Multi-Protocol On-board Ethernet Multi-function Print Server

NETWORK USER'S GUIDE

This Network User's Guide provides useful information of wired network settings and security settings using your Brother machine. You can also find supported protocol information and detailed troubleshooting tips.

To find basic information about network and advanced network features of your Brother machine, see the *Network Glossary*.

To download the latest manual, please visit the Brother Solutions Center at (http://solutions.brother.com/). You can also download the latest drivers and utilities for your machine, read FAQs and troubleshooting tips or learn about special printing solutions from the Brother Solutions Center.

Version 0

CHN-ENG

Definitions of notes

We use the following icons throughout this User's Guide:

IMPORTANT	IMPORTANT indicates a potentially hazardous situation which, if not avoided, may result in damage to property or loss of product functionality.
Note	Notes tell you how you should respond to a situation that may arise or give tips about how the operation works with other features.

IMPORTANT NOTE

- Windows® XP in this document represents Windows® XP Professional, Windows® XP Professional x64 Edition and Windows® XP Home Edition.
- Windows Server® 2003 in this document represents Windows Server® 2003 and Windows Server® 2003 x64 Edition.
- Windows Server® 2008 in this document represents Windows Server® 2008 and Windows Server® 2008 R2.
- Windows Vista® in this document represents all editions of Windows Vista®.
- Windows® 7 in this document represents all editions of Windows® 7.
- Please go to the Brother Solutions Center at http://solutions.brother.com/ and click Manuals on your model page to download the other manuals.

Table of Contents

1 Introduction

Network features

Your Brother machine can be shared on a 10/100 MB wired Ethernet network using the internal network print server. The print server supports various functions and methods of connection depending on the operating system you are running on a network supporting TCP/IP. The following chart shows what network features and connections are supported by each operating system.

Operating Systems	**Windows® 2000/XP** **Windows Vista®** **Windows® 7**	**Windows Server® 2003/2008**	**Mac OS X 10.4.11 - 10.6.x**
Printing	✔	✔	✔
Scanning See *Software User's Guide*.	✔		✔
PC Fax Send [1] See *Software User's Guide*.	✔		✔
PC Fax Receive [1] See *Software User's Guide*.	✔		
BRAdmin Light See page 3.	✔	✔	✔
BRAdmin Professional 3 [2] See page 6.	✔	✔	
Web BRAdmin [2] See page 6.	✔	✔	
Web Based Management (web browser) See page 16.	✔	✔	✔
Remote Setup [1] See *Software User's Guide*.	✔		✔
Status Monitor See *Software User's Guide*.	✔		✔
Driver Deployment Wizard	✔	✔	
Vertical Pairing See *Network Glossary*.	✔ [3]		

[1] Not available for DCP models.

[2] BRAdmin Professional 3 and Web BRAdmin are available as a download from http://solutions.brother.com/.

[3] Windows® 7 only.

Other Network features

Internet fax (MFC-9465CDN: available as a download)

Internet fax (IFAX) allows you to send and receive fax documents using the Internet as the transport mechanism.

In order to use this function, please download the necessary software from our web site, The Brother Solutions Center (http://solutions.brother.com/). Before using this function, you have to configure the necessary machine settings by using the machine's control panel. For details, please refer to the user's guide for Internet fax on the web site listed above.

Security

Your Brother machine employs some of the latest network security and encryption protocols available. (See *Security features* on page 30.)

Fax to Server (MFC-9465CDN: available as a download)

Fax to Server feature allows the machine to scan a document and send it over the network to a separate fax server.

In order to use this function, please download the necessary software from our web site, The Brother Solutions Center (http://solutions.brother.com/). Before using this function, you have to configure the necessary machine settings by using the machine's control panel. For details, please refer to the user's guide for Internet fax on the web site listed above.

Secure Function Lock 2.0

Secure Function Lock 2.0 increases security by restricting the use of functions. (See *Secure Function Lock 2.0* on page 18.)

Store Print Log to Network

The Store Print Log to Network feature allows you to save the print log file from your Brother machine to a network server using CIFS. (See *Store Print Log to Network* on page 23.)

2 Changing your machine's network settings

How to change your machine's network settings (IP address, Subnet mask and Gateway)

Using the control panel

You can configure your machine for a network using the control panel `Network` menu. (See *Control panel setup* on page 8.)

Using the BRAdmin Light utility

The BRAdmin Light utility is designed for initial setup of Brother network connected devices. It also can search for Brother products in a TCP/IP environment, view the status and configure basic network settings, such as IP address.

Installing BRAdmin Light

- Windows®

  1. Please make sure that your machine is ON.
  2. Turn on your computer. Close any applications running before configuration.
  3. Put the supplied CD-ROM into your CD-ROM drive. The opening screen will appear automatically. If the model name screen appears, choose your machine. If the language screen appears, choose your language.
  4. The CD-ROM main menu will appear. Click **Network Utilities**.
  5. Click **BRAdmin Light** and follow the on-screen instructions.

- Macintosh

  The BRAdmin Light software will be installed automatically when you install the printer driver. If you have already installed the printer driver, you do not have to install BRAdmin Light again.

Setting the IP address, Subnet Mask and Gateway using BRAdmin Light

Note

- You can download Brother's latest BRAdmin Light utility from http://solutions.brother.com/.
- If you require more advanced machine management, use the latest version of BRAdmin Professional 3 utility that is available as a download from http://solutions.brother.com/. This utility is only available for Windows® users.
- If you are using a firewall function of anti-spyware or antivirus applications, temporarily disable them. Once you are sure that you can print, re-enable the application.
- Node name: The Node name appears in the current BRAdmin Light window. The default node name of the print server in the machine is “BRNxxxxxxxxxxxx” for a wired network. (“xxxxxxxxxxxx” is your machine’s MAC Address / Ethernet Address.)
- The default password for Brother print servers is “access”.

1. Start the BRAdmin Light utility.

   - Windows®

     Click **Start** / **All Programs** [1] / **Brother** / **BRAdmin Light** / **BRAdmin Light**.

     [1] **Programs** for Windows® 2000 users

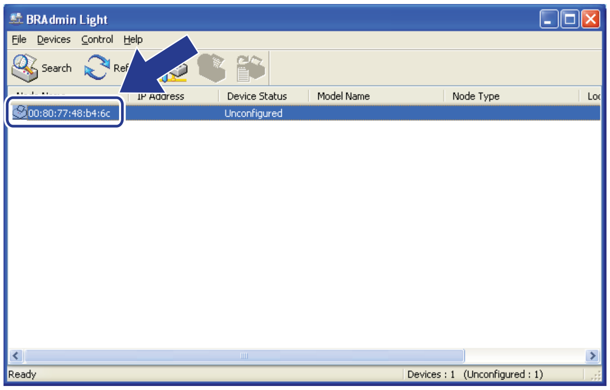
   - Macintosh

     Double-click **Macintosh HD** (Startup Disk) / **Library** / **Printers** / **Brother** / **Utilities** / **BRAdmin Light.jar** file.

2. BRAdmin Light will search for new devices automatically.

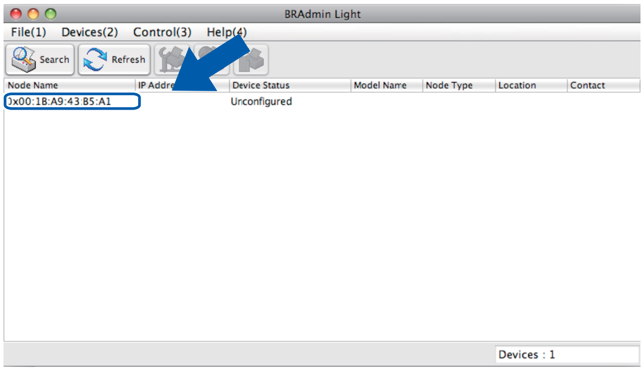
3. Double-click the unconfigured device.

Windows®



	IP Address	Device Status	Model Name	Node Type	Lo
00:80:77:48:b4:6c		Unconfigured			

Macintosh



Node Name	IP Addre	Device Status	Model Name	Node Type	Location	Contact
)x00:1B:A9:43:B5:A1		Unconfigured				

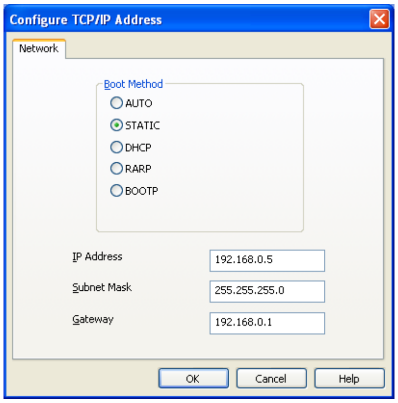
Note

- If the print server is set to its factory default settings (if you do not use a DHCP/BOOTP/RARP server), the device will appear as **Unconfigured** in the BRAdmin Light utility screen.

- You can find the Node Name and MAC Address (Ethernet Address) by printing the Network Configuration List. (See *Printing the Network Configuration List* on page 12 for information on how to print the Network Configuration List on your print server.) You can also find the Node Name and MAC Address from the control panel. (See *Chapter 3: Control panel setup*.)

4 Choose **STATIC** from **Boot Method (BOOT Method)**. Enter the **IP Address**, **Subnet Mask** and **Gateway** (if needed) of your print server.

Windows®



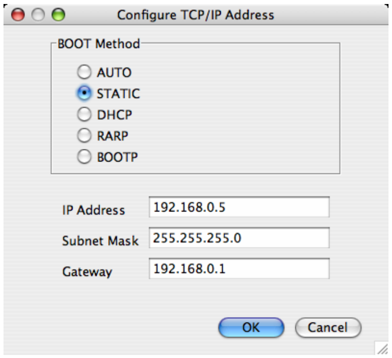
Configure TCP/IP Address

Network

Boot Method
○ AUTO
● STATIC
○ DHCP
○ RARP
○ BOOTP

IP Address 192.168.0.5
Subnet Mask 255.255.255.0
Gateway 192.168.0.1

Macintosh



Configure TCP/IP Address

BOOT Method
○ AUTO
● STATIC
○ DHCP
○ RARP
○ BOOTP

IP Address 192.168.0.5
Subnet Mask 255.255.255.0
Gateway 192.168.0.1

5 Click **OK**.

6 With the correctly programmed IP address, you will see the Brother print server in the device list.

Other Management Utilities

Your Brother machine has the following management utilities other than the BRAdmin Light utility. You can change your network settings using these utilities.

Web Based Management (web browser)

A standard web browser can be used to change your print server settings using the HTTP (Hyper Text Transfer Protocol). (See *How to configure the machine settings using Web Based Management (web browser)* on page 16.)

BRAdmin Professional 3 utility (Windows®)

BRAdmin Professional 3 is a utility for more advanced management of network connected Brother devices. This utility can search for Brother products on your network and view the device status from an easy to read Explorer style window that changes color identifying the status of each device. You can configure network and device settings along with the ability to update device firmware from a Windows® computer on your LAN. BRAdmin Professional 3 can also log activity of Brother devices on your network and export the log data in an HTML, CSV, TXT or SQL format.

For users who want to monitor locally connected machines, install the Print Auditor Client software on the client PC. This utility allows you to monitor machines that are connected to a client PC via the USB or parallel interface from BRAdmin Professional 3.

For more information and to download the software, visit us at http://solutions.brother.com/.

Note

- Please use the latest version of the BRAdmin Professional 3 utility that is available as a download from http://solutions.brother.com/. This utility is only available for Windows® users.
- If you are using a firewall function of anti-spyware or antivirus applications, temporarily disable them. Once you are sure that you can print, configure the software settings following the instructions.
- Node name: The Node name for each Brother device on the network appears in BRAdmin Professional 3. The default Node name is "BRNxxxxxxxxxxxx" for a wired network. ("xxxxxxxxxxxx" is your machine's MAC Address / Ethernet Address.)

Web BRAdmin (Windows®)

Web BRAdmin is a utility for managing network connected Brother devices. This utility can search for Brother products on your network, view the status and configure the network settings.

Unlike BRAdmin Professional 3, which is designed for Windows® only, Web BRAdmin is a server based utility that can be accessed from any client PC with a web browser that supports JRE (Java Runtime Environment). By installing the Web BRAdmin server utility on a computer running IIS [1], administrators can connect to the Web BRAdmin server using a web browser, which then communicates with the device itself.

For more information and to download the software, visit us at http://solutions.brother.com/.

[1] Internet Information Server 4.0 or Internet Information Services 5.0/5.1/6.0/7.0

BRPrint Auditor (Windows®)

The BRPrint Auditor software brings the monitoring power of Brother network management tools to locally connected machines. This utility allows a client computer to collect usage and status information from a Brother machine connected via the parallel or USB interface. The BRPrint Auditor can then pass this information to another computer on the network running BRAdmin Professional 3 or Web BRAdmin 1.45 or greater. This allows the administrator to check items such as page counts, toner and drum status and the firmware version. In addition to reporting to Brother network management applications this utility can E-mail the usage and status information directly to a predefined E-mail address in a CSV or XML file format (SMTP Mail support required). The BRPrint Auditor utility also supports E-mail notification for reporting warning and error conditions.

3 Control panel setup

Network menu

The Network menu selections of the control panel allow you to set up the Brother machine for your network configuration. (For more information on how to use the control panel, see the *Basic User's Guide*.) Press **Menu**, then press ▲ or ▼ to choose Network. Proceed to the menu selection you wish to configure. (For additional information on the menu, see *Function table and default factory settings* on page 13.)

Please note that the machine is supplied with the BRAdmin Light utility, Web Based Management or Remote Setup[1] applications, which also can be used to configure many aspects of the network. (See *Other Management Utilities* on page 6.)

[1] Not available for DCP models.

TCP/IP

This menu has ten sections: Boot Method, IP Address, Subnet Mask, Gateway, Node Name, WINS Config, WINS Server, DNS Server, APIPA and IPv6.

Boot Method

This selection controls how the machine obtains an IP address.

Auto mode

In this mode, the machine will scan the network for a DHCP server. If it can find one, and if the DHCP server is configured to allocate an IP address to the machine, then the IP address supplied by the DHCP server will be used. If no DHCP server is available, then the machine will scan for a BOOTP server. If a BOOTP server is available, and it is configured correctly, the machine will take its IP address from the BOOTP server. If a BOOTP server is not available, the machine will scan for a RARP server. If a RARP server also does not answer, the IP Address is set using the APIPA protocol. After the machine is initially powered ON, it may take a few minutes for the machine to scan the network for a server.

Static mode

In this mode the machine’s IP address must be manually assigned. Once entered the IP address is locked to the assigned address.

Note

If you do not want your print server configured via DHCP, BOOTP or RARP, you must set the Boot Method to Static so that the print server has a static IP address. This will prevent the print server from trying to obtain an IP address from any of these systems. To change the Boot Method, use the machine’s control panel, BRAdmin Light utility, Web Based Management or Remote Setup.

IP Address

This field displays the current IP address of the machine. If you have chosen a `Boot Method` of `Static`, enter the IP address that you wish to assign to the machine (check with your network administrator for the IP address to use). If you have chosen a method other than `Static`, the machine will attempt to determine its IP address using the DHCP or BOOTP protocols. The default IP address of your machine will probably be incompatible with the IP address numbering scheme of your network. We recommend that you contact your network administrator for an IP address for the network the unit will be connected on.

Subnet Mask

This field displays the current subnet mask used by the machine. If you are not using DHCP or BOOTP to obtain the subnet mask, enter the desired subnet mask. Check with your network administrator for the subnet mask to use.

