



Многофункциональный сервер печати со встроенной поддержкой нескольких протоколов Ethernet и беспроводной многофункциональный сервер печати с поддержкой протокола Ethernet

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ ПО РАБОТЕ В СЕТИ

В Руководстве пользователя по работе в сети указана полезная информация относительно параметров проводной и беспроводной сети безопасности аппарата Brother. Кроме того, представлена информация о поддерживаемых протоколах и советы по поиску и устранению неисправностей.

Для получения информации о сетевых и расширенных сетевых функциях аппарата Brother см. *Сетевая терминология*.

Для загрузки последней версии руководства посетите Brother Solutions Center по адресу (<http://solutions.brother.com/>). Посетив Brother Solutions Center, можно также загрузить обновленные драйверы и утилиты для аппарата, ознакомиться с ответами на часто задаваемые вопросы и советами по поиску и устранению неисправностей, а также получить информацию о специальных решениях для печати.

Сетевая терминология


В справочнике “Сетевая терминология” представлена основная информация о расширенных сетевых функциях устройств Brother, а также об общих терминах теории сетей.

Поддерживаемые протоколы и сетевые функции зависят от используемой модели. Для получения информации о поддерживаемых функциях и сетевых протоколах см. предоставленное *Руководство пользователя по работе в сети*. Для загрузки последней версии руководства посетите Brother Solutions Center по адресу (<http://solutions.brother.com/>).

Посетив Brother Solutions Center, можно также загрузить обновленные драйверы и утилиты для устройства, ознакомиться с ответами на часто задаваемые вопросы и советами по поиску и устранению неисправностей, а также получить информацию о специальных решениях для печати.

Обозначение примечаний

В настоящем руководстве пользователя используются следующие значки.

 Примечание	В примечаниях описывается способ действия в возникшей ситуации и содержатся советы по работе той или иной операции с другими функциями.
---	---

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.
- Windows® XP в настоящем документе обозначает 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.
- Windows Server® 2008 в настоящем документе обозначает Windows Server® 2008 и Windows Server® 2008 R2.
- Windows Vista® в настоящем документе обозначает все издания ОС Windows Vista®.
- Windows® 7 в настоящем документе обозначает все издания ОС Windows® 7.
- Для загрузки других руководств посетите Brother Solutions Center по адресу <http://solutions.brother.com/> и на странице соответствующей модели нажмите Руководства.

Содержание

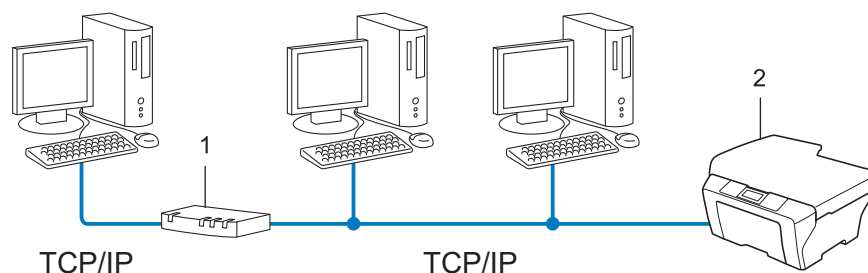
1	Типы сетевых подключений и протоколов	1
	Типы сетевых подключений.....	1
	Пример проводного сетевого подключения	1
	Протоколы	3
	Протоколы и функции TCP/IP	3
	Другой протокол.....	6
2	Настройка устройства для работы в сети	7
	IP-адреса, маски подсети и шлюзы.....	7
	IP-адрес	7
	Маска подсети.....	8
	Шлюз (и маршрутизатор)	8
	Аутентификация IEEE 802.1x.....	9
3	Термины и понятия, используемые в беспроводных сетях	11
	Определение типа сети.....	11
	Идентификатор SSID (Service Set Identifier – идентификатор набора услуг) и каналы	11
	Термины, относящиеся к безопасности.....	11
	Аутентификация и шифрование	11
	Методы аутентификации и шифрования для частной беспроводной сети	12
	Методы аутентификации и шифрования для корпоративной беспроводной сети	13
4	Дополнительные параметры сети в ОС Windows®	15
	Типы дополнительных параметров сети	15
	Установка сетевой печати с использованием Web Services (Windows Vista® и Windows® 7)	15
	Установка сетевой печати для режима инфраструктуры при использовании Vertical Pairing (вертикального сопряжения) (Windows® 7).....	17
5	Термины и понятия, относящиеся к безопасности	18
	Функции безопасности.....	18
	Термины, относящиеся к безопасности.....	18
	Протоколы безопасности	19
	Способы защиты для отправки и получения сообщений электронной почты.....	20
A	Приложение A	21
	Использование служб.....	21
	Другие способы настройки IP-адреса (для опытных пользователей и администраторов)	21
	Настройка IP-адреса с помощью DHCP.....	21
	Настройка IP-адреса с помощью RARP	22
	Настройка IP-адреса с помощью BOOTP	23
	Настройка IP-адреса с помощью APIPA	23
	Настройка IP-адреса с помощью ARP	24
	Настройка IP-адреса с помощью консоли TELNET	25

Типы сетевых подключений

Пример проводного сетевого подключения

Одноранговая печать с помощью 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 устройствам.



