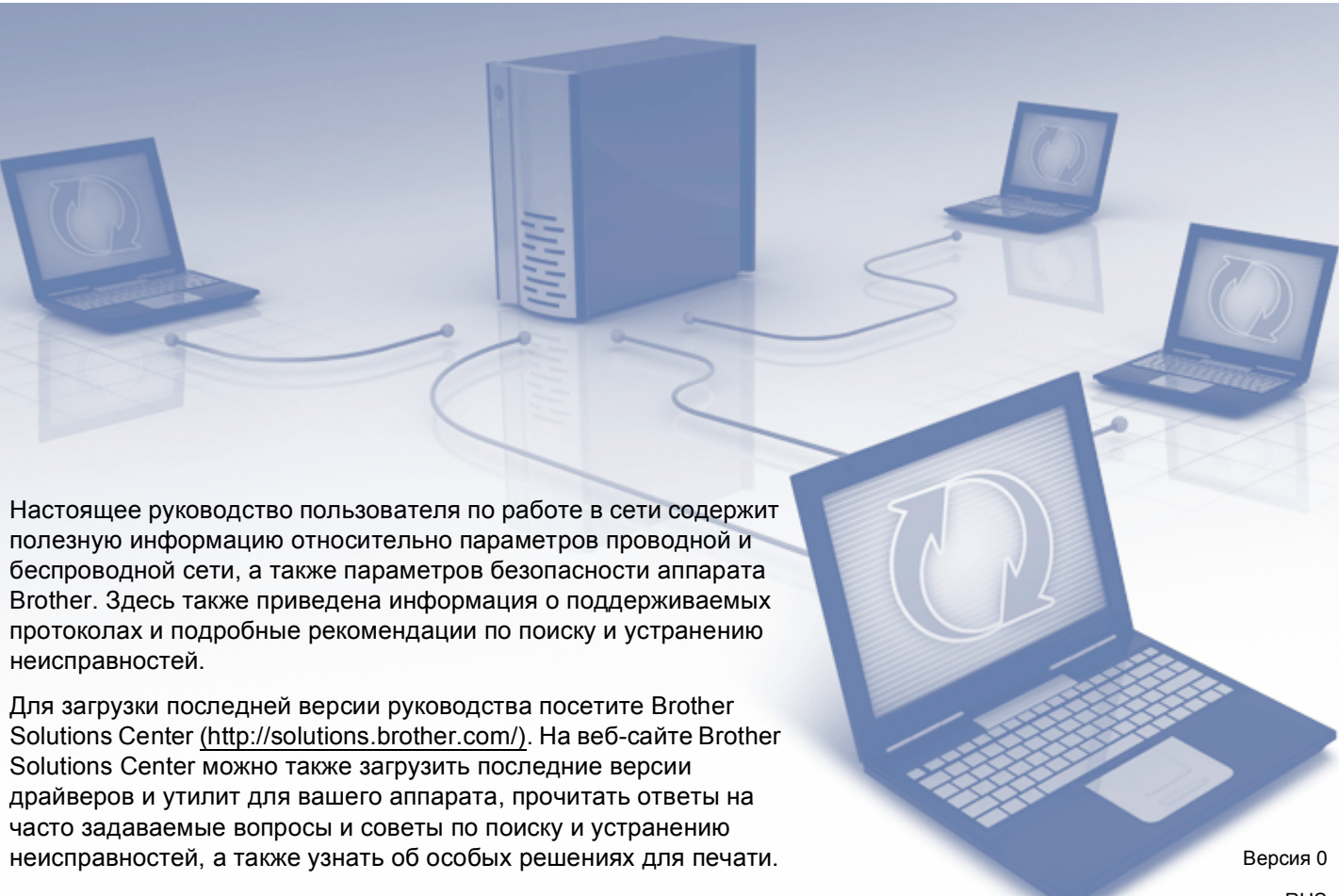


Руководство пользователя по работе в сети

Мультипротокольный сервер печати со встроенным Ethernet и беспроводной сервер печати

A blue-tinted illustration of a network setup. In the center is a server tower. To its left and right are several laptops. Cables connect the server to the laptops, representing a network configuration. The background is a light blue grid.

Настоящее руководство пользователя по работе в сети содержит полезную информацию относительно параметров проводной и беспроводной сети, а также параметров безопасности аппарата Brother. Здесь также приведена информация о поддерживаемых протоколах и подробные рекомендации по поиску и устранению неисправностей.

Для загрузки последней версии руководства посетите Brother Solutions Center (<http://solutions.brother.com/>). На веб-сайте Brother Solutions Center можно также загрузить последние версии драйверов и утилит для вашего аппарата, прочитать ответы на часто задаваемые вопросы и советы по поиску и устранению неисправностей, а также узнать об особых решениях для печати.

Модели, к которым относится данное руководство

Настоящее руководство пользователя относится к следующим моделям:

HL-3140CW/3150CDN/3150CDW/3170CDW

Обозначения примечаний

В настоящем руководстве пользователя используются следующие значки.

ВАЖНАЯ ИНФОРМАЦИЯ	ВАЖНАЯ ИНФОРМАЦИЯ указывает на потенциально опасную ситуацию, которая может привести к повреждению имущества или потере функциональности изделия.
ПРИМЕЧАНИЕ	В примечаниях содержатся инструкции на случай возникновения определенных ситуаций и советы о выполнении данной операции с другими параметрами.

ВАЖНОЕ ПРИМЕЧАНИЕ

- Данный продукт утвержден для использования только в стране покупки. Не используйте данный продукт за пределами страны покупки, так как это может привести к нарушению правил беспроводной связи и используемой мощности, установленных в этой стране.
- В настоящем документе наименование “Windows® XP” обозначает операционные системы Windows® XP Professional, Windows® XP Professional x64 Edition и Windows® XP Home Edition.
- Windows Server® 2003 в настоящем документе обозначает Windows Server® 2003 и Windows Server® 2003 x64 Edition.
- В настоящем документе наименование “Windows Server® 2008” обозначает операционные системы Windows Server® 2008 и Windows Server® 2008 R2.
- Под Windows Server® 2012 в данном документе понимаются все издания ОС Windows Server® 2012.
- Под Windows Vista® в данном документе понимаются все издания ОС Windows Vista®.
- Windows® 7 в настоящем документе обозначает все издания ОС Windows® 7.
- Windows® 8 в настоящем документе обозначает все издания ОС Windows® 8.
- Для загрузки других руководств посетите Brother Solutions Center по адресу: <http://solutions.brother.com/> и на странице соответствующей модели нажмите “Руководства”.
- В некоторых странах доступны не все модели.

Содержание

Раздел I Работа в сети

1	Введение	2
	Сетевые функции.....	2
	Другие сетевые функции.....	3
2	Изменение параметров сети аппарата	4
	Способы изменения параметров сети аппарата (IP-адрес, маска подсети и шлюз).....	4
	Использование панели управления.....	4
	Использование утилиты BRAdmin Light.....	4
	Другие утилиты управления.....	7
	Управление через веб-интерфейс (браузер).....	7
	Утилита BRAdmin Professional 3 (для Windows®).....	7
	BRPrint Auditor (Windows®).....	8
3	Настройка аппарата для работы в беспроводной сети (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)	9
	Общая информация.....	9
	Проверка сетевой среды.....	10
	Подключение к компьютеру через точку беспроводного доступа/маршрутизатор в сети (режим инфраструктуры).....	10
	Подключение к компьютеру, поддерживающему беспроводное соединение, в сети без точки беспроводного доступа/маршрутизатора (режим ad-hoc).....	11
	Настройка параметров беспроводной сети с временным использованием кабеля USB (рекомендуется).....	12
	Настройка при помощи мастера установки с панели управления аппарата.....	17
	Настройка вручную с панели управления.....	18
	Настройка аппарата, если рассылка SSID отключена.....	20
	Настройка аппарата для работы в корпоративной беспроводной сети.....	23
	Настройка одним нажатием при помощи WPS (Wi-Fi Protected Setup) или AOSS™.....	27
	Настройка при помощи PIN-кода функции WPS (Wi-Fi Protected Setup).....	29
	Настройка в режиме ad-hoc.....	32
	Использование настроенного идентификатора SSID.....	32
	Использование нового идентификатора SSID.....	34
4	Настройка с панели управления	36
	Общая информация.....	36
	Меню “Сеть”.....	37
	TCP/IP.....	37
	Ethernet (только для проводной сети).....	39
	Состояние проводной сети (для моделей HL-3150CDN, HL-3150CDW и HL-3170CDW).....	39
	Мастер установки (только для беспроводной сети).....	39
	WPS (Wi-Fi Protected Setup)/AOSS™ (только для беспроводной сети).....	39
	WPS (Wi-Fi Protected Setup) с PIN-кодом (только для беспроводной сети).....	39
	Состояние беспроводной сети (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW).....	39

MAC-адрес	40
Настройка по умолчанию (для моделей HL-3150CDW и HL-3170CDW)	40
Включение проводной сети (для моделей HL-3150CDW и HL-3170CDW)	40
Включение беспроводной сети (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)	40
Восстановление заводских настроек сети	41
Печать отчета о конфигурации сети	42
Печать отчета WLAN (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)	43
Таблица функций и заводские настройки по умолчанию	44
HL-3150CDN	44
HL-3140CW, HL-3150CDW и HL-3170CDW	45

5 Управление через веб-интерфейс 48

Общая информация	48
Настройка параметров аппарата с использованием системы управления через веб-интерфейс (браузер)	49
Установка пароля	50
Защитная блокировка функций 2.0	51
Настройка параметров утилиты “Защитная блокировка функций 2.0” с использованием системы управления через веб-интерфейс (браузер)	51
Настройка протокола SNMP с использованием управления через веб-интерфейс	53
Сохранение журнала в сети	54
Настройка параметров функции “Сохранение журнала в сети” с использованием системы управления через веб-интерфейс (браузер)	54
Настройка обнаружения ошибок	57
Значение сообщений об ошибках	58

6 Функции безопасности 59

Общая информация	59
Использование сертификатов для обеспечения безопасности аппарата	60
Настройка сертификата с помощью управления через веб-интерфейс	62
Создание и установка сертификата	63
Выбор сертификата	66
Установка самоподписанного сертификата на компьютер	66
Импорт и экспорт сертификата и секретного ключа	71
Импорт и экспорт сертификата ЦС	73
Управление несколькими сертификатами	74
Безопасное управление сетевым аппаратом с помощью SSL/TLS	75
Безопасное управление с помощью системы управления через веб-интерфейс (браузер)	75
Безопасное управление с помощью утилиты BRAdmin Professional 3 (Windows®)	78
Для безопасного использования утилиты BRAdmin Professional 3 необходимо выполнять следующие положения	78
Безопасная печать документов по протоколу SSL/TLS	79
Безопасная отправка электронной почты	80
Настройка с помощью системы управления через веб-интерфейс (браузер)	80
Отправка сообщений электронной почты с аутентификацией пользователей	81
Безопасная отправка электронной почты с использованием SSL/TLS	82
Использование аутентификации IEEE 802.1x	83
Настройка аутентификации IEEE 802.1x с помощью системы управления через веб-интерфейс (браузер)	83

7	Поиск и устранение неисправностей	86
	Общая информация	86
	Идентификация проблемы.....	86

Раздел II Сетевая терминология

8	Типы сетевых подключений и протоколов	95
	Типы сетевых подключений.....	95
	Пример подключения к проводной сети	95
	Протоколы	97
	Протоколы и функции TCP/IP	97
9	Настройка аппарата для работы в сети	101
	IP-адреса, маски подсети и шлюзы	101
	IP-адрес	101
	Маска подсети.....	102
	Шлюз (и маршрутизатор)	102
	Аутентификация IEEE 802.1x.....	103
10	Термины и понятия беспроводных сетей (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)	105
	Указание сети.....	105
	SSID (идентификатор беспроводной сети) и каналы	105
	Термины безопасности.....	105
	Аутентификация и шифрование	105
	Методы аутентификации и шифрования для частной беспроводной сети	106
	Методы аутентификации и шифрования для корпоративной беспроводной сети	107
11	Дополнительные сетевые настройки Windows®	109
	Типы дополнительных сетевых настроек	109
	Установка драйверов для печати через Web Services (Windows Vista®, Windows® 7 и Windows® 8).....	109
	Удаление драйверов для печати через Web Services (Windows Vista®, Windows® 7 и Windows® 8).....	110
	Установка сетевой печати для режима инфраструктуры при использовании Vertical Pairing (Windows® 7 и Windows® 8).....	111
12	Термины и понятия безопасности	113
	Функции безопасности.....	113
	Термины безопасности	113
	Протоколы безопасности	114
	Способы защиты при отправке электронной почты	115

Раздел III Приложения

A	Приложение А	117
	Поддерживаемые протоколы и функции безопасности	117
B	Приложение В	118
	Использование служб.....	118
	Другие способы задания IP-адреса (для продвинутых пользователей и администраторов).....	118
	Использование DHCP для настройки IP-адреса	118
	Использование RARP для настройки IP-адреса	119
	Использование BOOTP для настройки IP-адреса	120
	Использование APIPA для настройки IP-адреса	121
	Использование ARP для настройки IP-адреса.....	122
	Использование консоли TELNET для настройки IP-адреса.....	123
C	Указатель	124



Работа в сети

Введение	2
Изменение параметров сети аппарата	4
Настройка аппарата для работы в беспроводной сети (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)	9
Настройка с панели управления	36
Управление через веб-интерфейс	48
Функции безопасности	59
Поиск и устранение неисправностей	86

Сетевые функции

Аппарат Brother можно использовать для совместной работы в проводной сети 10/100 МБ¹ или беспроводной сети IEEE 802.11b/g/n (для моделей, поддерживающих работу в беспроводных сетях) Ethernet с помощью встроенного сетевого сервера печати. Сервер печати поддерживает различные функции и способы подключения в зависимости от операционной системы, которая используется в сети с поддержкой TCP/IP. В следующей таблице перечислены сетевые функции и подключения, поддерживаемые каждой операционной системой.

ПРИМЕЧАНИЕ

- Хотя аппарат Brother можно использовать как в проводной¹, так и в беспроводной сети, одновременно можно использовать только один способ подключения. Однако беспроводное сетевое подключение и подключение Wi-Fi Direct™, либо проводное сетевое подключение и подключение Wi-Fi Direct можно использовать одновременно.
- Подробные сведения см. в документе “Руководство по использованию Wi-Fi Direct™”, который можно скачать на странице “Руководства” для имеющейся модели аппарата на веб-сайте Brother Solutions Center (<http://solutions.brother.com/>).

¹ Интерфейс для проводной сети имеется на моделях HL-3150CDW и HL-3170CDW.

Операционные системы	Windows® XP Windows Vista® Windows® 7 Windows® 8	Windows Server® 2003/2008/2012	Mac OS X v10.6.8, 10.7.x, 10.8.x
Печать	✓	✓	✓
BRAdmin Light ¹ См. стр. 4.	✓	✓	✓
BRAdmin Professional 3 ² См. стр. 7.	✓	✓	
Управление через веб-интерфейс (браузер) См. стр. 48.	✓	✓	✓
Status Monitor ➤➤Руководство пользователя	✓	✓	✓
Мастер развертывания драйверов	✓	✓	
Vertical Pairing (метод беспроводного подключения) См. стр. 111.	✓ ³		

¹ Утилиту BRAdmin Light для Macintosh можно загрузить с веб-сайта <http://solutions.brother.com/>.

² Утилиту BRAdmin Professional 3 можно загрузить с веб-сайта <http://solutions.brother.com/>.

³ Только Windows® 7 и Windows® 8.

Другие сетевые функции

Безопасность

В данном аппарате Brother используются самые современные протоколы безопасности и шифрования. (См. раздел *Функции безопасности* >> стр. 59.)

Защитная блокировка функций 2.0

Защитная блокировка функций 2.0 позволяет повысить безопасность за счет ограничения некоторых функций аппарата. (См. раздел *Защитная блокировка функций 2.0* >> стр. 51.)

Сохранение журнала в сети

Функция “Сохранение журнала в сети” позволяет сохранять файл журнала печати с аппарата Brother на сетевой сервер с использованием CIFS. (См. раздел *Сохранение журнала в сети* >> стр. 54.)

Способы изменения параметров сети аппарата (IP-адрес, маска подсети и шлюз)

Параметры настройки сети аппарата можно изменить с помощью панели управления, утилиты BRAdmin Light, BRAdmin Professional 3 и системы управления через веб-интерфейс. Для получения подробной информации см. данную главу.

Использование панели управления

Можно настроить используемый аппарат для работы в сети с помощью соответствующего меню панели управления. (См. раздел *Настройка с панели управления* >> стр. 36.)

Использование утилиты BRAdmin Light

Утилита BRAdmin Light предназначена для начальной настройки устройств Brother, подключенных к сети. При помощи этой утилиты можно также выполнять поиск устройств Brother в сетевой среде TCP/IP, просматривать их состояние и изменять настройки сети (например, IP-адрес).

Установка BRAdmin Light для Windows®

- 1 Убедитесь, что устройство включено.
- 2 Включите компьютер. Перед настройкой закройте все работающие программы.
- 3 Вставьте компакт-диск с программой установки в дисковод для компакт-дисков. Автоматически отображается начальный экран. Если открывается диалоговое окно выбора модели, выберите соответствующую модель аппарата. Если открывается диалоговое окно выбора языка, выберите свой язык.
- 4 Открывается главное меню компакт-диска. Нажмите **Установка других драйверов или утилит**.
- 5 Щелкните **BRAdmin Light** и следуйте отображаемым на экране инструкциям.

Установка BRAdmin Light для Macintosh

Последнюю версию утилиты BRAdmin Light можно загрузить с веб-сайта <http://solutions.brother.com/>.

Задание IP-адреса, маски подсети и шлюза с помощью утилиты BRAdmin Light

ПРИМЕЧАНИЕ

- Последнюю версию утилиты BRAdmin Light можно загрузить с веб-сайта <http://solutions.brother.com/>.
 - Если необходимы более широкие возможности управления аппаратом, используйте последнюю версию утилиты BRAdmin Professional 3, которую можно загрузить с веб-сайта <http://solutions.brother.com/>. Эта утилита имеется только для Windows®.
 - Если используется функция брандмауэра антишпионской или антивирусной программы, временно отключите ее. После успешной проверки печати повторно включите эту функцию.
 - Имя узла: имя узла отображается в текущем окне утилиты BRAdmin Light. По умолчанию в аппарате используется имя узла сервера печати “BRNxxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxxx” — это MAC-адрес/Ethernet-адрес аппарата.)
 - По умолчанию пароль не требуется. Введите пароль, если он установлен, и нажмите кнопку **ОК**.
-

1 Запустите утилиту BRAdmin Light.

- Для Windows®

Выберите **Пуск / Все программы / Brother / BRAdmin Light / BRAdmin Light**.

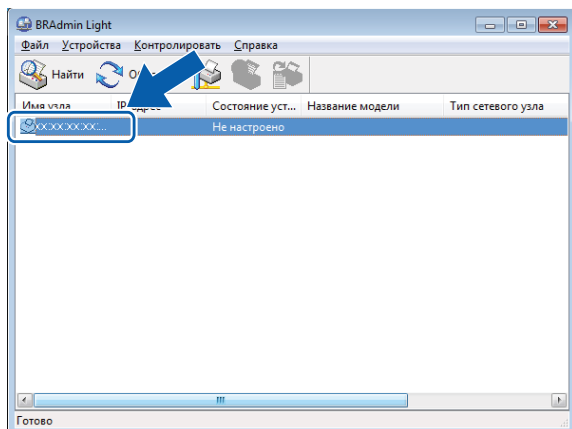
- Для Macintosh

По завершении загрузки дважды щелкните файл **BRAdmin Light.jar** для запуска утилиты BRAdmin Light.

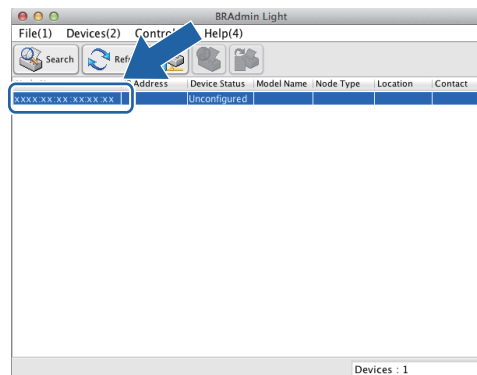
2 Утилита BRAdmin Light автоматически выполнит поиск новых устройств.

- 3 Дважды щелкните ненастроенное устройство.

Для Windows®



Для Macintosh

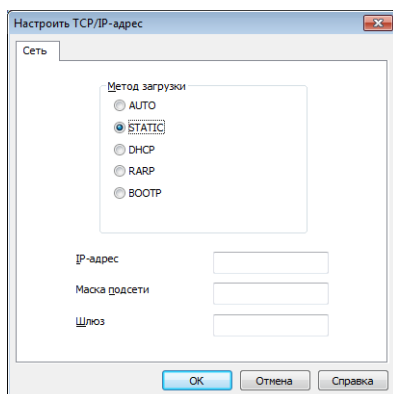


ПРИМЕЧАНИЕ

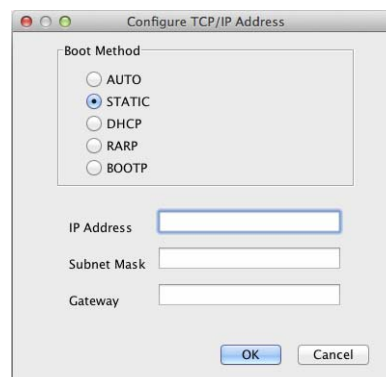
- Если для сервера печати установлены заводские настройки по умолчанию (если сервер DHCP/BOOTP/RARP не используется), устройство отобразится в окне утилиты BRAdmin Light как **Unconfigured (Не настроено)**.
- Можно узнать имя узла и MAC-адрес (Ethernet-адрес), распечатав отчет о конфигурации сети. См. раздел *Печать отчета о конфигурации сети* >> стр. 42). MAC-адрес можно также выяснить с помощью панели управления. (См. раздел *Глава 4: Настройка с панели управления*.)

- 4 Выберите **STATIC** (Статический) в меню **Boot Method (Метод загрузки)**. Введите **IP Address (IP-адрес)**, **Subnet Mask (Маска подсети)** и **Gateway (Шлюз)** (при необходимости) для аппарата.

Для Windows®



Для Macintosh



- 5 Нажмите **ОК**.
- 6 Если IP-адрес указан правильно, аппарат Brother появится в списке устройств.

Другие утилиты управления

Помимо утилиты BRAdmin Light аппарат Brother имеет следующие утилиты управления. Эти утилиты можно использовать для изменения параметров сети.

Управление через веб-интерфейс (браузер)

Используйте стандартный браузер для изменения настроек сервера печати с помощью протокола HTTP (Hyper Text Transfer Protocol – протокол передачи гипертекста) или HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer – протокол передачи гипертекста с уровнем защищенных сокетов). (См. раздел *Настройка параметров аппарата с использованием системы управления через веб-интерфейс (браузер)* >> стр. 49.)

Утилита BRAdmin Professional 3 (для Windows®)

BRAdmin Professional 3 – это утилита для расширенного управления аппаратами Brother, подключенными к сети. С помощью этой утилиты можно выполнять поиск устройств Brother в сети и просматривать состояние устройств в удобном окне (напоминающем окно Проводника Windows®), в котором состояния устройств обозначены разными цветами. Можно настроить параметры сети и устройства, а также возможность обновления микропрограммы устройства с компьютера Windows® в локальной сети. С помощью утилиты BRAdmin Professional 3 можно также вести журналы событий устройств Brother в сети и экспортировать данные журналов в форматах HTML, CSV, TXT или SQL.

Установите программу Print Auditor Client на клиентский ПК для пользователей, которым необходимо контролировать устройства, подключенные локально. Данная утилита позволяет контролировать аппараты, подключенные к клиентскому ПК через USB или параллельный интерфейс из программы BRAdmin Professional 3.

Для получения дополнительной информации и загрузки данной программы посетите веб-сайт <http://solutions.brother.com/>.

ПРИМЕЧАНИЕ

- Используйте последнюю версию утилиты BRAdmin Professional 3, которую можно загрузить с веб-сайта <http://solutions.brother.com/>. Эта утилита имеется только для Windows®.
- Если используется функция брандмауэра антишпионской или антивирусной программы, временно отключите ее. Убедившись в том, что можно выполнить печать, настройте программное обеспечение, следуя инструкциям.
- Имя узла: имя узла для каждого аппарата Brother в сети отображается в утилите BRAdmin Professional 3. По умолчанию используется имя узла “BRNxxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxxx” — это MAC-адрес/Ethernet-адрес аппарата.)

BRPrint Auditor (Windows®)

Благодаря программе BRPrint Auditor на аппаратах, подключенных локально, можно воспользоваться мощными средствами контроля сетевых инструментов управления Brother. Эта утилита позволяет клиентскому компьютеру собирать информацию об использовании и состоянии от аппарата Brother, подключенного через параллельный или USB-интерфейс. BRPrint Auditor может затем передать эту информацию на другой компьютер в сети с запущенной утилитой BRAdmin Professional 3. При этом администратор может проверить информацию о количестве страниц, состоянии тонера и фотобарабана, а также версию микропрограммы. В дополнение к отчетам на приложения сетевого управления Brother данная утилита может отправлять информацию об использовании и состоянии непосредственно на предварительно указанные адреса электронной почте в файлах формата CSV или XML (требуется поддержка протокола электронной почты SMTP). Утилита BRPrint Auditor также поддерживает функцию уведомления по электронной почте для передачи предупреждений и сообщений о состояниях ошибки.

Настройка аппарата для работы в беспроводной сети (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)

Общая информация

Для подключения аппарата к беспроводной сети рекомендуется следовать одному из способов настройки, указанных в документе “Руководство по быстрой установке”.

Самым простым является способ настройки беспроводной сети с помощью компакт-диска с программой установки и кабеля USB.

В случае других способов настройки беспроводного соединения изучите приведенные в настоящей главе подробные инструкции по настройке параметров беспроводной сети. Дополнительную информацию о параметрах TCP/IP см. в разделе *Способы изменения параметров сети аппарата (IP-адрес, маска подсети и шлюз)* >> стр. 4.

