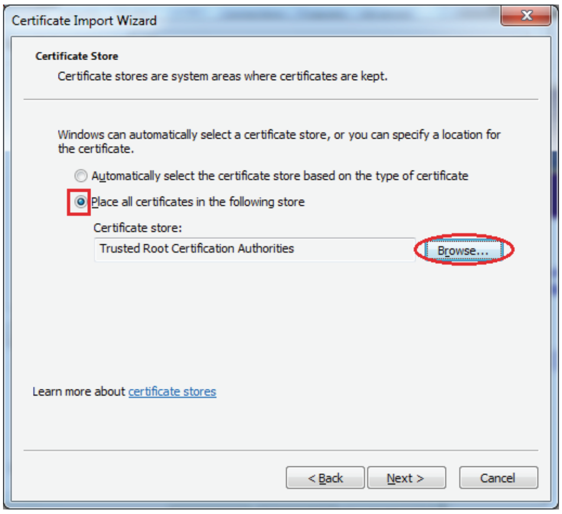
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Select "Place all certificates in the following store", and then click [Browse...].



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

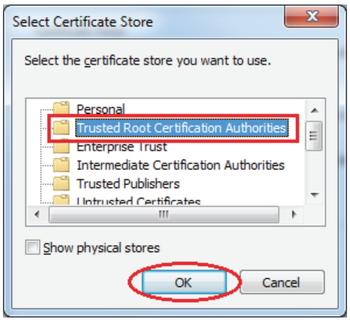
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

Select "Trusted Root Certification Authorities" and then click [OK].



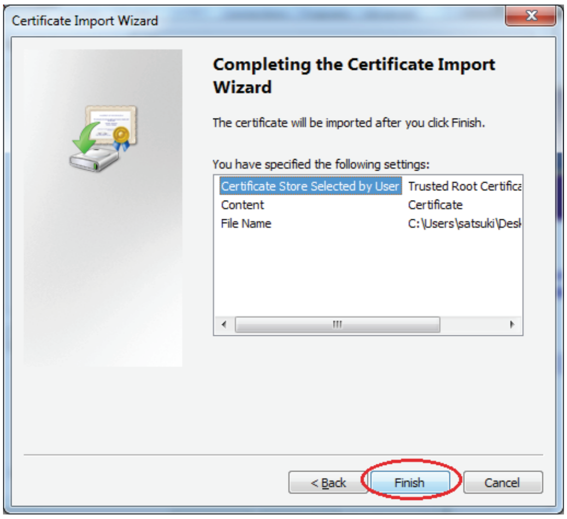
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

Click [Finish].



Certificate Import Wizard

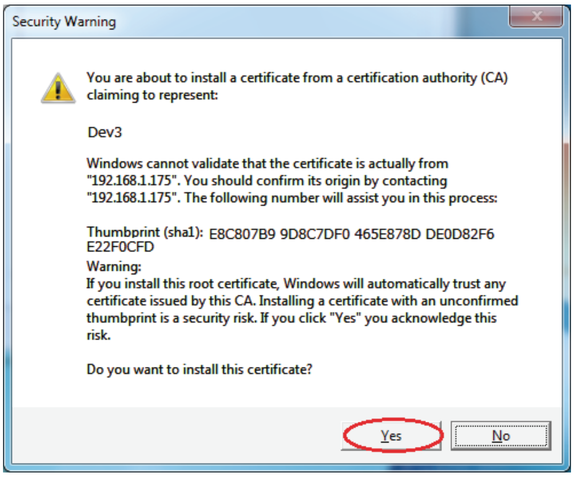
**Completing the Certificate Import Wizard**

The certificate will be imported after you click Finish.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected by User | Trusted Root Certifica |
| Content | Certificate |
| File Name | C:\Users\satsuki\Desl |

Click [Yes]. (The following example: the Certificate Authority (CA) name "Dev 3" is an example of an certificate authority's name imported to NIC.)