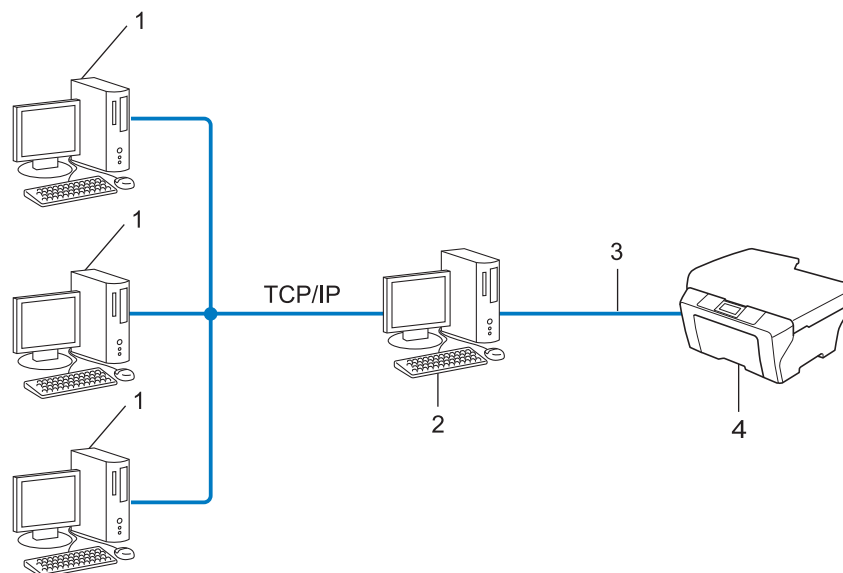
1 Маршрутизатор

2 Сетевое устройство (ваше устройство)

- 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 принт-сервер* на стр. 2.
- На каждом компьютере должен использоваться протокол TCP/IP.
- Устройству Brother необходимо назначить надлежащий IP-адрес.
- Если используются маршрутизаторы, на компьютерах и на устройстве Brother должен быть настроен адрес шлюза.

Печать через принт-сервер

В этом случае 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 “Сервер” или “сервер печати”

3 TCP/IP, USB или параллельный интерфейс (если доступно)

4 Сетевое устройство (ваше устройство)

- В большой сети печать рекомендуется выполнять через принт-сервер.
- “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 стандартизированные наборы правил передачи данных по сети. С помощью протоколов пользователи получают доступ к ресурсам, подключенным к сети.

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

TCP/IP является самым распространенным набором протоколов связи. В частности, он открывает доступ к Интернету и электронной почте. Этот протокол может применяться практически во всех операционных системах, например, в Windows®, Windows Server®, Mac OS X и Linux®. На этом устройстве Brother доступны следующие протоколы TCP/IP.



Примечание

- Настройки протокола можно выполнить с помощью интерфейса HTTP (веб-браузер). (См. *Руководство пользователя по работе в сети*.)
 - Для получения информации о поддерживаемых устройством Brother протоколах см. *Руководство пользователя по работе в сети*.
 - Для получения информации о поддерживаемых протоколах системы безопасности см. раздел *Протоколы безопасности* на стр. 19.
-

DHCP/BOOTP/RARP

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



Примечание

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

APIPA

Если IP-адрес не был назначен вручную (с помощью панели управления устройства (для моделей с жидкокристаллическими дисплеями) или программного обеспечения BRAdmin) или автоматически (с помощью сервера DHCP, BOOTP или RARP), протокол APIPA (Automatic Private IP Addressing – 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). 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 электронной почты) предназначен для отправки сообщений электронной почты через Интернет или интрасеть.

Custom Raw Port (по умолчанию используется порт Port 9100)

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

IPP

Протокол Internet Printing Protocol (IPP версии 1.0) позволяет выводить документы на печать напрямую на любое доступное устройство через Интернет.



Примечание

Информацию о протоколе IPPS см. в разделе *Протоколы безопасности* на стр. 19.

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* на стр. 19.

LLMNR

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

Web Services

Протокол Web Services позволяет пользователям ОС Windows Vista® или Windows® 7 установить драйвер принтера Brother, щелкнув правой кнопкой мыши значок устройства в папке **Сеть**. (См. раздел *Установка сетевой печати с использованием Web Services (Windows Vista® и Windows® 7)* на стр. 15.) Web Services также позволяют проверять текущее состояние устройства с компьютера.

HTTP

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



Примечание

Информацию о протоколе HTTPS см. в разделе *Протоколы безопасности* на стр. 19.

FTP (для функции “Сканировать на FTP”)

Протокол FTP (File Transfer Protocol) позволяет устройству Brother сканировать черно-белые или цветные документы непосредственно на сервер FTP, который расположен в локальной сети или в Интернете.

SNTP

Простой сетевой протокол синхронизации времени используется для синхронизации часов компьютера в сети TCP/IP. Протокол SNTP можно настроить с помощью системы управления через веб-интерфейс (веб-браузер). (Для получения дополнительной информации см. *Руководство пользователя по работе в сети.*)

CIFS

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

LDAP

Протокол LDAP (Lightweight Directory Access Protocol – облегченный протокол доступа к каталогам) позволяет устройству Brother выполнять поиск информации, например, номеров факса и адресов электронной почты, на сервере LDAP.

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/>.

Другой протокол

LLTD

Протокол LLTD (Link Layer Topology Discovery) позволяет легко найти устройство Brother на **Карта сети** Windows Vista®/Windows® 7. Устройство Brother отображается с отличительным значком и именем узла. По умолчанию этот протокол отключен. Протокол LLTD можно включить с помощью системы управления через веб-интерфейс (веб-браузер) (см. *Руководство пользователя по работе в сети*) или используя утилиту BRAdmin Professional 3. Чтобы загрузить утилиту BRAdmin Professional 3 для используемой модели посетите страницу загрузки по адресу <http://solutions.brother.com/>.

IP-адреса, маски подсети и шлюзы

Чтобы использовать устройство 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 сервером DHCP может также являться маршрутизатор.

Для получения дополнительной информации о DHCP, BOOTP и RARP см. раздел *Настройка IP-адреса с помощью DHCP* на стр. 21.
Настройка IP-адреса с помощью BOOTP на стр. 23.
Настройка IP-адреса с помощью RARP на стр. 22.

Если сервер DHCP, BOOTP и RARP не используется, протокол APIPA (Automatic Private IP Addressing – 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 *Настройка IP-адреса с помощью APIPA* на стр. 23.