ПРИМЕЧАНИЕ

- Для достижения оптимальных результатов при обычной ежедневной печати документов расположите аппарат Brother как можно ближе к точке беспроводного доступа/маршрутизатору, по возможности, без препятствий между ними. Наличие больших предметов и стен между двумя устройствами, а также помехи от других электронных устройств могут повлиять на скорость передачи данных при печати документов.

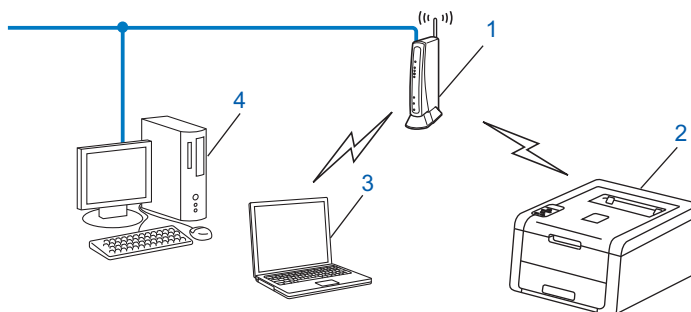
По этим причинам беспроводная сеть может оказаться не лучшим методом подключения для некоторых типов документов и приложений. При печати больших файлов (например, многостраничных документов с текстом и большими графическими изображениями) лучше использовать проводное Ethernet-соединение для более быстрой передачи данных¹ или USB для обеспечения самой большой скорости передачи.

- Хотя аппарат Brother можно использовать как в проводной¹, так и в беспроводной сети, одновременно можно использовать только один способ подключения. Однако беспроводное сетевое подключение и подключение Wi-Fi Direct, либо проводное сетевое подключение и подключение Wi-Fi Direct можно использовать одновременно.
- Подробные сведения см. в документе “Руководство по использованию Wi-Fi Direct™”, который можно скачать на странице “Руководства” для имеющейся модели аппарата на веб-сайте Brother Solutions Center (<http://solutions.brother.com/>).
- Перед настройкой параметров беспроводной связи необходимо знать имя сети (SSID) и сетевой ключ. При использовании корпоративной беспроводной сети также необходимо знать идентификатор пользователя и пароль.

¹ Интерфейс для проводной сети имеется на моделях HL-3150CDW и HL-3170CDW.

Проверка сетевой среды

Подключение к компьютеру через точку беспроводного доступа/маршрутизатор в сети (режим инфраструктуры)



1 Точка беспроводного доступа/маршрутизатор ¹

¹ Если компьютер поддерживает Intel® MWT (My WiFi Technology), можно использовать его в качестве точки доступа с поддержкой WPS (Wi-Fi Protected Setup).

2 Беспроводной сетевой аппарат (ваш аппарат)

3 Беспроводной компьютер, подключенный к точке беспроводного доступа/маршрутизатору

4 Проводной компьютер, не поддерживающий беспроводное подключение и подключенный к точке беспроводного доступа/маршрутизатору с помощью сетевого кабеля

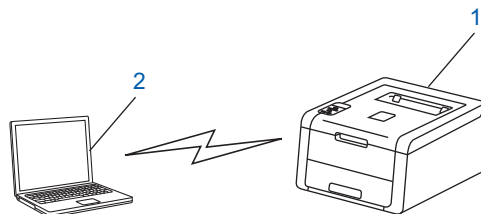
Метод настройки

В приведенных ниже инструкциях предлагаются четыре способа настройки аппарата Brother для работы в беспроводной сетевой среде. Выберите способ, который предпочтителен для вашей рабочей среды.

- Настройка параметров беспроводной сети с временным использованием кабеля USB (рекомендуется)
См. раздел *Настройка параметров беспроводной сети с временным использованием кабеля USB (рекомендуется)* >> стр. 12.
- Настройка беспроводного соединения с панели управления при помощи мастера установки
См. раздел *Настройка при помощи мастера установки с панели управления аппарата* >> стр. 17.
- Настройка беспроводной сети “одним нажатием” с использованием WPS (Wi-Fi Protected Setup™) или AOSS™
См. раздел *Настройка одним нажатием при помощи WPS (Wi-Fi Protected Setup) или AOSS™* >> стр. 27.
- Настройка беспроводной сети с PIN-кодом с помощью WPS
См. раздел *Настройка при помощи PIN-кода функции WPS (Wi-Fi Protected Setup)* >> стр. 29.

Подключение к компьютеру, поддерживающему беспроводное соединение, в сети без точки беспроводного доступа/маршрутизатора (режим ad-hoc)

В сети этого типа отсутствует централизованная точка беспроводного доступа/маршрутизатор. Все беспроводные клиенты обмениваются данными напрямую. Когда беспроводной аппарат Brother (ваш аппарат) является частью такой сети, он принимает все задания печати непосредственно с компьютера, отправляющего данные печати.



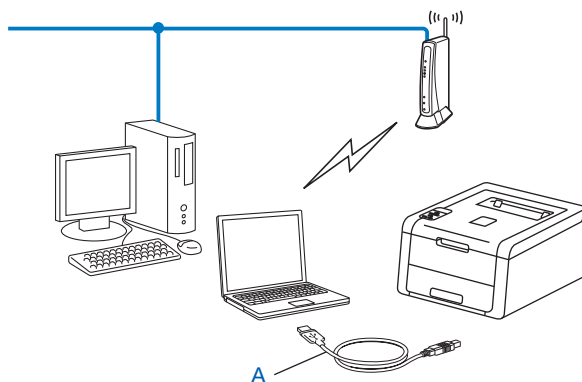
- 1 Беспроводной сетевой аппарат (ваш аппарат)**
- 2 Компьютер с поддержкой беспроводного соединения**

В режиме ad-hoc беспроводное сетевое подключение с использованием продуктов Windows Server® не гарантируется. Инструкции по настройке аппарата в режиме ad-hoc см. в разделе *Настройка в режиме ad-hoc* >> стр. 32.

Настройка параметров беспроводной сети с временным использованием кабеля USB (рекомендуется)

Для этого способа настройки рекомендуется использование компьютера, подключенного к беспроводной сети.

Можно удаленно настроить аппарат с подключенного к сети компьютера, используя кабель USB (A)¹.



¹ Параметры беспроводной сети на аппарате можно настроить, используя кабель USB, временно подсоединенный к компьютеру, подключенному к проводной или беспроводной сети.

ВАЖНАЯ ИНФОРМАЦИЯ

- Ниже приведены инструкции для установки аппарата Brother в сетевой среде при помощи программы установки Brother, записанной на компакт-диске, входящем в комплект поставки аппарата.
- Если на аппарате ранее были настроены параметры беспроводной сети, то перед новой настройкой параметров беспроводной сети необходимо сбросить предыдущие параметры локальной сети.

Инструкции по сбросу параметров локальной сети см. в разделе *Восстановление заводских настроек сети* >> стр. 41.

- Если используется брандмауэр ОС Windows[®], функция брандмауэра антишпионских программ или антивирусные приложения, временно отключите их. Убедившись, что печать выполняется, снова запустите брандмауэр.
- Во время настройки необходимо временно подключить кабель USB.
- **Перед выполнением этой установки необходимо выяснить параметры беспроводной сети.** Если требуется подключить аппарат Brother к сети, то перед установкой рекомендуется обратиться к системному администратору.
- Если в маршрутизаторе используется шифрование WEP, введите ключ, использованный в качестве первого ключа WEP. Аппарат Brother поддерживает использование только первого ключа WEP.

- 1 До настройки аппарата рекомендуется записать параметры беспроводной сети. Эти данные потребуются для продолжения процесса настройки.

Настройка для частной беспроводной сети

При настройке аппарата для работы в небольшой беспроводной сети, например в домашней среде, запишите SSID и сетевой ключ.

Если используется Windows® XP или если для подключения компьютера к точке беспроводного доступа/маршрутизатору используется сетевой кабель, то перед подключением необходимо узнать SSID и сетевой ключ точки беспроводного доступа/маршрутизатора.

3

Имя сети: (SSID)	Сетевой ключ

Пример:

Имя сети: (SSID)	Сетевой ключ
HELLO	12345678

Настройка для корпоративной беспроводной сети

При настройке аппарата для работы в беспроводной сети с поддержкой стандарта IEEE 802.1x запишите методы аутентификации и шифрования, идентификатор пользователя и пароль.

Имя сети: (SSID)

Режим обмена данными	Метод аутентификации	Режим шифрования	Идентификатор пользователя	Пароль
Инфраструктура	LEAP	CKIP		
	EAP-FAST/HET	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
TKIP				
EAP-TLS	AES		—	
	TKIP		—	

Пример:

Имя сети: (SSID)
HELLO

Режим обмена данными	Метод аутентификации	Режим шифрования	Идентификатор пользователя	Пароль
Инфраструктура	EAP-FAST/MS-CHAPv2	AES	Brother	12345678

ПРИМЕЧАНИЕ

- Если выполняется настройка аппарата, использующего аутентификацию EAP-TLS, необходимо установить сертификат клиента, выданный ЦС (центром сертификации), перед началом настройки. Для получения информации о сертификате клиента обратитесь к администратору сети. Если установлено более одного сертификата, рекомендуется записать имя сертификата, который будет использоваться. Для получения дополнительной информации об установке сертификата см. раздел *Использование сертификатов для обеспечения безопасности аппарата* >> стр. 60.
- Если на аппарате используется стандартное имя сертификата сервера, рекомендуется записать стандартное имя до начала настройки. Для получения информации о стандартном имени сертификата сервера обратитесь к администратору сети.

- 2 Включите компьютер и вставьте компакт-диск с программой установки в дисковод для компакт-дисков.

(Для Windows®)

- 1 Автоматически отображается начальный экран.
Выберите аппарат и язык.
- 2 Открывается главное меню компакт-диска. Нажмите **Установка драйвера принтера**, затем нажмите **Да**, если принимаете лицензионные соглашения. Следуйте инструкциям на экране.

ПРИМЕЧАНИЕ

- Если экран Brother не откроется автоматически, откройте папку **Компьютер (Мой компьютер)**, дважды щелкните значок компакт-диска, а затем дважды щелкните **start.exe**.
- Если отображается экран **Контроль учетных записей пользователей**, (Windows Vista®) нажмите **Разрешить**. (Windows® 7/Windows® 8) нажмите **Да**.

- 3 Выберите **Беспроводное сетевое подключение**, затем нажмите **Далее**.
- 4 Выберите **Принтер Brother в одноранговой сети** или **Сетевой коллективный принтер**, затем нажмите **Далее**.
- 5 При выборе значения **Сетевой коллективный принтер** выберите очередь принтера на экране **Просмотр для принтера** и нажмите **ОК**.
- 6 Выберите параметр брандмауэра на экране **Обнаружен брандмауэр/антивирусная программа**, а затем нажмите **Далее**.

(Для Macintosh)

- 1 Автоматически отображается начальный экран. Нажмите **Start Here OSX** (Запуск OSX). Выберите аппарат и нажмите **Next** (Далее).
- 2 Выберите **Wireless Network Connection** (Беспроводное сетевое соединение), а затем нажмите **Next** (Далее).

3 Выберите **Да, у меня есть USB-кабель для выполнения установки.**, а затем нажмите **Далее**.

4 Выполните инструкции на экране, чтобы настроить параметры беспроводной сети.

ПРИМЕЧАНИЕ

- При отображении диалогового окна **Доступные беспроводные сети**, если в настройках точки доступа рассылка идентификатора SSID запрещена, можно вручную включить ее, нажав кнопку **Дополнительно**. Введите **Имя (SSID)** в соответствии с инструкциями, отображаемыми на экране.
 - При отображении диалогового окна, информирующего о сбое настройки беспроводной сети, нажмите кнопку **Повторить** и повторите попытку.
-

OK! По завершении настройки параметров беспроводной связи можно продолжить установку драйвера принтера. Нажмите **Далее** в диалоговом окне установки и следуйте инструкциям на экране.

Настройка при помощи мастера установки с панели управления аппарата

Для настройки параметров беспроводной сети можно использовать панель управления аппарата. Используя функцию панели управления *Мастер уст-ки*, можно легко подключить аппарат Brother к беспроводной сети. **Перед выполнением этой установки необходимо выяснить параметры беспроводной сети.**

ВАЖНАЯ ИНФОРМАЦИЯ

- Если на аппарате ранее были настроены параметры беспроводной сети, то перед новой настройкой параметров беспроводной сети необходимо сбросить предыдущие параметры локальной сети.
Инструкции по сбросу параметров локальной сети см. в разделе *Восстановление заводских настроек сети* >> стр. 41.
 - Если в маршрутизаторе используется шифрование WEP, введите ключ, использованный в качестве первого ключа WEP. Аппарат Brother поддерживает использование только первого ключа WEP.
-
- При настройке аппарата для работы в небольшой беспроводной сети, например в домашней среде:
 - Для настройки работы аппарата в существующей беспроводной сети с помощью SSID и сетевого ключа (если требуется) см. *Настройка вручную с панели управления* >> стр. 18.
 - Если в настройках точки беспроводного доступа/маршрутизатора рассылка имени SSID запрещена, см. раздел *Настройка аппарата, если рассылка SSID отключена* >> стр. 20.
 - При настройке аппарата в режиме ad-hoc см. *Настройка в режиме ad-hoc* >> стр. 32.
 - Если аппарат настраивается для работы в беспроводной сети, поддерживающей стандарт IEEE 802.1х, см. раздел *Настройка аппарата для работы в корпоративной беспроводной сети* >> стр. 23.
 - Если точка беспроводного доступа/маршрутизатор поддерживает WPS или AOSS™, см. *Настройка одним нажатием при помощи WPS (Wi-Fi Protected Setup) или AOSS™* >> стр. 27.
 - При настройке аппарата с помощью функции WPS (PIN-код) см. *Настройка при помощи PIN-кода функции WPS (Wi-Fi Protected Setup)* >> стр. 29.

Настройка вручную с панели управления

- 1 До настройки аппарата рекомендуется записать параметры беспроводной сети. Эти данные потребуются для продолжения процесса настройки.

Проверьте и запишите текущие параметры беспроводной сети.

Имя сети: (SSID)	Сетевой ключ

Пример:

Имя сети: (SSID)	Сетевой ключ
HELLO	12345678

ПРИМЕЧАНИЕ

Если в маршрутизаторе используется шифрование WEP, введите ключ, использованный в качестве первого ключа WEP. Аппарат Brother поддерживает использование только первого ключа WEP.

- 2 Нажмите ▲ или ▼ для выбора параметра *Сеть*.
Нажмите **OK**.
- 3 Нажмите ▲ или ▼ для выбора параметра *Беспровод. сеть*.
Нажмите **OK**.
- 4 Нажмите ▲ или ▼ для выбора параметра *Мастер уст-ки*.
Нажмите **OK**.
- 5 При отображении сообщения *Беспр. сеть вкл.?* нажмите ▲ для подтверждения.
Запускается мастер настройки беспроводной сети.
Для отмены нажмите **Cancel**.
- 6 Аппарат выполнит поиск доступных идентификаторов SSID. При отображении списка идентификаторов SSID используйте ▲ или ▼ для выбора идентификатора SSID, записанного в шаге 1, а затем нажмите кнопку **OK**.
Выполните одно из следующих действий:
 - При использовании метода аутентификации и шифрования, требующего сетевого ключа, перейдите к шагу 7.
 - Если методом аутентификации является открытая система, а режим шифрования выключен, перейдите к шагу 9.
 - Если точка беспроводного доступа/маршрутизатор поддерживает WPS, отображается диалоговое окно *WPS доступна*. Нажмите ▲. Для подключения аппарата с помощью автоматического беспроводного режима, нажмите ▲, чтобы выбрать **Да**. (Если вы нажали ▼, чтобы выбрать **Нет**, перейдите к шагу 7 и введите сетевой ключ.) Когда отобразится сообщение *Наж. WPS на марш.*, нажмите кнопку WPS на точке беспроводного доступа/маршрутизаторе, затем дважды нажмите ▲. Перейдите к шагу 8.

ПРИМЕЧАНИЕ

Если идентификатор SSID не рассылается, см. раздел *Настройка аппарата, если рассылка SSID отключена* >> стр. 20.

- 7 Введите сетевой ключ, записанный в шаге 1. (Информация о вводе текста: >>Руководство по быстрой установке.)
Если введены все символы, нажмите кнопку **ОК**, а затем нажмите **▲**, чтобы выбрать **Да** для применения настроек. Перейдите к шагу 8.
- 8 Аппарат предпримет попытку подключиться к беспроводной сети, используя введенную информацию.
- 9 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение *Подключен*.
Аппарат распечатает отчет о состоянии беспроводной сети. Если происходит сбой соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке: *Устранение неисправностей*.



(Для Windows®)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите “Установка драйвера принтера”.

(Для Macintosh)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите **Start Here OSX (Запуск OSX).**

Настройка аппарата, если рассылка SSID отключена

- 1 До настройки аппарата рекомендуется записать параметры беспроводной сети. Эти данные потребуются для продолжения процесса настройки.

Проверьте и запишите текущие параметры беспроводной сети.

Имя сети: (SSID)

3

Режим обмена данными	Метод аутентификации	Режим шифрования	Сетевой ключ
Инфраструктура	Открытая система	WEP	—
		WEP	
	Общий ключ	WEP	
		AES	
		TKIP ¹	

¹ Режим TKIP поддерживается только для WPA-PSK.

Пример:

Имя сети: (SSID)
HELLO

Режим обмена данными	Метод аутентификации	Режим шифрования	Сетевой ключ
Инфраструктура	WPA2-PSK	AES	12345678

ПРИМЕЧАНИЕ

Если в маршрутизаторе используется шифрование WEP, введите ключ, использованный в качестве первого ключа WEP. Аппарат Brother поддерживает использование только первого ключа WEP.

- 2 Нажмите ▲ или ▼ для выбора параметра *Сеть*.
Нажмите **OK**.
- 3 Нажмите ▲ или ▼ для выбора параметра *Беспровод. сеть*.
Нажмите **OK**.
- 4 Нажмите ▲ или ▼ для выбора параметра *Мастер уст-ки*.
Нажмите **OK**.
- 5 При отображении сообщения *Беспр. сеть вкл.?* нажмите ▲ для подтверждения.
Запускается мастер настройки беспроводной сети.
Для отмены нажмите **Cancel**.
- 6 Аппарат выполняет поиск сети и отображает список доступных SSID.
Выберите <Новый SSID>, используя клавишу ▲ или ▼.
Нажмите **OK**.

- 7 Введите имя SSID. (Информация о вводе текста: ►►Руководство по быстрой установке.)
Нажмите **OK**.
- 8 Когда появится соответствующий запрос, при помощи ▲ или ▼ выберите **Инфраструктура**.
Нажмите **OK**.
- 9 Выберите метод аутентификации при помощи ▲ или ▼ и нажмите **OK**.
Выполните одно из следующих действий:
Если выбран пункт **Открытая система**, перейдите к шагу 10.
Если выбран пункт **Общий ключ**, перейдите к шагу 11.
Если выбран пункт **WPA/WPA2 - PSK**, перейдите к шагу 12.
- 10 Выберите тип шифрования **Нет** или **WEP**, нажав ▲ или ▼, а затем нажмите **OK**.
Выполните одно из следующих действий:
Если выбран пункт **Нет**, перейдите к шагу 14.
Если выбран пункт **WEP**, перейдите к шагу 11.
- 11 Введите ключ WEP, записанный в шаге 1. Нажмите **OK**. Перейдите к шагу 14. (Информация о вводе текста: ►►Руководство по быстрой установке.)
- 12 Выберите тип шифрования **TKIP** или **AES** клавишей ▲ или ▼. Нажмите **OK**. Перейдите к шагу 13.

- 13 Введите ключ WPA, записанный в шаге 1, и нажмите **ОК**. Перейдите к шагу 14. (Информация о вводе текста: >>Руководство по быстрой установке.)
 - 14 Чтобы применить настройки, выберите **Да**. Для отмены выберите **Нет**.
Выполните одно из следующих действий:
Если выбран пункт **Да**, перейдите к шагу 15.
Если выбран пункт **Нет**, вернитесь к шагу 6.
 - 15 Аппарат попытается выполнить подключение к выбранной беспроводной сети.
 - 16 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение **Подключен**.
Аппарат распечатает отчет о состоянии беспроводной сети. Если происходит сбой соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке:
Устранение неисправностей.
- ОК!** (Для Windows®)
На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите “Установка драйвера принтера”.
- (Для Macintosh)
На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите **Start Here OSX** (Запуск OSX).

Настройка аппарата для работы в корпоративной беспроводной сети

- 1 До настройки аппарата рекомендуется записать параметры беспроводной сети. Эти данные потребуются для продолжения процесса настройки.

Проверьте и запишите текущие параметры беспроводной сети.

Имя сети: (SSID)

3

Режим обмена данными	Метод аутентификации	Режим шифрования	Идентификатор пользователя	Пароль
Инфраструктура	LEAP	CKIP		
	EAP-FAST/HET	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		
TKIP				—

Пример:

Имя сети: (SSID)
HELLO

Режим обмена данными	Метод аутентификации	Режим шифрования	Идентификатор пользователя	Пароль
Инфраструктура	EAP-FAST/MS-CHAPv2	AES	Brother	12345678

ПРИМЕЧАНИЕ

- Если выполняется настройка аппарата, использующего аутентификацию EAP-TLS, необходимо установить сертификат клиента, выданный ЦС (центром сертификации), перед началом настройки. Для получения информации о сертификате клиента обратитесь к администратору сети. Если установлено более одного сертификата, рекомендуется записать имя сертификата, который будет использоваться. Для получения дополнительной информации об установке сертификата см. раздел *Использование сертификатов для обеспечения безопасности аппарата* >> стр. 60.
- Если на аппарате используется стандартное имя сертификата сервера, рекомендуется записать стандартное имя до начала настройки. Для получения информации о стандартном имени сертификата сервера обратитесь к администратору сети.

- 2 Нажмите ▲ или ▼ для выбора параметра *Сеть*.
Нажмите **OK**.
- 3 Нажмите ▲ или ▼ для выбора параметра *Беспровод. сеть*.
Нажмите **OK**.
- 4 Нажмите ▲ или ▼ для выбора параметра *Мастер уст-ки*.
Нажмите **OK**.
- 5 При отображении сообщения *Беспр. сеть вкл.?* нажмите ▲ для подтверждения.
Запускается мастер настройки беспроводной сети.
Для отмены нажмите **Cancel**.
- 6 Аппарат выполняет поиск сети и отображает список доступных SSID.
В списке должен присутствовать записанный ранее идентификатор SSID. Если аппарат обнаружил несколько используемых сетей, с помощью кнопок ▲ и ▼ выберите нужную сеть, а затем нажмите **OK**. Перейдите к шагу 10.
Если в точке доступа отключена рассылка идентификатора SSID, необходимо вручную добавить требуемое имя SSID. Перейдите к шагу 7.
- 7 Выберите <НОВЫЙ SSID>, используя клавишу ▲ или ▼.
Нажмите **OK**. Перейдите к шагу 8.
- 8 Введите имя SSID. (Информация о вводе текста: >>Руководство по быстрой установке.)
Нажмите **OK**. Перейдите к шагу 9.
- 9 Когда появится соответствующий запрос, при помощи ▲ или ▼ выберите *Инфраструктура*.
Нажмите **OK**.
- 10 Выберите метод аутентификации при помощи ▲ или ▼ и нажмите **OK**.
Выполните одно из следующих действий:
Если выбран пункт *LEAP*, перейдите к шагу 16.
Если выбран пункт *EAP-FAST*, перейдите к шагу 11.
Если выбран пункт *PEAP*, перейдите к шагу 11.
Если выбран пункт *EAP-TTLS*, перейдите к шагу 11.
Если выбран пункт *EAP-TLS*, перейдите к шагу 12.

- 11 Выберите метод внутренней аутентификации NONE, CHAP, MS-CHAP, MS-CHAPv2, GTC или PAP с помощью кнопок ▲ и ▼, а затем нажмите **OK**.
Перейдите к шагу 12.

ПРИМЕЧАНИЕ

В зависимости от метода аутентификации можно выбрать различные методы внутренней аутентификации.

- 12 Выберите тип шифрования TKIP или AES с помощью кнопок ▲ и ▼, а затем нажмите **OK**.
Выполните одно из следующих действий:
Если методом аутентификации является EAP-TLS, перейдите к шагу 13.
При использовании других методов аутентификации перейдите к шагу 14.
- 13 На аппарате отобразится список доступных сертификатов клиента. Выберите сертификат и перейдите к шагу 14.
- 14 Выберите метод проверки подлинности Без проверки, ЦС или ЦС + идент.серв с помощью кнопок ▲ и ▼, а затем нажмите **OK**.
Выполните одно из следующих действий:
Если выбран пункт ЦС + идент.серв, перейдите к шагу 15.
Если выбрано другое значение, перейдите к шагу 16.

ПРИМЕЧАНИЕ

Если в аппарат не был выполнен импорт сертификата ЦС, отобразится сообщение *Без проверки*. Для получения информации о выполнении импорта сертификата ЦС см. раздел *Использование сертификатов для обеспечения безопасности аппарата* >> стр. 60.

- 15 Введите идентификатор сервера. (Информация о вводе текста: >>>Руководство по быстрой установке.) Перейдите к шагу 16.

- 16 Введите идентификатор пользователя, записанный в шаге 1. Нажмите **ОК**. (Информация о вводе текста: >>Руководство по быстрой установке.)
Выполните одно из следующих действий:
Если методом аутентификации является EAP-TLS, перейдите к шагу 18.
При использовании других методов аутентификации перейдите к шагу 17.
- 17 Введите пароль, записанный в шаге 1. Нажмите **ОК**. Перейдите к шагу 18.
- 18 Чтобы применить настройки, выберите **Да**. Для отмены выберите **Нет**.
Выполните одно из следующих действий:
Если выбран пункт **Да**, перейдите к шагу 19.
Если выбран пункт **Нет**, вернитесь к шагу 6.
- 19 Аппарат попытается выполнить подключение к выбранной беспроводной сети.
- 20 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение *Подключен*.
Аппарат распечатает отчет о состоянии беспроводной сети. Если происходит сбой соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке: *Устранение неисправностей*.