Gateway

This field displays the current gateway or router address used by the machine. If you are not using DHCP or BOOTP to obtain the gateway or router address, enter the address you wish to assign. If you do not have a gateway or router, leave this field blank. Check with your network administrator if you are unsure.

Node Name

You can register the machine name on the Network. This name is often referred to as a NetBIOS name; it will be the name that is registered by the WINS server on your network. Brother recommends the name “BRNxxxxxxxxxxxx” for a wired network. (“xxxxxxxxxxxx” is your machine’s MAC Address / Ethernet Address.)

WINS Config

This selection controls how the machine obtains the IP address of the WINS server.

Auto

Automatically uses a DHCP request to determine the IP addresses for the primary and secondary WINS servers. You must set the BOOT Method to Auto for this feature to work.

Static

Uses a specified IP address for the primary and secondary WINS servers.

WINS Server

Primary WINS Server IP Address

This field specifies the IP address of the primary WINS (Windows® Internet Name Service) server. If set to a non-zero value, the machine will contact this server to register its name with the Windows® Internet Name Service.

Secondary WINS Server IP Address

This field specifies the IP address of the secondary WINS server. It is used as a backup to the Primary WINS server address. If the Primary server is unavailable, the machine still can register itself with a secondary server. If set to a non-zero value, the machine will contact this server to register its name with the Windows® Internet Name Service. If you have a primary WINS server, but no secondary WINS server, simply leave this field blank.

DNS Server

Primary DNS Server IP Address

This field specifies the IP address of the primary DNS (Domain Name System) server.

Secondary DNS Server IP Address

This field specifies the IP address of the secondary DNS server. It is used as a backup to the Primary DNS server address. If the Primary server is unavailable, the machine will contact the Secondary DNS server. If you have a primary DNS server, but no secondary DNS server, simply leave this field blank.

APIPA

The setting of `On` will cause the print server to automatically allocate a Link-Local IP address in the range (169.254.1.0 - 169.254.254.255) when the print server cannot obtain an IP address through the Boot Method you have set. (See *Boot Method* on page 8.) Choosing `Off` means the IP address does not change, when the print server cannot obtain an IP address through the Boot Method you have set.

IPv6

This machine is compatible with IPv6, the next generation Internet protocol. If you want to use the IPv6 protocol, choose `On`. The default setting for IPv6 is `Off`. For more information on the IPv6 protocol, visit http://solutions.brother.com/.

Note

- If you set IPv6 to `On`, turn off the power switch and then turn it back on to enable this protocol.
- After you choose IPv6 `On`, this setting will be applied to the wired LAN interface.

Ethernet

Ethernet link mode. Auto allows the print server to operate in 100BASE-TX full or half duplex, or in 10BASE-T full or half duplex mode by auto negotiation.

Note

If you set this value incorrectly, you may not be able to communicate with your print server.

Status (For DCP-9055CDN and MFC-9465CDN)

This field displays the current wired network status.

MAC Address

The MAC address is a unique number assigned for the machine's network interface. You can check your machine's MAC address from the control panel.

How to set a new default for Scan to FTP

You can choose the default color and file type for the Scan to FTP function. (For how to operate Scan to FTP, see Network Scanning in the *Software User's Guide*.)

How to set a new default for Scan to Network

You can choose the default color and file type for the Scan to Network function to scan a document directly to a server supporting CIFS on your local network or on the internet. (For the CIFS protocol, see the *Network Glossary*.) (For how to operate Scan to Network, see Network Scanning in the *Software User's Guide*.)

Reset the network settings to the factory default

You can reset the print server back to its default factory settings (resetting all information such as the password and IP address information).

Note

- This function resets all wired network settings to the factory default.
- You can also reset the print server back to its factory default settings using the BRAdmin applications or Web Based Management. (For more information, see *Other Management Utilities* on page 6.)

1. Press **Menu**.
2. Press ▲ or ▼ to choose `Network`.
   Press **OK**.
3. Press ▲ or ▼ to choose `Network Reset`.
   Press **OK**.
4. Press **1** to choose `Reset`.
5. Press **1** to choose `Yes` for reboot.
6. The machine will re-start.

Printing the Network Configuration List

Note

Node name: The Node name appears on the Network Configuration List. The default node name is "BRNxxxxxxxxxxxx" for a wired network. ("xxxxxxxxxxxx" is your machine's MAC Address / Ethernet Address.)

The Network Configuration List prints a report listing all the current network configuration including the network print server settings.

1. Press **Menu**.
2. (For MFC models) Press ▲ or ▼ to choose `Print Reports`.
   (For DCP models) Press ▲ or ▼ to choose `Machine Info.`.
   Press **OK**.
3. Press ▲ or ▼ to choose `Network Config`.
   Press **OK**.
4. Press **Mono Start** or **Color Start**.

Note

If the **IP Address** on the Network Configuration List shows **0.0.0.0**, wait for one minute and try again.

Function table and default factory settings

DCP-9055CDN and MFC-9465CDN

The factory settings are shown in Bold with an asterisk.

Main menu	Submenu	Menu selections	Options	
4.Network (DCP-9055CDN) 7.Network (MFC-9465CDN)	1.TCP/IP	1.Boot Method	**Auto*** Static RARP BOOTP DHCP (If you choose Auto, RARP, BOOTP or DHCP, you will be asked to enter how many times the machine tries to obtain the IP address.)	
		2.IP Address	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** [1]	
		3.Subnet Mask	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** [1]	
		4.Gateway	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***	
		5.Node Name	BRNxxxxxxxxxxxx (up to 32 characters)	
		6.WINS Config	**Auto*** Static	
		7.WINS Server	Primary	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
			Secondary	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
		8.DNS Server	Primary	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
			Secondary	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
		9.APIPA	**On*** Off	

Main menu	Submenu	Menu selections	Options	
4.Network (DCP-9055CDN) 7.Network (MFC-9465CDN) (continued)	1.TCP/IP (continued)	0.IPv6	On Off*	
	2.Ethernet	—	Auto* 100B-FD 100B-HD 10B-FD 10B-HD	
	3.Status	—	Active 100B-FD Active 100B-HD Active 10B-FD Active 10B-HD Inactive	
	4.MAC Address	—	—	
	5.Scan To FTP	—	Color 100 dpi* Color 200 dpi Color 300 dpi Color 600 dpi Gray 100 dpi Gray 200 dpi Gray 300 dpi B&W 200 dpi B&W 200x100 dpi	(If you choose Color option) PDF* PDF/A Secure PDF Signed PDF JPEG XPS (If you choose Gray option) PDF* PDF/A Secure PDF Signed PDF JPEG XPS (If you choose B&W option) PDF* PDF/A Secure PDF Signed PDF TIFF

Main menu	Submenu	Menu selections	Options	
4.Network (DCP-9055CDN) 7.Network (MFC-9465CDN) (continued)	6.ScanTo Network	—	Color 100 dpi* Color 200 dpi Color 300 dpi Color 600 dpi Gray 100 dpi Gray 200 dpi Gray 300 dpi B&W 200 dpi B&W 200x100 dpi	(If you choose Color option) **PDF*** PDF/A Secure PDF Signed PDF JPEG XPS (If you choose Gray option) **PDF*** PDF/A Secure PDF Signed PDF JPEG XPS (If you choose B&W option) **PDF*** PDF/A Secure PDF Signed PDF TIFF
	0.Network Reset	—	1.Reset	
		—	2.Exit	

[1] On connection to the network, the machine will automatically set the IP address and Subnet Mask to values appropriate for your network.

4 Web Based Management

Overview

A standard Web Browser can be used to manage your machine using the HTTP (Hyper Text Transfer Protocol). You can get the following information from a machine on your network using a web browser.

- Machine status information
- Change Fax configuration items, such as General Setup, Address Book settings and Remote Fax
- Change network settings such as TCP/IP information
- Configure Secure Function Lock 2.0
- Configure Store Print Log to Network
- Configure Scan to FTP
- Configure Scan to Network
- Software version information of the machine and print server
- Change network and machine configuration details

Note

We recommend Microsoft® Internet Explorer® 6.0 (or greater) or Firefox 3.0 (or greater) for Windows® and Safari 3.0 (or greater) for Macintosh. Please also make sure that JavaScript and Cookies are always enabled in whichever browser you use. If a different web browser is used, make sure it is compatible with HTTP 1.0 and HTTP 1.1.

You must use the TCP/IP protocol on your network and have a valid IP address programmed into the print server and your computer.

How to configure the machine settings using Web Based Management (web browser)

A standard web browser can be used to change your print server settings using the HTTP (Hyper Text Transfer Protocol).

Note

We recommend to use HTTPS protocol for your Internet security when configuring the settings using Web Based Management. To enable the HTTPS protocol, see *Managing your network machine securely using SSL/TLS* on page 31.

1 Start your web browser.

2 Type "`http://machine's IP address/`" into your browser (where "`machine's IP address`" is the machine's IP address).

- For example:

  `http://192.168.1.2/`

Note

- If you are using a Domain Name System or enable a NetBIOS name, you can enter another name such as “Shared_Printer” instead of the IP address.

  - For example:

  `http://Shared_Printer/`

  If you enable a NetBIOS name, you can also use the node name.

  - For example:

  `http://brnxxxxxxxxxxxx/`

  The NetBIOS name can be seen in the Network Configuration List. (To learn how to print the Network Configuration List, see *Printing the Network Configuration List* on page 12.)

- For Macintosh users, you can have easy access to the Web Based Management System by clicking the machine icon on the **Status Monitor** screen. For more information, see the *Software User's Guide*.

3. Click **Network Configuration**.
4. Enter a user name and a password. The default User Name is “**admin**” and the default password is “**access**”.
5. Click **OK**.
6. You can now change the print server settings.

Note

If you have changed the protocol settings, restart the machine after clicking **Submit** to activate the configuration.

Password information

Web Based Management offers two levels of password access. Users are able to access to the **General Setup**, **Fax Settings**, **Copy Settings**, **Printer Settings** and **USB Direct I/F**. The default user name for User is “**user**” (case sensitive) and the default password is “**access**”.

Administrators are able to access all settings. The login name for the Administrator is “**admin**” (case sensitive) and the default password is “**access**”.

Secure Function Lock 2.0

Secure Function Lock 2.0 from Brother helps you to save money and increase security by restricting the functions available on your Brother machine.

Secure Function Lock allows you to configure passwords for selected users, granting them access to some, or all, of these functions, or limiting them to a page limit. This means that only authorized people can use them.

You can configure and change the following Secure Function Lock 2.0 settings using BRAdmin Professional 3 or Web Based Management.

- **PC Print** [1]
- **USB Direct Print** [2]
- **Copy**
- **Color Print**
- **Page Limit**
- **Fax TX** [2]
- **Fax RX** [2]
- **Scan**
- **Page Counter**

[1] If you register the PC user login names, you can restrict PC print without the user entering a password. For more detail, see *Restricting PC print by PC user login name* on page 20.

[2] Supported models only.

How to configure the Secure Function Lock 2.0 settings using Web Based Management (web browser)

Basic configuration

1. Click **Administrator Settings** on the machine's web page, and then click **Secure Function Lock**.
2. Choose **On** from **Function Lock**.

Note

To configure Secure Function Lock through the embedded web server, you have to enter the Administrator Password (four digit number). If the settings have been configured previously using the Panel menu and you want to change the settings, you must fill in the blank in the **Administrator Password** box first.

3. Enter an up to 14 digit alphanumeric group name or user name in the **ID Number/Name** box and then enter a four-digit password in the **PIN** box.
4. Uncheck the functions that you want to restrict in the **Print** box or the **Others** box. If you want to configure the maximum page count, check the **On** box in **Page Limit**, and then enter the number in the **Max.** box. Then click **Submit**.

5 If you want to restrict the PC printing by PC user login name, click **PC Print Restriction by Login Name** and configure the settings. (See *Restricting PC print by PC user login name* on page 20.)

Scanning when using Secure Function Lock 2.0

The Secure Function Lock 2.0 feature allows the administrator to restrict which users are allowed to scan. When the scan feature is set to off for the public user setting, only users who have scan selected in the check box will be able to scan. To push scan from the control panel of the machine users must enter their PIN to access the scan mode. To pull scan from their computer, restricted users must also enter their PIN on the control panel of the machine before they can scan from their computer. If the PIN is not entered at the machines control panel the user will get an error message on their computer when they attempt to pull scan.

Restricting PC print by PC user login name

By configuring this setting, the machine can authenticate by PC user login name to allow a print job from a registered computer.

1. Click **PC Print Restriction by Login Name**. The **PC Print Restriction by Login Name** screen will appear.
2. Choose **On** from **PC Print Restriction**.
3. Choose the ID Number you set in the **ID Number/Name** in step ❸ in *Basic configuration* from the **ID Number** pull-down list for each Login Name and then enter the PC user login name in the **Login Name** box.
4. Click **Submit**.

Note

- If you want to restrict PC print per group, choose the same ID Number for each PC login name you want in the group.
- If you are using the PC login name feature you must also make sure that the **Use PC Login Name** box in the printer driver is checked. For more information about the printer driver, see the *Software User's Guide*.
- The Secure Function Lock feature does not support the BR-Script driver for printing.

Setting up public mode

You can set up the public mode to restrict what functions are available for public users. Public users do not need to enter a password to access the features made available through this setting.

1. Uncheck the check box for the function that you want to restrict in the **Public Mode** box.
2. Click **Submit**.

Other features

You can set up the following features in Secure Function Lock 2.0:

- **All Counter Reset**

  You can reset the page counter by clicking **All Counter Reset**.

- **Export to CSV file**

  You can export the current page counter including **ID Number/Name** information as a CSV file.

- **Last Counter Record**

  The machine retains the page count after the counter has been reset.

- **Counter Auto Reset Settings**

  You can automatically reset the page counters by configuring the time interval based on Daily, Weekly or Monthly settings during the machine is turned on.

Synchronize with SNTP server

SNTP is the protocol used to synchronize the time used by the machine for Authentication with the SNTP time server (this time is not the time displayed on the LCD of the machine). You can synchronize the time used by the machine on a regular basis with the Coordinated Universal Time (UTC) provided by the SNTP time server.

1. Click **Network Configuration**, and then click **Configure Protocol**.
2. Select the **SNTP** check box to activate the setting.
3. Click **Advanced Setting**.
   - **Status**

     Displays whether the SNTP server settings are enabled or disabled.
   - **SNTP Server Method**

     Choose **AUTO** or **STATIC**.
     - **AUTO**

       If you have a DHCP server in your network, the SNTP server will automatically obtain the address from that server.
     - **STATIC**

       Enter the address you want to use.
   - **Primary SNTP Server Address**, **Secondary SNTP Server Address**

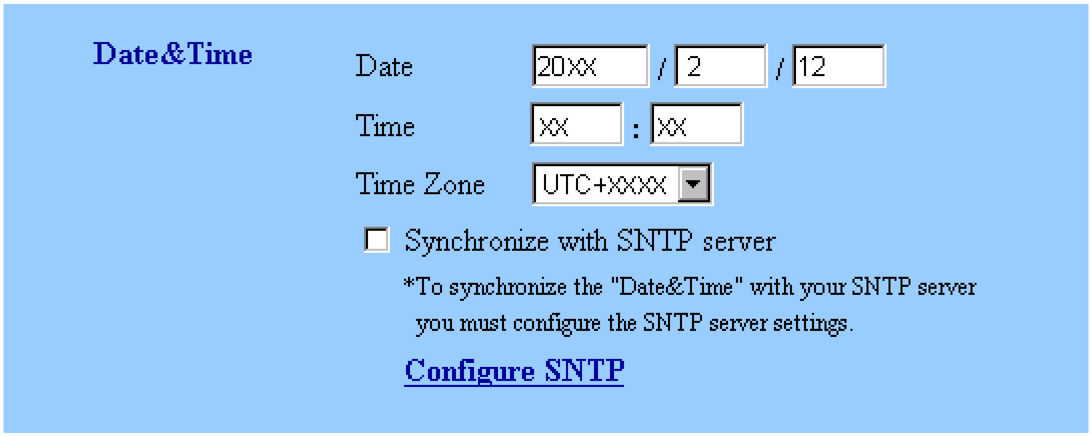
     Enter the server address (up to 64 characters).
   - **Primary SNTP Server Port**, **Secondary SNTP Server Port**

     Enter the Port number (1 to 65535).
   - **Synchronizing Interval**

     Enter the interval of hours which you want to synchronize to the server (1 to 168 hours).