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

Наличие в маске подсети цифры “0” означает, что в этой части адреса нет ограничения связи. В рассмотренном выше примере это означает, что связь осуществляется с любым устройством, IP-адрес которого начинается с 192.168.1.x. (где x. – числа 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 сетевому администратору.

Аутентификация IEEE 802.1x

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

2

Способы аутентификации

■ LEAP (для беспроводной сети)

Протокол Cisco LEAP (Light Extensible Authentication Protocol — легкий расширяемый протокол проверки подлинности) 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 Tunnel – расширяемый протокол проверки подлинности-гибкая аутентификация через защищенное туннелирование) разработан компанией Cisco Systems, Inc. Этот протокол использует идентификатор пользователя и пароль для аутентификации и алгоритмы шифрования-расшифрования с симметричным ключом для выполнения процесса туннельной аутентификации.

Устройство Brother поддерживает следующие способы 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 проверки подлинности-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 зашифрованного туннеля SSL (Secure Sockets Layer – протокол защищенных сокетов)/TLS (Transport Layer Security – протокол защиты транспортного уровня) между клиентом и сервером аутентификации для передачи идентификатора пользователя и пароля. PEAP обеспечивает выполнение взаимной аутентификации между сервером и клиентом.

Устройство Brother поддерживает следующие способы внутренней аутентификации.

- PEAP/MS-CHAPv2
- PEAP/GTC

■ EAP-TTLS

Протокол EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security – расширяемый протокол аутентификации-туннелированный протокол защиты транспортного уровня) разработан компаниями Funk Software и Certicom. Протокол EAP-TTLS используется для создания такого же шифрованного 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.

Устройство Brother поддерживает следующие способы 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 проверки-протокол защиты транспортного уровня) требует наличия цифрового сертификата у клиента и у сервера аутентификации.

Определение типа сети

Идентификатор SSID (Service Set Identifier – идентификатор набора услуг) 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 или ESSID (Extended Service Set Identifier – идентификатор расширенного набора услуг). 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 беспроводное сетевое устройство получает сообщение-маяк, можно определить беспроводную сеть, расположенную достаточно близко, чтобы ее радиосигналы доходили до данного устройства.

■ 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, относящиеся к 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 устройства Brother эти параметры заданы неправильно, устройство не сможет подключиться к беспроводной сети.** Поэтому настраивать эти параметры следует внимательно. Для получения информации о способах аутентификации и шифрования, поддерживаемых беспроводным устройством Brother, см. *Руководство пользователя по работе в сети*.

Методы аутентификации и шифрования для частной беспроводной сети

Частной беспроводной сетью называется небольшая сеть, организованная, например, с использованием устройства в беспроводной сети дома, не поддерживающая стандарт IEEE 802.1х.

При необходимости использования устройства в беспроводной сети, поддерживающей стандарт IEEE 802.1х, см. раздел *Методы аутентификации и шифрования для корпоративной беспроводной сети* на стр. 13.

Способы 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.

Беспроводное устройство 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 беспроводное устройство 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 способа WEP (Wired Equivalent Privacy) данные передаются и принимаются с ключом защиты.

■ TKIP

Протокол TKIP (Temporal Key Integrity Protocol) обеспечивает по пакетное шифрование, включающее проверку целостности сообщения и механизм повторного шифрования.

■ AES

Стандарт AES (Advanced Encryption Standard) представляет собой надежный стандарт шифрования для Wi-Fi®.

Сетевой ключ

■ Открытая система/общий ключ с WEP

Этот ключ представляет собой 64- или 128-битное число, которое требуется вводить 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 устройства в корпоративной беспроводной сети, поддерживающая стандарт IEEE 802.1x. Если устройство настроено на использование в беспроводной сети с поддержкой стандарта IEEE 802.1x, можно использовать следующие способы аутентификации и шифрования.

Способы аутентификации

■ LEAP

LEAP - см. раздел *LEAP (для беспроводной сети)* на стр. 9.

■ EAP-FAST

EAP-FAST – см. раздел *EAP-FAST* на стр. 9.

■ PEAP

PEAP – см. раздел *PEAP* на стр. 9.

■ EAP-TTLS

EAP-TTLS – см. раздел *EAP-TTLS* на стр. 10.

■ EAP-TLS

EAP-TLS – см. раздел *EAP-TLS* на стр. 10.

Способы шифрования

- TKIP

TKIP – см. раздел *TKIP* на стр. 12.

- AES

AES – см. раздел *AES* на стр. 12.

- 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 (идентификатор пользователя)

Типы дополнительных параметров сети

Следующие функции доступны при необходимости настройки дополнительных параметров сети.

- Web Services (Windows Vista® и Windows® 7)
- Vertical Paring (вертикальное сопряжение) (Windows® 7)



Примечание

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

Установка сетевой печати с использованием Web Services (Windows Vista® и Windows® 7)

Функция Web Services позволяет отслеживать информацию об устройстве, подключенном к сети. При этом также возможна установка драйвера принтера с помощью значка принтера и порта Web Services (порт WSD).



Примечание

- Прежде чем выполнять данную настройку, назначьте устройству IP-адрес.
- При использовании Windows Server® 2008 необходимо установить Print Services.
- Возможна установка только принтеров с поддержкой веб-служб.



1 Вставьте установочный компакт-диск.



2 Выберите привод компакт-дисков/`install/driver/gdi/32` или `64`.



3 Выберите язык и дважды щелкните файл `DPIInst.exe`.





Примечание

При появлении окна **Контроль учетных записей пользователей**

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

(Windows® 7) Щелкните **Да**.

- 4 (ОС Windows Vista®)
Нажмите кнопку , а затем выберите **Сеть**.
(Windows® 7)
Выберите , **Панель управления, Сеть и Интернет**, а затем выберите **Просмотр сетевых компьютеров и устройств**.
- 5 У значка принтера отображается имя Web Services устройства. Щелкните правой кнопкой мыши устройство, которое требуется установить.