(Для Windows®)

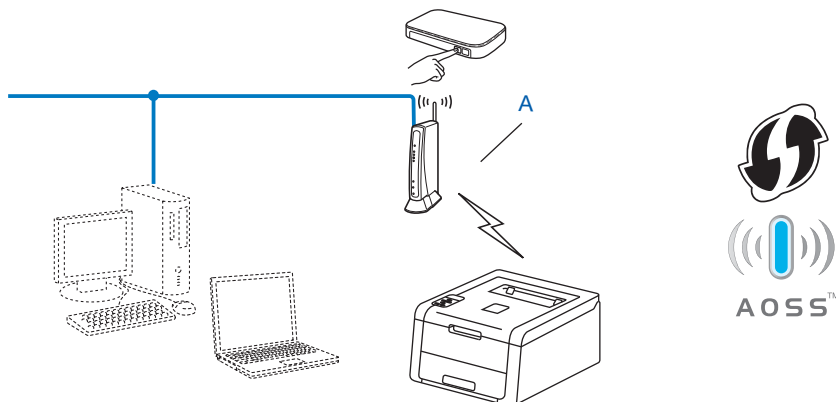
На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите “Установка драйвера принтера”.

(Для Macintosh)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите **Start Here OSX (Запуск OSX).**

Настройка одним нажатием при помощи WPS (Wi-Fi Protected Setup) или AOSS™

Если точка беспроводного доступа/маршрутизатор (A) поддерживает функцию WPS (PBC¹) или AOSS™, то для настройки параметров беспроводной сети можно использовать функцию WPS или AOSS™ в меню панели управления.



¹ Метод PBC (Push Button Configuration)

ВАЖНАЯ ИНФОРМАЦИЯ

- Если требуется подключить аппарат Brother к сети, то перед установкой рекомендуется обратиться к системному администратору. **Перед выполнением этой установки необходимо выяснить параметры беспроводной сети.**
- Если на аппарате ранее были настроены параметры беспроводной сети, то перед новой настройкой параметров беспроводной сети необходимо сбросить предыдущие параметры локальной сети.

Инструкции по сбросу параметров локальной сети см. в разделе *Восстановление заводских настроек сети* >> стр. 41.

- 1 Нажмите ▲ или ▼ для выбора параметра *Сеть*.
Нажмите **OK**.
- 2 Нажмите ▲ или ▼ для выбора параметра *Беспровод. сеть*.
Нажмите **OK**.
- 3 Нажмите ▲ или ▼ для выбора параметра *WPS/AOSS*.
Нажмите **OK**.
- 4 При отображении сообщения *Беспр. сеть вкл.?* нажмите ▲ для подтверждения.
Запускается мастер настройки беспроводной сети.
Для отмены нажмите **Cancel**.

- 5 Когда на ЖК-дисплее отобразится сообщение *Наж. клав. на марш*, нажмите кнопку WPS или AOSS™ на точке беспроводного доступа или маршрутизаторе. Инструкции см. в руководстве пользователя точки беспроводного доступа или маршрутизатора.
Затем нажмите ▲; при этом аппарат выполнит автоматическое распознавание режима (WPS или AOSS™), используемого точкой беспроводного доступа/маршрутизатором, и попытается подключиться к беспроводной сети.

- 6 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение *Подключен*.
Аппарат распечатает отчет о состоянии беспроводной сети. Если происходит сбой соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке: *Устранение неисправностей*.

OK! (Для Windows®)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите “Установка драйвера принтера”.

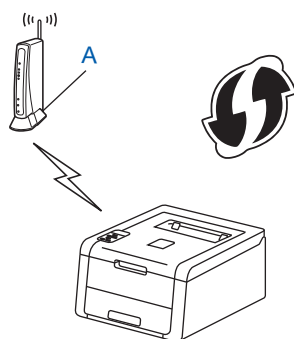
(Для Macintosh)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите Start Here OSX (Запуск OSX).

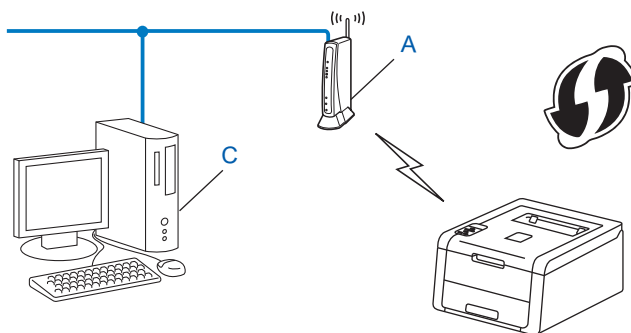
Настройка при помощи PIN-кода функции WPS (Wi-Fi Protected Setup)

Данный аппарат можно легко настроить, если точка беспроводного доступа/маршрутизатор поддерживает функцию WPS (метод PIN-кода). Метод PIN-кода — это один из методов подключения, разработанный компанией Wi-Fi Alliance®. Введя PIN-код, созданный регистрируемым (вашим) аппаратом в регистраторе (устройстве, управляющем беспроводной локальной сетью), можно настроить параметры беспроводной сети и безопасности. Инструкции по доступу к режиму WPS см. в руководстве пользователя, прилагаемом к точке беспроводного доступа/маршрутизатору.

- Подключение, при котором точка беспроводного доступа/маршрутизатор (A) одновременно является регистратором ¹.



- Подключение, при котором в качестве регистратора ¹ используется другое устройство (C) (например, компьютер).



¹ Регистратор — это устройство, управляющее беспроводной локальной сетью.

ПРИМЕЧАНИЕ

На маршрутизаторах или точках доступа, поддерживающих функцию WPS, имеется указанный ниже символ.



- 1 Нажмите ▲ или ▼ для выбора параметра **Сеть**.
Нажмите **ОК**.
- 2 Нажмите ▲ или ▼ для выбора параметра **Беспровод. сеть**.
Нажмите **ОК**.
- 3 Нажмите ▲ или ▼ для выбора параметра **WPS с PIN-код.**
Нажмите **ОК**.
- 4 При отображении сообщения **Беспр. сеть вкл.?** нажмите ▲ для подтверждения.
Запускается мастер настройки беспроводной сети.
Для отмены нажмите **Cancel**.
- 5 На ЖК-дисплее отображается 8-разрядный PIN-код, и аппарат производит поиск точки беспроводного доступа/маршрутизатора.
- 6 На компьютере, подключенном к сети, введите в адресной строке браузера “http://IP-адрес точки доступа”. (Где “IP-адрес точки доступа” – это IP-адрес устройства, используемого в качестве регистратора ¹) Перейдите на страницу настройки WPS и введите PIN-код регистратора, отображавшийся на ЖК-дисплее в шаге 5, затем следуйте инструкциям на экране.

¹ Регистратор — это обычно точка беспроводного доступа/маршрутизатор.

ПРИМЕЧАНИЕ



Вид страницы настроек может различаться для разных марок беспроводных точек доступа/маршрутизаторов. См. инструкции, прилагаемые к точке беспроводного доступа/маршрутизатору.

Windows Vista®/Windows® 7

При использовании компьютера в качестве регистратора выполните следующие операции:

ПРИМЕЧАНИЕ

- Чтобы использовать в качестве регистратора компьютер под управлением ОС Windows Vista® или Windows® 7, необходимо заранее зарегистрировать его в сети. См. инструкции, прилагаемые к точке беспроводного доступа/маршрутизатору.
- При использовании в качестве регистратора компьютера с ОС Windows® 7 можно установить драйвер принтера после настройки параметров беспроводной сети, следуя инструкциям на экране. Если требуется полная установка пакета драйверов и программ: ►►Руководство по быстрой установке.

- 1 (Windows Vista®)
Нажмите кнопку , а затем **Сеть**.
(Windows® 7)
Нажмите кнопку , а затем **Устройства и принтеры**.
- 2 (Windows Vista®)
Нажмите **Добавить беспроводное устройство**.
(Windows® 7)
Нажмите **Добавление устройства**.
- 3 Выберите аппарат и нажмите **Далее**.
- 4 Введите PIN-код, отображавшийся на ЖК-дисплее в шаге ⑤, а затем нажмите **Далее**.
- 5 Выберите сеть, к которой требуется подключиться, затем нажмите **Далее**.
- 6 Нажмите **Заккрыть**.

- 7 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение **Подключен**. Аппарат распечатает отчет о состоянии беспроводной сети. Если происходит сбой соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке: *Устранение неисправностей*.



(Для Windows®)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите “Установка драйвера принтера”.

(Для Macintosh)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите **Start Here OSX (Запуск OSX)**.

Настройка в режиме ad-hoc

Использование настроенного идентификатора SSID

При попытке подключения аппарата к компьютеру, который уже находится в режиме ad-hoc с настроенным идентификатором SSID, необходимо выполнить следующие действия:

- 1 До настройки аппарата рекомендуется записать параметры беспроводной сети. Эти данные потребуются для продолжения процесса настройки.

Проверьте и запишите текущие значения параметров беспроводной сети компьютера, к которому было выполнено подключение.

ПРИМЕЧАНИЕ

Параметры беспроводной сети на компьютере, к которому вы подключаетесь, должны быть настроены на режим ad-hoc с уже настроенным идентификатором SSID. Инструкции по переключению компьютера в режим ad-hoc см. в документации к компьютеру или обратитесь к администратору вашей сети.

Имя сети: (SSID)

Режим обмена данными	Режим шифрования	Сетевой ключ
Ad-hoc	NET	—
	WEP	

Пример:

Имя сети: (SSID)
HELLO

Режим обмена данными	Режим шифрования	Сетевой ключ
Ad-hoc	WEP	12345

ПРИМЕЧАНИЕ

Аппарат Brother поддерживает использование только первого ключа WEP.

- 2 Нажмите ▲ или ▼ для выбора параметра *Сеть*.
Нажмите **OK**.
- 3 Нажмите ▲ или ▼ для выбора параметра *Беспровод. сеть*.
Нажмите **OK**.
- 4 Нажмите ▲ или ▼ для выбора параметра *Мастер уст-ки*.
Нажмите **OK**.

- 5 При отображении сообщения *Беспр. сеть вкл.?* нажмите ▲ для подтверждения. Запускается мастер настройки беспроводной сети. Для отмены нажмите **Cancel**.
- 6 Аппарат выполняет поиск сети и отображает список доступных SSID. Если отображается список идентификаторов SSID, при помощи ▲ или ▼ выберите идентификатор SSID, записанный в пункте ❶. Выберите идентификатор SSID сети, к которой вы хотите подключиться. Нажмите **OK**.
Выполните одно из следующих действий:
Если выбран пункт *Нет*, перейдите к шагу ❹.
Если выбран пункт *ВЕР*, перейдите к шагу ❷.
- 7 Введите ключ WEP, записанный в шаге ❶. Нажмите **OK**. Перейдите к шагу ❸. (Информация о вводе текста: >>Руководство по быстрой установке.)
- 8 Чтобы применить настройки, выберите *Да*. Для отмены выберите *Нет*.
Выполните одно из следующих действий:
Если выбран пункт *Да*, перейдите к шагу ❹.
Если выбран пункт *Нет*, вернитесь к шагу ❶.
- 9 Аппарат попытается выполнить подключение к выбранному беспроводному устройству.
- 10 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение *Подключен*.
Аппарат распечатает отчет о состоянии беспроводной сети. Если происходит сбой соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке: *Устранение неисправностей*.



(Для Windows®)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите “Установка драйвера принтера”.

(Для Macintosh)

На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите **Start Here OSX (Запуск OSX)**.

Использование нового идентификатора SSID

При использовании нового идентификатора SSID все другие устройства будут подключены с помощью SSID, назначенного для аппарата в следующих шагах. К данному идентификатору SSID необходимо подключиться с компьютера, находящегося в режиме ad-hoc.

- 1 Нажмите ▲ или ▼ для выбора параметра *Сеть*.
Нажмите **ОК**.
- 2 Нажмите ▲ или ▼ для выбора параметра *Беспровод. сеть*.
Нажмите **ОК**.
- 3 Нажмите ▲ или ▼ для выбора параметра *Мастер уст-ки*.
Нажмите **ОК**.
- 4 При отображении сообщения *Беспр. сеть вкл.?* нажмите ▲ для подтверждения.
Запускается мастер настройки беспроводной сети.
Для отмены нажмите **Cancel**.
- 5 Аппарат выполняет поиск сети и отображает список доступных SSID.
Выберите <НОВЫЙ SSID>, используя клавишу ▲ или ▼.
Нажмите **ОК**.
- 6 Введите имя SSID. (Информация о вводе текста: >>Руководство по быстрой установке.)
Нажмите **ОК**.
- 7 Когда появится соответствующий запрос, при помощи ▲ или ▼ выберите *Ad-hoc*.
Нажмите **ОК**.
- 8 Выберите тип шифрования *Нет* или *WEP*, нажав ▲ или ▼, а затем нажмите **ОК**.
Выполните одно из следующих действий:
Если выбран пункт *Нет*, перейдите к шагу 10.
Если выбран пункт *WEP*, перейдите к шагу 9.
- 9 Введите ключ WEP. Нажмите **ОК**. Перейдите к шагу 10. (Информация о вводе текста:
>>Руководство по быстрой установке.)

ПРИМЕЧАНИЕ

Аппарат Brother поддерживает использование только первого ключа WEP.

- 10 Чтобы применить настройки, выберите **Да**. Для отмены выберите **Нет**.
Выполните одно из следующих действий:
Если выбран пункт **Да**, перейдите к шагу 11.
Если выбран пункт **Нет**, вернитесь к шагу 5.
 - 11 Аппарат попытается выполнить подключение к выбранному беспроводному устройству.
 - 12 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение **Подключен**.
Аппарат распечатает отчет о состоянии беспроводной сети. Если происходит сбой соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке:
Устранение неисправностей.
- OK!** **(Для Windows®)**
На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите "Установка драйвера принтера".
- (Для Macintosh)**
На этом настройка беспроводной сети завершена. Если вы хотите продолжить установку драйвера принтера, в меню компакт-диска выберите Start Here OSX (Запуск OSX).

Общая информация

Данный аппарат оснащен одним жидкокристаллическим дисплеем (ЖКД) с фоновой подсветкой и семью клавишами на панели управления. ЖК-дисплей представляет собой однострочный дисплей на 16 символов.



С помощью панели управления можно выполнить следующие действия:

Изменение настроек сервера печати с помощью панели управления

См. раздел *Меню "Сеть"* >> стр. 37.

Восстановление заводских настроек сети

См. раздел *Восстановление заводских настроек сети* >> стр. 41.

Печать отчета о конфигурации сети

См. раздел *Печать отчета о конфигурации сети* >> стр. 42.

Печать отчета WLAN (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)

См. раздел *Печать отчета WLAN (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)* >> стр. 43.

Меню “Сеть”

Команды меню **Сеть** на панели управления позволяют настроить аппарат Brother для вашей конфигурации сети. (Дополнительные сведения об использовании панели управления: >>>Руководство пользователя.) Нажмите любую клавишу меню (**▲**, **▼**, **OK** или **Back**), чтобы отобразить главное меню. Затем клавишей **▲** или **▼** выберите **Сеть**. Перейдите к пункту меню, который требуется настроить. (Дополнительные сведения о меню: см. *Таблица функций и заводские настройки по умолчанию* >>> стр. 44.)

Обратите внимание, что в комплект аппарата входит утилита BRAdmin Light ¹ или система управления через веб-интерфейс, которые также можно использовать для настройки различных параметров сети. (См. раздел *Другие утилиты управления* >>> стр. 7.)

¹ Пользователи компьютера Macintosh могут загрузить последнюю версию утилиты BRAdmin Light с веб-сайта <http://solutions.brother.com/>.

ТСР/IP

При подключении аппарата к сети с помощью сетевого кабеля используйте пункты меню **Проводная сеть**. При подключении аппарата к беспроводной сети Ethernet используйте пункты меню **Беспров.** (WLAN).

Метод загрузки

Этот параметр определяет, каким образом аппарат получает IP-адрес.

Автоматический режим

В этом режиме аппарат будет сканировать сеть для поиска сервера DHCP. Если сервер DHCP обнаружен, и его настройки позволяют выделить IP-адрес для аппарата, то будет использоваться IP-адрес, предоставленный сервером DHCP. Если сервер DHCP недоступен, IP-адрес задается с помощью протокола APIPA. После первого включения питания аппарату может потребоваться несколько минут для поиска сервера в сети.

Статический режим

В этом режиме необходимо вручную назначить аппарату IP-адрес. После ввода назначенного IP-адреса, он фиксируется.

ПРИМЕЧАНИЕ

Если не требуется настраивать сервер печати с помощью протокола DHCP, BOOTP или RARP, для параметра **Метод загрузки** необходимо выбрать значение **Статический**, чтобы сервер печати имел статический IP-адрес. В этом случае сервер печати не будет пытаться получить IP-адрес из этих систем. Чтобы изменить метод загрузки, воспользуйтесь панелью управления аппарата, утилитой BRAdmin Light или системой управления через веб-интерфейс.

IP-адрес

В этом поле отображается текущий IP-адрес аппарата. Если для параметра *Метод загрузки* выбрано значение *Статический*, введите IP-адрес, который требуется назначить аппарату (чтобы узнать нужный IP-адрес, обратитесь к администратору сети). Если выбран метод, отличный от *Статический*, аппарат будет пытаться определить свой IP-адрес с помощью протокола DHCP или BOOTP. Выбранный по умолчанию IP-адрес аппарата, вероятно, будет несовместим со схемой нумерации IP-адресов, используемой в сети. Для получения IP-адреса сети, к которой будет подключен аппарат, обратитесь к администратору сети.

Маска подсети

В этом поле отображается текущая маска подсети, используемая аппаратом. Если для получения маски подсети не используется протокол DHCP или BOOTP, введите необходимую маску подсети. Для получения маски подсети обратитесь к администратору сети.

Шлюз

В этом поле отображается текущий адрес шлюза или маршрутизатора, используемого аппаратом. Если для получения адреса шлюза или маршрутизатора не используется протокол DHCP или BOOTP, введите адрес, который необходимо назначить. Если шлюз или маршрутизатор отсутствует, оставьте это поле незаполненным. Если непонятно, каким образом следует настраивать этот параметр, обратитесь к администратору сети.

Количество попыток загрузки по IP

В этом поле отображается количество попыток получения IP-адреса аппаратом, если для параметра “Метод загрузки” установлено любое значение, кроме “Статический”.

APIPA

Если сервер печати не может получить IP-адрес выбранным методом загрузки, то установка значения *Вкл.* позволит серверу печати автоматически выделять IP-адрес локальной связи в диапазоне (169.254.1.0 – 169.254.254.255). (См. раздел *Метод загрузки* >> стр. 37.) При выборе значения *Выкл.*, если серверу печати не удастся получить IP-адрес с помощью выбранного метода загрузки, IP-адрес меняться не будет.

IPv6

Этот аппарат совместим с протоколом IPv6, протоколом Интернета нового поколения. Если нужно использовать протокол IPv6, выберите *Вкл.*. Настройка по умолчанию для протокола IPv6: *Выкл.*. Дополнительную информацию о протоколе IPv6 см. на веб-сайте <http://solutions.brother.com/>.

ПРИМЕЧАНИЕ

- Если для протокола IPv6 было задано *Вкл.*, то для активации этого параметра необходимо выключить аппарат кнопкой питания, а затем снова включить его.
- После того как для IPv6 выбрано значение *Вкл.*, эта настройка будет применена как к проводному, так и к беспроводному интерфейсу локальной сети.

Ethernet (только для проводной сети)

Режим связи Ethernet. Значение “Авто” означает, что сервер печати может работать в полно- или полудуплексном режиме 100BASE-TX или же в полно- или полудуплексном режиме 10BASE-T с автоматическим согласованием.

ПРИМЕЧАНИЕ

Неправильное задание этого значения может привести к невозможности обмена данными с сервером печати.

Состояние проводной сети (для моделей HL-3150CDN, HL-3150CDW и HL-3170CDW)

В данном поле отображается текущее состояние проводной сети.

Мастер установки (только для беспроводной сети)

Мастер уст-ки используется для настройки беспроводной сети. (Дополнительные сведения: >>Руководство по быстрой установке или *Настройка вручную с панели управления* >> стр. 18.)

WPS (Wi-Fi Protected Setup)/AOSS™ (только для беспроводной сети)

Данный аппарат можно легко настроить, если точка беспроводного доступа/маршрутизатор поддерживает функцию WPS (PBC ¹) или AOSS™ (автоматический беспроводной режим). (Дополнительные сведения: >>Руководство по быстрой установке или *Настройка одним нажатием при помощи WPS (Wi-Fi Protected Setup) или AOSS™* >> стр. 27.)

¹ Метод PBC (Push Button Configuration)

WPS (Wi-Fi Protected Setup) с PIN-кодом (только для беспроводной сети)

Данный аппарат можно легко настроить, если точка беспроводного доступа/маршрутизатор поддерживает функцию WPS (метод PIN-кода). (Подробнее см. в разделе *Настройка при помощи PIN-кода функции WPS (Wi-Fi Protected Setup)* >> стр. 29.)

Состояние беспроводной сети (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)

Состояние

В этом поле отображается текущее состояние беспроводной сети.

Сигнал

В этом поле отображается текущий уровень сигнала беспроводной сети.

Канал

В данном поле отображается текущий канал беспроводной сети.

Скорость

В данном поле отображается текущая скорость беспроводной сети.

SSID

В этом поле отображается текущий SSID беспроводной сети. На дисплее отображаются не более 32 символов имени SSID.

Режим связи

В этом поле отображается текущий режим обмена данными беспроводной сети.

MAC-адрес

MAC-адрес – это уникальный номер, который назначается сетевому интерфейсу аппарата. Можно проверить MAC-адрес аппарата на панели управления.

Настройка по умолчанию (для моделей HL-3150CDW и HL-3170CDW)

С помощью функции *Настр. по умлч.* можно установить для любого параметра проводной или беспроводной связи заводские настройки по умолчанию. Если требуется восстановить значения как для проводной, так и для беспроводной сетей, см. раздел *Восстановление заводских настроек сети* >> стр. 41.

Включение проводной сети (для моделей HL-3150CDW и HL-3170CDW)

Если требуется использовать проводное сетевое подключение, задайте для параметра *Пров. сеть* *вкл.* значение *Вкл.*

Включение беспроводной сети (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)

Если требуется использовать беспроводное сетевое подключение, задайте для параметра *Беспров. подкл.* значение *Вкл.*

ПРИМЕЧАНИЕ

Если к аппарату подключен сетевой кабель, установите для параметра *Пров. сеть* *вкл.* значение *Откл.*

Восстановление заводских настроек сети

На сервере печати можно восстановить заводские настройки по умолчанию (восстановление всей информации, такой как пароли и IP-адрес).

ПРИМЕЧАНИЕ

- Эта функция восстанавливает все заводские настройки проводной и беспроводной сети.
- Можно также восстановить заводские настройки сервера печати с помощью приложений BRAdmin или системы управления через веб-интерфейс. (Подробнее см. в разделе *Другие утилиты управления* >> стр. 7.)

- 1 Нажмите ▲ или ▼ для выбора параметра *Сеть*.
Нажмите **ОК**.
- 2 Нажмите ▲ или ▼ для выбора параметра *Сброс сет.наст.*
Нажмите **ОК**.
- 3 Нажмите клавишу ▲, чтобы выбрать *Да* для перезагрузки.
- 4 Аппарат перезагружается.

Печать отчета о конфигурации сети

ПРИМЕЧАНИЕ

Имя узла: имя узла отображается в отчете о конфигурации сети. По умолчанию используется имя узла “BRNxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxx” — это MAC-адрес/Ethernet-адрес аппарата.)

Отчет о конфигурации сети позволяет напечатать отчет, содержащий все текущие параметры конфигурации сети, в том числе параметры сетевого сервера печати.

- 1 Нажмите ▲ или ▼ для выбора параметра *Инф. об уст-ве*.
Нажмите **ОК**.
- 2 Нажмите ▲ или ▼ для выбора параметра *Печать сет.настр.*
Нажмите **ОК**.

ПРИМЕЧАНИЕ

Если для параметра **IP Address** в отчете о конфигурации сети отображается **0.0.0.0**, подождите в течение минуты, затем повторите попытку.

Печать отчета WLAN (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)

С помощью функции **Печать отч. WLAN** можно распечатать отчет о состоянии беспроводной сети аппарата. Если происходит сбой беспроводного соединения, проверьте код ошибки в напечатанном отчете. >>Руководство по быстрой установке: *Устранение неисправностей*.

- 1 Нажмите ▲ или ▼ для выбора параметра **Инф. об уст-ве**.
Нажмите **ОК**.
- 2 Нажмите ▲ или ▼ для выбора параметра **Печать отч. WLAN**.
Нажмите **ОК**.

Таблица функций и заводские настройки по умолчанию

HL-3150CDN

Заводские настройки выделены полужирным шрифтом со звездочкой.

Главное меню	Подменю	Пункты меню	Параметры
Сеть	TCP/IP	Метод загрузки	Автоматический* Статический RARP BOOTP DHCP
		IP-адрес	(000.000.000.000)* ¹
		Маска подсети	(000.000.000.000)* ¹
		Шлюз	(000.000.000.000)* ¹
		Попытки получ. IP	0/1/2/3*.../32767
		APIPA	Вкл.* Выкл.
		IPv6	Вкл. Выкл.*
	Ethernet	—	Автоматический* 100В-FD 100В-HD 10В-FD 10В-HD
	Сост. пров. сети	—	Активна 100В-FD Активна 100В-HD Активна 10В-FD Активна 10В-HD Неактивна Провод. сеть откл
	MAC-адрес	—	—
	Сброс сет. наст	Восстановление заводских настроек для всех параметров сети внутреннего сервера печати.	

¹ При подключении к сети аппарат автоматически задает допустимые для сети значения IP-адреса и маски подсети.

HL-3140CW, HL-3150CDW и HL-3170CDW

Заводские настройки выделены полужирным шрифтом со звездочкой.