Note

- You must configure **Date&Time** to synchronize the time used by the machine with the SNTP time server. Click **Configure Date&Time** and then configure **Date&Time** on the **General Setup** screen. You can also configure the Date & Time from the machine's control panel.



Date&Time

Date 20XX / 2 / 12

Time XX : XX

Time Zone UTC+XXXX

□ Synchronize with SNTP server

*To synchronize the "Date&Time" with your SNTP server you must configure the SNTP server settings.

Configure SNTP

- Choose the **Synchronize with SNTP server** check box. You also need to verify your time zone settings correctly. Choose the time difference between your location and UTC from the **Time Zone** pull-down list. For example, the time zone for Eastern Time in the USA and Canada is UTC-05:00.

■ **Synchronization Status**

You can confirm the latest synchronization status.

4 Click **Submit** to apply the settings.

Store Print Log to Network

The Store Print Log to Network feature allows you to save the print log file from your Brother machine to a network server using CIFS [1]. You can record the ID, type of print job, job name, user name, date, time, the number of printed pages and color pages [2] for every print job.

[1] CIFS is the Common Internet File System protocol that runs over TCP/IP allowing computers on a network to share files over an intranet or the Internet.

[2] Supported models only.

The following print functions are recorded in the print log:

- Print jobs from your computer
- USB Direct Print (Supported models only)
- Copy
- Received Fax (Supported models only)

Note

- The Store Print Log to Network feature supports **Kerberos** Authentication and **NTLMv2** Authentication.

  You must configure the SNTP protocol (network time server), or you must set the date, time and time zone correctly for Authentication.
- You can set the file type to **TXT** or **CSV** when storing a file to the server.

How to configure the Store Print Log to Network settings using Web Based Management (web browser)

1. Click **Administrator Settings** on the machine's web page, and then click **Store Print Log to Network**.
2. Choose **On** from **Print Log**.
3. You can configure the following settings using a web browser.
   - **Host Address**

     The Host Address is the Host name of the CIFS server. Enter the Host Address (for example: example.com) (up to 64 characters) or the IP address (for example: 192.168.56.189).
   - **Store Directory**

     Enter the destination folder where your log will be stored on the CIFS server (for example: brother\abc) (up to 60 characters).
   - **File Name**

     Enter the file name you want to use for the print log up to 15 characters.
   - **File Type**

     Choose the file type for the print log **TXT** or **CSV**.

- **Auth. Method**

  Choose the authentication method required for access to the CIFS server **Auto**, **Kerberos**[1] or **NTLMv2**[2].

  [1] Kerberos is an authentication protocol which allows devices or individuals to securely prove their identity to network servers using a single sign-on.

  [2] NTLMv2 is the default authentication method used by Windows to log into servers.

  For Kerberos and NTLMv2 Authentication you must also configure the Date&Time settings or the SNTP protocol (network time server).

  You can configure the Date&Time and the SNTP settings using Web Based Management.

  You can also configure the Date&Time settings from the machine's control panel.

  - **Auto**: If you choose Auto, the machine will initially search for a Kerberos server. If the Kerberos server is not detected, NTLMv2 will be used for the authentication method.
  - **Kerberos**: Choose Kerberos, to use Kerberos authentication only.
  - **NTLMv2**: Choose NTLMv2, to use NTLMv2 authentication only.

- **Username**

  Enter the Username for the authentication up to 96 characters.

Note

If the username is part of a domain, please input the username in one of the following styles: user@domain or domain\user.

- **Password**

  Enter the password for the authentication up to 32 characters.

- **Kerberos Server Address** (if needed)

  Enter the KDC Host Address (for example: example.com) (up to 64 characters) or the IP address (for example: 192.168.56.189).

4. In the **Connection Status**, you can confirm the last log status. For more information, see *Understanding Error Messages* on page 26.

5. Click **Submit** to apply your settings.

Error Detection Setting

You can choose what action is taken when the print log cannot be stored to the server due to a network error.

1. Choose **Cancel Print** or **Ignore Log & Print** in the **Error Detection Setting** of **Store Print Log to Network**.

   - **Cancel Print**

     If you choose **Cancel Print**, the print jobs are canceled when the print log cannot be stored to the server.

Note

Even if you choose **Cancel Print**, your machine will print a received fax.

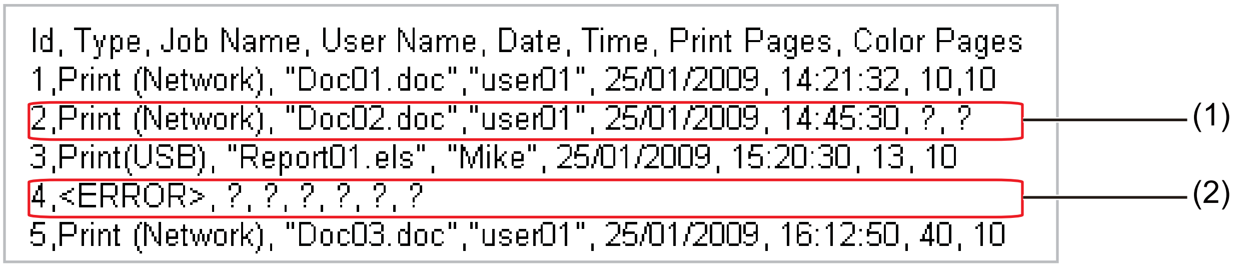
- **Ignore Log & Print**

  If you choose **Ignore Log & Print**, the machine prints the document even if the print log cannot be stored to the server.

  When the store print log function has recovered, the print log is recorded as follows:

  - If the log cannot be stored at the end of printing, the print log except the number of printed pages and color pages will be recorded. (1)
  - If the Print Log cannot be stored at the beginning and the end of printing, the print log of the job will not be recorded. When the function has recovered, the occurrence of an error is shown in the log. (2)

  Example of the print log:



```
Id, Type, Job Name, User Name, Date, Time, Print Pages, Color Pages
1,Print (Network), "Doc01.doc","user01", 25/01/2009, 14:21:32, 10,10
2,Print (Network), "Doc02.doc","user01", 25/01/2009, 14:45:30, ?, ?
3,Print(USB), "Report01.els", "Mike", 25/01/2009, 15:20:30, 13, 10
4,<ERROR>, ?, ?, ?, ?, ?, ?
5,Print (Network), "Doc03.doc","user01", 25/01/2009, 16:12:50, 40, 10
```

2. Click **Submit** to apply your settings.

Understanding Error Messages

You can confirm the error status on the LCD of your machine or **Connection Status** in Web Based Management.

- `Server Timeout`

  This message will appear when you cannot connect to the server.
  Make sure that:

  - Your server address is correct.
  - Your server is connected to the network.
  - The machine is connected to the network.

- `Authentication Error`

  The message will appear when your **Authentication Setting** is not correct.
  Make sure that:

  - Username [1] and Password in Authentication Setting is correct.

    [1] If the username is part of a domain, please input the username in one of the following styles: user@domain or domain\user.

  - Confirm the time of the log file sever matches the time from the SNTP server, or the **Date&Time** settings.
  - Confirm the SNTP time server settings are configured correctly so the time matches the time used for authentication by Kerberos or NTLMv2. If there is no SNTP server make sure the **Date&Time** and **Time Zone** settings are set correctly using Web Based Management or the control panel so the machine matches the time being used by the server providing the authentication.

- `File Access Error`

  This message will appear when you cannot access the destination folder.
  Make sure that:

  - Directory name is correct.
  - Directory is write-enabled.
  - File is not locked.

- `Wrong Date&Time`

  This message will appear when your machine does not obtain the time from the SNTP time server. Make sure that:

  - Confirm the settings to access the SNTP time correctly using Web Based Management.
  - If no SNTP server is being used, confirm the Date & Time set on the control panel matches the time used by the server providing the authentication.

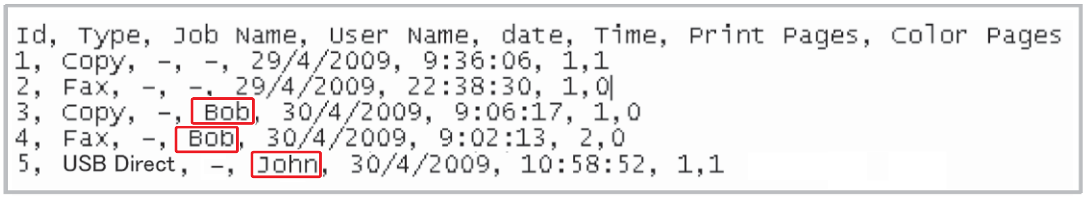
Note

If you choose the **Cancel Print** option in Web Based Management the `Log Access Error` message will remain on the LCD for about 60 seconds.

Using Store Print Log to Network with Secure Function Lock 2.0

When Secure Function Lock 2.0 is active the names of the registered users for copy, Fax RX and USB Direct Print (if available) functions will be recorded in the Store Print Log to Network report.

Example of the print Log with Secure Function Lock 2.0 users:



```
Id, Type, Job Name, User Name, date, Time, Print Pages, Color Pages
1, Copy, -, -, 29/4/2009, 9:36:06, 1,1
2, Fax, -, -, 29/4/2009, 22:38:30, 1,0
3, Copy, -, Bob, 30/4/2009, 9:06:17, 1,0
4, Fax, -, Bob, 30/4/2009, 9:02:13, 2,0
5, USB Direct, -, John, 30/4/2009, 10:58:52, 1,1
```

Changing the Scan to FTP configuration using a web browser

Scan to FTP allows you to scan a document directly to an FTP server on your local network or on the Internet.

See Network Scanning in the *Software User's Guide* for more details on Scan to FTP.

1. Click **Administrator Settings** on the MFC-XXXX (or DCP-XXXX) web page, and then click **FTP/Network Scan Settings**.

2. You can choose what profile numbers (1 to 10) to use for Scan to FTP settings.
You can also store two user defined file names that can be used for creating an FTP Server Profile in addition to the seven present file names in **Create a User Defined File Name**. A maximum of 15 characters can be entered in each of the two fields.
After setting, click **Submit**.

3. Click **FTP/Network Scan Profile** on **Administrator Settings** page.
Now you can configure and change the following Scan to FTP settings using a web browser.

- **Profile Name** (Up to 14 characters)
- **Host Address** (FTP server address)
- **Username**
- **Password**
- **Store Directory**
- **File Name**
- **Quality**
- **File Type**
- **File Size**
- **Passive Mode**
- **Port Number**

You can set **Passive Mode** to **Off** or **On** depending on your FTP server and network firewall configuration. By default this setting is **On**, you can also change the port number used to access the FTP server. The default for this setting is port 21. In most cases these two settings can remain as default.

Note

Scan to FTP is available when FTP server profiles are configured using Web Based Management.

Changing the Scan to Network configuration using a web browser

Scan to Network allows you to scan documents directly to a shared folder on a CIFS server located on your local network or the Internet. (For more information on the CIFS protocol, see the *Network Glossary*.) To enable the CIFS protocol, check the box for **CIFS** on **Configure Protocol** from the **Network Configuration** page.

See Network Scanning in the *Software User's Guide* for more details on Scan to Network.

Note

Scan to Network supports Kerberos Authentication and NTLMv2 Authentication.

You must configure the SNTP protocol (network time server), or you must set the date, time and time zone correctly for Authentication.

1. Click **Administrator Settings** on the MFC-XXXX (or DCP-XXXX) web page, and then click **FTP/Network Scan Settings**.

2. You can choose what profile numbers (1 to 10) to use for Scan to Network settings.
   You can also store two user defined file names that can be used for creating a Scan to Network Profile in addition to the seven present file names in **Create a User Defined File Name**. A maximum of 15 characters can be entered in each of the two fields.
   After setting, click **Submit**.

3. Click **FTP/Network Scan Profile** on **Administrator Settings** page.
   Now you can configure and change the following Scan to Network settings using a web browser.

- **Profile Name** (Up to 14 characters)
- **Host Address**
- **Store Directory**
- **File Name**
- **Quality**
- **File Type**
- **File Size**
- **Use PIN for authentication**
- **PIN Code**
- **Auth. Method**
- **Username**
- **Password**
- **Kerberos Server Address**

Note

Scan to Network is available when Network server profiles are configured using Web Based Management.

5 Security features

Overview

In today's world there are many security threats to your network and the data that travels over it. Your Brother machine employs some of the latest network security and encryption protocols available today. These network features can be integrated into your overall network security plan to help protect your data and prevent unauthorized access to the machine. This chapter explains how to configure them.

You can configure the following security features:

- Managing your network machine securely using SSL/TLS (See *Managing your network machine securely using SSL/TLS* on page 31.)
- Managing your network machine securely using SNMPv3 protocol (See *Secure Management using Web Based Management (web browser)* on page 31 or *Secure Management using BRAdmin Professional 3 (Windows®)* on page 38.)
- Printing documents securely using SSL/TLS (See *Printing documents securely using SSL/TLS* on page 33.)
- Sending and Receiving an E-mail securely (See *Sending or Receiving an E-mail securely* on page 34.)
- Using IEEE 802.1x authentication (See *Using IEEE 802.1x authentication* on page 36.)
- Secure Management using BRAdmin Professional 3 (Windows®) (See *Secure Management using BRAdmin Professional 3 (Windows®)* on page 38.)
- Certificate for secure management (See *Using Certificates for device security* on page 39.)
- Managing multiple certificates (See *Managing multiple certificates* on page 49.)

Note

We recommend to disable the Telnet, FTP and TFTP protocols. Accessing the machine using these protocols is not secure. (For how to configure the protocol settings, see *How to configure the machine settings using Web Based Management (web browser)* on page 16.) If you disable FTP, the Scan to FTP function will be disabled.

Managing your network machine securely using SSL/TLS

To manage your network machine securely, you need to use the management utilities with security protocols.

Secure Management using Web Based Management (web browser)

We recommend to use HTTPS and SNMPv3 protocol for secure management. To use the HTTPS protocol, the following machine settings are required.

- A self-signed certificate or a certificate issued by a CA, and a private key must be installed in the machine. (For how to install a certificate and private key, see *Using Certificates for device security* on page 39.)
- The HTTPS protocol must be enabled. To enable the HTTPS protocol, choose an installed certificate from the pull-down list in the **HTTP Server Settings** page of **Web Based Management** on the **Configure Protocol** page, and then enable **SSL communication is used (port 443)**. (For information on how to access the **Configure Protocol** page, see *How to configure the machine settings using Web Based Management (web browser)* on page 16.)