Примечание

Имя Web Services для устройства Brother состоит из названия модели и MAC-адреса (адреса Ethernet) устройства (например, Brother MFC-XXXX (название модели) [XXXXXXXXXXXXX] (MAC-адрес / адрес Ethernet)).

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

Установка сетевой печати для режима инфраструктуры при использовании Vertical Pairing (вертикального сопряжения) (Windows® 7)


Windows® Vertical Pairing (вертикальное сопряжение) - это технология, позволяющая беспроводным устройствам, поддерживающим эту функцию, подключаться к местным сетям с помощью PIN-кода функции Wi-Fi Protected Setup и функции веб-служб. При этом также возможна установка драйвера принтера с помощью значка на экране **Добавление устройства**.

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



Примечание

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

- 1 Включите устройство.
- 2 Запустите на устройстве установку Wi-Fi Protected Setup (с помощью PIN-кода). Для получения информации о беспроводной настройке устройства с помощью PIN-кода см. Wi-Fi Protected Setup (с помощью PIN-кода) в *Руководстве пользователя по работе в сети*.
- 3 Нажмите кнопку , а затем **Устройства и принтеры**.
- 4 В окне **Устройства и принтеры** выберите **Добавление устройства**.
- 5 Выберите имеющееся устройство и введите PIN-код, указанный в устройстве.
- 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, относящиеся к 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 о подписи сертификата)

Запрос о подписи сертификата (CSR) отправляется от лица-заявителя в центр сертификатов, чтобы имелась возможность применить подпись для выдачи сертификата. В запросе на подпись сертификата 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



Примечание

Протокол можно настроить с помощью системы управления через веб-интерфейс (веб-браузер). Для получения дополнительной информации см. *Руководство пользователя по работе в сети*.

SSL (Secure Socket Layer - протокол защищенных сокетов) / TLS (Transport Layer Security – протокол защиты транспортного уровня)

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

HTTPS

Протокол Интернета HTTP (Hyper Text Transfer Protocol – протокол передачи гипертекста) использует SSL.

IPPS

Протокол IPP (Internet Printing Protocol – протокол печати по Интернету) версии 1.0 использует 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 для отправки и получения сообщений электронной почты



Примечание

Способы защиты можно настроить с помощью системы управления через веб-интерфейс (веб-браузер). Для получения дополнительной информации см. *Руководство пользователя по работе в сети*.

POP перед SMTP (PbS)

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

SMTP-AUTH (Аутентификация SMTP)

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

APOP (Authenticated Post Office Protocol)

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

SMTP с использованием SSL

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

POP с использованием SSL

Функция “POP с использованием SSL” позволяет принимать зашифрованные сообщения электронной почты с помощью протокола SSL.

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 удаленной консоли сервера 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	Служба PostScript® для Macintosh
POSTSCRIPT_P1	Служба PostScript® (переключает PJL-совместимый аппарат в режим PostScript®)

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

Другие способы настройки IP-адреса (для опытных пользователей и администраторов)

Настройка IP-адреса с помощью DHCP

Протокол DHCP (Dynamic Host Configuration Protocol) 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, BOOTP или RARP, необходимо выбрать статический способ загрузки, чтобы сервер печати имел статический IP-адрес. Это предотвратит попытки сервера печати получить IP-адрес от какой-либо из этих систем. Чтобы изменить способ загрузки, используйте меню “Сеть” панели управления аппарата (для моделей с жидкокристаллическими дисплеями), приложения BRAdmin, программу удаленной настройки или систему управления через веб-интерфейс (веб-браузер).

Настройка IP-адреса с помощью RARP

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)
```

Первая часть является MAC-адресом (адресом Ethernet) 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 какую-либо другую; введите `man rarpd` или см. документацию к системе для получения дополнительной информации). Чтобы убедиться, что демон RARP запущен в системе на платформе Berkeley UNIX, введите следующую команду:

```
ps -ax &#x2502; grep -v grep &#x2502; grep rarpd
```

Для систем на платформе AT&T UNIX введите:

```
ps -ef &#x2502; grep -v grep &#x2502; grep rarpd
```

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

Настройка IP-адреса с помощью BOOTP

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 (адрес Ethernet) 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.

Так же, как при использовании протокола RARP, сервер печати загрузит свой IP-адрес с сервера BOOTP при включении аппарата.

Настройка IP-адреса с помощью APIPA

Сервер печати Brother поддерживает протокол APIPA (Automatic Private IP Addressing). 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 отключить протокол APIPA, это можно выполнить с помощью панели управления аппарата (для моделей с жидкокристаллическими дисплеями), программного обеспечения BRAdmin Light или системы управления через веб-интерфейс (веб-браузер).

Настройка IP-адреса с помощью ARP

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 (адрес Ethernet) сервера печати, а `ipaddress` — это IP-адрес сервера печати. Пример:

■ ОС Windows®

Для ОС Windows® необходимо использовать тире “-” между каждой цифрой MAC-адреса (адреса Ethernet).