Главное меню	Подменю	Пункты меню		Параметры
Сеть	Проводная сеть (HL-3150CDW и HL-3170CDW)	TCP/IP	Метод загрузки	Автоматический* Статический RARP BOOTP DHCP
			IP-адрес	(000.000.000.000)*¹
			Маска подсети	(000.000.000.000)*¹
			Шлюз	(000.000.000.000)*¹
			Попытки получ. IP	0/1/2/3*.../32767
			APIPA	Вкл.* Выкл.
			IPv6	Вкл. Выкл.*
		Ethernet	—	Автоматический* 100B-FD 100B-HD 10B-FD 10B-HD
		Сост. пров. сети	—	Активна 100B-FD Активна 100B-HD Активна 10B-FD Активна 10B-HD Неактивна Провод. сеть откл
		MAC-адрес	—	—
		Настр. по умлч.	Восстановление заводских настроек для всех параметров проводной сети внутреннего сервера печати.	
		Пров. сеть вкл.	—	Вкл.* Откл.

Главное меню	Подменю	Пункты меню		Параметры	
Сеть (продолжение)	Беспровод. сеть	TCP/IP	Метод загрузки	Автоматический* Статический RARP BOOTP DHCP	
			IP-адрес	(000.000.000.000)* ¹	
			Маска подсети	(000.000.000.000)* ¹	
			Шлюз	(000.000.000.000)* ¹	
			Попытки получ. IP	0/1/2/3*.../32767	
			APIPA	Вкл.* Выкл.	
			IPv6	Вкл. Выкл.*	
		Мастер уст-ки	—	—	
		WPS/AOSS	—	—	
		WPS с PIN-код.	—	—	
		Сост. бесп. сети	Состояние	Состояние	Активно (11n) Активна (11b) Активна (11g) Проводная сеть активна (недоступно для модели HL-3140CW) Беспр. сеть откл AOSS активен Разрыв соедин.
				Сигнал	(Отображается только при установке для параметра Беспров. подкл. значения Вкл..)
				Канал	
				Скорость	
				SSID	
		Режим связи	Ad-hoc Инфраструктура		
		MAC-адрес	—	—	
Настр. по умлч. (HL-3150CDW и HL-3170CDW)	Восстановление заводских настроек для всех параметров беспроводной сети внутреннего сервера печати.				
Беспров. подкл.	—	Вкл. Откл.*			

Главное меню	Подменю	Пункты меню		Параметры	
Сеть (продолжение)	Wi-Fi Direct ²	Кнопка	—	—	
		PIN-код	—	—	
		Вручную	—	—	
		Владел. группы	—	Вкл. Выкл.*	
		Об устройстве	Имя устройства	—	
			SSID	—	
			IP-адрес	—	
		Состояние	Состояние	Вл. гр. актив. (**) ** = количество устройств Клиент активен Не подключено Выкл. Пров. сеть актив. (недоступно для модели HL-3140CW)	
				Сигнал Сильный Средний Слабый Нет (Если для параметра Владел. группы установлено значение Вкл., для сигнала будет установлено значение Сильный).	
				Канал	
	Скорость				
	Включ. интерф.	—	Вкл. Выкл.*		
	Сброс сет.наст	Восстановление заводских настроек для всех параметров сети внутреннего сервера печати.			

¹ При подключении к сети аппарат автоматически задает допустимые для сети значения IP-адреса и маски подсети.

² Подробные сведения см. в руководстве по использованию Wi-Fi Direct™, которое можно скачать на странице "Руководства" для имеющейся модели аппарата на веб-сайте Brother Solutions Center (<http://solutions.brother.com/>).

Общая информация

Используйте стандартный браузер для изменения настроек аппарата с помощью протокола HTTP (Hyper Text Transfer Protocol – протокол передачи гипертекста) или HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer – протокол передачи гипертекста с уровнем защищенных сокетов). С помощью браузера можно включить указанную функцию или получить следующую информацию о настройке параметров сети аппарата.

- Получить информацию о состоянии аппарата
- Изменить параметры сети (например, информацию о TCP/IP)
- Настройка утилиты “Защитная блокировка функций 2.0” (см. раздел *Защитная блокировка функций 2.0* >> стр. 51).
- Настройка функции “Сохранение журнала в сети” (см. раздел *Сохранение журнала в сети* >> стр. 54).
- Получить информацию о версии программного обеспечения аппарата и сервера печати
- Изменить данные о конфигурации сети и аппарата

ПРИМЕЧАНИЕ

Рекомендуется использовать Windows® Internet Explorer® 8.0/9.0 или Safari 5.0 для Macintosh. Кроме того, вне зависимости от используемого браузера необходимо, чтобы были постоянно включены JavaScript и файлы “cookie”. Любой другой браузер должен быть совместим с HTTP 1.0 и HTTP 1.1.

В сети необходимо использовать протокол TCP/IP и запрограммировать допустимый IP-адрес на сервере печати и на компьютере.

Настройка параметров аппарата с использованием системы управления через веб-интерфейс (браузер)

Используйте стандартный браузер для изменения настроек сервера печати с помощью протокола HTTP (Hyper Text Transfer Protocol – протокол передачи гипертекста) или HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer – протокол передачи гипертекста с уровнем защищенных сокетов).

ПРИМЕЧАНИЕ

- При выполнении настроек с помощью системы управления через веб-интерфейс в целях безопасности рекомендуется использовать протокол HTTPS.
- При использовании протокола HTTPS для конфигурации с управлением через веб-интерфейс в браузере отобразится диалоговое окно с предупреждением.

- 1 Запустите браузер.
- 2 В адресную строку браузера введите “http://IP-адрес аппарата/” (где “IP-адрес аппарата” соответствует IP-адресу аппарата или имени сервера печати).
 - Например: http://192.168.1.2/

ПРИМЕЧАНИЕ

- При использовании Domain Name System (система имен доменов) или включении имени NetBIOS вместо IP-адреса можно ввести другое название, например “SharedPrinter”.


- Например: http://SharedPrinter/

Если включено имя NetBIOS, можно также использовать имя узла.

- Например: http://brnxxxxxxxxxxxxx/

Отчет о конфигурации сети (см. *Печать отчета о конфигурации сети* >> стр. 42).

- При работе на компьютере Macintosh можно легко перейти в систему управления через веб-интерфейс, щелкнув значок устройства на экране **Status Monitor**. Дополнительные сведения: >>Руководство пользователя.



- 3 По умолчанию пароль не требуется. Если был установлен пароль, введите его и нажмите .
- 4 Теперь параметры сервера печати можно изменять.

ПРИМЕЧАНИЕ

При изменении параметров протокола нажмите кнопку **Отправить**, чтобы активировать настройку, а затем перезагрузите аппарат.

Установка пароля

Чтобы предотвратить несанкционированный доступ к управлению через веб-интерфейс, рекомендуется установить пароль для входа.

- 1 Нажмите **Администратор**.
- 2 Введите пароль (не более 32 символов).
- 3 Повторно введите пароль в поле **Подтвердите новый пароль**.
- 4 Нажмите **Отправить**.
При следующем доступе к управлению через веб-интерфейс введите пароль в поле **Вход**, затем нажмите .
После настройки всех параметров выйдите из системы, нажав кнопку .

ПРИМЕЧАНИЕ

Если не устанавливается пароль для входа в систему, то можно также задать пароль, выбрав пункт **Установите пароль** на веб-странице аппарата.

Защитная блокировка функций 2.0

Утилита “Защитная блокировка функций 2.0”, разработанная компанией Brother, позволяет экономить деньги и повышает безопасность, ограничивая число функций, доступных на аппарате Brother.

Защитная блокировка функций позволяет настраивать пароли для избранных пользователей, предоставлять им доступ к выбранным или всем функциям, а также установить для них ограничение на количество страниц. Это означает, что эти функции могут использоваться только уполномоченными пользователями.

Следующие настройки утилиты Защитная блокировка функций 2.0 можно изменить с помощью управления через веб-интерфейс или приложения BRAdmin Professional 3 (только для Windows®).

- Печать^{1 2}
- Цветная печать^{1 2 3}
- Макс. число страниц³
- Счетчик страниц³

¹ К **Печать** относятся задания печати, отправленные через AirPrint, сервис Google Cloud Print и приложение Brother iPrint&Scan.

² Если зарегистрировать имена пользователей для входа в систему на ПК, то можно ограничить печать с ПК без ввода пароля. См. дополнительную информацию в разделе *Ограничение печати с ПК по логину пользователя ПК* >> стр. 52.

³ Доступно для модели **Печать**.

Настройка параметров утилиты “Защитная блокировка функций 2.0” с использованием системы управления через веб-интерфейс (браузер)

Настройка основных функций

- 1 Нажмите **Администратор** на веб-странице аппарата, после чего нажмите **Защитная блокировка функций**.
- 2 Выберите **Вкл.** в пункте **Блокировка функций**.
- 3 Введите имя группы или пользователя длиной не более 15 алфавитно-цифровых символов в поле **Идентификатор/Имя**, после чего введите пароль из четырех цифр в поле **PIN-код**.
- 4 Снимите флажки функций, которые нужно ограничить, в поле **Операции печати**. Если нужно настроить максимальное количество страниц, установите флажок **Вкл.** в поле **Макс. число страниц**, после чего введите значение в поле **Макс.**. После этого нажмите **Отправить**.

ПРИМЕЧАНИЕ

Если нужно ограничить печать с компьютера с помощью логина пользователя компьютера, нажмите **Ограничение заданий с ПК по имени пользователя** и выполните настройку параметров. (См. раздел *Ограничение печати с ПК по логину пользователя ПК* >> стр. 52.)

Настройка режима “для всех”

Чтобы задать, какие функции должны быть доступны для всех пользователей, можно настроить режим открытого доступа. Для использования функций, доступных в результате этой настройки, вводить пароль не требуется.

ПРИМЕЧАНИЕ

К общедоступному режиму относятся задания печати, отправленные через AirPrint, сервис Google Cloud Print и приложение Brother iPrint&Scan.

- 1 Снимите флажки для функций, которые нужно ограничить, в поле **Режим "для всех"**.
- 2 Нажмите **Отправить**.

Ограничение печати с ПК по логину пользователя ПК

После настройки этого параметра аппарат может выполнять аутентификацию по логину пользователя ПК, чтобы разрешить задание печати с зарегистрированного компьютера.

- 1 Нажмите **Ограничение заданий с ПК по имени пользователя**.
- 2 Выберите **Вкл.** в пункте **Ограничение заданий с ПК**.
- 3 Выберите идентификационный номер, заданный в поле **Идентификатор/Имя** в шаге ③. (см. *Настройка основных функций* >> стр. 51), из выпадающего списка **Идентификатор** и введите в поле **Имя пользователя** логин пользователя ПК.
- 4 Нажмите **Отправить**.

ПРИМЕЧАНИЕ

- Чтобы ограничить печать с ПК для группы, выберите одинаковый идентификационный номер для всех логинов, которые необходимо включить в группу.
- В случае использования функции логинов пользователей ПК необходимо убедиться, что в драйвере принтера установлен флажок **Использовать имя пользователя компьютера**.
Дополнительные сведения о драйвере принтера: >>Руководство пользователя.
- Защитная блокировка функций не поддерживает драйвер BR-Script3 для печати.

Другие функции

Защитная блокировка функций 2.0 позволяет настроить следующие функции:

■ Сброс всех счетчиков

Можно сбросить счетчик страниц, нажав **Сброс всех счетчиков**.

■ Экспорт в CSV-файл

Можно экспортировать текущий счетчик страниц, включая информацию **Идентификатор/Имя** в виде файла CSV.

■ Последнее значение счетчика

Аппарат сохраняет число страниц после сброса счетчика.

Настройка протокола SNTP с использованием управления через веб-интерфейс

SNTP – это протокол для синхронизации времени, используемого аппаратом для аутентификации на сервере времени SNTP.

1 Нажмите **Сеть**, а затем **Протокол**.

2 Для включения параметра установите флажок в поле **SNTP**.

3 Нажмите **Дополнительные параметры**.

■ **Состояние**

Отображение состояния синхронизации с сервером SNTP: включено или выключено.

■ **Метод сервера SNTP**

Выберите **АВТОМАТИЧЕСКИЙ** или **СТАТИЧЕСКИЙ**.

• **АВТОМАТИЧЕСКИЙ**

Если в сети установлен сервер DHCP, сервер SNTP автоматически получит адрес с этого сервера.

• **СТАТИЧЕСКИЙ**

Введите нужный адрес.

■ **Адрес первичного сервера SNTP, Адрес вторичного сервера SNTP**

Введите адрес сервера (до 64 знаков).

Адрес вторичного SNTP-сервера используется в качестве резервного адреса первичного SNTP-сервера. При отсутствии доступа к первичному SNTP-серверу аппарат обратится к вторичному SNTP-серверу. Если имеется первичный SNTP-сервер, а вторичный SNTP-сервер отсутствует, оставьте это поле незаполненным.

■ **Порт первичного сервера SNTP, Порт вторичного сервера SNTP**

Введите номер порта (1 – 65535).

Порт вторичного SNTP-сервера используется в качестве резервного порта первичного SNTP-сервера. При отсутствии доступа к первичному порту аппарат обратится к вторичному порту SNTP-сервера. Если имеется первичный порт SNTP, а вторичный порт SNTP отсутствует, оставьте это поле незаполненным.

■ **Интервал синхронизации**

Введите интервал в часах между попытками синхронизации с сервером (от 1 до 168 часов).

■ **Состояние синхронизации**

Можно проверить последнее состояние синхронизации.

4 Нажмите **Отправить** для применения параметров.

Сохранение журнала в сети

Функция “Сохранение журнала в сети” позволяет сохранять файл журнала печати с аппарата Brother на сетевой сервер с использованием CIFS¹. Можно сохранить идентификатор, тип задания печати, название задания печати, имя пользователя, дату, время и число напечатанных страниц для каждого задания печати.

¹ CIFS – общий протокол доступа к интернет-файлам с помощью протокола TCP/IP, позволяющий компьютерам в сети обмениваться файлами через локальную сеть или Интернет.

В журнал печати сохраняются следующие функции печати:

- Задания печати с компьютера

ПРИМЕЧАНИЕ

- Функция “Сохранение журнала в сети” поддерживает аутентификацию **Kerberos** и **NTLMv2**.
Необходимо настроить протокол SNTP (сетевой сервер времени) для выполнения аутентификации. (Для получения информации о настройке SNTP см. раздел *Настройка протокола SNTP с использованием управления через веб-интерфейс* >> стр. 53.)
- При сохранении файла на сервер для него можно установить тип **TXT** или **CSV**.

Настройка параметров функции “Сохранение журнала в сети” с использованием системы управления через веб-интерфейс (браузер)

- 1 Нажмите **Администратор** на веб-странице аппарата, после чего нажмите **Сохранение журнала печати в сеть**.
- 2 Выберите **Вкл.** в пункте **Журнал печати**.
- 3 С помощью браузера можно настроить следующие параметры.
 - **Адрес хоста**
Адрес хоста – это имя хоста сервера CIFS. Введите адрес хоста (например, mурc.example.com) (не более 64 символов) или IP-адрес (например, 192.168.56.189).
 - **Папка сохранения**
Введите целевую папку, в которой будет сохранен журнал на сервере CIFS (например, brother\abc) (не более 60 символов).
 - **Имя файла**
Введите нужное имя файла журнала печати длиной до 15 символов.
 - **Тип файла**
Выберите тип файла для журнала печати: **TXT** или **CSV**.

■ Метод аутентификации

Выберите метод аутентификации для доступа к серверу CIFS: **Автоматически**, **Kerberos**¹ или **NTLMv2**².

¹ Kerberos является протоколом аутентификации, позволяющим устройствам или отдельным людям подтверждать подлинность с помощью технологии единого входа.

² Методом аутентификации для доступа к серверам, используемым в Windows, является NTLMv2.

- **Автоматически:** при установке значения Auto (“Авто”) аппарат будет выполнять сначала поиск сервера Kerberos. Если сервер Kerberos не будет обнаружен, в качестве метода аутентификации будет установлен NTLMv2.
- **Kerberos:** выберите значение Kerberos, чтобы использовать только аутентификацию Kerberos.
- **NTLMv2:** выберите значение NTLMv2, чтобы использовать только аутентификацию NTLMv2.

Для аутентификации Kerberos и NTLMv2 необходимо также настроить протокол SNTP (сетевой сервер времени).

Для получения информации о настройке параметров SNTP см. раздел *Настройка протокола SNTP с использованием управления через веб-интерфейс* >> стр. 53.

■ Имя пользователя

Введите имя пользователя для аутентификации длиной до 96 символов.

ПРИМЕЧАНИЕ

Если имя пользователя входит в домен, введите его одним из следующих образов: user@domain или domain\user.

■ Пароль

Введите пароль для аутентификации длиной до 32 символов.

■ Адрес сервера Kerberos (при необходимости)

Введите адрес хоста KDC (например, турс.example.com) (не более 64 символов) или IP-адрес (например, 192.168.56.189).

■ Настройка определения ошибок (см. *Настройка обнаружения ошибок* >> стр. 57.)

- 4 С помощью параметра **Состояние подключения** можно проверить состояние последнего журнала. Для получения дополнительной информации см. раздел *Значение сообщений об ошибках* >> стр. 58.

- 5 Нажмите **Отправить** для отображения страницы **Тестовое сохранение журнала печати в сетевую папку**.
Чтобы проверить настройки, нажмите кнопку **Да** и перейдите к шагу 6.
Чтобы пропустить проверку, нажмите **Нет**. Настройки будут переданы автоматически.
- 6 Аппарат проверит заданные настройки.
- 7 Если настройки принимаются, на странице появится индикация **Тестовое сканирование выполнено успешно**.
В случае появления индикации **Ошибка тестового сканирования** проверьте все настройки и нажмите кнопку **Отправить**, чтобы отобразить страницу проверки повторно.

Настройка обнаружения ошибок

Можно выбрать действие, которое будет выполняться, если не удастся сохранить журнал печати на сервере из-за сетевой ошибки.

- 1 Для параметра **Настройка определения ошибок** установите значение **Отменить печать** или **Игнор. журнал и печать** в разделе **Сохранение журнала печати в сеть**.

■ Отменить печать

При выборе значения **Отменить печать** задания печати отменяются, если журнал печати не удастся сохранить на сервере.

■ Игнор. журнал и печать

При выборе значения **Игнор. журнал и печать** аппарат производит печать документа, даже если журнал печати не удастся сохранить на сервере.

При восстановлении функции сохранения журнала печати запись журнала производится следующим образом:

- Если журнал не удастся сохранить в конце печати, сохраняется журнал печати без числа отпечатанных страниц. (1)
- Если журнал печати не удастся сохранить в начале печати, журнал задания печати не сохраняется. После восстановления функции в журнале будет показана ошибка. (2)

Пример журнала печати:

Id	Type	Job Name	User Name	Date	Time	Print Pages	Color Pages
1	Print (xxxxxxx)	"Document01.doc"	"user01"	03/03/20xx	14:01:32	52	21
2	Print (xxxxxxx)	"Document02.doc"	"user01"	03/03/20xx	14:45:30	?	?
3	<Error>	?, ?, ?, ?, ?, ?					
4	Print (xxxxxxx)	"Report01.xls"	"user02"	03/03/20xx	19:30:40	4	4

- 2 Нажмите **Отправить** для отображения страницы **Тестовое сохранение журнала печати в сетевую папку**.

Чтобы проверить настройки, нажмите кнопку **Да** и перейдите к шагу 3.

Чтобы пропустить проверку, нажмите **Нет**. Настройки будут переданы автоматически.

- 3 Аппарат проверит заданные настройки.

- 4 Если настройки принимаются, на странице появится индикация **Тестовое сканирование выполнено успешно**.

В случае появления индикации **Ошибка тестового сканирования** проверьте все настройки и нажмите кнопку **Отправить**, чтобы отобразить страницу проверки повторно.

Значение сообщений об ошибках

Состояние ошибки можно проверить на ЖК-дисплее аппарата или с помощью пункта **Состояние подключения** в системе управления через веб-интерфейс.

- Тайм-аут сервера, обратитесь к администратору.

Данное сообщение появляется, если не удается подключиться к серверу.

Убедитесь, что выполнены следующие условия:

- Адрес сервера введен правильно.
- Сервер подключен к сети.
- Аппарат подключен к сети.

- Ошибка аутентификации, обратитесь к администратору.

Если параметр **Настройка аутентификации** установлен неправильно, появится сообщение.

Убедитесь, что выполнены следующие условия:

- Имя пользователя¹ и пароль в параметрах аутентификации указаны правильно.

¹ Если имя пользователя входит в домен, введите его одним из следующих образов: user@domain или domain\user.

- Время сервера файла журнала совпадает со временем SNTP-сервера.
- Параметры сервера времени SNTP настроены правильно и время сервера совпадает со временем, используемым для аутентификации с помощью протоколов Kerberos или NTLMv2.

- Ошибка доступа к файлу, обратитесь к администратору.

Данное сообщение появляется, если не удается получить доступ к целевой папке.

Убедитесь, что выполнены следующие условия:

- Имя каталога хранения указано правильно.
- Разрешена запись в каталог хранения.
- Файл не заблокирован.

- Неверная дата и время. Обратитесь к администратору.

Данное сообщение появляется, если аппарат не получает время с сервера времени SNTP. С помощью управления через веб-интерфейс проверьте, правильно ли настроены параметры доступа к серверу времени SNTP.

ПРИМЕЧАНИЕ

При выборе параметра **Отменить печать** в системе управления через веб-интерфейс сообщение `Ошиб. дост. к журн` будет отображаться на ЖК-дисплее в течение 30 секунд.

Общая информация

В современном мире существует множество угроз безопасности для сетей и передаваемых по ним данных. В аппарате Brother используются самые современные протоколы безопасности и шифрования. Эти сетевые функции можно включить в общий план обеспечения сетевой безопасности для защиты данных и предотвращения несанкционированного доступа к аппарату. В этой главе объясняются процедуры их настройки.

Можно настроить следующие функции безопасности:

- Безопасное управление сетевым аппаратом с помощью SSL/TLS (см. *Безопасное управление сетевым аппаратом с помощью SSL/TLS* >> стр. 75).
- Безопасное управление сетевым аппаратом с помощью протокола SNMPv3 (см. *Безопасное управление с помощью системы управления через веб-интерфейс (браузер)* >> стр. 75 или *Безопасное управление с помощью утилиты BRAdmin Professional 3 (Windows®)* >> стр. 78).
- Безопасное управление с помощью утилиты BRAdmin Professional 3 (Windows®) (см. раздел *Безопасное управление с помощью утилиты BRAdmin Professional 3 (Windows®)* >> стр. 78.)
- Безопасная печать документов по протоколу SSL/TLS (см. *Безопасная печать документов по протоколу SSL/TLS* >> стр. 79).
- Безопасная отправка сообщений электронной почты (см. раздел *Безопасная отправка электронной почты* >> стр. 80).
- Использование аутентификации IEEE 802.1x (см. *Использование аутентификации IEEE 802.1x* >> стр. 83).
- Сертификат для безопасного управления (см. *Использование сертификатов для обеспечения безопасности аппарата* >> стр. 60).
- Управление несколькими сертификатами (см. *Управление несколькими сертификатами* >> стр. 74).

ПРИМЕЧАНИЕ

Рекомендуется отключить протоколы Telnet, FTP и TFTP. Доступ к аппарату с использованием этих протоколов небезопасен. (См. информацию о настройке протоколов в разделе *Настройка параметров аппарата с использованием системы управления через веб-интерфейс (браузер)* >> стр. 49.)

Использование сертификатов для обеспечения безопасности аппарата

Аппарат Brother поддерживает использование нескольких сертификатов безопасности, позволяющих осуществлять безопасное управление и аутентификацию, а также устанавливать безопасное соединение с аппаратом. Для аппарата можно использовать следующие функции безопасности.

- Связь с использованием протоколов SSL/TLS
- Аутентификация IEEE 802.1x
- Соединение по протоколу SSL для SMTP/POP3

Аппарат Brother поддерживает следующие сертификаты.

- Предварительно установленный сертификат

На этом аппарате имеется предварительно установленный самозаверяющий сертификат.

Пользуясь этим сертификатом, можно с легкостью использовать соединение по протоколу SSL/TLS без создания или установки сертификата.

ПРИМЕЧАНИЕ

Предварительно установленный самозаверяющий сертификат не обеспечивает защиту от спуфинга. Для повышения безопасности рекомендуется использовать сертификат, выданный надежной организацией.

- Самозаверяющий сертификат

Сервер печати использует свой собственный сертификат. Пользуясь этим сертификатом, можно с легкостью использовать связь по протоколу SSL/TLS без получения сертификата от центра сертификации. (См. раздел *Создание и установка сертификата* >> стр. 63.)

- Сертификат от ЦС

Существует два способа установки такого сертификата. Если сертификат ЦС уже имеется или если требуется использовать сертификат от стороннего заслуживающего доверие ЦС:

- С использованием CSR (запрос на подпись сертификата) от данного сервера печати. (См. раздел *Создание CSR* >> стр. 64.)
- С импортированием сертификата и секретного ключа. (См. раздел *Импорт и экспорт сертификата и секретного ключа* >> стр. 71.)

■ Сертификат ЦС


Если используется сертификат ЦС, определяющий сам ЦС (центр сертификации), а также имеющий собственный секретный ключ, необходимо импортировать сертификат ЦС из ЦС до выполнения настройки. (См. раздел *Импорт и экспорт сертификата ЦС* >> стр. 73.)