1. Start your web browser.
2. Type "`https://Common Name/`" into your browser. (Where "`Common Name`" is the Common Name that you assigned for the certificate, such as an IP address, node name or domain name. For how to assign a Common Name for the certificate, see *Using Certificates for device security* on page 39.)
   - For example:

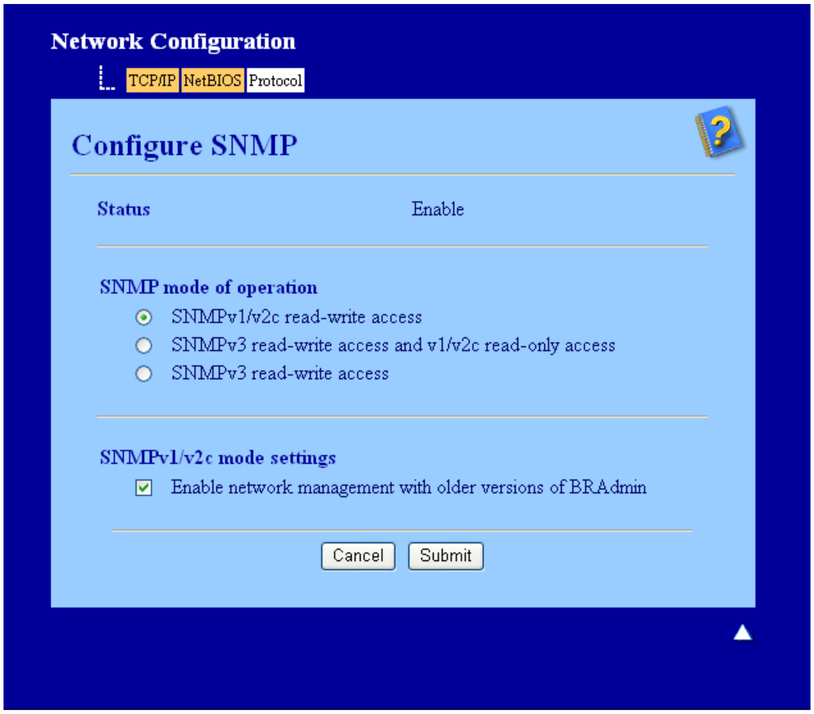
     `https://192.168.1.2/` (if the Common Name is the printer's IP address)
3. You can now access the machine using HTTPS.
   We recommend secure management (SNMPv3) be used along with the HTTPS protocol. If you use the SNMPv3 protocol, follow the steps below.

Note

You can also change the SNMP settings by using BRAdmin Professional 3 or Web BRAdmin.

4. Click **Network Configuration**.
5. Enter a user name and a password. The default User Name is "**admin**" and the default Password is "**access**".
6. Click **OK**.
7. Click **Configure Protocol**.
8. Make sure that the **SNMP** setting is enabled, and then click **Advanced Setting** of **SNMP**.

9 You can configure the SNMP settings from the screen below.



Configure SNMP

Status Enable

SNMP mode of operation

● SNMPv1/v2c read-write access
○ SNMPv3 read-write access and v1/v2c read-only access
○ SNMPv3 read-write access

SNMPv1/v2c mode settings

☑ Enable network management with older versions of BRAdmin

We have three SNMP connection modes of operation.

- **SNMPv3 read-write access**

  With this mode the print server uses version 3 of the SNMP protocol. If you want to manage the print server securely, use this mode.

Note

When you use the **SNMPv3 read-write access** mode, please note the following.

- You can manage the print server by using BRAdmin Professional 3, Web BRAdmin or Web Based Management only.
- We recommend secure SSL communication (HTTPS) be used.
- Except for BRAdmin Professional 3 and Web BRAdmin, all applications that use SNMPv1/v2c will be restricted. To allow the use of SNMPv1/v2c applications, use **SNMPv3 read-write access and v1/v2c read-only access** or **SNMPv1/v2c read-write access** mode.

- **SNMPv3 read-write access and v1/v2c read-only access**

  In this mode the print server uses the read-write access of version 3 and the read-only access of version 1 and version 2c of the SNMP protocol.

Note

When you use the **SNMPv3 read-write access and v1/v2c read-only access** mode, some Brother applications (e.g. BRAdmin Light) that access to the print server do not work properly since they authorize the read-only access of version 1 and version 2c. If you want to use all applications, use the **SNMPv1/v2c read-write access** mode.

- **SNMPv1/v2c read-write access**

  In this mode the print server uses version 1 and version 2c of the SNMP protocol. You can use all Brother applications under this mode. However, it is not secure since it will not authenticate the user and the data will not be encrypted.

Note

For more information, see the Help text in Web Based Management.

Printing documents securely using SSL/TLS

To print documents securely over the Internet, you can use the IPPS protocol.

Note

- Communication using IPPS cannot prevent unauthorized access to the print server.
- IPPS is available for Windows® 2000/XP, Windows Vista®, Windows® 7 and Windows Server® 2003/2008.

To use the IPPS protocol, the following machine settings are required.

- A self-signed certificate or a certificate issued by a CA, and a private key must be installed in the machine. For how to install a certificate and private key, see *Using Certificates for device security* on page 39.
- The IPPS protocol must be enabled. To enable the IPPS protocol, choose an installed certificate from the pull-down list in the **HTTP Server Settings** page of **IPP** on the **Configure Protocol** page, and then enable **SSL communication is used (port 443)**. For information on how to access the **Configure Protocol** page, see *How to configure the machine settings using Web Based Management (web browser)* on page 16.

Sending or Receiving an E-mail securely

Configuration using Web Based Management (web browser)

You can configure secured E-mail sending with user authentication or E-mail sending and receiving using SSL/TLS on the Web Based Management screen.

1. Start your web browser.
2. Type "`http://printer's IP address/`" into your browser (where "`printer's IP address`" is the printer's IP address).
   - For example:

     `http://192.168.1.2/`
3. Click **Network Configuration**.
4. Enter a user name and a password. The default User Name is "**admin**" and the default Password is "**access**".
5. Click **OK**.
6. Click **Configure Protocol**.
7. Click **Advanced Setting** of **POP3/SMTP** and make sure that the status of **POP3/SMTP** is **Enable**.
8. You can configure the **POP3/SMTP** settings on this page.

Note

- For more information, see the Help text in Web Based Management.
- You can also confirm whether the E-mail settings are correct after configuration by sending a test E-mail.

9. After configuring, click **Submit**. The Test E-mail Send/Receive Configuration dialog appears.
10. Follow the instructions on-screen if you want to test with the current settings.

Sending an E-mail with user authentication

This machine supports POP before SMTP and SMTP-AUTH methods to send an E-mail via an E-mail server that requires a user authentication. These methods prevent an unauthorized user from accessing the E-mail server. You can use Web Based Management, BRAdmin Professional 3 and Web BRAdmin to configure these settings. You can use POP before SMTP and SMTP-AUTH methods for E-mail Notification and E-mail reports.

E-mail server settings

You need to match the settings of SMTP authentication method with the method used by your E-mail server. Contact your network administrator or your ISP (Internet Service Provider) about the E-mail server configuration.

You will also need to check **SMTP-AUTH** of **SMTP Server Authentication Method** to enable the SMTP server authentication.

SMTP settings

- You can change the SMTP port number using Web Based Management. This is useful if your ISP (Internet Service Provider) implements the “Outbound Port 25 Blocking (OP25B)” service.
- By changing the SMTP port number to a specific number which your ISP is using for the SMTP server (for example, port 587), you would then be able to send an E-mail via the SMTP server.
- If you can use both POP before SMTP and SMTP-AUTH, we recommend choosing SMTP-AUTH.
- If you choose POP before SMTP for the SMTP Server Authentication Method, you need to configure the POP3 settings. You can also use the APOP method if needed.

Sending or Receiving an E-mail securely using SSL/TLS

This machine supports SSL/TLS methods to send or receive an E-mail via an E-mail server that requires secure SSL/TLS communication. To send or receive E-mail via an E-mail server that is using SSL/TLS communication, you must configure SMTP over SSL/TLS or POP3 over SSL/TLS correctly.

Verifying Server Certificate

- If you choose SSL or TLS for **SMTP over SSL/TLS** or **POP3 over SSL/TLS**, the **Verify Server Certificate** check box will be automatically checked to verify the Server Certificate.
  - Before you verify the Server Certificate, you must import the CA certificate that has been issued by the CA that signed the Server Certificate. Contact your system administrator about the CA certificate. For importing the certificate, see *Import and export a CA certificate* on page 49.
  - If you do not need to verify the Server Certificate, uncheck **Verify Server Certificate**.

Port Number

- If you choose SSL or TLS, the **SMTP Port** or **POP3 Port** value will be changed to match the protocol. If you want to change the port number manually, enter the port number after you choose **SMTP over SSL/TLS** or **POP3 over SSL/TLS**.
- You must configure the POP3/SMTP communication method to match the E-mail server. For details of the E-mail server settings, contact your network administrator or Internet services provider.

  In most cases, the secured webmail services require the following settings:

  (SMTP)

  SMTP Port: 587

  SMTP Server Authentication Method: SMTP-AUTH

  SMTP over SSL/TLS: TLS

  (POP3)

  POP3 Port: 995

  POP3 over SSL/TLS: SSL

Using IEEE 802.1x authentication

You can configure IEEE 802.1x authentication for a wired.

To use IEEE 802.1x authentication, you must install a certificate issued by a CA. Contact your network administrator or your ISP (Internet Service Provider) whether a CA certificate import is necessary. (For how to install a certificate, see *Using Certificates for device security* on page 39.)

IEEE 802.1x authentication configuration using Web Based Management (web browser)

If you are configuring IEEE 802.1x authentication for a wired network using Web Based Management, follow the instructions.

You can also configure IEEE 802.1x authentication using:

- BRAdmin Professional 3

Note

- If you configure your machine using EAP-TLS Authentication, you must install the Client Certificate before you start configuration. If you have installed more than one certificate, we recommend you write down the certificate you want to use. For installing the certificate, see *Using Certificates for device security* on page 39.
- Before you verify the Server Certificate, you must import the CA certificate that has been issued by the CA that signed the Server Certificate. Contact your system administrator about the CA certificate. For importing the certificate, see *Import and export a CA certificate* on page 49.
- For the details of each certificate, see *Using Certificates for device security* on page 39.

1. Start your web browser.
2. Type “`http://machine’s IP address/`” into your browser (where “`machine’s IP address`” is the machine’s IP address).
   - For example:

     `http://192.168.1.2/`

Note

- If you are using a Domain Name System or enable a NetBIOS name, you can enter another name such as “Shared_Printer” instead of the IP address.
  - For example:

    `http://Shared_Printer/`

  If you enable a NetBIOS name, you can also use the node name.
  - For example:

    `http://brnxxxxxxxxxxxx/`

  The NetBIOS name can be seen in the Network Configuration List. (To learn how to print the Network Configuration List, see *Printing the Network Configuration List* on page 12.)

- For Macintosh users, you can have easy access to the Web Based Management System by clicking the machine icon on the **Status Monitor** screen. For more information, see the *Software User's Guide*.

3 Click **Network Configuration**.

4 Enter a user name and a password. The default User Name is “**admin**” and the default password is “**access**”.

5 Click **OK**.

6 Click **Configure Wired802.1x**.

7 Now you can configure the IEEE 802.1x authentication settings.

- If you want to enable IEEE 802.1x authentication for wired network, check **Enable** for **Wired 802.1x status** on the **Configure Wired802.1x** page.
- For the details of IEEE 802.1x authentication and the inner authentication methods, see the *Network Glossary*.
- If you are using EAP-TLS authentication, you must choose the Client Certificate that has been installed (shown with Certificate Name) for verification from the **Client Certificate** pull-down list.
- If you choose EAP-FAST, PEAP, EAP-TTLS or EAP-TLS authentication, you can choose the verification method from the **Server Certificate Verification** pull-down list. You can verify the Server Certificate by using the CA certificate imported to the machine in advance, that has been issued by the CA that signed the Server Certificate.

You can choose following verification methods from the **Server Certificate Verification** pull-down list.

- **No Verification**

  The Server Certificate can always be trusted. The verification is not performed.

- **CA Cert.**

  The verification method to check the CA reliability of the Server Certificate, using the CA certificate that has been issued by the CA that signed the Server Certificate.

- **CA Cert. + ServerID**

  The verification method to check the Common Name [1] value of the Server Certificate, in addition to the CA reliability of the Server Certificate.

[1] The Common Name verification compares the Common Name of the Server Certificate to the character string configured for the **Server ID**. Before you use this method, contact your system administrator about the Server Certificate’s Common Name and then configure **Server ID**.

8 After configuring, click **Submit**.
After configuring, connect your machine to the IEEE 802.1x supported network. After a few minutes, print the Network Configuration List to check the **<Wired IEEE 802.1x> Status.** (See *Printing the Network Configuration List* on page 12 for information on how to print the Network Configuration List on your print server.)

- **Success**

  The wired IEEE 802.1x function is enabled and the authentication was successful.

- **Failed**

  The wired IEEE 802.1x function is enabled, however, the authentication failed.

- **Off**

  The wired IEEE 802.1x function is not available.

Secure Management using BRAdmin Professional 3 (Windows®)

To use the BRAdmin Professional 3 utility securely, you need to follow the points below

- We strongly recommend to use the latest version of the BRAdmin Professional 3 utility or Web BRAdmin that are available as a download from http://solutions.brother.com/. If you use an older version of BRAdmin [1] to manage your Brother machines the user authentication will not be secure.
- If you want to avoid access to your machine from older versions of BRAdmin [1], you need to disable the access from older versions of BRAdmin [1] from **Advanced Setting** of **SNMP** on **Configure Protocol** page using Web Based Management. (See *Secure Management using Web Based Management (web browser)* on page 31.)
- If you use BRAdmin Professional 3 and Web Based Management together, use Web Based Management with the HTTPS protocol. (See *Secure Management using Web Based Management (web browser)* on page 31.)
- If you are managing a mixed group of older print servers [2] and the print servers with BRAdmin Professional 3, we recommend using a different password in each group. This will ensure security is maintained on the new print servers.

[1] BRAdmin Professional older than Ver. 2.80, Web BRAdmin older than Ver. 1.40, BRAdmin Light for Macintosh older than Ver. 1.10

[2] NC-2000 series, NC-2100p, NC-3100h, NC-3100s, NC-4100h, NC-5100h, NC-5200h, NC-6100h, NC-6200h, NC-6300h, NC-6400h, NC-8000, NC-100h, NC-110h, NC-120w, NC-130h, NC-140w, NC-8100h, NC-9100h, NC-7100w, NC-7200w, NC-2200w

Using Certificates for device security

Your Brother machine supports the use of multiple security certificates allowing secure management, authentication and communication with the machine. The following security certificate features can be used with the machine.

- SSL/TLS communication
- IEEE 802.1x authentication
- SSL communication for SMTP/POP3

The Brother machine supports the following certificates.

- Self-signed certificate

  This print server issues its own certificate. Using this certificate, you can easily use the SSL/TLS communication without having a certificate from a CA. (See *Creating and installing a certificate* on page 41.)

- Certificate from a CA

  There are two methods for installing a certificate from a CA. If you already have a CA or if you want to use a certificate from an external trusted CA:

  - When using a CSR (Certificate Signing Request) from this print server. (See *How to create a CSR* on page 46.)
  - When importing a certificate and a private key. (See *Import and export the certificate and private key* on page 47.)