```
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 между цифрами MAC-адреса (адреса Ethernet) требуется ставить двоеточие “:”.

```
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 система управления через веб-интерфейс, TELNET (с помощью команды SET IP ADDRESS) или восстановите заводские параметры сервера печати (это позволит снова использовать команду ARP).

Настройка IP-адреса с помощью консоли TELNET

Для изменения IP-адреса можно также использовать команду TELNET.

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

Введите в командной строке TELNET <command line>, где <command line> – 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 сетевому администратору 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 сетевому администратору 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 удаленного сеанса работы с консолью введите EXIT или нажмите Ctrl-D (нажмите и удерживайте клавишу Ctrl, а затем нажмите клавишу D).

В

Указатель

A

AES	12
APIPA	3, 23
APOP	20
ARP	3, 24

B

BINARY_P1	21
BOOTP	3, 23
BRNxxxxxxxxxxxx	21
BRNxxxxxxxxxxxx_AT	21

C

CIFS	6
CKIP	14
CSR	18
Custom Raw Port	4

D

DHCP	3, 21
------------	-------

E

EAP-FAST	9
EAP-MD5	9
EAP-TLS	10
EAP-TTLS	10

F

FTP	5
-----------	---

H

HTTP	5
HTTPS	19

I

IEEE 802.1x	9
IPP	4
IPPS	19
IPv6	6
IP-адрес	7

L

LDAP	6
LEAP	9
LLMNR	5
LLTD	6
LPR/LPD	4

M

MAC-адрес	16, 21, 22, 23, 24
mDNS	4

P

PCL_P1	21
PEAP	9
POP перед SMTP	20
POP с использованием SSL	20
Port 9100	4
POSTSCRIPT_P1	21

R

RARP	3, 22
RFC 1001	21

S

SMTP с использованием SSL	20
SMTP-AUTH	20
SNMP	5
SNMPv3	19
SNTP	6
SSID	11
SSL/TLS	19

T

TCP/IP	3
TELNET	5, 25
TEXT_P1	21
TKIP	12

V

Vertical Paring (вертикальное сопряжение)	15
---	----

W

Web Services	5, 15
WEF	12
WINS	4
WPA-PSK/WPA2-PSK	12

A

Аутентификация	12
----------------------	----

Б

Беспроводная сеть	11
-------------------------	----

К

Каналы	11
Клиент DNS	4
Клиент SMTP	4
Криптосистема с общим ключом	18
Криптосистема с открытым ключом	18

М

Маска подсети	8
---------------------	---

О

Общий ключ	12
Одноранговая печать	1
Открытая система	12

П

Печать TCP/IP	15
Печать через принт-сервер	2
Протокол	3

Р

Разрешение имен NetBIOS	4
-------------------------------	---

С

Сертификат	18
Сертификат ЦС	18
Сетевая печать	15
Сетевой ключ	13
Службы	21

Т

Термины, относящиеся к безопасности	18
---	----

Ц



Цифровая подпись	18
ЦС	18

Ш

Шифрование	12
------------------	----

Обозначение 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 описывается способ действия в возникшей ситуации и содержатся советы по работе той или иной операции с другими функциями.

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.
- Windows® XP в настоящем документе обозначает 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.
- Windows Server® 2008 в настоящем документе обозначает Windows Server® 2008 и Windows Server® 2008 R2.
- Под Windows Vista® в данном документе понимаются все издания ОС Windows Vista®.
- Windows® 7 в настоящем документе обозначает все издания ОС Windows® 7.
- Для загрузки других руководств посетите Brother Solutions Center по адресу <http://solutions.brother.com/> и на странице соответствующей модели нажмите Руководства.
- Некоторые модели продаются не во всех странах.

Содержание

1	Введение	1
	Сетевые функции.....	1
	Другие сетевые функции.....	2
2	Изменение сетевых настроек устройства	3
	Как изменить сетевые настройки аппарата (IP-адрес, маска подсети и шлюз)	3
	Использование панели управления	3
	Использование утилиты BRAdmin Light	3
	Другие утилиты управления.....	6
	Система управления через веб-интерфейс (веб-браузер)	6
	Утилита BRAdmin Professional 3 (Windows®).....	6
	Web BRAdmin (Windows®).....	7
	BRPrint Auditor (Windows®).....	7
3	Настройка аппарата для работы в беспроводной сети (для модели MFC-9560CDW)	8
	Обзор	8
	Пошаговая схема настройки конфигурации беспроводной сети	9
	Для режима инфраструктуры	9
	Для режима ad-hoc	10
	Проверьте свою сетевую среду.....	11
	Подключение к компьютеру через беспроводную точку доступа/маршрутизатор в сети (режим инфраструктуры)	11
	Подключение к компьютеру, поддерживающему беспроводную связь, без беспроводной точки доступа/маршрутизатора в сети (режим ad-hoc)	11
	Проверьте способ настройки беспроводной сети.....	12
	Настройка аппарата с помощью WPS или AOSS™ в меню панели управления для работы в беспроводной сети (автоматический беспроводной режим, только режим инфраструктуры) (рекомендуется).....	12
	Настройка с помощью мастера установки панели управления аппарата для работы в беспроводной сети	12
	Настройка с использованием находящейся на компакт-диске программы установки Brother, предназначенной для настройки беспроводного сетевого аппарата	13
	Настройка с помощью PIN-кода функции Wi-Fi Protected Setup для работы в беспроводной сети (только режим инфраструктуры).....	15
	Настройка аппарата для работы в беспроводной сети (Для режима инфраструктуры и режима ad-hoc)	16