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Dev3

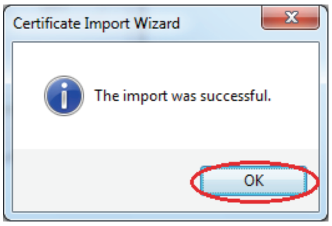
Windows cannot validate that the certificate is actually from "192.168.1.175". You should confirm its origin by contacting "192.168.1.175". The following number will assist you in this process:

Thumbprint (sha1): E8C807B9 9D8C7DF0 465E878D DE0D82F6 E22F0CFD

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

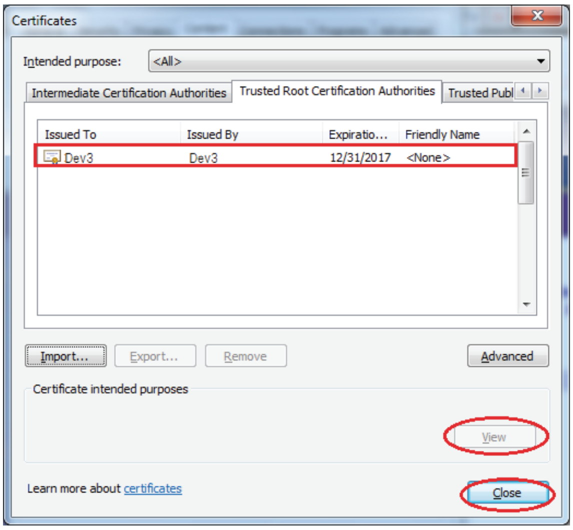
Click [OK].



Certificate Import Wizard

The import was successful.

Check that the Certificate Authority has been registered. Click [View], confirm the details of the certificate, and then click [Close].



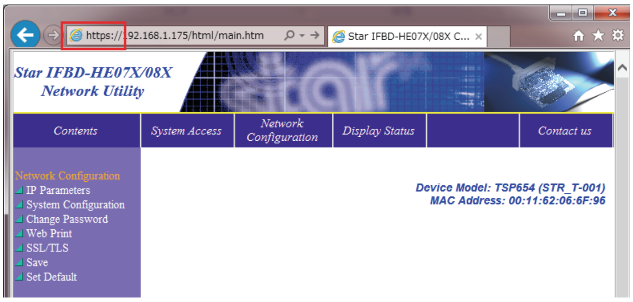
Certificates

Intended purpose: <All>

| Issued To | Issued By | Expiratio... | Friendly Name |
|---|---|---|---|
| Dev3 | Dev3 | 12/31/2017 | <None> |

Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Learn more about certificates
Close

Turn on the printer's power again, and check that the printer's web screen displays normally by entering an address beginning with "https://".



https://92.168.1.175/html/main.htm

Star IFBD-HE07X/08X C...

Star IFBD-HE07X/08X Network Utility

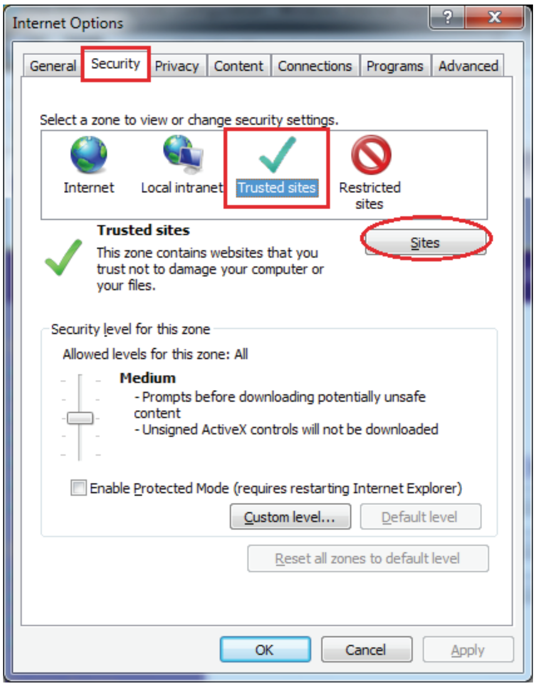
Device Model: TSP654 (STR_T-001)
MAC Address: 00:11:62:06:6F:96

The procedure is complete.
However, depending on the client device environment, you may need to add the address as a "Trusted Sites".
(→ See "7.1.3 Additional Information".)