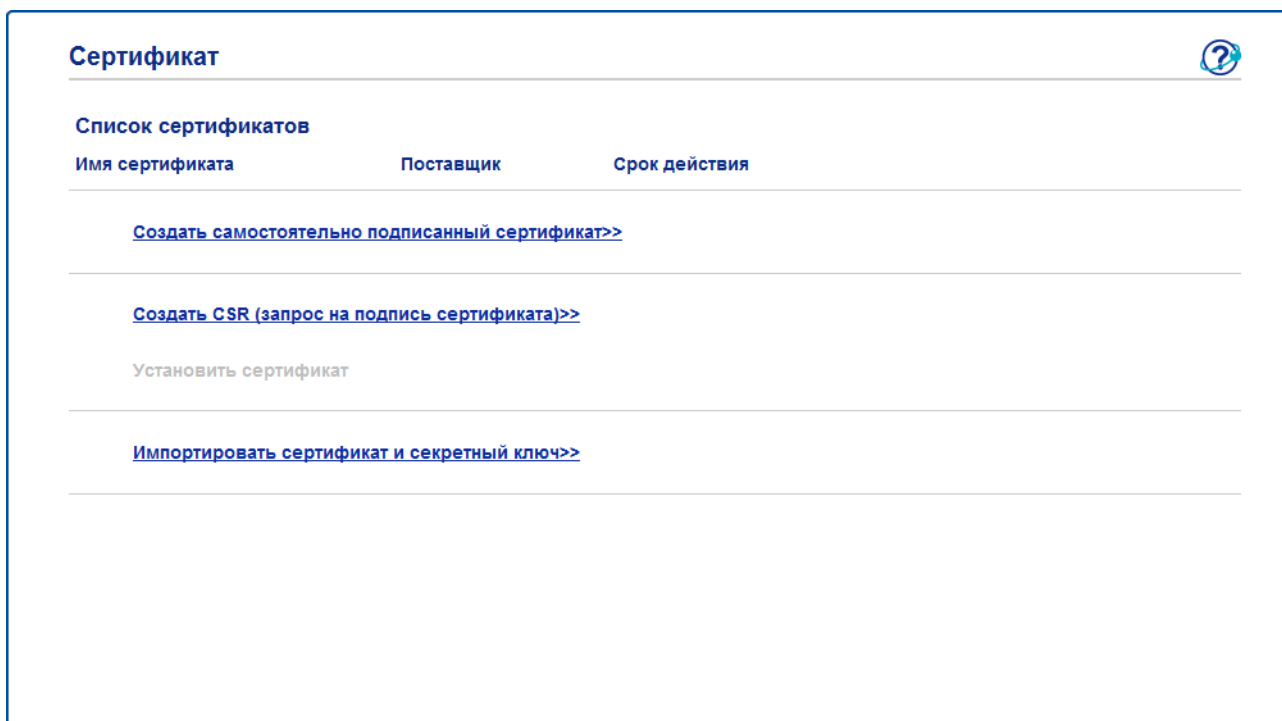
ПРИМЕЧАНИЕ

- При использовании соединения SSL/TLS сначала рекомендуется связаться со своим системным администратором.
 - При восстановлении заводских параметров сервера печати установленный сертификат и секретный ключ будут удалены. Если после перезагрузки сервера печати требуется использование того же сертификата и секретного ключа, следует их экспортировать и установить повторно после перезагрузки. (См. раздел *Экспорт самоподписанного сертификата, сертификата ЦС и секретного ключа* >> стр. 72.)
-

Настройка сертификата с помощью управления через веб-интерфейс

Эту функцию можно настроить только с помощью системы управления через веб-интерфейс. Чтобы получить доступ к странице настройки сертификата с помощью системы управления через веб-интерфейс, выполните следующие действия.

- 1 Запустите браузер.
- 2 В адресную строку браузера введите “http://IP-адрес аппарата/” (где “IP-адрес аппарата” соответствует IP-адресу аппарата или имени сервера печати).
 - Например: http://192.168.1.2/
- 3 По умолчанию пароль не требуется. Если был установлен пароль, введите его и нажмите .
- 4 Нажмите **Сеть**.
- 5 Нажмите **Безопасность**.
- 6 Нажмите **Сертификат**.
- 7 С помощью экрана, приведенного ниже, можно настроить параметры сертификата.

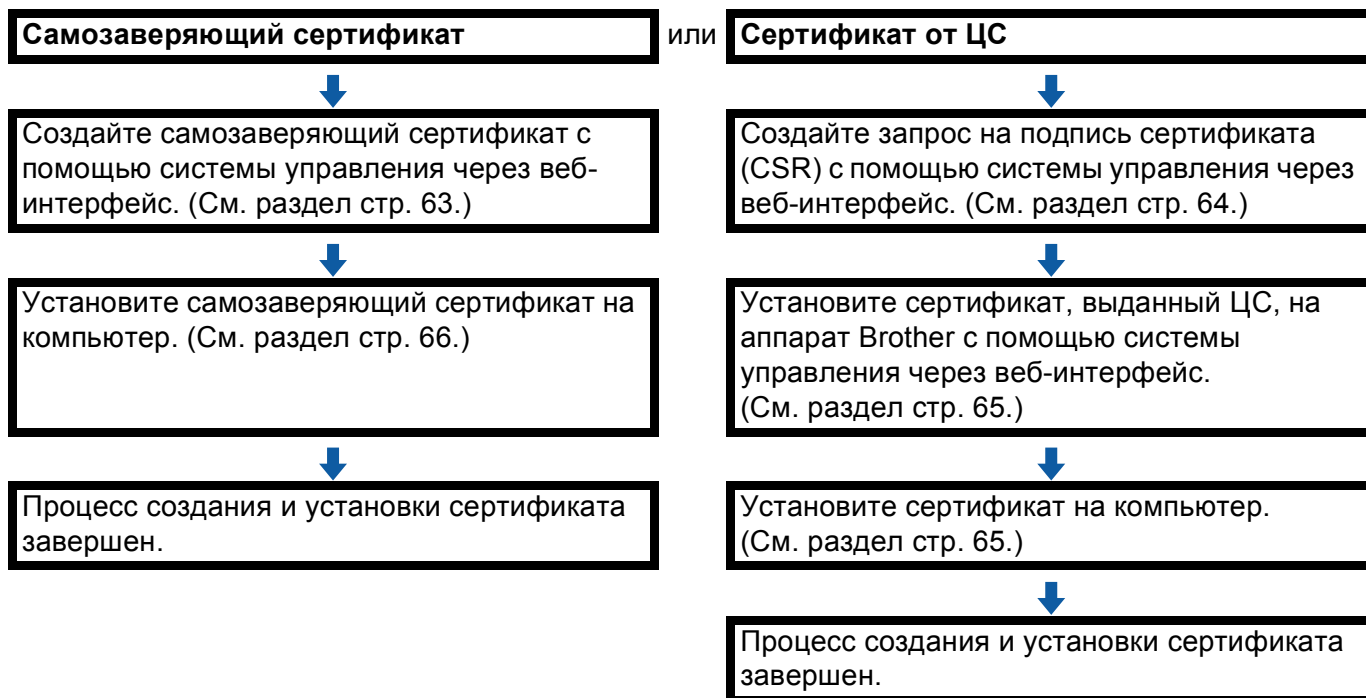


ПРИМЕЧАНИЕ

- Затененные функции, не оформленные в виде ссылок, недоступны.
- Чтобы получить дополнительную информацию по настройке, обратитесь к справке системы управления через веб-интерфейс.

Создание и установка сертификата

Пошаговая схема создания и установки сертификата



Создание и установка самозаверяющего сертификата

- 1 Нажмите **Создать самостоятельно подписанный сертификат** на стр. **Сертификат**.
- 2 Введите **Общее название** и **Срок действия**.

ПРИМЕЧАНИЕ

- Длина имени в поле **Общее название** должна быть меньше 64 символов. Введите идентификатор, такой как IP-адрес, имя узла или имя домена, чтобы использовать его при доступе к аппарату через соединение по протоколу SSL/TLS. По умолчанию отображается имя узла.
- Если используется протокол IPPS или HTTPS, при вводе адреса URL, отличного от указанного в параметре **Общее название**, который был использован для заполнения самозаверяющего сертификата, будет отображаться всплывающее сообщение.

- 3 В выпадающем списке можно выбрать значения параметров **Алгоритм с использованием открытых ключей** и **Алгоритм выборки**. Настройки по умолчанию: **RSA (2048 бит)** для параметра **Алгоритм с использованием открытых ключей** и **SHA-256** для параметра **Алгоритм выборки**.
- 4 Нажмите **Отправить**.

- 5 Создание и установка самозаверяющего сертификата в память аппарата завершена успешно. Чтобы использовать соединение по протоколу SSL/TLS, на компьютере необходимо установить самозаверяющий сертификат. Для получения дополнительной информации см. раздел *Установка самозаверяющего сертификата на компьютер* >> стр. 66.

Создание CSR

- 1 Нажмите **Создать CSR (запрос на подпись сертификата)** на стр. **Сертификат**.
- 2 Введите **Общее название** и свои данные, такие как **Организация**.

ПРИМЕЧАНИЕ

- Перед созданием запроса на подпись сертификата рекомендуется установить на компьютере корневой сертификат, полученный от ЦС.
- Длина имени в поле **Общее название** должна быть меньше 64 символов. Введите идентификатор, такой как IP-адрес, имя узла или имя домена, чтобы использовать его при доступе к принтеру через по каналу связи, защищенному с помощью SSL/TLS. По умолчанию отображается имя узла. Поле **Общее название** является обязательным для заполнения.
- При вводе адреса URL, отличного от стандартного имени, которое было использовано для заполнения сертификата, будет отображаться всплывающее сообщение.
- Длина наименований в полях **Организация**, **Подразделение**, **Город/район**, **Страна/регион** должна быть меньше 64 символов.
- В поле **Страна/регион** необходимо указать код страны, состоящий из двух символов, в соответствии со стандартом ISO 3166.
- Если выполняется настройка расширения сертификата X.509v3, установите флажок в поле **Настройка дополнительного раздела**, а затем выберите **Авто (Регистрация IPv4)** или **Вручную**.

- 3 В выпадающем списке можно выбрать значения параметров **Алгоритм с использованием открытых ключей** и **Алгоритм выборки**. Настройки по умолчанию: **RSA (2048 бит)** для параметра **Алгоритм с использованием открытых ключей** и **SHA-256** для параметра **Алгоритм выборки**.
- 4 Нажмите **Отправить**.
- 5 При отображении содержания запроса на подпись сертификата нажмите **Сохранить**, чтобы сохранить файл запроса на своем компьютере.

- 6 Запрос на подпись сертификата создан.

ПРИМЕЧАНИЕ

- Чтобы отправить запрос на подпись сертификата в центр сертификации, выполните соответствующие указания своего ЦС.
 - Если используется Enterprise root CA операционной системы Windows Server® 2003/2008/2012, то при создании сертификата клиента для обеспечения безопасного управления рекомендуется использовать для шаблона сертификата **Веб-сервер**. При создании сертификата клиента для среды IEEE 802.1x с аутентификацией EAP-TLS рекомендуется использовать для шаблона сертификата **Пользователь**. Для получения дополнительной информации перейдите с главной страницы своей модели по адресу: <http://solutions.brother.com/> на страницу соединения по протоколу SSL.
-

Установка сертификата на аппарат

При получении сертификата из ЦС выполните следующие действия, чтобы установить полученный сертификат на сервер печати.

ПРИМЕЧАНИЕ

Возможна установка только того сертификата, который был получен по запросу, отправленному с этого аппарата. Если необходимо создать еще один запрос на подпись сертификата, перед созданием убедитесь, что сертификат установлен. После установки сертификата на аппарат создайте другой запрос на подпись сертификата. В противном случае созданный перед установкой сертификата запрос на подпись будет неверным.

- 1 Нажмите **Установить сертификат** на стр. **Сертификат**.
- 2 Укажите файл сертификата, выданный ЦС, и нажмите **Отправить**.
- 3 Теперь создание и установка сертификата в память аппарата завершена успешно. Чтобы использовать связь по протоколу SSL/TLS, на компьютере необходимо установить корневой сертификат, полученный из ЦС. Чтобы получить консультацию по его установке, обратитесь к администратору сети.

Выбор сертификата

После установки сертификата выполните следующие действия, чтобы выбрать нужный сертификат.

- 1 Нажмите **Сеть**.
- 2 Нажмите **Протокол**.
- 3 Нажмите **Настройки сервера HTTP** и выберите сертификат в выпадающем списке **Выбор сертификата**.

Настройки сервера HTTP

Если требуется безопасное соединение, рекомендуется использовать SSL.
(Рекомендуемые настройки безопасности будут заданы после выбора сертификата.)

Выбор сертификата Предустановка

(Можно выбрать или отменить выбор следующих протоколов для сертификата SSL.)

Система управления через веб-интерфейс

HTTPS(Порт 443)
 HTTP(Порт 80)

IPP

HTTPS(Порт 443)
 HTTP
 Порт 80
 Порт 631

Веб-службы

HTTP

[Сертификат](#)

Установка самозаверяющего сертификата на компьютер

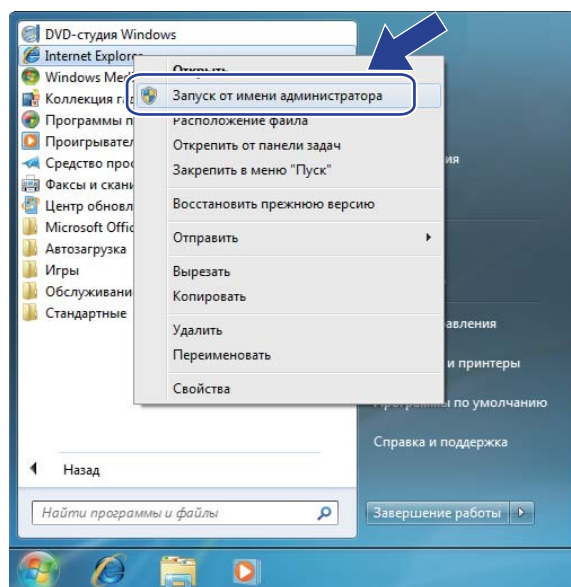
ПРИМЕЧАНИЕ

- При работе в программе Windows® Internet Explorer® необходимо выполнить следующие шаги. При использовании другого браузера следует обратиться к справке этого браузера.
- Для установки самозаверяющего сертификата требуются права администратора.

Для пользователей Windows Vista®, Windows® 7 и Windows Server® 2008, имеющих права администратора

- 1 Нажмите кнопку  и выберите **Все программы**.

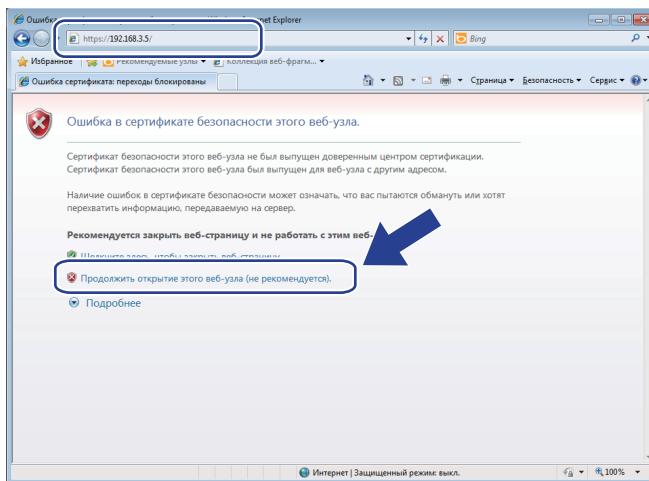
- Щелкните правой кнопкой мыши **Internet Explorer**, а затем выберите **Запуск от имени администратора**.



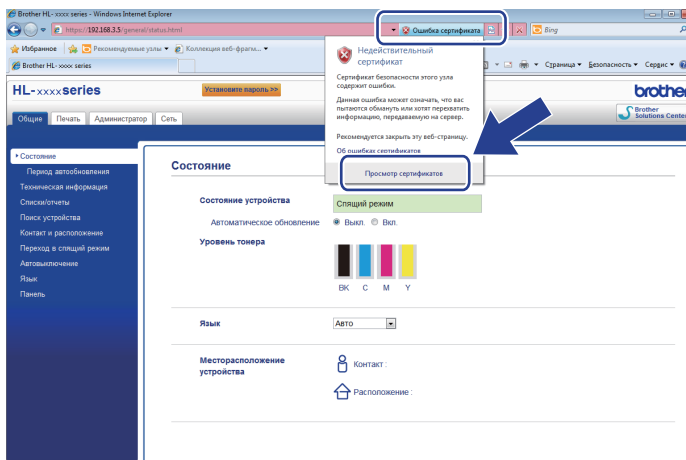
ПРИМЕЧАНИЕ

Если отображается экран **Контроль учетных записей пользователей**,
(Windows Vista®) щелкните **Продолжить (Разрешить)**.
(Windows® 7/Windows® 8) щелкните **Да**.

- 3 Чтобы получить доступ к аппарату, введите в браузере “https://IP-адрес аппарата/” (где “IP-адрес аппарата” – это IP-адрес или имя узла, назначенное для сертификата). После этого нажмите **Продолжить открытие этого веб-узла (не рекомендуется)**.

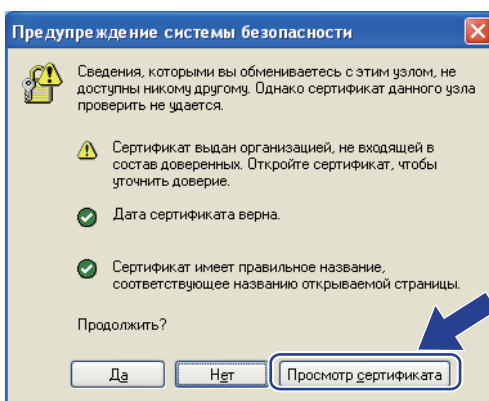


- 4 Нажмите **Ошибка сертификата**, а затем **Просмотр сертификатов**. Чтобы выполнить остальные инструкции, выполните шаги с 4 в разделе *Для пользователей Windows® XP и Windows Server® 2003* >> стр. 69.

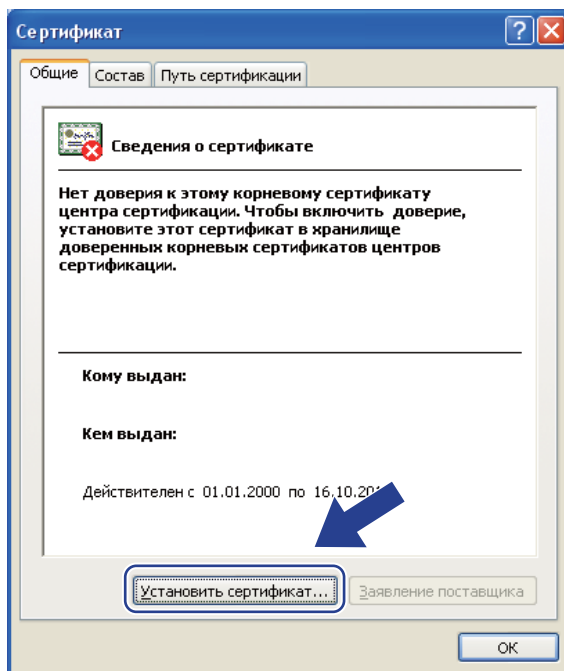


Для пользователей Windows® XP и Windows Server® 2003

- 1 Запустите браузер.
- 2 Чтобы получить доступ к аппарату, введите в браузере “https://IP-адрес аппарата/” (где “IP-адрес аппарата” – это IP-адрес или имя узла, назначенное для сертификата).
- 3 После появления диалогового окна оповещения о безопасности выполните одно из следующих действий:
 - Нажмите **Продолжить открытие этого веб-узла (не рекомендуется)**.. Нажмите **Ошибка сертификата**, а затем **Просмотр сертификатов**.
 - Если появится следующее диалоговое окно, нажмите **Просмотр сертификата**.

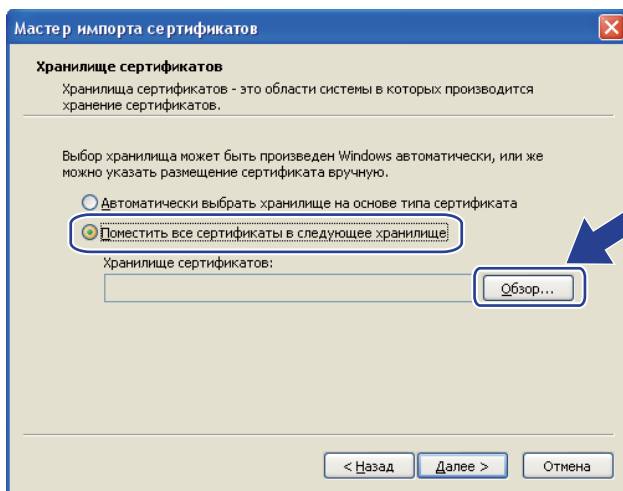


- 4 Нажмите **Установить сертификат...** на вкладке **Общие**.

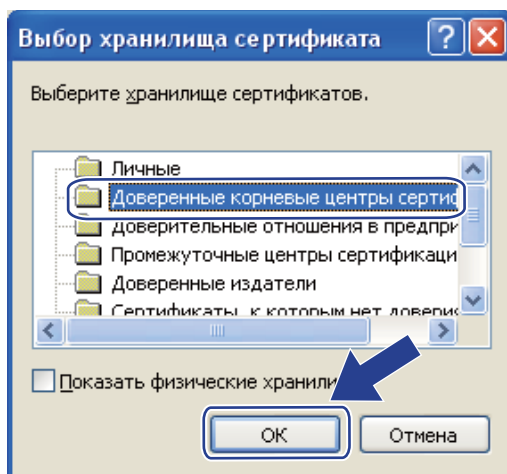


- 5 Когда отобразится **Мастер импорта сертификатов**, нажмите **Далее**.

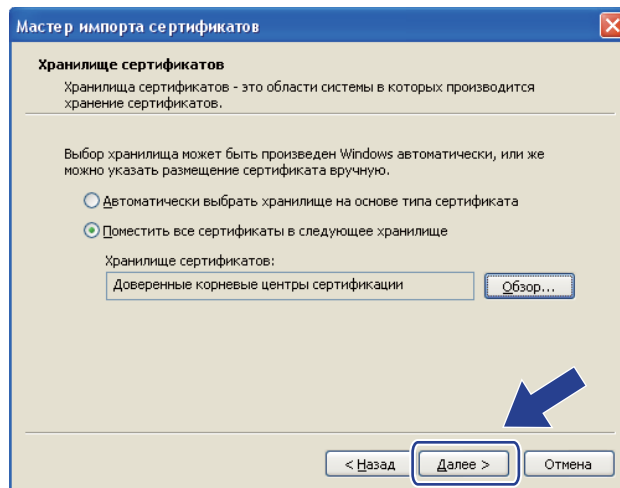
- 6 Необходимо указать папку для установки сертификата. Рекомендуется выбрать опцию **Поместить все сертификаты в следующее хранилище** и нажать **Обзор....**



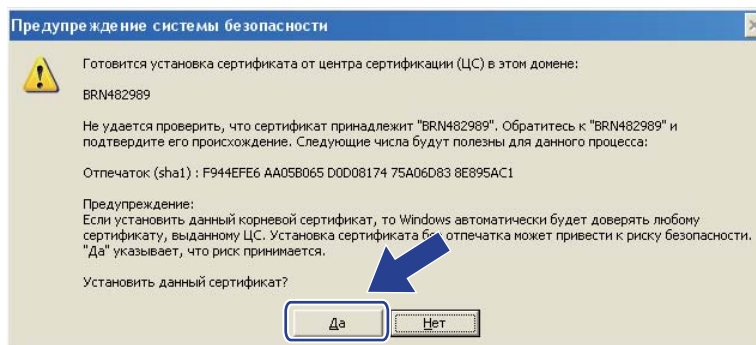
- 7 Выберите **Доверенные корневые центры сертификации**, затем нажмите **ОК**.



- 8 Нажмите **Далее**.



- 9 Нажмите **Готово**.
- 10 Нажмите **Да**, если отпечаток пальца (отпечаток большого пальца) верен.



ПРИМЕЧАНИЕ

Отпечаток пальца (отпечаток большого пальца) печатается в отчете о конфигурации сети (см. *Печать отчета о конфигурации сети* >> стр. 42).

6

- 11 Нажмите **ОК**.
- 12 Теперь самозаверяющий сертификат установлен на компьютере, и имеется возможность осуществлять связь по протоколу SSL/TLS.

Импорт и экспорт сертификата и секретного ключа

В аппарате можно хранить сертификат и секретный ключ и управлять ими с помощью импорта и экспорта.

Импорт самозаверяющего сертификата, сертификата ЦС и секретного ключа

- 1 Нажмите **Импортировать сертификат и секретный ключ** на стр. **Сертификат**.
- 2 Укажите файл, который необходимо импортировать.
- 3 Введите пароль, если файл зашифрован, и нажмите **Отправить**.
- 4 Теперь сертификат и секретный ключ успешно импортированы в аппарат. Чтобы использовать связь по протоколу SSL/TLS, на компьютере необходимо также установить корневой сертификат, полученный из ЦС. Чтобы получить консультацию по его установке, обратитесь к администратору сети.

Экспорт самоподписанного сертификата, сертификата ЦС и секретного ключа

- 1 Нажмите **Экспорт** рядом с пунктом **Список сертификатов** на странице **Сертификат**.
- 2 Введите пароль, если необходимо зашифровать файл.

ПРИМЕЧАНИЕ

Если пароль не используется, то шифровка файла не будет выполнена.

- 3 Введите пароль повторно для подтверждения и нажмите **Отправить**.
- 4 Укажите, где необходимо сохранить файл.
- 5 Теперь сертификат и секретный ключ экспортированы в компьютер.

ПРИМЕЧАНИЕ

Экспортированный файл можно импортировать.

Импорт и экспорт сертификата ЦС

В аппарате можно хранить сертификат ЦС и осуществлять его импорт и экспорт.

Импорт сертификата ЦС

- 1 Нажмите **Сертификат ЦС** на стр. **Безопасность**.
- 2 Нажмите **Импорт сертификата ЦС** и выберите сертификат. Нажмите **Отправить**.

Экспорт сертификата ЦС

- 1 Нажмите **Сертификат ЦС** на стр. **Безопасность**.
- 2 Выберите сертификат, который требуется экспортировать, и нажмите **Экспорт**. Нажмите **Отправить**.
- 3 Нажмите **Сохранить**, чтобы выбрать целевую папку.
- 4 Выберите папку для сохранения экспортированного сертификата, затем сохраните сертификат.