	Настройка аппарата с помощью WPS или AOSS™ в меню панели управления для работы в беспроводной сети (автоматический беспроводной режим)	16
	Использование Мастера установки с панели управления	16
	Настройка аппарата, если отключена передача идентификатора SSID	17
	Настройка аппарата для работы в корпоративной беспроводной сети.....	20
	Использование программы установки Brother с компакт-диска для настройки аппарата для работы в беспроводной сети	23
	Использование PIN-кода функции Wi-Fi Protected Setup	24

4	Настройка параметров беспроводной сети с помощью программы установки Brother (для MFC-9560CDW)	26
	Перед настройкой параметров беспроводной связи	26
	Настройка параметров беспроводной связи	26
5	Настройка с панели управления	31
	Меню “Сеть”	31
	TCP/IP	31
	Ethernet (только для проводной сети)	34
	Состояние (Для DCP-9055CDN, MFC-9460CDN и MFC-9465CDN)/Состояние проводного подключения (Для MFC-9560CDW)	34
	Мастер установки (только для беспроводной сети)	34
	WPS или AOSS™ (только для беспроводной сети)	34
	WPS с PIN-кодом (только для беспроводной сети)	34
	Состояние беспроводной сети (только для беспроводной сети)	34
	MAC-адрес	35
	Установка значений по умолчанию (для модели MFC-9560CDW)	35
	Проводное подключение (для модели MFC-9560CDW)	35
	Беспроводное подключение (для MFC-9560CDW)	35
	Установка нового значения по умолчанию для функции “Сканировать на FTP”	35
	Установка нового значения по умолчанию для функции “Сканировать в сеть”	35
	Восстановление заводских настроек сети	36
	Печать Списка конфигурации сети	36
	Печать отчета о состоянии беспроводной сети (для MFC-9560CDW)	37
	Таблица функций и заводские настройки	38
	DCP-9055CDN, MFC-9460CDN и MFC-9465CDN	38
	MFC-9560CDW	41
6	Управление через веб-интерфейс	46
	Обзор	46
	Настройка параметров аппарата с помощью системы управления через веб-интерфейс (веб-браузер)	46
	Информация о пароле	47
	Защитная блокировка функций 2.0	48
	Настройка параметров защитной блокировки функций 2.0 с помощью системы управления через веб-интерфейс (веб-браузер)	48
	Синхронизация с сервером SNTP	51
	Сохранение журнала в сети	53
	Настройка параметров сохранения журнала в сети с помощью системы управления через веб-интерфейс (веб-браузер)	53
	Настройка обнаружения ошибки	55
	Сообщения об ошибках	56
	Использование функции “Сохранение журнала в сети” с защитной блокировкой функций 2.0	57
	Изменение параметров функции “Сканировать на FTP” с помощью веб-браузера	57
	Изменение параметров функции “Сканировать в сеть” с помощью веб-браузера	59

7	Протоколы безопасности	60
	Обзор	60
	Безопасное управление сетевым аппаратом с помощью SSL/TLS	61
	Безопасное управление с помощью системы управления через веб-интерфейс (веб-браузер)	61
	Безопасная печать документов по протоколу SSL/TLS	63
	Безопасная отправка и получение электронной почты	64
	Настройка с помощью системы управления через веб-интерфейс (веб-браузер)	64
	Отправка электронной почты с аутентификацией пользователя	64
	Безопасная отправка и получение электронной почты с помощью SSL/TLS	65
	Использование аутентификации IEEE 802.1x	66
	Настройка аутентификации IEEE 802.1x с помощью системы управления через веб-интерфейс (веб-браузер)	66
	Безопасное управление с использованием утилиты BRAdmin Professional 3 (Windows®)	68
	Для безопасного использования утилиты BRAdmin Professional 3 необходимо соблюдать условия, приведенные ниже.	68
	Использование сертификатов для защиты устройств	69
	Настройка сертификата с помощью системы управления через веб-интерфейс	70
	Создание и установка сертификата	71
	Импорт и экспорт сертификата и секретного ключа	77
	Управление несколькими сертификатами	78
	Импорт и экспорт сертификата ЦС	79
8	Устранение неисправностей	80
	Обзор	80
	Определение проблемы	80
A	Приложение A	88
	Поддерживаемые протоколы и сетевые функции	88
B	Указатель	89

Сетевые функции

Аппарат Brother можно совместно использовать в проводной сети Ethernet 10/100 Мбит или в беспроводной сети Ethernet IEEE 802.11b/g с помощью внутреннего 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 показаны сетевые функции и соединения, поддерживаемые каждой операционной системой.



Примечание

Хотя аппарат Brother может использоваться как в проводной, так и в беспроводной сети, одновременно может использоваться только один способ подключения.

Операционные системы	Windows® 2000/XP Windows Vista® Windows® 7	Windows Server® 2003/2008	Mac OS X 10.4.11 - 10.6.x
Печать	✓	✓	✓
Сканирование <i>См. Руководство по использованию программного обеспечения.</i>	✓		✓
Отправка факсов с ПК ¹ <i>См. Руководство по использованию программного обеспечения.</i>	✓		✓
Прием факсов на ПК ¹ <i>См. Руководство по использованию программного обеспечения.</i>	✓		
BRAdmin Light <i>См. раздел на стр. 3.</i>	✓	✓	✓
BRAdmin Professional 3 ² <i>См. раздел на стр. 6.</i>	✓	✓	
Web BRAdmin ² <i>См. раздел на стр. 7.</i>	✓	✓	
Система управления через веб-интерфейс (веб-браузер) <i>См. раздел на стр. 46.</i>	✓	✓	✓