- CA certificate

  If you use a CA certificate that identifies the CA (Certificate Authority) itself and owns its private key, you must import a CA certificate from the CA, prior to the configuration. (See *Import and export a CA certificate* on page 49.)

Note

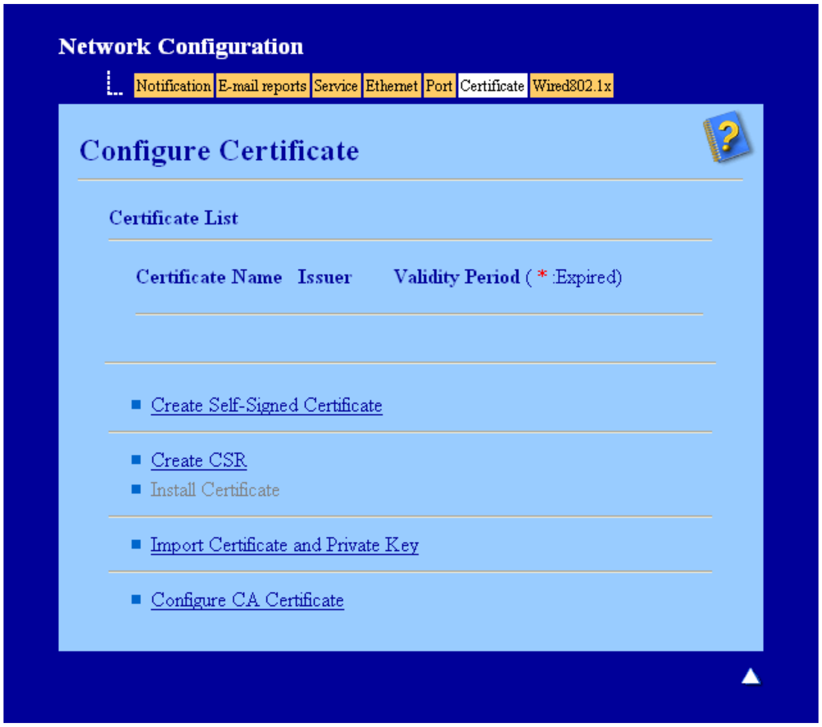
- If you are going to use SSL/TLS communication, we recommend that you contact your system administrator first.
- When you reset the print server back to its default factory settings, the certificate and the private key that are installed will be deleted. If you want to keep the same certificate and the private key after resetting the print server, export them before resetting and re-install them. (See *How to export the self-signed certificate, the certificate issued by a CA, and the private key* on page 48.)

Configure certificate using Web Based Management

This feature can be configured using Web Based Management only. Follow these steps to access the configure certificate page using Web Based Management.

1. Start your web browser.
2. Type "`http://printer's IP address/`" into your browser (where "`printer's IP address`" is the printer's IP address).
   - For example:

     `http://192.168.1.2/`
3. Click **Network Configuration**.
4. Enter a user name and a password. The default User Name is "**admin**" and the default Password is "**access**".
5. Click **OK**.
6. Click **Configure Certificate**.
7. You can configure the certificate settings from the screen below.



Network Configuration

Configure Certificate

Certificate List

Certificate Name Issuer Validity Period (* :Expired)

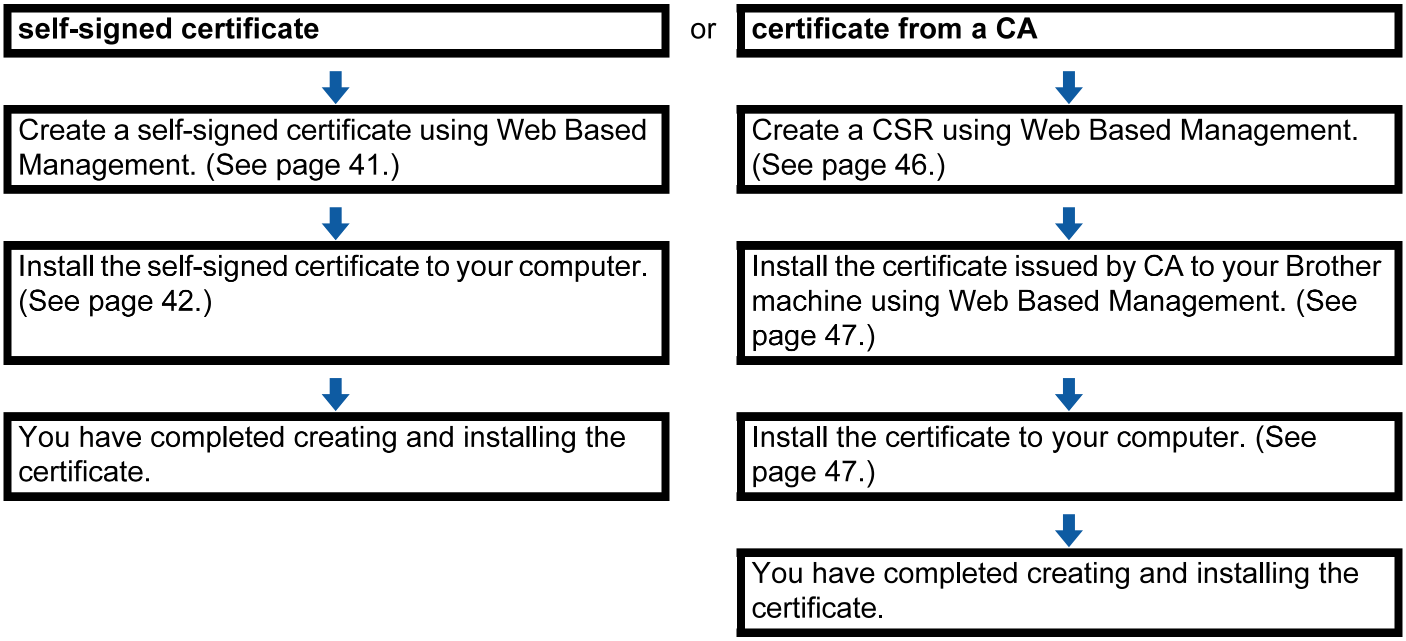
- Create Self-Signed Certificate
- Create CSR
- Install Certificate
- Import Certificate and Private Key
- Configure CA Certificate

Note

- The functions that are grayed and unlinked indicate they are not available.
- For more information on configuration, see the Help text in the Web Based Management.

Creating and installing a certificate

Step by step chart for creating and installing a certificate



self-signed certificate or **certificate from a CA**

self-signed certificate:

- Create a self-signed certificate using Web Based Management. (See page 41.)
- Install the self-signed certificate to your computer. (See page 42.)
- You have completed creating and installing the certificate.

certificate from a CA:

- Create a CSR using Web Based Management. (See page 46.)
- Install the certificate issued by CA to your Brother machine using Web Based Management. (See page 47.)
- Install the certificate to your computer. (See page 47.)
- You have completed creating and installing the certificate.

How to create and install a self-signed certificate

1. Click **Create Self-Signed Certificate** on the **Configure Certificate** page.

2. Enter a **Common Name** and a **Valid Date**, then click **Submit**.

Note

- The length of the **Common Name** is less than 64 bytes. Enter an identifier such as an IP address, node name or domain name to use when accessing this machine through SSL/TLS communication. The node name is displayed by default.
- A warning will pop-up if you use the IPPS or HTTPS protocol and enter a different name in the URL than the **Common Name** that was used for the self-signed certificate.

3. The self-signed certificate is created and saved in your machine's memory successfully.
To use SSL/TLS communication, the self-signed certificate also needs to be installed on your computer.
Proceed to the next section.

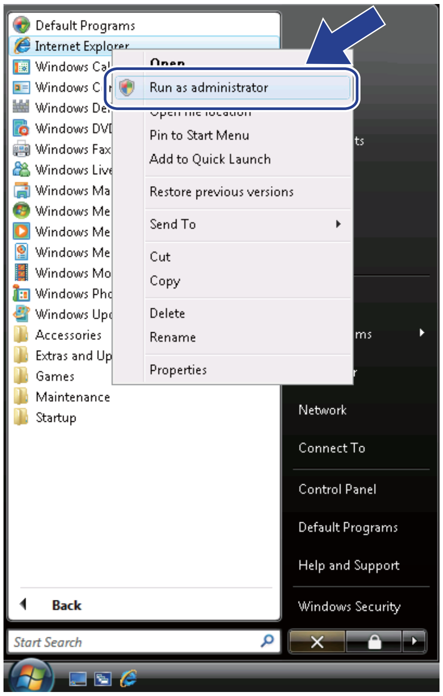
How to install the self-signed certificate on your computer

Note

The following steps are for Microsoft® Internet Explorer®. If you use another web browser, follow the help text of the web browser itself.

For Windows Vista®, Windows® 7 and Windows Server® 2008 users that have administrator rights

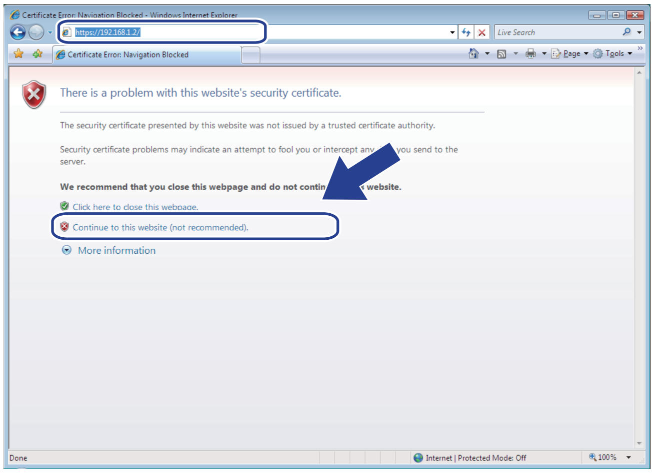
1. Click the button and **All Programs**.
2. Right-click **Internet Explorer**, and then click **Run as administrator**.



Note

If the **User Account Control** screen appears,
(Windows Vista®) Click **Continue (Allow)**.
(Windows® 7) Click **Yes**.

3 Type "`https://printer's IP address/`" into your browser to access your machine (where "`printer's IP address`" is the printer's IP address or the node name that you assigned for the certificate).
Then, click **Continue to this website (not recommended).**.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.1.2/
Live Search
Certificate Error: Navigation Blocked
Page
Tools
Done
Internet | Protected Mode: Off
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any you send to the server.

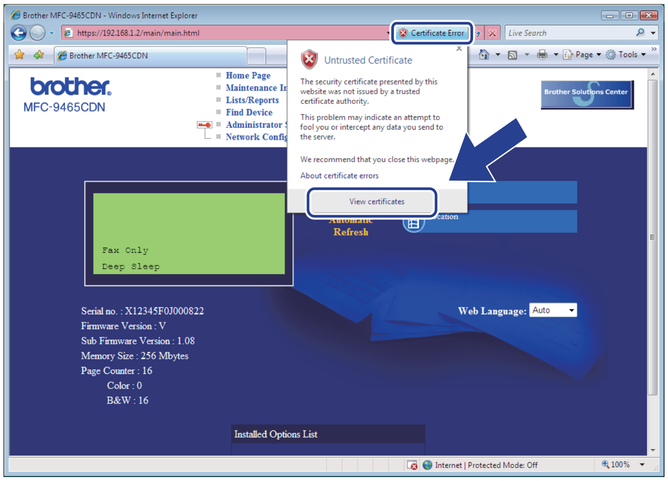
We recommend that you close this webpage and do not contin s website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

4 Click **Certificate Error**, and then click **View certificates**. For the rest of the instructions, follow the steps from step ❹ in *For Windows® 2000/XP and Windows Server® 2003 users* on page 44.



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

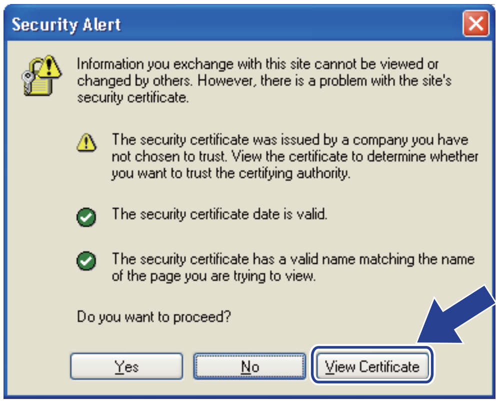
Serial no. : X12345F0J000822
Firmware Version : V
Sub Firmware Version : 1.08
Memory Size : 256 Mbytes
Page Counter : 16
Color : 0
B&W : 16

For Windows® 2000/XP and Windows Server® 2003 users

1. Start your web browser.

2. Type "`https://printer's IP address/`" into your browser to access your machine (where "`printer's IP address`" is the IP address or the node name that you assigned for the certificate).

3. When the following dialog appears, click **View Certificate**.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

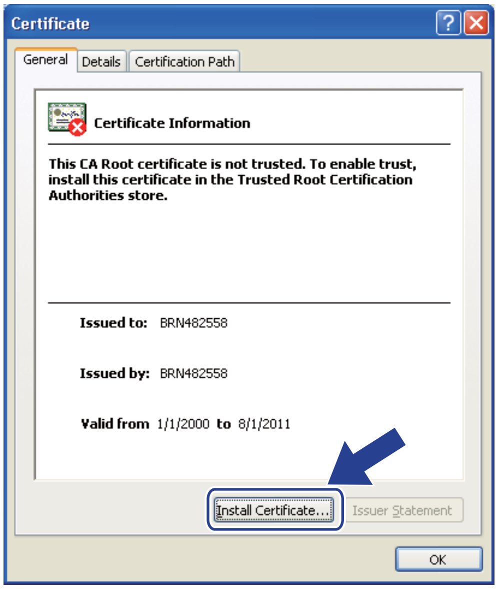
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

4. Click **Install Certificate...** from the **General** tab.



Certificate

Certificate Information

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

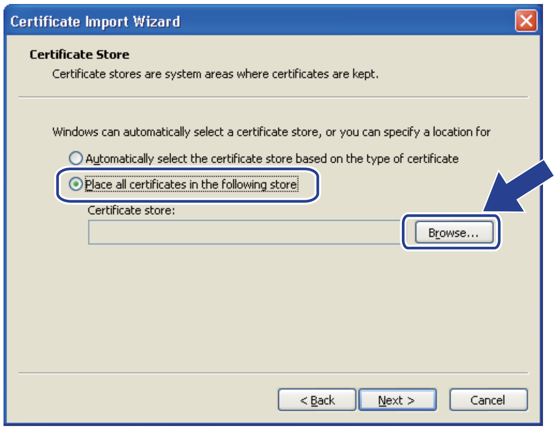
Issued to: BRN482558

Issued by: BRN482558

Valid from 1/1/2000 to 8/1/2011

5. When the **Certificate Import Wizard** appears, click **Next**.

6 Choose **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.

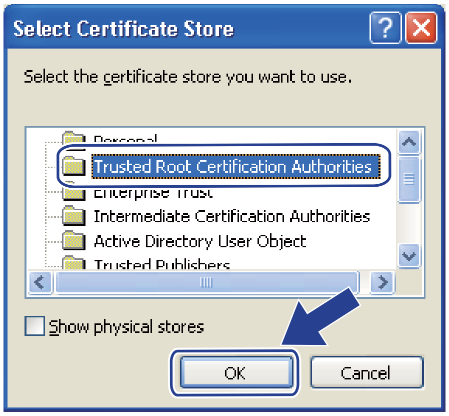
Windows can automatically select a certificate store, or you can specify a location for

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

● Place all certificates in the following store

Certificate store:

7 Choose **Trusted Root Certification Authorities** and then click **OK**.



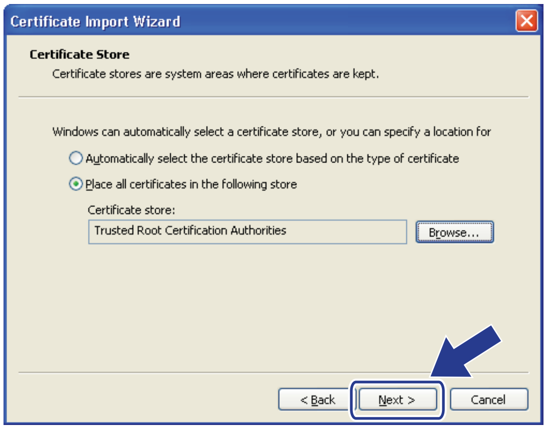
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

8 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

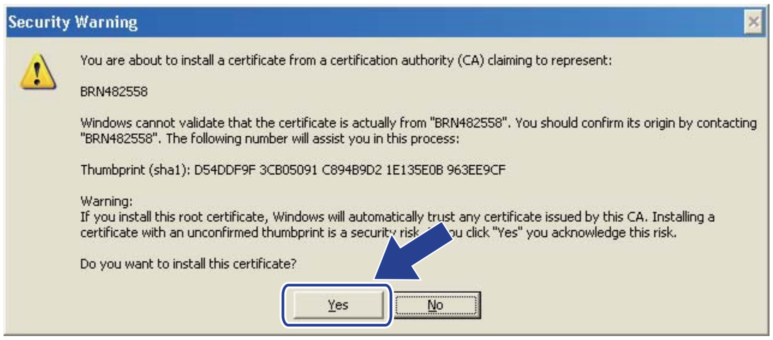
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

9 Click **Finish**.

10 Click **Yes**, if the fingerprint (thumbprint) is correct.



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

BRN482558

Windows cannot validate that the certificate is actually from "BRN482558". You should confirm its origin by contacting "BRN482558". The following number will assist you in this process:

Thumbprint (sha1): D54DDF9F 3CB05091 C894B9D2 1E135E0B 963EE9CF

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?