Управление несколькими сертификатами

Функция использования нескольких сертификатов позволяет управлять отдельно каждым сертификатом, установленным с помощью системы управления через веб-интерфейс. После установки сертификатов на странице **Сертификат** можно просмотреть установленные сертификаты, ознакомиться с содержимым каждого сертификата, удалить или экспортировать сертификат. Сведения о доступе к странице **Сертификат** см. в разделе *Настройка сертификата с помощью управления через веб-интерфейс* >> стр. 62. Аппарат Brother позволяет хранить до трех самоподписанных сертификатов или до трех сертификатов, выданных ЦС. Сохраненные сертификаты можно задействовать для использования протокола HTTPS/IPPS или для аутентификации IEEE 802.1x.

Можно также хранить до четырех сертификатов ЦС для использования аутентификации IEEE 802.1x и протокола SSL для SMTP/POP3.

Рекомендуется хранить на один сертификат меньше максимального числа, чтобы иметь одно свободное место в случае истечения срока действия сертификата. Например, если необходимо хранить сертификат ЦС, храните три сертификата и оставьте одну ячейку хранения в качестве резервной. В этом случае при повторной выдаче сертификата, например в случае истечения срока его действия, можно будет импортировать новый сертификат в резервную ячейку а затем удалить истекший сертификат, чтобы избежать сброса настроек.

ПРИМЕЧАНИЕ

- При использовании протокола HTTPS/IPPS или IEEE 802.1x, необходимо выбрать сертификат, который будет использоваться.
- При использовании SSL для соединений SMTP выбирать сертификат нет необходимости. Нужный сертификат будет выбран автоматически.

Безопасное управление сетевым аппаратом с помощью SSL/TLS

Для безопасного управления сетевым аппаратом необходимо использовать утилиты управления с протоколами безопасности.


Безопасное управление с помощью системы управления через веб-интерфейс (браузер)

Для безопасного управления рекомендуется использовать протокол HTTPS. Чтобы использовать эти протоколы, необходимо настроить следующие параметры аппарата.

ПРИМЕЧАНИЕ

По умолчанию протокол HTTPS включен.

Параметры протокола HTTPS и сертификат можно изменить на экране управления через веб-интерфейс, нажав **Сеть**, **Протокол**, затем нажав **Настройки сервера HTTP**.


- 1 Запустите браузер.
- 2 Введите в браузере “http://IP-адрес аппарата”. (Если используется созданный сертификат, введите в браузере “http://стандартное_имя”, где “стандартное_имя” – это стандартное имя, назначенное для сертификата, например, IP-адрес, имя узла или домена. О назначении стандартного имени для сертификата см. раздел *Использование сертификатов для обеспечения безопасности аппарата* >> стр. 60.)
 - Пример:
http://192.168.1.2/ (если стандартным именем является IP-адрес аппарата)
- 3 По умолчанию пароль не требуется. Если был установлен пароль, введите его и нажмите .
- 4 Теперь имеется доступ к аппарату с помощью протокола HTTPS. Если используется протокол SNMPv3, следуйте описанным ниже действиям.

ПРИМЕЧАНИЕ

Можно также изменить настройки SNMP с помощью утилиты BRAdmin Professional 3.

- 5 Нажмите **Сеть**.
- 6 Нажмите **Протокол**.

- 7 Убедитесь в том, что включена настройка **SNMP**, после чего нажмите **Дополнительные параметры** протокола **SNMP**.
- 8 С помощью экрана, приведенного ниже, можно настроить параметры протокола SNMP.

SNMP 

Состояние: Включено

Режим работы SNMP

- Доступ SNMP v1/v2c для чтения/записи
- Доступ SNMPv3 для чтения/записи и SNMPv1/v2c только для чтения
- Доступ SNMPv3 для чтения/записи

Настройки режима SNMP v1/v2c

- Разрешить управление сетью более старыми версиями BRAdmin

Существует три режима соединений **SNMP**.

■ **Доступ SNMP v1/v2c для чтения/записи**

В этом режиме сервер печати использует версию 1 и 2с протокола SNMP. В этом режиме можно использовать все приложения Brother. Однако не обеспечивается достаточный уровень безопасности, поскольку не выполняется аутентификация пользователя и шифрование данных.

■ **Доступ SNMPv3 для чтения/записи и SNMPv1/v2c только для чтения**

В этом режиме сервер печати использует доступ для чтения-записи версии 3, доступ только для чтения версии 1 и версию 2с протокола SNMP.

ПРИМЕЧАНИЕ

Если используется режим **Доступ SNMPv3 для чтения/записи и SNMPv1/v2c только для чтения**, некоторые из приложений Brother (например, BRAdmin Light), которые выполняют доступ к серверу печати, будут работать некорректно, поскольку они разрешают доступ только для чтения версии 1 и версии 2с. Если требуется использовать все приложения, используйте режим **Доступ SNMP v1/v2c для чтения/записи**.

■ Доступ SNMPv3 для чтения/записи

При этом режиме сервер печати использует версию 3 протокола SNMP. Используйте этот режим, если нужно безопасно управлять сервером печати.

ПРИМЕЧАНИЕ

- Если используется режим **Доступ SNMPv3 для чтения/записи**, имейте в виду следующее.
 - Управлять сервером печати можно только с помощью утилиты BRAdmin Professional 3 или системы управления через веб-интерфейс.
 - Будет ограничено использование всех приложений, в которых используется протокол SNMPv1/v2c, за исключением утилиты BRAdmin Professional 3. Чтобы разрешить использование приложений SNMPv1/v2c, используйте режим **Доступ SNMPv3 для чтения/записи и SNMPv1/v2c только для чтения** или **Доступ SNMP v1/v2c для чтения/записи**.
 - Подробнее см. в справке утилиты управления через веб-интерфейс.
-

Безопасное управление с помощью утилиты BRAdmin Professional 3 (Windows®)

Для безопасного использования утилиты BRAdmin Professional 3 необходимо выполнять следующие положения

- Настоятельно рекомендуется использовать последнюю версию утилиты BRAdmin Professional 3, которую можно загрузить с веб-сайта <http://solutions.brother.com/>. Если для управления аппаратами Brother используется более ранняя версия утилиты BRAdmin¹, аутентификация пользователей не будет безопасной.
- При необходимости ограничения доступа к аппарату с помощью более ранних версий утилиты BRAdmin¹ необходимо отключить доступ с помощью более ранних версий утилиты BRAdmin¹ в параметре **Дополнительные параметры** раздела **SNMP** на странице **Протокол** с помощью системы управления через веб-интерфейс. (См. раздел *Безопасное управление с помощью системы управления через веб-интерфейс (браузер)* >> стр. 75.)
- При одновременном использовании утилиты BRAdmin Professional 3 и системы управления через веб-интерфейс используйте систему управления через веб-интерфейс с протоколом HTTPS.
- При управлении смешанной группой серверов печати более ранних моделей² и серверами печати с помощью программы BRAdmin Professional 3 рекомендуется использовать для каждой группы отдельный пароль. Это позволит обеспечить безопасность на новых серверах печати.

¹ Утилита BRAdmin Professional версии 2.80 и более ранних, утилита BRAdmin Light для Macintosh версии 1.10 и более ранних.

² Серия NC-2000, 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.

Безопасная печать документов по протоколу SSL/TLS

Для безопасной печати документов с применением протокола IPP можно использовать протокол IPPS.

Настройка параметров IPPS с использованием браузера:

- 1 Нажмите **Сеть** на веб-странице аппарата, затем нажмите **Протокол**. Если поле **IPP** уже выбрано, перейдите к шагу 5.
- 2 Выберите поле **IPP** и нажмите **Отправить**.
- 3 Перезагрузите аппарат для активации конфигурации.
- 4 Нажмите **Сеть** на веб-странице аппарата, затем нажмите **Протокол**.
- 5 Нажмите **Настройки сервера HTTP**.
- 6 Выберите поле **HTTPS(Port443)** и нажмите **Отправить**.
- 7 Перезагрузите аппарат для активации конфигурации.


ПРИМЕЧАНИЕ

Соединение с использованием протокола IPPS не может предотвратить несанкционированный доступ к серверу печати.

Безопасная отправка электронной почты

Настройка с помощью системы управления через веб-интерфейс (браузер)

На экране системы управления через веб-интерфейс можно настроить безопасную отставку электронной почты с помощью аутентификации пользователя или отставку электронной почты с помощью SSL/TLS.

- 1 Запустите браузер.
- 2 В адресную строку браузера введите “http://IP-адрес аппарата/” (где “IP-адрес аппарата” соответствует IP-адресу аппарата или имени сервера печати).
 - Например: http:// 192.168.1.2/
- 3 По умолчанию пароль не требуется. Если был установлен пароль, введите его и нажмите .
- 4 Нажмите **Сеть**.
- 5 Нажмите **Протокол**.
- 6 Нажмите **Дополнительные параметры** в пункте **POP3/SMTP** и убедитесь, что для параметра **POP3/SMTP** установлено значение **Включено**.
- 7 На этой странице можно настроить параметры **POP3/SMTP**.

ПРИМЕЧАНИЕ

- Подробнее см. в справке утилиты управления через веб-интерфейс.
 - Здесь также можно проверить правильность параметров электронной почты, отправив тестовое сообщение электронной почты после выполнения настройки.
 - Если настройки POP3-/SMTP-сервера неизвестны, для получения дополнительной информации обратитесь к системному администратору или провайдеру Интернета.
-
- 8 После настройки нажмите **Отправить**. Открывается диалоговое окно настройки отправки тестового сообщения электронной почты.
 - 9 Следуйте инструкциям на экране, чтобы выполнить тестирование с текущими параметрами.

Отправка сообщений электронной почты с аутентификацией пользователей

Для отправки сообщений электронной почты через почтовый сервер, запрашивающий аутентификацию пользователей, в этом аппарате поддерживаются методы “POP перед SMTP” и “SMTP-AUTH”. Эти методы позволяют предотвратить доступ неавторизованного пользователя к почтовому серверу. Для настройки этих параметров можно воспользоваться системой управления через веб-интерфейс или утилитой BRAdmin Professional 3. Для уведомлений по электронной почте можно использовать методы авторизации “POP перед использованием SMTP” и SMTP-AUTH.

Параметры почтового сервера

Параметры метода аутентификации SMTP должны соответствовать методу, используемому на почтовом сервере. Уточните конфигурацию почтового сервера у администратора сети или интернет-провайдера.

Необходимо также установить флажок в поле **SMTP-AUTH** раздела **Способ проверки подлинности на сервере SMTP**, чтобы включить аутентификацию сервера SMTP.

Параметры SMTP

- С помощью утилиты управления через веб-интерфейс можно изменить номер порта SMTP. Это может оказаться полезным, если у интернет-провайдера реализована служба блокировки порта 25 для исходящих сообщений (OP25B).
- Изменив номер порта SMTP на номер, который используется поставщиком услуг Интернета для сервера SMTP (например, порт 587), можно будет отправлять сообщения электронной почты через сервер SMTP.
- Если можно использовать и метод “POP перед SMTP”, и метод “SMTP-AUTH”, рекомендуется выбрать метод “SMTP-AUTH”.
- Если в качестве метода аутентификации на SMTP-сервере выбран метод “POP перед SMTP”, необходимо настроить параметры POP3. При необходимости можно также использовать метод APOP.

Безопасная отправка электронной почты с использованием SSL/TLS

Данный аппарат поддерживает методы SSL/TLS для отправки электронной почты через почтовый сервер, требующий наличия защиты связи SSL/TLS. Для отправки электронной почты через почтовый сервер, использующий связь SSL/TLS, необходимо правильно настроить SMTP с использованием SSL/TLS или POP3 с использованием SSL/TLS.

Проверка подлинности сертификата сервера

- Если для параметра **SMTP через SSL/TLS** или **POP3 через SSL/TLS** установлено значение SSL или TLS, произойдет автоматическая установка флажка в поле **Проверять сертификат сервера** для проверки подлинности сертификата сервера.
 - Перед проверкой подлинности сертификата сервера необходимо импортировать сертификат ЦС, выданный тем ЦС, который подписал сертификат сервера. При необходимости импорта сертификата ЦС обратитесь к администратору сети или к интернет-провайдеру. Для получения информации об импорте сертификата см. раздел *Импорт и экспорт сертификата ЦС* >> стр. 73.
 - Если нет необходимости проверять подлинность сертификат сервера, снимите флажок **Проверять сертификат сервера**.

Номер порта

- При выборе SSL или TLS значения параметров **Порт SMTP** или **Порт POP3** автоматически изменятся, чтобы соответствовать протоколу. Если необходимо изменить номер порта вручную, введите номер порта после выбора параметра **SMTP через SSL/TLS** или **POP3 через SSL/TLS**.
- Протокол соединения POP3/SMTP необходимо настроить так, чтобы он совпадал с протоколом почтового сервера. Для получения подробной информации о параметрах почтового сервера обратитесь к администратору сети или интернет-провайдеру.

В большинстве случаев для служб защищенной передачи электронной почты требуется установка следующих параметров:

(SMTP)

Порт SMTP: 587

Способ проверки подлинности на сервере SMTP: SMTP-AUTH

SMTP через SSL/TLS: TLS

(POP3)

Порт POP3: 995

POP3 через SSL/TLS: SSL

Использование аутентификации IEEE 802.1x

Аутентификацию IEEE 802.1x можно настроить для проводной или беспроводной сети.

Настройка аутентификации IEEE 802.1x с помощью системы управления через веб-интерфейс (браузер)

При выполнении настройки аутентификации IEEE 802.1x для проводной или беспроводной сети с помощью системы управления через веб-интерфейс следуйте инструкциям ниже.

Аутентификацию IEEE 802.1x можно также настроить следующими методами:

(Проводная сеть)

- BRAdmin Professional 3

(Беспроводная сеть)

- Мастер настройки беспроводной сети на панели управления (для получения дополнительной информации см. раздел *Настройка аппарата для работы в корпоративной беспроводной сети* >> стр. 23.)
- Мастер настройки беспроводной сети на компакт-диске (для получения дополнительной информации см. раздел *Настройка параметров беспроводной сети с временным использованием кабеля USB (рекомендуется)* >> стр. 12).
- BRAdmin Professional 3

ПРИМЕЧАНИЕ

- Если выполняется настройка аппарата, использующего аутентификацию EAP-TLS, необходимо установить сертификат клиента, выданный ЦС (центром сертификации), перед началом настройки. Для получения информации о сертификате клиента обратитесь к администратору сети. Если установлено более одного сертификата, рекомендуется записать сертификат, который будет использоваться. Для получения дополнительной информации об установке сертификата см. раздел *Использование сертификатов для обеспечения безопасности аппарата* >> стр. 60.
 - Перед проверкой подлинности сертификата сервера необходимо импортировать сертификат ЦС, выданный тем ЦС, который подписал сертификат сервера. При необходимости импорта сертификата ЦС обратитесь к администратору сети или к интернет-провайдеру. Для получения дополнительной информации об импорте сертификата см. раздел *Импорт и экспорт сертификата ЦС* >> стр. 73.
 - Для получения дополнительной информации о каждом сертификате см. раздел *Использование сертификатов для обеспечения безопасности аппарата* >> стр. 60.
-

- 1 Запустите браузер.
- 2 В адресную строку браузера введите “http://IP-адрес аппарата/” (где “IP-адрес аппарата” соответствует IP-адресу аппарата или имени сервера печати).
 - Например: http://192.168.1.2/

ПРИМЕЧАНИЕ

- При использовании Domain Name System (система имен доменов) или включении имени NetBIOS вместо IP-адреса можно ввести другое название, например “SharedPrinter”.

- Например: http://SharedPrinter/

Если включено имя NetBIOS, можно также использовать имя узла.

- Например: http://brnxxxxxxxxxxxxx/

Имя NetBIOS отображается в отчете о конфигурации сети (см. *Печать отчета о конфигурации сети* >> стр. 42).

- При работе на компьютере Macintosh можно легко перейти в систему управления через веб-интерфейс, щелкнув значок устройства на экране **Status Monitor**. Дополнительные сведения: >>>Руководство пользователя.

- 3 По умолчанию пароль не требуется. Если был установлен пароль, введите его и нажмите ➔.
- 4 Нажмите **Сеть**.
- 5 (Проводная связь) Нажмите **Проводной**, затем выберите параметр **проверки подлинности 802.1x**.
(Беспроводная связь) Нажмите **Беспроводной**, затем выберите **Беспроводной (Предприятие)**.
- 6 Теперь можно настраивать параметры аутентификации IEEE 802.1x.
 - Если необходимо включить аутентификацию IEEE 802.1x для проводной сети, установите флажок **Включено** для параметра **Состояние проводной сети 802.1x** на странице **проверки подлинности 802.1x**.
 - Для получения дополнительной информации об аутентификации IEEE 802.1x и о методах внутренней аутентификации см. раздел *Аутентификация IEEE 802.1x* >> стр. 103.
 - При использовании аутентификации EAP-TLS необходимо в выпадающем списке **Сертификат клиента** выбрать сертификат клиента, который был установлен (показан с именем сертификата) для проверки подлинности.
 - Если выбрана аутентификация EAP-FAST, PEAP, EAP-TTLS или EAP-TLS, метод проверки подлинности можно выбрать в выпадающем списке **Проверка сертификата сервера**. Проверить подлинность сертификата сервера можно с помощью заранее импортированного на аппарат сертификата ЦС, выданного тем ЦС, который подписал сертификат сервера.

В выпадающем списке **Проверка сертификата сервера** можно выбрать один из следующих методов проверки подлинности.

■ **Без проверки**

Сертификату сервера всегда можно доверять. Проверка подлинности не производится.

■ **Серт. ЦС**

Метод проверки надежности ЦС сертификата сервера путем использования сертификата ЦС, выданного тем ЦС, который подписал сертификат сервера.

■ **Серт. ЦС + идентификатор сервера**

Метод проверки подлинности, при котором кроме надежности ЦС сертификата сервера проверяется значение стандартного имени ¹ сертификата сервера.

¹ Проверка стандартного имени сопоставляет стандартное имя сертификата сервера со строкой символов, составленной для параметра **Идентификатор сервера**. Перед использованием данного метода обратитесь к системному администратору для получения информации о стандартном имени сертификата сервера, а затем настройте параметр **Идентификатор сервера**.

7 После настройки нажмите **Отправить**.

(Проводная сеть)

Выполнив настройку, подключите аппарат к сети, поддерживающей IEEE 802.1x. Через несколько минут распечатайте отчет о конфигурации сети, чтобы проверить **<Wired IEEE 802.1x> Status**. (см. *Печать отчета о конфигурации сети* >> стр. 42.)

■ **Success**

Функция аутентификации IEEE 802.1x для проводной сети включена и аутентификация пройдена успешно.

■ **Failed**

Функция аутентификации IEEE 802.1x для проводной сети включена, однако аутентификация не пройдена.

■ **Off**

Функция аутентификации IEEE 802.1x для проводной сети недоступна.

(Беспроводная сеть)

Через некоторое время после настройки отчет WLAN распечатается автоматически. Проверьте в отчете состояние беспроводной конфигурации. См. раздел *Печать отчета WLAN (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)* >> стр. 43.

Общая информация

В этой главе рассказывается об устранении возможных проблем сети, с которыми можно столкнуться при эксплуатации аппарата Brother. Если даже после прочтения этой главы возникшую проблему устранить не удастся, обратитесь на веб-сайт Brother Solutions Center по адресу: <http://solutions.brother.com/>.

Для загрузки других руководств посетите Brother Solutions Center по адресу: <http://solutions.brother.com/> и на странице соответствующей модели нажмите “Руководства”.

Идентификация проблемы

Перед прочтением данной главы убедитесь, что настроены следующие параметры.

Сначала убедитесь, что выполнены следующие действия:
Кабель питания подключен надлежащим образом, и аппарат Brother включен.
Точка доступа (для беспроводных сетей), маршрутизатор или концентратор включены и мигает кнопка связи.
С устройства снята вся защитная упаковка.
Тонер-картриджи и фотобарабан установлены правильно.
Верхняя и задняя крышка полностью закрыты.
Бумага правильно вставлена в лоток для бумаги.
(Для проводных сетей) Сетевой кабель надежно подсоединен к аппарату Brother и маршрутизатору или концентратору.

В следующем списке перечислены страницы, содержащие решения определенных проблем

- Не удастся завершить настройку параметров беспроводной сети. (См. стр. 87.)
- Аппарат Brother не распознается в сети во время установки драйвера принтера. (См. стр. 88.)
- Аппарат Brother не выполняет печать по сети. (См. стр. 89.)
- Аппарат Brother не распознается в сети даже после успешной установки. (См. стр. 89.)
- Используется программа безопасности. (См. стр. 92.)
- Необходимо проверить надлежащее функционирование используемых сетевых устройств. (См. стр. 93.)

Не удается завершить настройку параметров беспроводной сети.

Вопрос	Интерфейс	Решение
Аппарат не подключается во время настройки беспроводной сети?	Беспроводной	Выключите, а затем включите беспроводной маршрутизатор. Затем попытайтесь повторно настроить параметры беспроводной сети.
Правильно ли настроены параметры безопасности (SSID/сетевой ключ)?	Беспроводной	<ul style="list-style-type: none"> ■ Проверьте еще раз и выберите правильные параметры безопасности. <ul style="list-style-type: none"> • Имя производителя или номер модели точки беспроводного доступа/маршрутизатора могут использоваться в качестве параметров безопасности по умолчанию. • См. информацию о поиске параметров безопасности в документации, поставляемой с точкой беспроводного доступа/маршрутизатором. • Обратитесь к производителю точки беспроводного доступа/маршрутизатора, интернет-провайдеру или администратору сети. ■ Для получения информации о SSID и сетевом ключе см. раздел <i>Термины и понятия беспроводных сетей (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)</i> >> стр. 105.
Используется ли фильтрация MAC-адресов?	Беспроводной	Убедитесь, что MAC-адрес аппарата Brother включен в фильтрации в список разрешенных. MAC-адрес аппарата Brother можно посмотреть на панели управления. (См. раздел <i>Таблица функций и заводские настройки по умолчанию</i> >> стр. 44.)
Точка беспроводного доступа/маршрутизатор работает в скрытом режиме? (передача SSID запрещена)	Беспроводной	<ul style="list-style-type: none"> ■ Необходимо вручную ввести правильное имя SSID или сетевой ключ. ■ Проверьте имя SSID и сетевой ключ в документации, поставляемой с точкой беспроводного доступа/маршрутизатором. Измените настройку параметров беспроводной сети. (Дополнительные сведения: <i>Настройка аппарата, если рассылка SSID отключена</i> >> стр. 20.)
Проверены все настройки и опробованы все описанные выше рекомендации, однако по-прежнему не удается завершить настройку беспроводной сети. Что еще можно сделать в данной ситуации?	Беспроводной	Используйте утилиту Network Connection Repair Tool (Восстановление сетевых подключений). См. раздел <i>Аппарат Brother не выполняет печать по сети. Аппарат Brother не распознается в сети даже после успешной установки.</i> >> стр. 89.


Аппарат Brother не обнаружен в сети при установке драйвера принтера.

Вопрос	Интерфейс	Решение
Аппарат подключен к сети и имеет действительный IP-адрес?	Проводной/ беспроводной	Распечатайте отчет о конфигурации сети и проверьте, имеют ли параметры Ethernet Link Status или Wireless Link Status статус Link OK . См. раздел <i>Печать отчета о конфигурации сети</i> >> стр. 42.
Используется ли программа безопасности?	Проводной/ беспроводной	<ul style="list-style-type: none"> ■ В диалоговом окне программы установки выполните поиск аппарата Brother еще раз. ■ Разрешите доступ, когда во время установки драйвера принтера отображается предупреждающее сообщение программы безопасности. ■ Дополнительную информацию о программах безопасности см. в разделе <i>Используется программа безопасности</i>. >> стр. 92.
Аппарат Brother расположен слишком далеко от точки беспроводного доступа/маршрутизатора?	Беспроводной	При настройке параметров беспроводной сети располагайте аппарат Brother на расстоянии не более 1 метра от точки беспроводного доступа/маршрутизатора.
Нет ли препятствий (например, стены или мебель) между аппаратом и точкой беспроводного доступа/маршрутизатором?	Беспроводной	Переместите аппарат Brother в место, где таких препятствий нет, или ближе к точке беспроводного доступа/маршрутизатору.
Нет ли рядом с устройством Brother или точкой беспроводного доступа/маршрутизатором беспроводного компьютера, устройства Bluetooth, микроволновой печи или цифрового беспроводного телефона?	Беспроводной	Уберите эти устройства от аппарата Brother или точки беспроводного доступа/маршрутизатора.



Аппарат Brother не выполняет печать по сети.**Аппарат Brother не распознается в сети даже после успешной установки.**

Вопрос	Интерфейс	Решение
Используется ли программа безопасности?	Проводной/ беспроводной	См. раздел <i>Используется программа безопасности.</i> ►► стр. 92.
Назначен ли аппарату Brother доступный IP-адрес?	Проводной/ беспроводной	<p>■ (Windows®)</p> <p>Проверьте IP-адрес и маску подсети с помощью утилиты Network Connection Repair Tool.</p> <p>При помощи утилиты Network Connection Repair Tool исправьте параметры сети аппарата Brother. Программа назначит верный IP-адрес и маску подсети.</p> <p>Для получения информации об использовании программы Network Connection Repair Tool обратитесь к администратору сети и выполните следующие действия:</p> <p>ПРИМЕЧАНИЕ</p> <ul style="list-style-type: none"> • (Windows® XP/XP Professional x64 Edition/Windows Vista®/Windows® 7/Windows® 8) Необходимо войти в систему с полномочиями администратора. • Убедитесь, что аппарат Brother включен и подключен к той же сети, что и компьютер.