Удаленная настройка ¹ <i>См. Руководство по использованию программного обеспечения.</i>	✓		✓

Операционные системы	Windows® 2000/XP Windows Vista® Windows® 7	Windows Server® 2003/2008	Mac OS X 10.4.11 - 10.6.x
Status Monitor <i>См. Руководство по использованию программного обеспечения.</i>	✓		✓
Мастер развертывания драйверов	✓	✓	
Vertical Pairing (метод беспроводного подключения) <i>См. справочник Сетевая терминология.</i>	✓ ³		

¹ Не поддерживается для модели DCP.

² Программы BRAdmin Professional 3 и Web BRAdmin можно загрузить с веб-сайта по адресу <http://solutions.brother.com/>.

³ Только для Windows® 7.

Другие сетевые функции

Интернет-факс (функция доступна для загрузки для моделей MFC-9460CDN, MFC-9465CDN и MFC-9560CDW)

Интернет-факс (IFAX) позволяет передавать и принимать факсимильные документы, используя в качестве транспортного механизма сеть Интернет.

Для использования этой функции загрузите необходимое программное обеспечение с веб-узла Brother Solutions Center (<http://solutions.brother.com/>). Перед использованием этой функции необходимо настроить требуемые параметры устройства с помощью панели управления устройства. Подробные сведения см. в руководстве пользователя Интернет-факса на указанном выше веб-сайте.

Безопасность

Данный аппарат Brother оснащен некоторыми из последних протоколов безопасности и шифрования данных, разработанных на сегодняшний день. (См. раздел *Протоколы безопасности* на стр. 60.)

Факс на сервер (функция доступна для загрузки для моделей MFC-9460CDN, MFC-9465CDN и MFC-9560CDW)

Функция «Факс на сервер» позволяет аппарату сканировать документы и передавать их по сети на отдельный факсимильный сервер.

Для использования этой функции загрузите необходимое программное обеспечение с веб-узла Brother Solutions Center (<http://solutions.brother.com/>). Перед использованием этой функции необходимо настроить требуемые параметры устройства с помощью панели управления устройства. Подробные сведения см. в руководстве пользователя Интернет-факса на указанном выше веб-сайте.

Защитная блокировка функций 2.0

Защитная блокировка функций 2.0 повышает безопасность путем ограничения использования функций. (См. раздел *Защитная блокировка функций 2.0* на стр. 48.)

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* на стр. 53.)

Как изменить сетевые настройки аппарата (IP-адрес, маска подсети и шлюз)

Использование панели управления

Можно настроить используемый аппарат для работы в сети с помощью меню *Сеть* панели управления. (См. раздел *Настройка с панели управления* на стр. 31.)

Использование утилиты BRAdmin Light

Утилита BRAdmin Light предназначена для первоначальной настройки аппаратов Brother, подключенных к сети. Данная утилита также предназначена для обнаружения аппаратов Brother в сети в окружении TCP/IP, для просмотра их состояния и для изменения настроек сети, таких как IP-адрес.

Установка BRAdmin Light

■ Windows®

- 1 Убедитесь в том, что аппарат включен.
- 2 Включите компьютер. Перед настройкой закройте все работающие программы.
- 3 Вставьте сопроводительный компакт-диск в дисковод для компакт-дисков. Автоматически откроется начальное окно. Если откроется экран выбора модели, выберите имеющийся аппарат. Если отображается экран выбора языка выберите требуемый язык.
- 4 Откроется главное меню установочного компакт-диска. Нажмите **Сетевые утилиты**.
- 5 Щелкните **BRAdmin Light** и следуйте отображаемым на экране инструкциям.

■ Macintosh

Утилита BRAdmin Light устанавливается автоматически при установке драйвера принтера. Если драйвер принтера уже установлен, BRAdmin Light не требуется устанавливать повторно.

Задание IP-адреса, маски подсети и шлюза при помощи BRAdmin Light



Примечание

- Можно загрузить последнюю версию утилиты BRAdmin Light с веб-сайта Brother <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 доступна только для пользователей ОС Windows®.
- Если используется функция брандмауэра антишпионских программ или антивирусные приложения, временно отключите их. Убедившись, что печать выполняется, снова запустите приложение.
- Имя узла: имя узла отображается в текущем окне утилиты BRAdmin Light. По умолчанию в аппарате используется имя узла сервера печати “BRNxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxx” – это MAC-адрес / адрес Ethernet аппарата.)
- По умолчанию для серверов печати Brother установлен пароль “access”.

1 Запустите утилиту BRAdmin Light.

■ Windows®

Выберите **Пуск / Все программы**¹ / **Brother / BRAdmin Light / BRAdmin Light**.

¹ **Программы** для пользователей ОС Windows® 2000

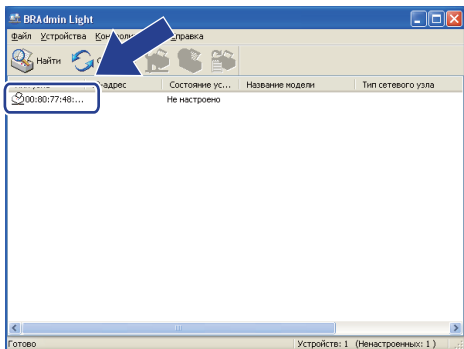
■ Macintosh

Дважды щелкните **Macintosh HD** (загрузочный диск) / **Library** (Библиотека) / **Printers** (Принтеры) / **Brother / Utilities** (Утилиты) / файл **BRAdmin Light.jar**.

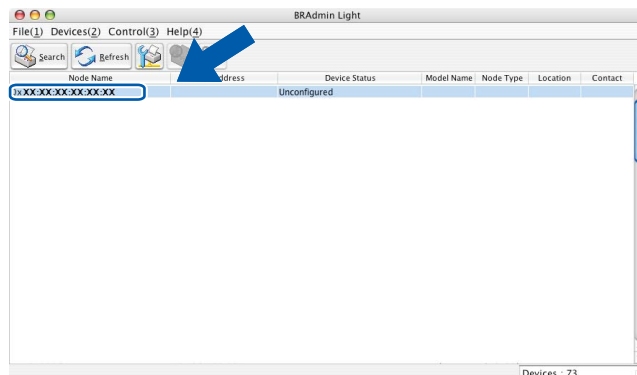
2 Утилита BRAdmin Light автоматически начнет поиск новых устройств.

3 Дважды щелкните ненастроенное устройство.

Windows®



Macintosh