Note

The fingerprint (thumbprint) is printed on the Network Configuration List. (To learn how to print the Network Configuration List, see *Printing the Network Configuration List* on page 12.)

11 Click **OK**.

12 The self-signed certificate is now installed on your computer, and SSL/TLS communication is available.

How to create a CSR

1 Click **Create CSR** on the **Configure Certificate** page.

2 Enter a **Common Name** and your information, such as **Organization**. Then click **Submit**.

Note

- We recommend that the Root Certificate from the CA be installed on your computer before creating the CSR.
- The length of the **Common Name** is less than 64 bytes. Enter an identifier such as an IP address, node name or domain name to use when accessing this printer through SSL/TLS communication. The node name is displayed by default. The **Common Name** is required.
- A warning will pop-up if you enter a different name in the URL than the Common Name that was used for the certificate.
- The length of the **Organization**, the **Organization Unit**, the **City/Locality** and the **State/Province** is less than 64 bytes.
- The **Country/Region** should be an ISO 3166 country code composed of two characters.
- If you are configuring X.509v3 certificate extension, choose the **Configure extended partition** check box and then choose **Auto** or **Manual**.

3 When the contents of the CSR appear, click **Save** to save the CSR file to your computer.

4 The CSR is created.

Note

- Follow your CA policy regarding the method to send a CSR to your CA.
- If you are using Enterprise root CA of Windows Server® 2003/2008, we recommend using the **Web Server** for the certificate template when creating the Client Certificate for secure management. If you are creating a Client Certificate for an IEEE 802.1x environment with EAP-TLS authentication, we recommend using **User** for the certificate template. For more information, see the SSL communication page from the top page for your model at http://solutions.brother.com/.

How to install the certificate to your machine

When you receive the certificate from a CA, follow the steps below to install it into the print server.

Note

Only a certificate issued with this machine’s CSR can be installed. When you want to create another CSR, make sure that the certificate is installed before creating another CSR. Create another CSR after installing the certificate to the machine. Otherwise the CSR you have made before installing will be invalid.

1. Click **Install Certificate** on the **Configure Certificate** page.
2. Specify the file of the certificate that has been issued by a CA, and then click **Submit**.
3. Now the certificate is created and saved in your machine memory successfully.
   To use SSL/TLS communication, the Root Certificate from the CA needs to be installed on your computer. Contact your network administrator about installation.

Import and export the certificate and private key

You can store the certificate and private key on the machine and manage them by importing and exporting.

How to import the self-signed certificate, the certificate issued by a CA, and the private key

1. Click **Import Certificate and Private Key** on the **Configure Certificate** page.
2. Specify the file that you want to import.
3. Enter the password if the file is encrypted, and then click **Submit**.
4. Now the certificate and private key are imported to your machine successfully.
   To use SSL/TLS communication, the Root Certificate from the CA needs to also be installed on your computer. Contact your network administrator about the installation.

How to export the self-signed certificate, the certificate issued by a CA, and the private key

1. Click **Export** shown with **Certificate List** on the **Configure Certificate** page.
2. Enter the password if you want to encrypt the file.

Note

If a blank password is used, the output is not encrypted.

3. Enter the password again for confirmation, and then click **Submit**.
4. Specify the location where you want to save the file.
5. Now the certificate and private key are exported to your computer.

Note

You can import the file that you exported.

Managing multiple certificates

This multiple certificate feature allows you to manage each certificate that you have installed using Web Based Management. After installing certificates, you can view what certificates are installed from the **Configure Certificate** page and then view each certificate's content, delete or export the certificate. For information on how to access the **Configure Certificate** page, see *Configure certificate using Web Based Management* on page 40. The Brother machine allows you to store up to four self-signed certificates or up to four certificates issued by a CA. You can use the stored certificates for using the HTTPS/IPPS protocol, IEEE 802.1x authentication or a Signed PDF.

You can also store up to four CA certificates for using IEEE 802.1x authentication and SSL for SMTP/POP3.

We recommend you store one certificate less and keep the last free to deal with certificate expiration. For example, if you want to store a CA certificate, store three certificates and leave one storage as a backup. In the case of re-issuing the certificate, such as when the certificate is expired, you can import a new certificate to the backup and then you can delete the expired certificate, to avoid configuration failure.

Note

When you use HTTPS/IPPS, IEEE 802.1x or Signed PDF, you must choose which certificate you are using.

Import and export a CA certificate

You can store a CA certificate on the machine by importing and exporting.

How to import a CA certificate

1. Click **Configure CA Certificate** on the **Configure Certificate** page.
2. Click **Import CA Certificate**. Click **Submit**.

How to export a CA certificate

1. Click **Configure CA Certificate** on the **Configure Certificate** page.
2. Choose the certificate you want to export and click **Export**. Click **Submit**.

6 Troubleshooting

Overview

This chapter explains how to resolve typical network problems you may encounter when using Brother machine. If, after reading this chapter, you are unable to resolve your problem, please visit the Brother Solutions Center at: http://solutions.brother.com/.

Please go to the Brother Solutions Center at http://solutions.brother.com/ and click Manuals on your model page to download the other manuals.

Identifying your problem

Make sure that the following items are configured before reading this chapter.

First check the following:
The power cord is connected properly and the Brother machine is turned on.
All protective packaging has been removed from the machine.
The toner cartridges and drum unit are installed properly.
The front and back covers are fully closed.
Paper is inserted properly in the paper tray.
A network cable is securely connected to the Brother machine and the router or hub.

Go to the page for your solution from the lists below

- The Brother machine is not found on the network during the MFL-Pro Suite installation. (See page 50.)
- The Brother machine cannot print or scan over the network. (See page 51.)
- The Brother machine is not found on the network even after successful installation. (See page 51.)
- I'm using security software. (See page 53.)
- I want to check my network devices are working properly. (See page 54.)

Brother machine is not found on the network during the MFL-Pro Suite installation.

Question	Interface	Solution
Are you using security software?	wired	■ Choose to search for Brother machine again on the installer dialog. ■ Allow access when the alert message of the security software appears during the MFL-Pro Suite installation. ■ For more information about security software, see *I'm using security software.* on page 53.

Brother machine cannot print or scan over the network.
Brother machine is not found on the network even after the successful installation.

Question	Interface	Solution
Are you using security software?	wired	See *I'm using security software.* on page 53.
Is your Brother machine assigned with an available IP address?	wired	■ Confirm the IP address and the Subnet Mask Verify that both the IP addresses and Subnet Masks of your computer and the Brother machine are correct and located on the same network. For more information on how to verify the IP address and the Subnet Mask, ask the network administrator or visit the Brother Solutions Center at http://solutions.brother.com/. ■ (Windows®) Confirm the IP address and the Subnet Mask using the Network Connection Repair Tool. Use the Network Connection Repair Tool to fix the Brother machine's network settings. It will assign the correct IP address and the Subnet Mask. To use the Network Connection Repair Tool, ask the network administrator for the details and then follow the steps below: **Note** • (Windows® 2000 Professional/XP/XP Professional x64 Edition/Windows Vista®/Windows® 7) You must log on with Administrator rights. • Make sure that the Brother machine is turned on and is network-connected to your computer.

Brother machine cannot print or scan over the network.
Brother machine is not found on the network even after the successful installation. (continued)

Question	Interface	Solution
Is your Brother machine assigned with an available IP address? (continued)	wired	1 (Windows® 2000/XP, Windows Server® 2003/2008) Click the **Start** button, **All Programs** (**Programs** for Windows® 2000), **Accessories** and **Windows Explorer**, and then **My computer**. (Windows Vista®/Windows® 7) Click the ⊞ button and **Computer**. 2 Double-click **Local Disk (C:)**, **Program Files** or **Program Files (x86)** for 64-bit OS users, **Browny02**, **Brother**, **BrotherNetTool.exe** to run the program. **Note** If the **User Account Control** screen appears, (Windows Vista®) Click **Continue**. (Windows® 7) Click **Yes**. 3 Follow the on screen instructions. 4 Check the diagnosis by printing the Network Configuration List. **Note** The Network Connection Repair Tool will start automatically if you check the **Enable Network Connection Repair Tool** box using Status Monitor. Right-click on the Status Monitor screen, click **Options**, **Details** and then click the **Diagnostic** tab. This is not recommended when your network administrator has set the IP address to static, since it will automatically change the IP address. If the correct IP address and the Subnet mask are still not assigned even after using the Network Connection Repair Tool, ask the network administrator for this information, or visit the Brother Solutions Center at http://solutions.brother.com/.

Brother machine cannot print or scan over the network.
Brother machine is not found on the network even after the successful installation. (continued)

Question	Interface	Solution
Did your previous printing job fail?	wired	■ If the failed printing job is still in the print queue of your computer, delete it. ■ Double-click the printer icon in the following folder and then choose the **Cancel All Documents** in the **Printer** menu: (Windows® 2000) **Start**, **Settings** and then **Printers**. (Windows® XP) **Start** and **Printers and Faxes**. (Windows Vista®) ⊞, **Control Panel**, **Hardware and Sound** and then **Printers**. (Windows® 7) Click the ⊞ button and then **Devices and Printers**.
I have checked and tried all of above, however the Brother machine does not print/scan. Is there anything else I can do?	wired	Uninstall the MFL-Pro Suite and reinstall it.

I'm using security software.

Question	Interface	Solution
Did you choose to accept the security alert dialog during the MFL-Pro Suite installation, applications' start-up process or when using the printing/scanning features?	wired	If you did not choose to accept the security alert dialog, the firewall function of your security software may be rejecting access. Some security software might block access without showing a security alert dialog. To allow access, see the instructions of your security software or ask the manufacturer.
I want to know the necessary port number for the security software settings.	wired	The following port numbers are used for Brother network features: ■ Network scanning → Port number 54925 / Protocol UDP ■ PC-FAX RX → Port number 54926 / Protocol UDP ■ Network scanning/printing, PC-FAX RX, Remote Setup → Port number 137 / Protocol UDP ■ BRAdmin Light → Port number 161 / Protocol UDP For details on how to open the port, see the instructions of the security software or ask the manufacturer.

I want to check my network devices are working properly.

Question	Interface	Solution
Is your Brother machine, access point/router or network hub turned on?	wired	Make sure you have confirmed all instructions in *First check the following:* on page 50.
Where can I find Brother machine's network settings, such as IP address?	wired	Print the Network Configuration List. See *Printing the Network Configuration List* on page 12.
How can I check the link status of Brother machine?	wired	Print the Network Configuration List and check that **Ethernet Link Status** is **Link OK**. If the **Link Status** shows **Link DOWN**, start over again from the *First check the following:* on page 50.
Can you “ping” Brother machine from your computer?	wired	Ping the Brother machine from your computer using the IP address or the node name. ■ Successful → Your Brother machine is working correctly and connected to the same network as your computer. ■ Unsuccessful → Your Brother machine is not connected to the same network as your computer. (Windows®) Ask the network administrator and use the Network Connection Repair Tool to fix the IP address and the subnet mask automatically. For the detail of the Network Connection Repair Tool, see *(Windows®) Confirm the IP address and the Subnet Mask using the Network Connection Repair Tool.* in *Is your Brother machine assigned with an available IP address?* on page 51. (Macintosh) Confirm the IP address and the Subnet Mask are set correctly. See *Confirm the IP address and the Subnet Mask* in *Is your Brother machine assigned with an available IP address?* on page 51.

A Appendix A

Supported protocols and security features

Interface	Ethernet	10/100BASE-TX
Network (common)	Protocol (IPv4)	ARP, RARP, BOOTP, DHCP, APIPA (Auto IP), WINS/NetBIOS name resolution, DNS Resolver, mDNS, LLMNR responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP Client and Server, TELNET Server, HTTP/HTTPS server, TFTP client and server, SMTP Client, SNMPv1/v2c/v3, ICMP, LLTD responder, Web Services (Print), CIFS client, SNTP client
	Protocol (IPv6)	NDP, RA, DNS resolver, mDNS, LLMNR responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP Client and Server, TELNET Server, HTTP/HTTPS server, TFTP client and server, SMTP Client, SNMPv1/v2c/v3, ICMPv6, LLTD responder, Web Services (Print), CIFS Client, SNTP Client
Network (Security)	Wired	APOP, POP before SMTP, SMTP-AUTH, SSL/TLS (IPPS, HTTPS, SMTP, POP), SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos

B

Index

Network Glossary

In this Network Glossary, you will find basic information about advanced network features of Brother machines along general networking and common terms.

The supported protocols and the network features differ depending on the model you are using. To find what features and network protocols are supported, see the *Network User's Guide* we have provided. To download the latest manual, please visit the Brother Solutions Center at (http://solutions.brother.com/).

You can also download the latest drivers and utilities for your machine, read FAQs and troubleshooting tips or learn about special printing solutions from the Brother Solutions Center.

Version 0

ENG

Definitions of notes

We use the following icon throughout this User's Guide:

Note	Notes tell you how you should respond to a situation that may arise or give tips about how the operation works with other features.