Аппарат Brother не выполняет печать по сети.**Аппарат Brother не распознается в сети даже после успешной установки. (продолжение)**

Вопрос	Интерфейс	Решение
<p>Назначен ли аппарату Brother доступный IP-адрес? (продолжение)</p>	<p>Проводной/ беспроводной</p>	<p>1 (Windows® XP, Windows Server® 2003/2008) Нажмите кнопку Пуск, затем выберите Все программы, Стандартные и Проводник, а затем нажмите Мой компьютер (Компьютер).</p> <p>(Windows Vista®/Windows® 7) Нажмите кнопку  и Компьютер.</p> <p>2 Дважды щелкните Локальный диск (C:), Program Files или Program Files (x86), если используется 64-разрядная ОС, Brownny02, Brother, BrotherNetTool.exe, чтобы запустить программу.</p> <p>ПРИМЕЧАНИЕ</p> <p>Если откроется окно Контроль учетных записей пользователей, разрешите продолжение установки.</p> <p>3 Следуйте инструкциям на экране.</p> <p>4 Убедитесь, что функции печати или сканирования работают.</p> <p>ПРИМЕЧАНИЕ</p> <p>Программа Network Connection Repair Tool запустится автоматически, если установлен флажок Включить утилиту восстановления сетевых подключений с помощью Status Monitor. Щелкните правой кнопкой мыши экран Status Monitor, выберите Опции, Детали, а затем откройте вкладку Диагностика. Это действие не рекомендуется, если администратор сети назначил статический IP-адрес, поскольку при этом IP-адрес автоматически изменяется.</p> <p>Если верные IP-адрес и маска подсети не назначены даже после использования программы Network Connection Repair Tool, для получения информации обратитесь к администратору сети или посетите веб-сайт Brother Solutions Center по адресу: http://solutions.brother.com/.</p>

Аппарат Brother не выполняет печать по сети.**Аппарат Brother не распознается в сети даже после успешной установки. (продолжение)**

Вопрос	Интерфейс	Решение
<p>Предыдущее задание печати не было выполнено?</p>	<p>Проводной/ беспроводной</p>	<ul style="list-style-type: none"> ■ Если задание печати, которое не удалось выполнить, все еще находится в очереди печати, удалите его. ■ Дважды щелкните значок принтера в следующей папке и выберите Очистить очередь печати в меню Printer (Принтер): (OC Windows® XP/Windows Server® 2003) Пуск и Принтеры и факсы. (Windows Vista®)  Панель управления, Оборудование и звук и затем Принтеры. (Windows® 7)  Устройства и принтеры и затем Принтеры и факсы. (OC Windows Server® 2008) Пуск, Панель управления и Принтеры.
<p>Выполняется подключение аппарата Brother к сети с использованием беспроводного соединения?</p>	<p>Беспроводной</p>	<ul style="list-style-type: none"> ■ Напечатайте отчет WLAN, чтобы проверить состояние беспроводного соединения. (Инструкции по печати см. в разделе <i>Печать отчета WLAN (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)</i> >> стр. 43.) Если напечатанный отчет WLAN содержит код ошибки – >>>Руководство по быстрой установке: <i>Устранение неисправностей.</i> ■ См. раздел <i>Аппарат Brother не обнаружен в сети при установке драйвера принтера.</i> >> стр. 88.
<p>Проверены все настройки и произведены попытки воспользоваться всеми приведенными выше советами, однако аппарат Brother не выполняет печать. Что еще можно сделать в данной ситуации?</p>	<p>Проводной/ беспроводной</p>	<p>Удалите драйвер принтера и установите его заново.</p>

Используется программа безопасности.

Вопрос	Интерфейс	Решение
<p>Был ли разрешен доступ при отображении диалогового окна с предупредительным сообщением при установке драйвера принтера, запуске приложений или использовании операций печати?</p>	<p>Проводной/ беспроводной</p>	<p>Если доступ не был разрешен на диалоговом окне с предупредительным сообщением, функция брандмауэра программного обеспечения системы безопасности может блокировать доступ. Некоторые программы безопасности могут блокировать доступ, не отображая диалоговое окно с предупреждением системы безопасности. Чтобы разрешить доступ, см. инструкции к программе безопасности или обратитесь к производителю.</p>
<p>Требуется узнать номер порта, необходимого для настроек программы безопасности.</p>	<p>Проводной/ беспроводной</p>	<p>Для сетевых функций Brother используются следующие номера портов:</p> <ul style="list-style-type: none"> ■ Сетевая печать ¹ → порт 161 и 137/протокол UDP ■ Утилита BRAdmin Light ¹ – номер порта 161 / протокол UDP <p>¹ Только для Windows®.</p> <p>Описание процедуры открытия порта см. в инструкциях к программе безопасности, или обратитесь к производителю.</p>

Необходимо убедиться, что сетевые устройства работают правильно.

Вопрос	Интерфейс	Решение
Включены ли аппарат Brother, точка доступа/маршрутизатор или сетевой концентратор?	Проводной/ беспроводной	Убедитесь, что выполнены все инструкции в разделе <i>Сначала убедитесь, что выполнены следующие действия:</i> >> стр. 86.
Как можно узнать сетевые параметры имеющегося аппарата Brother, например IP-адрес?	Проводной/ беспроводной	Распечатайте отчет о конфигурации сети. См. раздел <i>Печать отчета о конфигурации сети</i> >> стр. 42.
Как можно узнать состояние подключения имеющегося аппарата Brother?	Проводной/ беспроводной	Распечатайте отчет о конфигурации сети и проверьте, имеют ли параметры Ethernet Link Status или Wireless Link Status статус Link OK . См. раздел <i>Печать отчета о конфигурации сети</i> >> стр. 42.
Можно ли проверить связь (ping) с аппаратом Brother на компьютере?	Проводной/ беспроводной	Отправьте команду “ping” с компьютера на аппарат Brother, используя IP-адрес или имя узла. <ul style="list-style-type: none"> ■ Успешно – Аппарат Brother работает правильно и подключен к той же сети, что и компьютер. ■ Неуспешно – Аппарат Brother не подключен к той же сети, что и компьютер. <p>(Windows®) Обратитесь к администратору сети и при помощи утилиты Network Connection Repair Tool автоматически исправьте IP-адрес и маску подсети. Подробнее об утилите Network Connection Repair Tool см. (Windows®) <i>Проверьте IP-адрес и маску подсети с помощью утилиты Network Connection Repair Tool.</i> в разделе <i>Назначен ли аппарату Brother доступный IP-адрес?</i> >> стр. 89.</p>
Аппарат Brother подключен к беспроводной сети?	Беспроводной	Напечатайте отчет WLAN, чтобы проверить состояние беспроводного соединения. Инструкции по печати см. в разделе <i>Печать отчета WLAN (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)</i> >> стр. 43. Если напечатанный отчет WLAN содержит код ошибки – >>>Руководство по быстрой установке: <i>Устранение неисправностей.</i>
Проверены все настройки и опробованы все описанные выше рекомендации, однако проблемы так и не устранены. Что еще можно сделать в данной ситуации?	Беспроводной	Используя инструкции в документации к точке беспроводного доступа/маршрутизатору, найдите идентификатор SSID и сетевой ключ и правильно настройте их. Подробную информацию об идентификаторе SSID и сетевом ключе см. <i>Правильно ли настроены параметры безопасности (SSID/сетевой ключ)?</i> в разделе <i>Не удается завершить настройку параметров беспроводной сети.</i> >> стр. 87.



Сетевая терминология

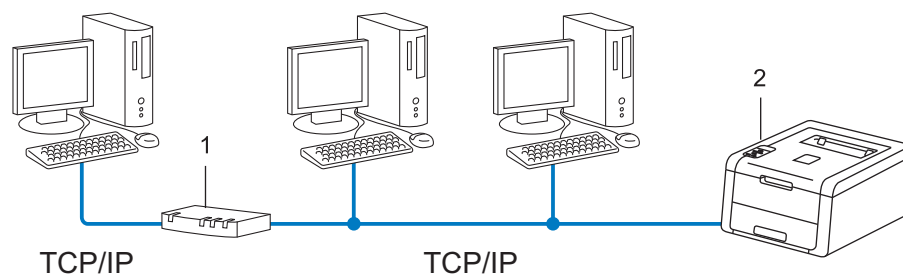
Типы сетевых подключений и протоколов	95
Настройка аппарата для работы в сети	101
Термины и понятия беспроводных сетей (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)	105
Дополнительные сетевые настройки Windows®	109
Термины и понятия безопасности	113

Типы сетевых подключений

Пример подключения к проводной сети

Печать в одноранговой сети с использованием TCP/IP

В одноранговой среде каждый компьютер отправляет данные непосредственно на другое устройство и получает данные от него. В такой среде отсутствует центральный сервер, контролирующей общий доступ к файлам и аппаратам.



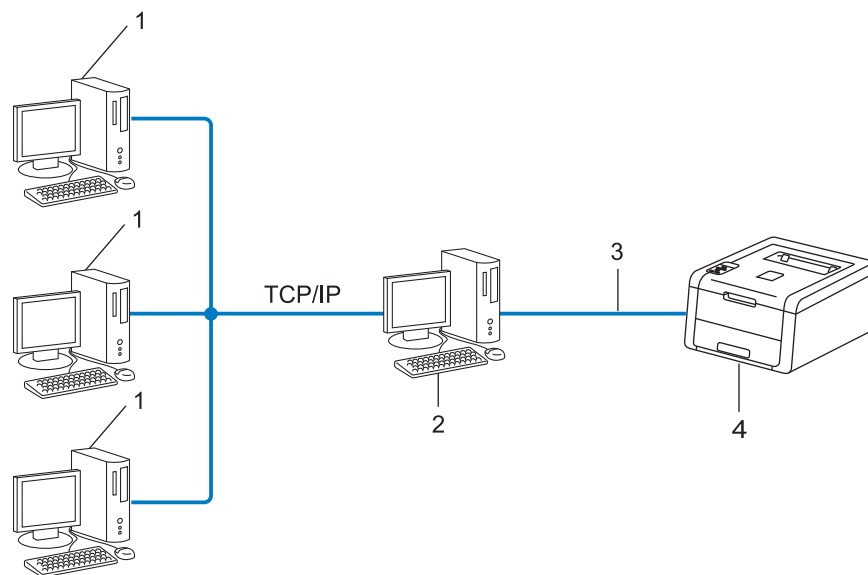
1 Маршрутизатор

2 Сетевой аппарат (ваш аппарат)

- В небольшой сети, состоящей из 2 или 3 компьютеров, рекомендуется использовать одноранговую печать, поскольку настроить ее гораздо легче, чем печать через сервер печати. См. раздел *Печать через сервер печати* >> стр. 96.
- На каждом компьютере должен использоваться протокол TCP/IP.
- Аппарату Brother необходимо назначить надлежащий IP-адрес.
- Если используются маршрутизаторы, на компьютерах и на аппарате Brother должен быть настроен адрес шлюза.

Печать через сервер печати

При использовании сервера печати каждый компьютер отправляет данные через центральный управляющий компьютер. Такой компьютер часто называют “сервером” или “сервером печати”. Задачей этого сервера является управление всеми заданиями печати.



- 1 Клиентский компьютер
- 2 Компьютер, который называется “сервером” или “сервером печати”
- 3 TCP/IP, USB или параллельный интерфейс (если доступно)
- 4 Сетевой аппарат (ваш аппарат)

- В большой сети печать рекомендуется выполнять через сервер печати.
- “Сервер” или “сервер печати” должен использовать протокол печати TCP/IP.
- Аппарату Brother необходимо назначить соответствующий IP-адрес, за исключением случаев, когда аппарат подключен к серверу через USB или параллельный интерфейс.

Протоколы

Протоколы и функции TCP/IP

Протоколами называются стандартизованные наборы правил передачи данных по сети. С помощью протоколов пользователи получают доступ к ресурсам, подключенным к сети.

Сервер печати, используемый в этом аппарате Brother, поддерживает протокол TCP/IP (Transmission Control Protocol/Internet Protocol).

TCP/IP – это самый распространенный набор протоколов для связи (например, Интернет и электронная почта). Этот протокол можно использовать почти во всех операционных системах, таких как Windows®, Windows Server®, Mac OS X и Linux®. Аппарат Brother поддерживает следующие протоколы TCP/IP.

ПРИМЕЧАНИЕ

- Настройки протокола можно выполнить с помощью интерфейса HTTP (браузер). (См. раздел *Настройка параметров аппарата с использованием системы управления через веб-интерфейс (браузер)* >> стр. 49.)
- Для получения информации о поддерживаемых аппаратом Brother протоколах см. раздел *Поддерживаемые протоколы и функции безопасности* >> стр. 117.
- Для получения информации о поддерживаемых протоколах системы безопасности см. раздел *Протоколы безопасности* >> стр. 114.

DHCP/BOOTP/RARP

С помощью протоколов DHCP, BOOTP и RARP IP-адреса назначаются автоматически.

ПРИМЕЧАНИЕ

Чтобы воспользоваться протоколами DHCP, BOOTP и RARP, обратитесь к администратору сети.

APIPA

Если IP-адрес не был назначен вручную (с помощью панели управления аппарата или программного обеспечения BRAdmin) или автоматически (с помощью сервера DHCP/BOOTP/RARP), протокол Automatic Private IP Addressing (APIPA) (автоматическое назначение частных IP-адресов) автоматически назначит IP-адрес из диапазона от 169.254.1.0 до 169.254.254.255.

ARP

Протокол разрешения адресов выполняет преобразование IP-адреса в MAC-адрес в сети TCP/IP.

Клиент DNS

Сервер печати Brother поддерживает функцию клиента DNS (Domain Name System – система имен доменов). Благодаря этой функции сервер печати связывается с другими устройствами, используя свое имя DNS.

Разрешение имен NetBIOS

Разрешение имен сетевой системы ввода-вывода позволяет получить IP-адрес другого устройства, используя имя NetBIOS во время сетевого подключения.

WINS

Windows® Internet Name Service (служба имен в Интернете для Windows) – это служба предоставления информации для разрешения имен NetBIOS путем объединения IP-адреса и имени NetBIOS в локальной сети.

LPR/LPD

Это весьма распространенные протоколы печати в сети TCP/IP.

Клиент SMTP

Клиент SMTP (Simple Mail Transfer Protocol – простой протокол передачи почты) предназначен для отправки сообщений электронной почты через Интернет или интрасеть.

Custom Raw Port (по умолчанию Port 9100)

Это еще один распространенный протокол печати в сети TCP/IP. Используется для передачи интерактивных данных.

IPP

Протокол Internet Printing Protocol (протокол печати через Интернет) позволяет выводить документы на печать напрямую на любое доступное устройство через Интернет.

ПРИМЕЧАНИЕ

Информацию о протоколе IPPS см. в разделе *Протоколы безопасности* >> стр. 114.

mDNS

Протокол mDNS позволяет серверу печати Brother автоматически настраиваться для работы в ОС Mac OS X с конфигурацией простой сети.

TELNET

Протокол TELNET позволяет управлять удаленными сетевыми устройствами в сети TCP/IP с компьютера.

SNMP

Протокол SNMP (Simple Network Management Protocol) используется для управления сетевыми устройствами, в том числе компьютерами, маршрутизаторами и аппаратами Brother, поддерживающими работу в сети. Сервер печати Brother поддерживает протоколы SNMPv1, SNMPv2c и SNMPv3.

ПРИМЕЧАНИЕ

Информацию о протоколе SNMPv3 см. в разделе *Протоколы безопасности* >> стр. 114.

LLMNR

В протоколе LLMNR (Link-Local Multicast Name Resolution) разрешены имена соседних компьютеров, если у сети нет сервера DNS (Domain Name System – система имен доменов). Функция LLMNR Responder работает в среде IPv4 или IPv6 при использовании компьютеров, поддерживающих функцию LLMNR Sender (например, ОС Windows Vista®, Windows® 7 и Windows® 8).

Web Services

Протокол Web Services позволяет пользователям ОС Windows Vista®, Windows® 7 или Windows® 8 установить драйверы печати, щелкнув правой кнопкой мыши значок аппарата в папке **Сеть**. (См. раздел *Установка драйверов для печати через Web Services (Windows Vista®, Windows® 7 и Windows® 8)* >> стр. 109.) Web Services также позволяют проверять текущее состояние аппарата с компьютера.

HTTP

Протокол HTTP используется для передачи данных между веб-сервером и браузером.

ПРИМЕЧАНИЕ

Информацию о протоколе HTTPS см. в разделе *Протоколы безопасности* >> стр. 114.

SNTP

Простой сетевой протокол синхронизации времени используется для синхронизации часов компьютера в сети TCP/IP. Параметры SNTP можно настроить с помощью системы управления через веб-интерфейс (браузер). (Для получения дополнительной информации см. раздел *Настройка протокола SNTP с использованием управления через веб-интерфейс* ►► стр. 53.)

CIFS

Общий протокол доступа к интернет-файлам – это стандартный протокол для совместного использования файлов и принтеров в ОС Windows®.

IPv6

IPv6 является протоколом Интернета следующего поколения. Для получения дополнительной информации о протоколе IPv6 посетите страницу используемой модели устройства по адресу: <http://solutions.brother.com/>.

IP-адреса, маски подсети и шлюзы

Чтобы использовать аппарат в сетевой среде TCP/IP, настройте IP-адрес и маску подсети. IP-адрес, назначенный серверу печати, должен находиться в той же логической сети, что и хост-компьютеры. В противном случае настройте надлежащим образом маску подсети и адрес шлюза.

IP-адрес

IP-адрес представляет собой набор чисел, который определяет каждое подключенное к сети устройство. IP-адрес состоит из четырех чисел, разделенных точками. Каждое число находится в диапазоне от 0 до 255.

■ Пример. В небольшой сети обычно меняются только последние цифры.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

Назначение IP-адреса серверу печати:

Если в сети установлен сервер DHCP/BOOTP/RARP, сервер печати автоматически получит IP-адрес с этого сервера.

ПРИМЕЧАНИЕ

В небольших сетях сервер DHCP может также служить маршрутизатором.

Для получения дополнительной информации о DHCP, BOOTP и RARP см. разделы:

Использование DHCP для настройки IP-адреса >> стр. 118.

Использование BOOTP для настройки IP-адреса >> стр. 120.

Использование RARP для настройки IP-адреса >> стр. 119.

Если сервер DHCP/BOOTP/RARP не используется, протокол Automatic Private IP Addressing (APIPA) (автоматическое назначение частных IP-адресов) автоматически назначит IP-адрес из диапазона от 169.254.1.0 до 169.254.254.255. Для получения дополнительной информации об APIPA см. раздел *Использование APIPA для настройки IP-адреса* >> стр. 121.

Маска подсети

Маски подсети ограничивают связь в сети.

■ Пример. Компьютер 1 может установить связь с компьютером 2

- Компьютер 1

IP-адрес: 192.168. 1. 2

Маска подсети: 255.255.255.000

- Компьютер 2

IP-адрес: 192.168. 1. 3

Маска подсети: 255.255.255.000

Если в маске подсети указан 0, в этой части адреса ограничений на связь нет. В приведенном выше примере это означает следующее: существует возможность устанавливать связь с любым устройством, IP-адрес которого начинается с 192.168.1.x. (x. обозначает номера в диапазоне от 0 до 255).

Шлюз (и маршрутизатор)

Шлюзом называется точка сети, которая служит входом в другую сеть и отправляет данные, переданные через сеть, по указанному назначению. Маршрутизатор определяет место назначения данных, полученных на шлюзе. Если место назначения данных находится во внешней сети, маршрутизатор передает их в эту сеть. Если сеть связана с другими сетями, возможно, потребуется настроить IP-адрес шлюза. Если IP-адрес шлюза неизвестен, обратитесь к администратору сети.

Аутентификация IEEE 802.1x

IEEE 802.1x является стандартом IEEE для проводных и беспроводных сетей, ограничивающим доступ с устройств, находящихся в неавторизованных сетях. Аппарат Brother (клиент) посылает запрос аутентификации на сервер RADIUS (сервер аутентификации) через точку доступа (аутентификатор). После проверки подлинности сервером RADIUS аппарат получает доступ к сети.

Методы аутентификации

■ LEAP (для беспроводной сети)

Протокол Cisco LEAP (Lightweight Extensible Authentication Protocol – легкий расширяемый протокол аутентификации) был разработан компанией Cisco Systems, Inc. Для выполнения аутентификации этот протокол использует идентификатор пользователя и пароль.

■ EAP-FAST

Протокол EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling – расширяемый протокол аутентификации – гибкая аутентификация через защищенное туннелирование) разработан компанией Cisco Systems, Inc. Этот протокол использует идентификатор пользователя и пароль для аутентификации и алгоритм ключа шифрования-дешифровки для выполнения процесса туннельной аутентификации.

Аппарат Brother поддерживает следующие методы внутренней аутентификации:

- EAP-FAST/HET
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

■ EAP-MD5 (для проводной сети)

Протокол EAP-MD5 (Extensible Authentication Protocol-Message digest algorithm 5 – расширяемый протокол аутентификации – алгоритм создания отпечатков сообщений 5) использует идентификатор пользователя и пароль для аутентификации методом “вызов-ответ”.

■ PEAP

Протокол PEAP (Protected Extensible Authentication Protocol – защищенный расширяемый протокол аутентификации) разработан корпорацией Microsoft, компанией Cisco Systems и компанией RSA Security. Протокол PEAP используется для создания шифрованного туннеля SSL (Secure Sockets Layer – уровень защищенных сокетов)/TLS (Transport Layer Security – безопасность на транспортном уровне) между клиентом и сервером аутентификации для передачи идентификатора пользователя и пароля. PEAP обеспечивает выполнение взаимной аутентификации между сервером и клиентом.

Аппарат Brother поддерживает следующие методы внутренней аутентификации:

- PEAP/MS-CHAPv2
- PEAP/GTC

■ EAP-TTLS

Протокол EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security – расширяемый протокол аутентификации – туннелированный протокол безопасности на транспортном уровне) разработан компаниями Funk Software и Certicom. Протокол EAP-TTLS используется для создания такого же зашифрованного туннеля SSL, как и в PEAP между клиентом и сервером аутентификации для передачи идентификатора пользователя и пароля. EAP-TTLS обеспечивает выполнение взаимной аутентификации между сервером и клиентом.

Аппарат Brother поддерживает следующие методы внутренней аутентификации:

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

■ EAP-TLS

Для выполнения аутентификации протокол EAP-TLS (Extensible Authentication Protocol-Transport Layer Security – расширяемый протокол аутентификации – протокол безопасности на транспортном уровне) требует наличия цифрового сертификата аутентификации у клиента и у сервера аутентификации.

Термины и понятия беспроводных сетей (для моделей HL-3140CW, HL-3150CDW и HL-3170CDW)

Указание сети

SSID (идентификатор беспроводной сети) и каналы

Для указания беспроводной сети, к которой требуется подключиться, необходимо задать идентификатор SSID и канал.

■ SSID

Каждая беспроводная сеть обладает собственным уникальным именем сети, которое технически называется идентификатором SSID. Идентификатор SSID представляет собой значение длиной 32 байта или менее, которое присваивается точке доступа. Беспроводные сетевые устройства, которые требуется связать с беспроводной сетью, должны соответствовать точке доступа. Точка доступа и беспроводные сетевые устройства регулярно передают сетевые пакеты (называемые маяками), содержащие информацию об идентификаторе SSID. Когда устройство в вашей беспроводной сети принимает маяк, это дает возможность идентифицировать беспроводные сети, к которым можно подключиться.

■ Каналы

В беспроводных сетях используются каналы. Каждый беспроводной канал имеет собственную частоту. При работе в беспроводной сети можно использовать до 14 различных каналов. Однако во многих странах количество доступных каналов ограничено.

Термины безопасности

Аутентификация и шифрование

В большинстве беспроводных сетей используются определенные настройки защиты. Эти настройки защиты определяют аутентификацию (порядок идентификации устройства сетью) и шифрование (порядок шифрования данных при передаче по сети). **Если при настройке беспроводного аппарата Brother эти параметры указаны неправильно, то обеспечить подключение к беспроводной сети будет невозможно.** Поэтому настройку этих параметров следует выполнять особо тщательно. Для получения информации о методах аутентификации и шифрования, поддерживаемых беспроводным аппаратом Brother, см. раздел *Поддерживаемые протоколы и функции безопасности* >> стр. 117.

Методы аутентификации и шифрования для частной беспроводной сети

Частной беспроводной сетью называется небольшая сеть, например домашняя беспроводная сеть, без поддержки IEEE 802.1х.

При необходимости использования аппарата в беспроводной сети, поддерживающей стандарт IEEE 802.1х, см. раздел *Методы аутентификации и шифрования для корпоративной беспроводной сети* >> стр. 107.

Методы аутентификации

■ Открытая система

Беспроводным устройствам разрешен доступ к сети без выполнения аутентификации.

■ Общий ключ

Все устройства используют для доступа к беспроводной сети общий предварительно заданный секретный ключ.

Беспроводной аппарат Brother использует ключ WEP в качестве предварительно заданного.

■ WPA-PSK/WPA2-PSK

Использует ключ Wi-Fi Protected Access™ Pre-shared key (WPA-PSK/WPA2-PSK), с помощью которого беспроводной аппарат Brother связывается с точками доступа, используя шифрование TKIP для WPA-PSK или AES для WPA-PSK и WPA2-PSK (WPA-Personal).

Методы шифрования

■ Нет

Шифрование не используется.

■ WEP

При использовании метода WEP (Wired Equivalent Privacy) данные передаются и принимаются с ключом защиты.

■ TKIP

Протокол TKIP (Temporal Key Integrity Protocol – протокол обеспечения целостности ключа) обеспечивает по пакетному шифрование, включающее проверку целостности сообщения и механизм повторного шифрования.

■ AES

Стандарт AES (Advanced Encryption Standard) обеспечивает повышенную защиту данных с использованием шифрования с симметричным ключом.

ПРИМЕЧАНИЕ

- Стандарт IEEE 802.11n не поддерживает методы шифрования WEP и TKIP.
- Для подключения устройства к беспроводной сети с использованием стандарта IEEE 802.11n рекомендуется выбрать AES.

Сетевой ключ

■ Открытая система/общий ключ с WEP

Этот ключ представляет собой 64- или 128-битное значение, которое должно вводиться в формате ASCII или в шестнадцатеричном формате.

- 64 (40) бит ASCII:

Используются 5 текстовых символов, например, “WLAN” (с учетом регистра)

- 64 (40) бит шестнадцатеричный:

Используются 10 шестнадцатеричных цифр, например, “71f2234aba”

- 128 (104) бит ASCII:

Используются 13 текстовых символов, например, “Wirelesscomms” (с учетом регистра)

- 128 (104) бит шестнадцатеричный:

Используются 26 шестнадцатеричных цифр, например, “71f2234ab56cd709e5412aa2ba”

■ WPA-PSK/WPA2-PSK и TKIP или AES

Использует ключ Pre-Shared Key (PSK) длиной от 8 до 63 символов.