### 7.1.3. Additional Information

Depending on the client device environment, you may need to add the address as a "Trusted Sites" in the web browser.
The following is an example of settings using Internet Explorer (Windows).

Select "Trusted Sites" from the "Security" tab in Internet Options, and then click [Sites].



Select a zone to view or change security settings.

**Trusted sites**

This zone contains websites that you trust not to damage your computer or your files.

Security level for this zone

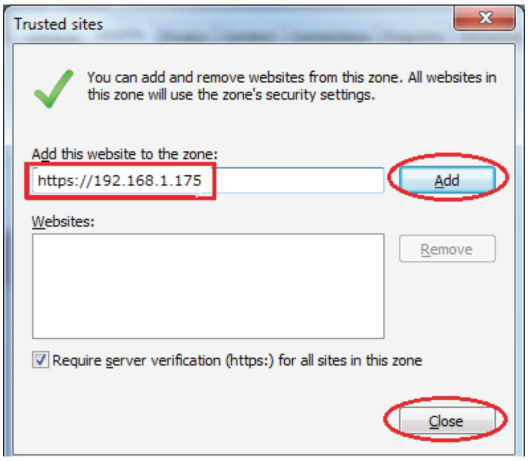
Allowed levels for this zone: All

**Medium**

- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

□ Enable Protected Mode (requires restarting Internet Explorer)

Enter the printer's IP address (the domain value of the certificate) beginning with "https://". Click [Add], and then click [Close].



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone: https://192.168.1.175

Websites:

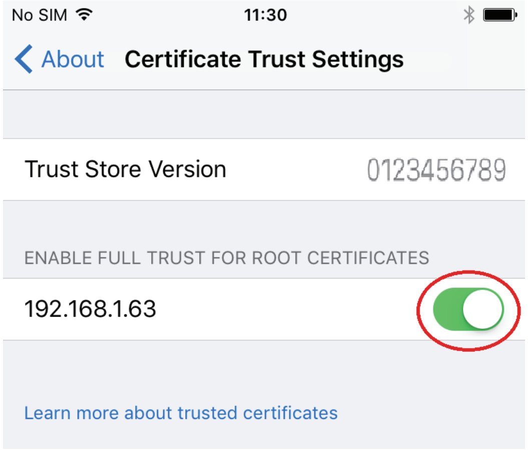
☑ Require server verification (https:) for all sites in this zone

After returning to the Internet Options screen, click [OK] to exit.

## 7.1.4. Required Settings when Registering Certificates with iOS 10.3 or Later

With iOS 10.3 or later, when a certificate was installed manually, that certificate is not automatically trusted for SSL communication. Settings at the iOS device are needed. An example of the iOS settings is shown below for reference.
(For details, check the Apple HP. https://support.apple.com/ja-jp/HT204477)

1. Follow the procedure in "3. Import a certificate to the web browser" in section "7.1.1. Using a self-signed certificate" and import the certificate.
2. In sequence, select "Settings" > "General" > "About" > "Certificate Trust Settings".
3. Enable certificate trust with "ENABLE FULL TRUST FOR ROOT CERTIFICATES".



No SIM
11:30
About
Certificate Trust Settings

Trust Store Version 0123456789

ENABLE FULL TRUST FOR ROOT CERTIFICATES

192.168.1.63

Learn more about trusted certificates

Use the address beginning with "https://" and check that the printer web setting screen is displayed correctly.

URL:http://www.starmicronics.com/support/