IMPORTANT NOTE

- Your product is approved for use in the country of purchase only. Do not use this product outside the country of purchase as it may violate the wireless telecommunication and power regulations of that country.
- Windows® XP in this document represents Windows® XP Professional, Windows® XP Professional x64 Edition and Windows® XP Home Edition.
- Windows Server® 2003 in this document represents Windows Server® 2003 and Windows Server® 2003 x64 Edition.
- Windows Server® 2008 in this document represents Windows Server® 2008 and Windows Server® 2008 R2.
- Windows Vista® in this document represents all editions of Windows Vista®.
- Windows® 7 in this document represents all editions of Windows® 7.
- Please go to the Brother Solutions Center at http://solutions.brother.com/ and click Manuals on your model page to download the other manuals.

Table of Contents

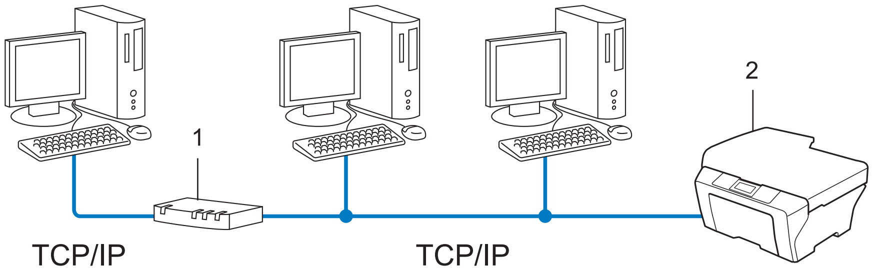
1 Types of network connections and protocols

Types of network connections

Wired network connection example

Peer-to-Peer printing using TCP/IP

In a Peer-to-Peer environment, each computer directly sends and receives data to each device. There is no central server controlling file access or machine sharing.



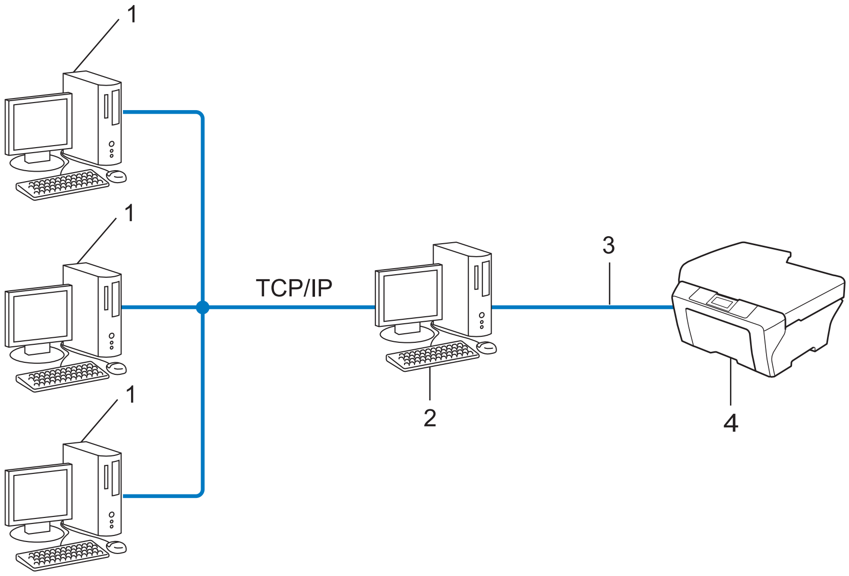
1 Router

2 Network machine (your machine)

- In a smaller network of 2 or 3 computers, we recommend the Peer-to-Peer printing method as it is easier to configure than the Network Shared printing method. See *Network Shared printing* on page 2.
- Each computer must use the TCP/IP Protocol.
- The Brother machine needs an appropriate IP address configuration.
- If you are using a router, the Gateway address must be configured on the computers and the Brother machine.

Network Shared printing

In a Network Shared environment, each computer sends data via a centrally controlled computer. This type of computer is often called a “Server” or a “Print Server”. Its job is to control the printing of all print jobs.



1 Client computer

2 Also known as “Server” or “Print server”

3 TCP/IP, USB or parallel (where available)

4 Network machine (your machine)

- In a larger network, we recommend a Network Shared printing environment.
- The “server” or the “print server” must use the TCP/IP print protocol.
- The Brother machine needs to have an appropriate IP address configuration unless the machine is connected via the USB or the parallel interface at the server.

Protocols

TCP/IP protocols and functions

Protocols are the standardized sets of rules for transmitting data on a network. Protocols allow users to gain access to network connected resources.

The print server used on the Brother machine supports the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol.

TCP/IP is the most popular set of protocols used for communication such as Internet and E-mail. This protocol can be used in almost all operating systems such as Windows®, Windows Server®, Mac OS X and Linux®. The following TCP/IP protocols are available on the Brother machine.

Note

- You can configure the protocol settings by using the HTTP interface (web browser). (See the *Network User's Guide*.)
- To find what protocols your Brother machine supports, see the *Network User's Guide*.
- For information about supported security protocols, see *Security protocols* on page 19.

DHCP/BOOTP/RARP

By using the DHCP/BOOTP/RARP protocols, the IP address can be automatically configured.

Note

To use the DHCP/BOOTP/RARP protocols, please contact your network administrator.

APIPA

If you do not assign an IP address manually (using the control panel (for LCD models) of the machine or the BRAdmin software) or automatically (using a DHCP/BOOTP/RARP server), the Automatic Private IP Addressing (APIPA) protocol will automatically assign an IP address from the range 169.254.1.0 to 169.254.254.255.

ARP

Address Resolution Protocol performs mapping of an IP address to MAC address in a TCP/IP network.

DNS client

The Brother print server supports the Domain Name System (DNS) client function. This function allows the print server to communicate with other devices by using its DNS name.

NetBIOS name resolution

Network Basic Input/Output System name resolution enables you to obtain the IP address of the other device using its NetBIOS name during the network connection.

WINS

Windows Internet Name Service is an information providing service for the NetBIOS name resolution by consolidating an IP address and a NetBIOS name that is in the local network.

LPR/LPD

Commonly used printing protocols on a TCP/IP network.

SMTP client

Simple Mail Transfer Protocol (SMTP) client is used to send E-mails via the Internet or Intranet.

Custom Raw Port (Default is Port 9100)

Another commonly used printing protocol on a TCP/IP network. It enables interactive data transmission.

IPP

The Internet Printing Protocol (IPP Version 1.0) allows you to print documents directly to any accessible machine via the internet.

Note

For the IPPS protocol, see *Security protocols* on page 19.

mDNS

mDNS allows the Brother print server to automatically configure itself to work in a Mac OS X Simple Network Configured system.

TELNET

The TELNET protocol allows you to control the remote network devices on a TCP/IP network from your computer.

SNMP

The Simple Network Management Protocol (SNMP) is used to manage network devices including computers, routers and Brother network ready machines. The Brother print server supports SNMPv1, SNMPv2c and SNMPv3.

Note

For the SNMPv3 protocol, see *Security protocols* on page 19.

LLMNR

The Link-Local Multicast Name Resolution protocol (LLMNR) resolves the names of neighboring computers, if the network does not have a Domain Name System (DNS) server. The LLMNR Responder function works in both the IPv4 or IPv6 environment when using a computer that has the LLMNR Sender function such as Windows Vista® and Windows® 7.

Web Services

The Web Services protocol enables Windows Vista® or Windows® 7 users to install the Brother printer driver by right-clicking the machine icon from the **Network** folder. (See *Network printing Installation when using Web Services (Windows Vista® and Windows® 7)* on page 15.) The Web Services also lets you check the current status of the machine from your computer.

HTTP

The HTTP protocol is used to transmit the data between a web server and a web browser.

Note

For the HTTPS protocol, see *Security protocols* on page 19.

FTP (For the Scan to FTP feature)

The File Transfer Protocol (FTP) allows the Brother machine to scan black and white or color documents directly to an FTP server located locally on your network or on the internet.

SNTP

The Simple Network Time Protocol is used to synchronize computer clocks on a TCP/IP network. You can configure the SNTP settings using Web Based Management (web browser). (For the details, see the *Network User's Guide*.)

CIFS

The Common Internet File System is the standard way that computer users share files and printers in Windows®.

LDAP

The Lightweight Directory Access Protocol (LDAP) allows the Brother machine to search for information such as fax numbers and E-mail addresses from an LDAP server.

IPv6

IPv6 is the next generation internet protocol. For more information on the IPv6 protocol, visit the model page for the machine you are using at http://solutions.brother.com/.

Other protocol

LLTD

The Link Layer Topology Discovery protocol (LLTD) lets you locate the Brother machine easily on the Windows Vista®/Windows® 7 **Network Map**. Your Brother machine will be shown with a distinctive icon and the node name. The default setting for this protocol is Off. You can activate LLTD using Web Based Management (web browser) (See the *Network User's Guide*.), and the BRAdmin Professional 3 utility software. Visit the download page for your model at http://solutions.brother.com/ to download BRAdmin Professional 3.

2 Configuring your machine for a network

IP addresses, subnet masks and gateways

To use the machine in a networked TCP/IP environment, you need to configure its IP address and subnet mask. The IP address you assign to the print server must be on the same logical network as your host computers. If it is not, you must properly configure the subnet mask and the gateway address.

IP address

An IP address is a series of numbers that identifies each device connected to a network. An IP address consists of four numbers separated by dots. Each number is between 0 and 255.

- Example: In a small network, you would normally change the final number.
  - `192.168.1.1`
  - `192.168.1.2`
  - `192.168.1.3`

How the IP address is assigned to your print server:

If you have a DHCP/BOOTP/RARP server in your network the print server will automatically obtain its IP address from that server.

Note

On smaller networks, the DHCP server may also be the Router.

For more information on DHCP, BOOTP and RARP, see:
Using DHCP to configure the IP address on page 21.
Using BOOTP to configure the IP address on page 23.
Using RARP to configure the IP address on page 22.

If you do not have a DHCP/BOOTP/RARP server, the Automatic Private IP Addressing (APIPA) protocol will automatically assign an IP address from the range 169.254.1.0 to 169.254.254.255. For more information on APIPA, see *Using APIPA to configure the IP address* on page 23.

Subnet mask

Subnet masks restrict network communication.

- Example: Computer 1 can talk to Computer 2
  - Computer 1

    IP Address: 192.168. 1. 2

    Subnet Mask: 255.255.255.000
  - Computer 2

    IP Address: 192.168. 1. 3

    Subnet Mask: 255.255.255.000

Where the 0 is in the Subnet mask, there is no limit to communication at this part of the address. What this means in the above example is, we can communicate with any device that has an IP address that begins with 192.168.1.x. (where x. are numbers between 0 and 255).

Gateway (and router)

A gateway is a network point that acts as an entrance to another network and sends data transmitted via the network to an exact destination. The router knows where to direct data that arrives at the gateway. If a destination is located on an external network, the router transmits data to the external network. If your network communicates with other networks, you may need to configure the Gateway IP address. If you do not know the Gateway IP address then contact your Network Administrator.

IEEE 802.1x Authentication

IEEE 802.1x is an IEEE standard for wired and wireless network that limits an access from unauthorized network devices. Your Brother machine (supplicant) sends an authentication request to a RADIUS server (Authentication server) through your access point (Authenticator). After your request has been verified by the RADIUS server, your machine can have an access to the network.

Authentication methods

- LEAP (For wireless network)

  Cisco LEAP (Light Extensible Authentication Protocol) has been developed by Cisco Systems, Inc. which uses a user ID and password for authentication.

- EAP-FAST

  EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunnel) has been developed by Cisco Systems, Inc. which uses a user ID and password for authentication, and symmetric key algorithms to achieve a tunneled authentication process.

  The Brother machine supports the following inner authentications:

  - EAP-FAST/NONE
  - EAP-FAST/MS-CHAPv2
  - EAP-FAST/GTC

- EAP-MD5 (For wired network)

  EAP-MD5 (Extensible Authentication Protocol-Message digest algorithm 5) uses a user ID and password for challenge-response authentication.

- PEAP

  PEAP (Protected Extensible Authentication Protocol) has been developed by Microsoft Corporation, Cisco Systems and RSA Security. PEAP creates an encrypt SSL (Secure Sockets Layer)/TLS (Transport Layer Security) tunnel between a client and an authentication server, for sending a user ID and password. PEAP provides mutual authentication between the server and the client.

  The Brother machine supports the following inner authentications:

  - PEAP/MS-CHAPv2
  - PEAP/GTC

- EAP-TTLS

  EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) has been developed by Funk Software and Certicom. EAP-TTLS creates a similar encrypt SSL tunnel to PEAP, between a client and an authentication server, for sending a user ID and password. EAP-TTLS provides mutual authentication between the server and the client.

  The Brother machine supports the following inner authentications:

  - EAP-TTLS/CHAP
  - EAP-TTLS/MS-CHAP
  - EAP-TTLS/MS-CHAPv2
  - EAP-TTLS/PAP

- EAP-TLS

  EAP-TLS (Extensible Authentication Protocol Transport Layer Security) requires digital certificate authentication both at a client and an authentication server.

3 Wireless network terms and concepts

Specifying your network

SSID (Service Set Identifier) and channels

You need to configure the SSID and a channel to specify the wireless network you want to connect to.

- SSID

  Each wireless network has its own unique network name and it is technically referred to as SSID or ESSID (Extended Service Set Identifier). The SSID is a 32-byte or less value and is assigned to the access point. The wireless network devices you want to associate to the wireless network should match the access point. The access point and wireless network devices regularly send wireless packets (referred to as a beacon) which has the SSID information. When your wireless network device receives a beacon, you can identify the wireless network that is close enough for the radio waves to reach your device.

- Channels

  Wireless networks use channels. Each wireless channel is on a different frequency. There are up to 14 different channels that can be used when using a wireless network. However, in many countries the number of channels available are restricted.

Security terms

Authentication and encryption

Most wireless networks use some kind of security settings. These security settings define the authentication (how the device identifies itself to the network) and encryption (how the data is encrypted as it is sent on the network). **If you do not correctly specify these options when you are configuring your Brother wireless machine, it will not be able to connect to the wireless network.** Therefore care must be taken when configuring these options. Please refer to the information in the *Network User's Guide* to see which authentication and encryption methods your Brother wireless machine supports.

Authentication and Encryption methods for a personal wireless network

Personal wireless network is a small network, for example using your machine in a wireless network at home, without IEEE 802.1x support.

If you want to use your machine in an IEEE 802.1x supported wireless network, see *Authentication and Encryption methods for an enterprise wireless network* on page 13.

Authentication methods

- Open system

  Wireless devices are allowed to access the network without any authentication.

- Shared key

  A secret pre-determined key is shared by all devices that will access the wireless network.

  The Brother wireless machine uses the WEP key as the pre-determined key.

- WPA-PSK/WPA2-PSK

  Enables a Wi-Fi Protected Access Pre-shared key (WPA-PSK/WPA2-PSK), which enables the Brother wireless machine to associate with access points using TKIP for WPA-PSK or AES for WPA-PSK and WPA2-PSK (WPA-Personal).

Encryption methods

- None

  No encryption method is used.

- WEP

  By using WEP (Wired Equivalent Privacy), the data is transmitted and received with a secure key.

- TKIP

  TKIP (Temporal Key Integrity Protocol) provides per-packet key mixing a message integrity check and rekeying mechanism.

- AES

  AES (Advanced Encryption Standard) is the Wi-Fi® authorized strong encryption standard.

Network key

- Open system/Shared key with WEP

  This key is a 64-bit or 128-bit value that must be entered in an ASCII or hexadecimal format.

  - 64 (40) bit ASCII:

    Uses 5 text characters. e.g. “WSLAN” (this is case sensitive).