Методы аутентификации и шифрования для корпоративной беспроводной сети

Корпоративной беспроводной сетью называется крупная сеть, организованная, например, с использованием аппарата в корпоративной беспроводной сети, с поддержкой стандарта IEEE 802.1x. Если аппарат настроен на использование в беспроводной сети с поддержкой стандарта IEEE 802.1x, можно использовать следующие методы аутентификации и шифрования.

10

Методы аутентификации

■ LEAP

LEAP: см. раздел *LEAP (для беспроводной сети)* >> стр. 103.

■ EAP-FAST

EAP-FAST: см. раздел *EAP-FAST* >> стр. 103.

■ PEAP

PEAP: см. раздел *PEAP* >> стр. 103.

■ EAP-TTLS

EAP-TTLS: см. раздел *EAP-TTLS* >> стр. 104.

■ EAP-TLS

EAP-TLS: см. раздел *EAP-TLS* >> стр. 104.

Методы шифрования

- TKIP

TKIP: см. раздел *TKIP* >> стр. 106.

- AES

AES: см. раздел *AES* >> стр. 106.

- SKIP

Оригинальный протокол обеспечения целостности ключа для протокола LEAP, разработанного корпорацией Cisco Systems, Inc.

Идентификатор пользователя и пароль

Следующие способы защиты используют идентификатор пользователя длиной менее 64 символов и пароль длиной менее 32 символов.

- LEAP

- EAP-FAST

- PEAP

- EAP-TTLS

- EAP-TLS (для идентификатора пользователя)

Типы дополнительных сетевых настроек

Следующие функции доступны при необходимости настройки дополнительных параметров сети.

- Web Services для печати (Windows Vista®, Windows® 7 и Windows® 8)
- Vertical Pairing (метод беспроводного подключения) (Windows® 7 и Windows® 8)

ПРИМЕЧАНИЕ

Убедитесь, что хост-компьютер и данный аппарат находятся в одной подсети или маршрутизатор настроен так, чтобы надлежащим образом пропускать данные между двумя устройствами.

Установка драйверов для печати через Web Services (Windows Vista®, Windows® 7 и Windows® 8)

Функция Web Services позволяет отслеживать состояние аппаратов в сети. Это также упрощает процесс установки драйверов. Драйверы, используемые для печати с помощью Web Services, можно установить, щелкнув правой кнопкой мыши значок принтера на компьютере. Порт Web Services компьютера (порт WSD) будет создан автоматически.

ПРИМЕЧАНИЕ

- Прежде чем выполнять данную настройку, назначьте аппарату IP-адрес.
- При использовании Windows Server® 2008/2012 необходимо установить Print Services.

- 1 Вставьте компакт-диск с программой установки.
- 2 Выберите дисковод для компакт-дисков/`install/driver/gdi/32_64`.
- 3 Дважды щелкните `dpinst86.exe` или `dpinst64.exe`.

ПРИМЕЧАНИЕ


Если откроется экран **Контроль учетных записей пользователей**,

(Windows Vista®) нажмите **Разрешить**.

(Windows® 7/Windows® 8) нажмите **Да**.

4 (Windows Vista®)

Нажмите кнопку , затем выберите **Сеть**.
(Windows® 7)

Нажмите кнопку  и выберите **Панель управления, Сеть и Интернет**, затем выберите **Просмотр сетевых компьютеров и устройств**.

5 У значка принтера отображается имя Web Services аппарата. Щелкните правой кнопкой мыши аппарат, который требуется установить.

ПРИМЕЧАНИЕ

Имя аппарата Brother Web Services соответствует названию модели и MAC-адресу (Ethernet-адресу) вашего аппарата (например, Brother HL-XXXX (название модели) [XXXXXXXXXXXXX] (MAC-адрес / Ethernet-адрес)).


6 В контекстном меню выберите параметр **Установить**.

Удаление драйверов для печати через Web Services (Windows Vista®, Windows® 7 и Windows® 8)

Чтобы удалить Web Services с компьютера, выполните следующие действия.

1 (Windows Vista®)

Нажмите кнопку , затем выберите **Сеть**.
(Windows® 7)

Нажмите кнопку  , затем выберите **Панель управления, Сеть и Интернет** и **Просмотр сетевых компьютеров и устройств**.

2 У значка принтера отображается имя Web Services аппарата. Щелкните правой кнопкой мыши аппарат, который требуется удалить.

3 В контекстном меню выберите параметр **Удалить**.


Установка сетевой печати для режима инфраструктуры при использовании Vertical Pairing (Windows® 7 и Windows® 8)

Windows® Vertical Pairing (вертикальное сопряжение) – это технология, позволяющая беспроводным аппаратам, поддерживающим эту функцию, подключаться к местным сетям с помощью PIN-кода функции WPS и функции Web Services. При этом также возможна установка драйвера принтера с помощью значка на экране **Добавление устройства**.

При использовании режима инфраструктуры можно подключить аппарат к беспроводной сети, а затем выполнить установку драйвера принтера с помощью данной функции. Выполните следующие действия.

ПРИМЕЧАНИЕ

- Если до этого функция Web Services аппарата была выключена, необходимо снова ее включить. По умолчанию настройка Web Services для аппарата Brother включена. Настройки Web Services можно изменить с помощью управления через веб-интерфейс (браузер) или используя утилиту BRAdmin Professional 3.
- Убедитесь, что точка беспроводного доступа/беспроводной маршрутизатор имеет логотип совместимости с ОС Windows® 7 или Windows® 8. Если неизвестно, имеет ли устройство логотип совместимости, обратитесь к производителю точки доступа/маршрутизатора.
- Убедитесь, что компьютер имеет логотип совместимости с ОС Windows® 7 или Windows® 8. Если неизвестно, имеет ли компьютер логотип совместимости, обратитесь к производителю компьютера.
- Если выполняется настройка беспроводной сети с помощью внешнего беспроводного сетевого адаптера (NIC – Network Interface Card), убедитесь, что беспроводной сетевой адаптер NIC имеет логотип совместимости с ОС Windows® 7 или Windows® 8. Для получения дополнительной информации обратитесь к производителю беспроводного сетевого адаптера NIC.
- Чтобы использовать в качестве регистратора компьютер под управлением Windows® 7 или Windows® 8, необходимо заранее зарегистрировать его в сети. См. инструкции, прилагаемые к точке беспроводного доступа/маршрутизатору.

- 1 Включите аппарат.
- 2 Настройте аппарат для использования в режиме WPS (с помощью PIN-кода).
Для получения информации о настройке аппарата с использованием PIN-кода см. раздел *Настройка при помощи PIN-кода функции WPS (Wi-Fi Protected Setup)* >> стр. 29.
- 3 Нажмите кнопку , а затем **Устройства и принтеры**.
- 4 В диалоговом окне **Устройства и принтеры** выберите **Добавление устройства**.
- 5 Выберите имеющийся аппарат и введите PIN-код, указанный в аппарате.
- 6 Выберите местную сеть, к которой требуется подключиться, затем нажмите кнопку **Далее**.
- 7 Появление устройства в окне **Устройства и принтеры** будет означать, что беспроводная настройка и установка драйвера принтера успешно завершены.

Функции безопасности

Термины безопасности

■ ЦС (центр сертификации)

Центр сертификации — организация, которая выдает цифровые сертификаты (особенно сертификаты X.509) и гарантирует взаимосвязь между всеми данными, содержащимися в сертификате.

■ CSR (запрос на подпись сертификата)

CSR — это сообщение, отправляемое от лица-заявителя в центр сертификации и представляющее собой запрос на выдачу сертификата. В CSR содержится информация, идентифицирующая заявителя, открытый ключ, сгенерированный заявителем и цифровая подпись заявителя.

■ Сертификат

Сертификат — это информация, которая объединяет открытый ключ и личность заявителя. Сертификат может использоваться для того, чтобы подтвердить принадлежность открытого ключа определенному лицу. Формат определяется по стандарту x.509.

■ Сертификат ЦС

Сертификат ЦС — это сертификат, определяющий сам ЦС (центр сертификации), а также имеющий собственный секретный ключ. Он осуществляет проверку сертификата, выпущенного ЦС.

■ Цифровая подпись

Цифровая подпись — это значение, рассчитанное с помощью криптографического алгоритма и прилагаемое к объекту данных таким образом, чтобы получатель данных мог использовать подпись для подтверждения происхождения данных и их целостности.

■ Криптосистема с открытым ключом

Криптосистема с открытым ключом — это современная отрасль криптографии, в которой алгоритм задействует пару ключей (открытый ключ и секретный ключ) и использует компонент из каждой пары для различных шагов реализации алгоритма.

■ Криптосистема с общим ключом

Криптосистема с общим ключом — это отрасль криптографии, использующая алгоритмы, которые задействуют один и тот же ключ для реализации двух различных шагов алгоритма (таких как шифрование и расшифровка данных).

Протоколы безопасности

SSL (Secure Socket Layer – уровень защищенных сокетов) / TLS (Transport Layer Security – безопасность на транспортном уровне)

При использовании этих протоколов безопасности данные шифруются с целью предотвращения угрозы их безопасности.

HTTPS

Версия протокола Интернета HTTP (Hyper Text Transfer Protocol – протокол передачи гипертекста), использующая SSL.

IPPS

Версия протокола Internet Printing Protocol (протокол печати через Интернет), использующая SSL.

SNMPv3

Протокол SNMPv3 (Simple Network Management Protocol – простой протокол сетевого управления), версия 3 обеспечивает аутентификацию пользователя и шифрование данных для безопасного управления сетевыми устройствами.

Способы защиты при отправке электронной почты

ПРИМЕЧАНИЕ

Способы защиты можно настроить с помощью системы управления через веб-интерфейс (браузер). Для получения дополнительной информации см. раздел *Настройка параметров аппарата с использованием системы управления через веб-интерфейс (браузер)* >> стр. 49.

POP перед SMTP (PbS)

Метод аутентификации пользователя для отправки сообщения электронной почты с клиента. Клиенту дается разрешение на использование сервера SMTP путем доступа к серверу POP3 перед отправкой электронного сообщения.

SMTP-AUTH (SMTP-аутентификация)

SMTP-AUTH расширяет возможности SMTP (протокола отправки электронных сообщений через Интернет) путем использования метода аутентификации, обеспечивающего наиболее достоверную идентификацию отправителя.

APOP (Authenticated Post Office Protocol – почтовый протокол с поддержкой шифрования пароля)

APOP расширяет возможности POP3 (протокол получения электронных сообщений через Интернет) путем использования метода аутентификации, шифрующего пароль при получении клиентом сообщений электронной почты.

SMTP через SSL

Функция “SMTP через SSL” позволяет отправлять зашифрованные сообщения электронной почты с использованием SSL.

POP через SSL

Функция “POP через SSL” позволяет получать зашифрованные сообщения электронной почты с использованием SSL.



Приложения

Приложение А

117

Приложение В

118

Поддерживаемые протоколы и функции безопасности

Интерфейс	Ethernet ¹	10BASE-T, 100BASE-TX
	Беспроводная сеть ²	IEEE 802.11b/g/n (режим инфраструктуры/режим ad-hoc) IEEE 802.11g/n (Wi-Fi Direct)
Сеть (общие параметры)	Протоколы (IPv4)	ARP, RARP, BOOTP, DHCP, APIPA (автоматический IP), разрешение имен WINS/NetBIOS, преобразователь адресов DNS, mDNS, передатчик LLMNR, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP-сервер, сервер TELNET, сервер HTTP/HTTPS, клиент и сервер TFTP, SMTP-клиент, SNMPv1/v2c/v3, ICMP, Web Services (печать), клиент CIFS, клиент SNTP
	Протоколы (IPv6)	NDP, RA, преобразователь адресов DNS, mDNS, передатчик LLMNR, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP-сервер, сервер TELNET, сервер HTTP/HTTPS, клиент и сервер TFTP, SMTP-клиент, SNMPv1/v2c/v3, ICMPv6, Web Services (печать), клиент CIFS, клиент SNTP
Сеть (безопасность)	Проводная сеть ¹	SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
	Беспроводная сеть ²	WEP 64/128 бит, WPA-PSK (TKIP/AES), WPA2-PSK (AES), SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
Электронная почта (безопасность)	Проводная ¹ и беспроводная сеть ²	APOP, POP перед использованием SMTP, SMTP-AUTH, SSL/TLS (SMTP/POP)
Сеть (беспроводные функции) ²	Сертификация беспроводной сети	Лицензия на использование знака сертификации Wi-Fi (WPA™/WPA2™ – Enterprise, Personal), лицензия на использование знака идентификации Wi-Fi Protected Setup™ (WPS), логотип AOSS, Wi-Fi CERTIFIED™ Wi-Fi Direct™

¹ Для моделей HL-3150CDN, HL-3150CDW, HL-3170CDW

² Для моделей HL-3140CW, HL-3150CDW, HL-3170CDW

Использование служб

Служба – это ресурс, к которому могут обращаться компьютеры с целью выполнить печать на сервере печати Brother. Сервер печати Brother предоставляет следующие предварительно настроенные службы (для просмотра списка доступных служб выполните в консоли удаленного управления сервером печати Brother команду SHOW SERVICE). Для просмотра списка поддерживаемых команд введите в командной строке HELP.

Служба (пример)	Определение
BINARY_P1	Бинарный протокол TCP/IP
TEXT_P1	Текстовая служба TCP/IP (добавляет возврат каретки после каждого перевода строки)
PCL_P1	Служба PCL (переключает PJL-совместимый аппарат в режим PCL)
BRNxxxxxxxxxxxx	Бинарный протокол TCP/IP
BRNxxxxxxxxxxxx_AT ¹	Служба PostScript® для Macintosh
POSTSCRIPT_P1 ¹	Служба PostScript® (переключает PJL-совместимый аппарат в режим PostScript®)

Где “xxxxxxxxxxxx” — это MAC-адрес аппарата (Ethernet-адрес).

¹ Для модели HL-3170CDW

Другие способы задания IP-адреса (для продвинутых пользователей и администраторов)

Использование DHCP для настройки IP-адреса

DHCP (Dynamic Host Configuration Protocol – протокол динамической настройки хостов) является одним из нескольких автоматизированных механизмов выделения IP-адреса. Если в сети используется сервер DHCP, сервер печати автоматически получит IP-адрес с сервера DHCP и зарегистрирует свое имя во всех службах динамического именования, совместимых с RFC 1001 и 1002.

ПРИМЕЧАНИЕ

Если сервер печати не требуется настраивать с помощью DHCP, необходимо выбрать статический метод загрузки, чтобы сервер печати имел статический IP-адрес. В этом случае сервер печати не будет пытаться получить IP-адрес из этих систем. Чтобы изменить метод загрузки, воспользуйтесь меню “Сеть” на панели управления аппарата, приложениями BRAdmin или системой управления через веб-интерфейс (браузер).

Использование RARP для настройки IP-адреса

Перед тем как настраивать IP-адрес с применением RARP, в качестве метода загрузки аппарата необходимо выбрать RARP. Чтобы изменить метод загрузки, воспользуйтесь меню “Сеть” на панели управления аппарата, приложениями BRAdmin или системой управления через веб-интерфейс (браузер).

IP-адрес сервера печати Brother можно настроить с помощью средства RARP (Reverse ARP) на хост-компьютере. Для этого необходимо отредактировать файл `/etc/ethers` (если этот файл не существует, его можно создать) и добавить в него запись, аналогичную следующей:

```
00:80:77:31:01:07   BRN008077310107 (или BRW008077310107 для беспроводной сети)
```

Где первая запись – это MAC-адрес (Ethernet-адрес) сервера печати, а вторая часть – это имя сервера печати (необходимо использовать такое же имя, которое было добавлено в файл `/etc/hosts`).

Если демон RARP еще не запущен, запустите его (в зависимости от системы необходимо использовать команду `rarpd`, `rarpd -a`, `in.rarpd -a` или другую команду; введите `man rarpd` или см. документацию на систему для получения дополнительной информации). Чтобы убедиться, что демон RARP запущен в системе на платформе Berkeley UNIX, введите следующую команду:

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

Для систем на платформе AT&T UNIX введите:

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

Сервер печати Brother получит IP-адрес от демона RARP при включении аппарата.

Использование BOOTP для настройки IP-адреса

Перед тем как настраивать IP-адрес с применением BOOTP, в качестве метода загрузки аппарата необходимо выбрать BOOTP. Чтобы изменить метод загрузки, воспользуйтесь меню “Сеть” на панели управления аппарата, приложениями BRAdmin или системой управления через веб-интерфейс (браузер).

Протокол BOOTP является альтернативой протоколу RARP и обладает тем преимуществом, что позволяет настраивать маску подсети и шлюз. Чтобы использовать режим BOOTP для настройки IP-адреса, убедитесь, что служба BOOTP установлена и запущена на хост-компьютере (она должна быть указана в файле `/etc/services` на хост-компьютере в качестве реальной службы; введите `man bootpd` или см. информацию в документации к системе). Служба BOOTP обычно запускается с помощью файла `/etc/inetd.conf`, поэтому, возможно, ее потребуется включить, удалив символ “#” перед записью `bootp` в этом файле. Например, обычная запись `bootp` в файле `/etc/inetd.conf` выглядит следующим образом:

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

В зависимости от системы эта запись может называться “bootps”, а не “bootp”.

ПРИМЕЧАНИЕ

Чтобы включить службу BOOTP, воспользуйтесь текстовым редактором и просто удалите символ “#” (если символ “#” отсутствует, значит, служба BOOTP уже включена). Затем отредактируйте файл конфигурации BOOTP (обычно `/etc/bootptab`) и введите имя, тип сети (1 для Ethernet), MAC-адрес (Ethernet-адрес) и IP-адрес, маску подсети и шлюз сервера печати. К сожалению, для выполнения этой процедуры не существует единого стандартного формата, поэтому потребуется воспользоваться документацией к системе для получения информации о вводе этих данных (многие системы UNIX также имеют примеры шаблонов в файле `bootptab`, которые можно использовать в справочных целях). Примеры типичных записей `/etc/bootptab`: (при подключении к беспроводной сети “BRN” ниже следует заменить на “BRW”).

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

и

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

Некоторые реализации программного обеспечения BOOTP на хост-компьютере не будут отвечать на запросы BOOTP, если в файле конфигурации не указано имя загрузочного файла. В этом случае просто создайте пустой файл на хост-компьютере и укажите имя этого файла и путь к нему в файле конфигурации.

Как и при использовании протокола RARP, сервер печати загрузит свой IP-адрес с сервера BOOTP при включении аппарата.

Использование APIPA для настройки IP-адреса

Сервер печати Brother поддерживает протокол Automatic Private IP Addressing (APIPA) (автоматическое назначение частных IP-адресов). Протокол APIPA позволяет клиентам DHCP автоматически настраивать IP-адрес и маску подсети, когда сервер DHCP недоступен. Устройство выбирает IP-адрес в диапазоне от 169.254.1.0 до 169.254.254.255. Для маски подсети автоматически устанавливается значение 255.255.0.0, а для адреса шлюза — 0.0.0.0.

По умолчанию протокол APIPA включен. Если требуется выключить протокол APIPA, это можно сделать на панели управления аппарата, с помощью приложения BRAdmin Light или системы управления через веб-интерфейс (браузер).

Использование ARP для настройки IP-адреса

Если невозможно использовать приложение BRAdmin и в сети отсутствует сервер DHCP, можно использовать команду ARP. Команда ARP доступна в системах Windows® с установленным протоколом TCP/IP, а также в системах UNIX. Для использования команды ARP введите в командную строку следующее:

```
arp -s ipaddress ethernetaddress
```

```
ping ipaddress
```

Где `ethernetaddress` – это MAC-адрес (Ethernet-адрес) сервера печати, а `ipaddress` – IP-адрес сервера печати. Пример:

■ ОС Windows®

В ОС Windows® необходимо использовать символ тире “-” для разделения цифр в MAC-адресе (Ethernet-адресе).

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

```
ping 192.168.1.2
```

■ Системы UNIX/Linux

Обычно в системах UNIX и Linux используется двоеточие “:” для разделения цифр в MAC-адресе (Ethernet-адресе).

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

```
ping 192.168.1.2
```

ПРИМЕЧАНИЕ

Для использования команды `arp -s` необходимо находиться в одном и том же сегменте Ethernet (между сервером печати и операционной системой не должно быть маршрутизатора).

Если используется маршрутизатор, для настройки IP-адреса необходимо использовать BOOTP или другой способ, описанный в этой главе. Если администратор настроил систему выделения IP-адресов с использованием BOOTP, DHCP или RARP, сервер печати Brother может получить IP-адрес от любой из этих систем выделения IP-адресов. В таком случае не требуется использовать команду ARP. Команду ARP можно применить только один раз. В целях безопасности после успешной настройки IP-адреса сервера печати Brother с помощью команды ARP повторно использовать эту команду для изменения адреса нельзя. Сервер печати будет игнорировать любые попытки использования этой команды. При необходимости изменить IP-адрес используйте систему управления через веб-интерфейс (браузер), TELNET (с помощью команды SET IP ADDRESS) или восстановите заводские настройки сервера печати (это позволит снова использовать команду ARP).

Использование консоли TELNET для настройки IP-адреса

Для изменения IP-адреса можно также использовать команду TELNET.

TELNET – это эффективный способ изменения IP-адреса аппарата. Но сервер печати должен быть уже настроен для использования действующего IP-адреса.

Введите в командной строке TELNET <командная строка>, где <командная строка> – это IP-адрес сервера печати. Выполнив подсоединение, нажмите клавишу Return или Enter, чтобы отобразился запрос “#”. Введите пароль “**access**” (пароль не отображается на экране).

Появится запрос на ввод имени пользователя. Введите любое имя в ответ на этот запрос.

Появится запрос командной строки Local>. Введите SET IP ADDRESS ipaddress, где ipaddress — это IP-адрес, который требуется назначить серверу печати (обратитесь к администратору сети для получения информации об IP-адресе, который следует использовать). Пример:

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

Теперь необходимо настроить маску подсети. Для этого введите SET IP SUBNET маска подсети, где маска подсети – это маска подсети, которую требуется назначить серверу печати (обратитесь к администратору сети для получения информации о маске подсети, которую следует использовать). Пример:

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

Если подсети отсутствуют, воспользуйтесь одной из следующих масок подсети по умолчанию:

255.0.0.0 для сетей класса А

255.255.0.0 для сетей класса В

255.255.255.0 для сетей класса С

Крайняя левая группа разрядов IP-адреса может определять тип используемой сети. Значение этой группы варьируется в диапазоне от 1 до 127 для сетей класса А (например, 13.27.7.1), от 128 до 191 для сетей класса В (например, 128.10.1.30) и от 192 до 255 для сетей класса С (например, 192.168.1.4).

При наличии шлюза (маршрутизатора) введите его адрес с помощью команды SET IP ROUTER routeraddress, где routeraddress – IP-адрес шлюза, который требуется назначить серверу печати. Пример:

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

Введите SET IP METHOD STATIC для установки статического способа настройки IP-адреса.

Чтобы проверить правильность указанного IP-адреса, введите SHOW IP.

Для завершения сеанса работы с консолью удаленного управления введите EXIT или нажмите Ctrl-D (то есть нажмите и удерживайте клавишу Ctrl, а затем нажмите клавишу D).

A

AES	106
AOSS™	27, 39
APIPA	38, 97, 121
APOP	115
ARP	97, 122

B

BINARY_P1	118
BOOTP	97, 120
BRAdmin Light	2, 4
BRAdmin Professional 3	2, 7, 78
BRNxxxxxxxxxxxx	118
BRNxxxxxxxxxxxx_AT	118
BRPrint Auditor	8

C

CIFS	100
CKIP	108
CSR	113
Custom Raw Port	98

D

DHCP	97, 118
------------	---------

E

EAP-FAST	103
EAP-MD5	103
EAP-TLS	104
EAP-TTLS	104
Ethernet	39

H

HTTP	48, 99
HTTPS	75, 114

I

IEEE 802.1x	13, 17, 103
IPP	98
IPPS	79, 114
IPv6	38, 100
IP-адрес	38, 101

L

LEAP	103
LLMNR	99
LPR/LPD	98

M

MAC-адрес	5, 6, 7, 40, 42, 110, 118, 119, 120, 122
mDNS	98

N

Network Connection Repair Tool	89
--------------------------------------	----

P

PBC	27, 39
PCL_P1	118
PEAP	103
POP перед SMTP	81, 115
POP через SSL	115
Port 9100	98
POSTSCRIPT_P1	118

R

RARP	97, 119
RFC 1001	118

S

SMTP через SSL	115
SMTP-AUTH	81, 115
SNMP	99
SNMPv3	75, 114
SNTP	100
SSID	105
SSL/TLS	60, 114
Status Monitor	2

T

TCP/IP	37, 44, 45, 46, 97
TELNET	99, 123
TEXT_P1	118
TKIP	106

V

Vertical Pairing
(метод беспроводного подключения)2, 109

W

Web Services 99, 109, 110
 WEP 106
 WINS 98
 WPA-PSK/WPA2-PSK 106
 WPS (Wi-Fi Protected Setup) 27, 29, 39

A

Аутентификация 106

Б

Беспроводная сеть9, 105

З

Заводские настройки 41

К

Каналы 105
 Клиент DNS 98
 Клиент SMTP 98
 Количество попыток загрузки по IP 38
 Криптосистема с общим ключом 113
 Криптосистема с открытым ключом 113

М

Маска подсети38, 102
 Мастер развертывания драйверов 2
 Метод PIN-кода29, 39

О

Общий ключ 106
 Одноранговая сеть 95
 Открытая система 106
 Отчет о конфигурации сети 42
 Отчет WLAN 43, 91, 93

П

Панель управления 36
 Печать через сервер печати 96
 Поддерживаемые протоколы и функции
 безопасности 117
 Протокол 97

Р

Разрешение имен NetBIOS98
 Режим ad-hoc11, 32
 Режим инфраструктуры 10

С

Сброс сетевых настроек 41
 Сертификат60, 113
 Сертификат ЦС 113
 Сетевой ключ 107
 Служба 118

Т

Термины безопасности 113

У

Управление через веб-интерфейс
(браузер) 2, 7, 75

Ц

Цифровая подпись 113
 ЦС 113

Ш

Шифрование 106
 Шлюз 38