  - 64 (40) bit hexadecimal:

    Uses 10 digits of hexadecimal data. e.g. “71f2234aba”

  - 128 (104) bit ASCII:

    Uses 13 text characters. e.g. “Wirelesscomms” (this is case sensitive)

  - 128 (104) bit hexadecimal:

    Uses 26 digits of hexadecimal data. e.g. “71f2234ab56cd709e5412aa2ba”

- WPA-PSK/WPA2-PSK and TKIP or AES

  Uses a Pre-Shared Key (PSK) that is 8 or more characters in length, up to a maximum of 63 characters.

Authentication and Encryption methods for an enterprise wireless network

Enterprise wireless network is a large network, for example using your machine in a business enterprise wireless network, with IEEE 802.1x support. If you configure your machine in an IEEE 802.1x supported wireless network, you can use following authentication and encryption methods.

Authentication methods

- LEAP

  For LEAP, see *LEAP (For wireless network)* on page 9.

- EAP-FAST

  For EAP-FAST, see *EAP-FAST* on page 9.

- PEAP

  For PEAP, see *PEAP* on page 9.

- EAP-TTLS

  For EAP-TTLS, see *EAP-TTLS* on page 10.

- EAP-TLS

  For EAP-TLS, see *EAP-TLS* on page 10.

Encryption methods

- TKIP

  For TKIP, see *TKIP* on page 12.

- AES

  For AES, see *AES* on page 12.

- CKIP

  The original Key Integrity Protocol for LEAP by Cisco Systems, Inc.

User ID and password

The following security methods use the user ID less than 64 characters and the password less than 32 characters in length.

- LEAP
- EAP-FAST
- PEAP
- EAP-TTLS
- EAP-TLS (For user ID)

4 Additional network settings from Windows®

Types of additional network settings

Following features are available to use if you want to configure additional network settings.

- Web Services (Windows Vista® and Windows® 7)
- Vertical Paring (Windows® 7)

Note

Verify the host computer and the machine are either on the same subnet, or that the router is properly configured to pass data between the two devices.

Network printing Installation when using Web Services (Windows Vista® and Windows® 7)

The Web Services feature allows you to monitor its machine information which is connected to the network. This also enables the printer driver installation from the printer icon and the Web Services port (WSD port) will be made.

Note

- You must configure the IP address on your machine before you configure this setting.
- For Windows Server® 2008, you must install Print Services.
- Only printer support is installed with Web Services.

1. Insert the installation CD-ROM.
2. Choose your CD-ROM drive/**install**/**driver**/**gdi**/**32** or **64**.
3. Choose your language and then double-click **DPInst.exe**.

Note

If the **User Account Control** screen appears,

(Windows Vista®) Click **Allow**.

(Windows® 7) Click **Yes**.

4. (Windows Vista®)

   Click , then choose **Network**.

   (Windows® 7)

   Click , **Control Panel**, **Network and Internet**, and then **View network computers and devices**.

5. The machine’s Web Services Name will be shown with the printer icon. Right-click the machine you want to install.

Note

The Web Services Name for the Brother machine is your model name and the MAC Address (Ethernet Address) of your machine (e.g. Brother MFC-XXXX (model name) [XXXXXXXXXXXX] (MAC Address / Ethernet Address).

6. From the pull down menu, click **Install**.

Network printing installation for Infrastructure mode when using Vertical Pairing (Windows® 7)

Windows® Vertical Pairing is a technology to allow your Vertical Pairing supported wireless machine to connect to your Infrastructure network using the PIN Method of Wi-Fi Protected Setup and the Web Services feature. This also enables the printer driver installation from the printer icon that is in the **Add a device** screen.

If you are in Infrastructure mode, you can connect your machine to the wireless network and then install the printer driver using this feature. Follow the steps below:

Note

- If you have set your machine’s Web Services feature to Off, you must set back to On. The default setting of the Web Services for the Brother machine is On. You can change the Web Services setting by using the Web Based Management (web browser) or BRAdmin Professional 3.
- Make sure your WLAN access point/router includes the Windows® 7 compatibility logo. If you are not sure about the compatibility logo, contact your access point/router manufacturer.
- Make sure your computer includes Windows® 7 compatibility logo. If you are not sure about the compatibility logo, contact your computer manufacturer.
- If you are configuring wireless network using an external wireless NIC (Network Interface Card), make sure the wireless NIC includes Windows® 7 compatibility logo. For more information, contact your wireless NIC manufacturer.
- To use a Windows® 7 computer as a Registrar, you need to register it to your network in advance. See the instruction supplied with your WLAN access point/router.

1. Turn on your machine.
2. Set your machine in Wi-Fi Protected Setup (PIN Method).
   See Wi-Fi Protected Setup (PIN Method) wireless configuration in the *Network User's Guide*, on how to set your machine in the PIN Method.
3. Click the ⊞ button and then **Devices and Printers**.
4. Choose **Add a device** on the **Devices and Printers** dialog.
5. Choose your machine and input the PIN which your machine has indicated.
6. Choose the Infrastructure network that you want to connect to, and then click **Next**.
7. When your machine appears in the **Devices and Printers** dialog, the wireless configuration and the printer driver installation are successfully completed.

5 Security terms and concepts

Security features

Security terms

- CA (Certificate Authority)

  A CA is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

- CSR (Certificate Signing Request)

  A CSR is a message sent from an applicant to a CA in order to apply for issue of a certificate. The CSR contains information identifying the applicant, the public key generated by the applicant and the digital signature of the applicant.

- Certificate

  A Certificate is the information that binds together a public key with an identity. The certificate can be used to verify that a public key belongs to an individual. The format is defined by the x.509 standard.

- CA Certificate

  A CA Certificate is the certification that identifies the CA (Certificate Authority) itself and owns its private key. It verifies a certificate issued by the CA.

- Digital signature

  A Digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

- Public key cryptosystem

  A Public key cryptosystem is a modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

- Shared key cryptosystem

  A Shared key cryptosystem is a branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption).

Security protocols

Note

You can configure the protocol settings using Web Based Management (web browser). For the details, see the *Network User's Guide*.

SSL (Secure Socket Layer) / TLS (Transport Layer Security)

These security communication protocols encrypt data to prevent security threats.

HTTPS

The internet protocol that the Hyper Text Transfer Protocol (HTTP) uses SSL.

IPPS

The printing protocol that the Internet Printing Protocol (IPP Version 1.0) uses SSL.

SNMPv3

The Simple Network Management Protocol version 3 (SNMPv3) provides user authentication and data encryption to manage network devices securely.

Security methods for E-mail Sending and Receiving

Note

You can configure the security methods settings using Web Based Management (web browser). For the details, see the *Network User's Guide*.

POP before SMTP (PbS)

The user authentication method for sending E-mail from a client. The client is given permission to use the SMTP server by accessing the POP3 server before sending the E-mail.

SMTP-AUTH (SMTP Authentication)

SMTP-AUTH expands SMTP (the Internet E-mail sending protocol) to include an authentication method that ensures the true identity of the sender is known.

APOP (Authenticated Post Office Protocol)

APOP expands POP3 (the Internet receiving protocol) to include an authentication method that encrypts the password when the client receives E-mail.

SMTP over SSL

SMTP over SSL feature enables sending encrypted E-mail using SSL.

POP over SSL

POP over SSL feature enables receiving encrypted E-mail using SSL.

A Appendix A

Using services

A service is a resource that can be accessed by computers that wish to print to the Brother print server. The Brother print server provides the following predefined services (do a SHOW SERVICE command in the Brother print server remote console to see a list of available services): Enter `HELP` at the command prompt for a list of supported commands.

Service (Example)	Definition
BINARY_P1	TCP/IP binary
TEXT_P1	TCP/IP text service (adds carriage return after each line feed)
PCL_P1	PCL service (switches PJL-compatible machine to PCL mode)
BRNxxxxxxxxxxxx	TCP/IP binary
BRNxxxxxxxxxxxx_AT	PostScript® service for Macintosh
POSTSCRIPT_P1	PostScript® service (switches PJL-compatible machine to PostScript® mode)

Where “xxxxxxxxxxxx” is your machine’s MAC Address (Ethernet Address).

Other ways to set the IP address (for advanced users and administrators)

Using DHCP to configure the IP address

The Dynamic Host Configuration Protocol (DHCP) is one of several automated mechanisms for IP address allocation. If you have a DHCP server in your network, the print server will automatically obtain its IP address from the DHCP server and register its name with any RFC 1001 and 1002-compliant dynamic name services.

Note

If you do not want your print server configured via DHCP, BOOTP or RARP, you must set the Boot Method to static so that the print server has a static IP address. This will prevent the print server from trying to obtain an IP address from any of these systems. To change the Boot Method, use the machine’s control panel Network menu (for LCD models), BRAdmin applications, Remote Setup or Web Based Management (web browser).

Using RARP to configure the IP address

The Brother print server's IP address can be configured using the Reverse ARP (RARP) facility on your host computer. This is done by editing the `/etc/ethers` file (if this file does not exist, you can create it) with an entry similar to the following:

`00:80:77:31:01:07    BRN008077310107` (or `BRW008077310107` for a wireless network)

Where the first entry is the MAC Address (Ethernet Address) of the print server and the second entry is the name of the print server (the name must be the same as the one you put in the `/etc/hosts` file).

If the RARP daemon is not already running, start it (depending on the system the command can be `rarpd`, `rarpd -a`, `in.rarpd -a` or something else; type `man rarpd` or refer to your system documentation for additional information). To verify that the RARP daemon is running on a Berkeley UNIX based system, type the following command:

```
ps -ax | grep -v grep | grep rarpd
```

For AT&T UNIX-based systems, type:

```
ps -ef | grep -v grep | grep rarpd
```

The Brother print server will get the IP address from the RARP daemon when the machine is powered on.

Using BOOTP to configure the IP address

BOOTP is an alternative to RARP that has the advantage of allowing configuration of the subnet mask and gateway. In order to use BOOTP to configure the IP address make sure that BOOTP is installed and running on your host computer (it should appear in the `/etc/services` file on your host as a real service; type `man bootpd` or refer to your system documentation for information). BOOTP is usually started up via the `/etc/inetd.conf` file, so you may need to enable it by removing the "#" in front of the bootp entry in that file. For example, a typical bootp entry in the /etc/inetd.conf file would be:

```
#bootp dgram udp wait /usr/etc/bootpd bootpd -i
```

Depending on the system, this entry might be called "bootps" instead of "bootp".

Note

In order to enable BOOTP, simply use an editor to delete the "#" (if there is no "#", then BOOTP is already enabled). Then edit the BOOTP configuration file (usually `/etc/bootptab`) and enter the name, network type (1 for Ethernet), MAC Address (Ethernet Address) and the IP address, subnet mask and gateway of the print server. Unfortunately, the exact format for doing this is not standardized, so you will need to refer to your system documentation to determine how to enter this information (many UNIX systems also have template examples in the bootptab file that you can use for reference). Some examples of typical `/etc/bootptab` entries include: ("BRN" below is "BRW" for a wireless network.)

```
BRN310107 1  00:80:77:31:01:07 192.168.1.2
```

and:

```
BRN310107:ht=ethernet:ha=008077310107:\ip=192.168.1.2:
```

Certain BOOTP host software implementations will not respond to BOOTP requests if you have not included a download filename in the configuration file. If this is the case, simply create a null file on the host and specify the name of this file and its path in the configuration file.

As with RARP, the print server will load its IP address from the BOOTP server when the machine is powered on.

Using APIPA to configure the IP address

The Brother print server supports the Automatic Private IP Addressing (APIPA) protocol. With APIPA, DHCP clients automatically configure an IP address and subnet mask when a DHCP server is not available. The device chooses it's own IP address in the range 169.254.1.0 through to 169.254.254.255. The subnet mask is automatically set to 255.255.0.0 and the gateway address is set to 0.0.0.0.

By default, the APIPA protocol is enabled. If you want to disable the APIPA protocol, you can disable it using control panel of the machine (for LCD models), BRAdmin Light or Web Based Management (web browser).

Using ARP to configure the IP address

If you are unable to use the BRAdmin application and your network does not use a DHCP server, you can also use the ARP command. The ARP command is available on Windows® systems that have TCP/IP installed as well as UNIX systems. To use ARP enter the following command at the command prompt:

```
arp -s ipaddress ethernetaddress
```

```
ping ipaddress
```

Where `ethernetaddress` is the MAC Address (Ethernet Address) of the print server and `ipaddress` is the IP address of the print server. For example:

- **Windows® systems**

  Windows® systems require the dash "-" character between each digit of the MAC Address (Ethernet Address).

  ```
  arp -s 192.168.1.2 00-80-77-31-01-07
  ```

  ```
  ping 192.168.1.2
  ```

- **UNIX/Linux systems**

  Typically, UNIX and Linux systems require the colon ":" character between each digit of the MAC Address (Ethernet Address).

  ```
  arp -s 192.168.1.2 00:80:77:31:01:07
  ```

  ```
  ping 192.168.1.2
  ```

Note

You must be on the same Ethernet segment (that is, there cannot be a router between the print server and operating system) to use the arp -s command.

If there is a router, you may use BOOTP or other methods described in this chapter to enter the IP address. If your administrator has configured the system to deliver IP addresses using BOOTP, DHCP or RARP your Brother print server can receive an IP address from any one of these IP address allocation systems. In which case, you will not need to use the ARP command. The ARP command only works once. For security reasons, once you have successfully configured the IP address of a Brother print server using the ARP command, you cannot use the ARP command again to change the address. The print server will ignore any attempts to do this. If you wish to change the IP address again, use a Web Based Management (web browser), TELNET (using the SET IP ADDRESS command) or factory reset the print server (which will then allow you to use the ARP command again).

Using the TELNET console to configure the IP address

You can also use the TELNET command to change the IP address.

TELNET is an effective method to change the machine’s IP address. But a valid IP address must already be programmed into the print server.

Type `TELNET <command line>` at the command prompt of the system prompt, where `<command line>` is the IP address of the print server. When you are connected, push the Return or Enter key to get the “#” prompt. Enter the password “**access**” (the password will not appear on the screen).

You will be prompted for a user name. Enter anything in response to this prompt.

You will then get the `Local>` prompt. Type `SET IP ADDRESS ipaddress`, where `ipaddress` is the desired IP address you wish to assign to the print server (check with your network administrator for the IP address to use). For example:

```
Local> SET IP ADDRESS 192.168.1.3
```

You will now need to set the subnet mask by typing `SET IP SUBNET subnet mask`, where `subnet mask` is the desired subnet mask you wish to assign to the print server (check with your network administrator for the subnet mask to use). For example:

```
Local> SET IP SUBNET 255.255.255.0
```

If you do not have any subnets, use one of the following default subnet masks:

255.0.0.0 for class A networks

255.255.0.0 for class B networks

255.255.255.0 for class C networks

The leftmost group of digits in your IP address can identify the type of network you have. The value of this group ranges from 1 through 127 for Class A networks (e.g., 13.27.7.1), 128 through 191 for Class B networks (e.g.,128.10.1.30), and 192 through 255 for Class C networks (e.g., 192.168.1.4).

If you have a gateway (router), enter its address with the command `SET IP ROUTER routeraddress`, where `routeraddress` is the desired IP address of the gateway you wish to assign to the print server. For example:

```
Local> SET IP ROUTER 192.168.1.4
```

Type `SET IP METHOD STATIC` to set the method of IP access configuration to static.

To verify that you have entered the IP information correctly, type `SHOW IP`.

Type `EXIT` or Ctrl-D (i.e., hold down the control key and type “D”) to end the remote console session.

B Index