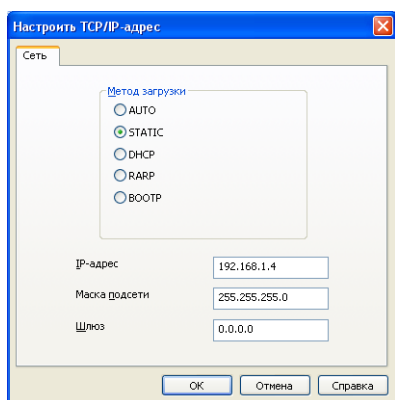
2

 **Примечание**

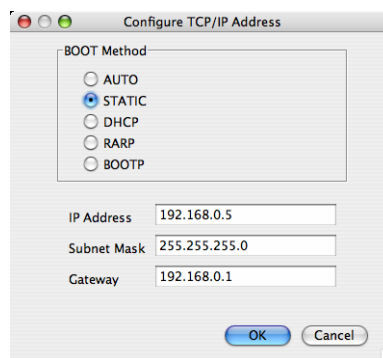
- Если для сервера печати установлены заводские настройки по умолчанию (если сервер DHCP/BOOTP/RARP не используется), устройство отобразится в окне утилиты BRAdmin Light как **Unconfigured (Не настроено)**.
- Чтобы узнать имя узла и MAC-адрес (адрес Ethernet), распечатайте список конфигурации сети. (Для получения информации о печати списка конфигурации сети на сервере печати см. раздел *Печать Списка конфигурации сети* на стр. 36.) Имя узла и MAC-адрес можно также найти с помощью панели управления. (См. раздел *Глава 5: Настройка с панели управления*.)

4 Выберите **STATIC** (Статический) в **BOOT Method (Метод загрузки)**. Введите **IP Address (IP-адрес)**, **Subnet Mask (Маска подсети)** и **Gateway (Шлюз)** (при необходимости) сервера печати.

Windows®



Macintosh



5 Нажмите **ОК**.

6 Если IP-адрес указан правильно, сервер печати Brother появится в списке устройств.

Другие утилиты управления

Помимо утилиты BRAdmin Light аппарат Brother имеет следующие утилиты управления. С помощью этих утилит можно изменять сетевые настройки.

Система управления через веб-интерфейс (веб-браузер)

Используйте стандартный веб-браузер для изменения настроек принтера с помощью протокола HTTP (Hyper Text Transfer Protocol). (См. раздел *Настройка параметров аппарата с помощью системы управления через веб-интерфейс (веб-браузер)* на стр. 46.)

Утилита BRAdmin Professional 3 (Windows®)

BRAdmin Professional 3 – это утилита для расширенного управления аппаратами Brother, подключенными к сети. С помощью этой утилиты можно осуществлять поиск аппаратов Brother в сети и просматривать состояние устройства в удобном окне, напоминающем окно проводника, цвет которого меняется в зависимости от состояния каждого устройства. Можно настроить параметры сети и устройства, а также возможность обновления микропрограммы устройства из компьютера Windows® по ЛВС. Утилита BRAdmin Professional 3 может также регистрировать активность аппаратов Brother по сети и экспортировать полученные данные в формате HTML, CSV, TXT или SQL.

Установите программу Print Auditor Client на клиентский компьютер для пользователей, которым необходимо контролировать устройства, подключенные локально. Данная утилита позволяет контролировать устройства, подключенные к клиентскому компьютеру 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 доступна только для пользователей ОС Windows®.
- Если используется функция брандмауэра антишпионских программ или антивирусные приложения, временно отключите их. 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 / адрес Ethernet аппарата.)

Web BRAdmin (Windows®)

Утилита Web BRAdmin предназначена для управления аппаратами Brother, подключенными к сети. С помощью этой утилиты можно осуществлять поиск аппаратов Brother в сети, просмотр их состояния и настройку параметров сети.

В отличие от утилиты BRAdmin Professional 3, которая предназначена только для ОС Windows®, доступ к установленной на сервере утилите Web BRAdmin можно получать с любого клиентского компьютера, на котором установлен веб-браузер с поддержкой JRE (Java Runtime Environment – среда исполнения Java). Установив серверную утилиту Web BRAdmin на компьютер с запущенной службой IIS¹, администраторы получают возможность подключаться с помощью веб-браузера к серверу Web BRAdmin, который, в свою очередь, соединяется с самим устройством.

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

¹ Internet Information Server 4.0 или Internet Information Services 5.0/5.1/6.0/7.0

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. Утилита BRPrint Auditor может передавать эту информацию на другой компьютер по сети с помощью утилиты BRAdmin Professional 3 или Web BRAdmin 1.45 или более поздней версии. 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 модели MFC-9560CDW)

Обзор

Для подключения устройства к беспроводной сети рекомендуется следовать шагам, приведенным в *Руководство по быстрой установке*, используя WPS или AOSS™ в меню панели управления. Этот способ позволяет легко подключить аппарат к беспроводной сети.

В этой главе приведены дополнительные способы настройки параметров беспроводной сети. Для получения информации о настройках TCP/IP см. раздел *Как изменить сетевые настройки аппарата (IP-адрес, маска подсети и шлюз)* на стр. 3.



Примечание

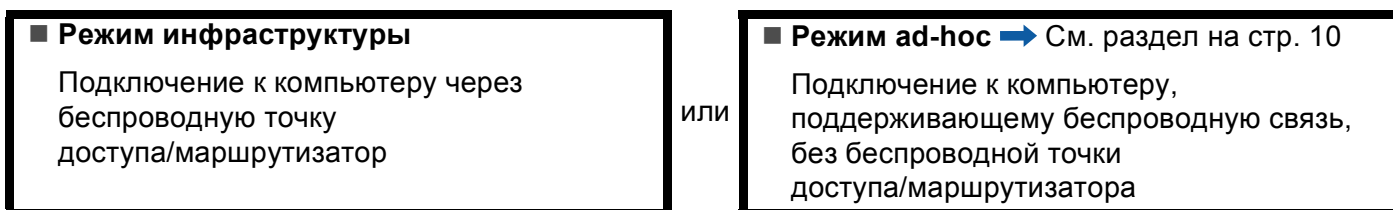
- Для достижения оптимальных результатов при обычной ежедневной печати документов расположите аппарат Brother как можно ближе к беспроводной точке доступа/маршрутизатору, по возможности, без препятствий между ними. Крупные объекты и стены между двумя устройствами, а также помехи от других электронных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

Из-за этих факторов беспроводное соединение может оказаться не лучшим выбором для некоторых типов документов или приложений. При печати больших файлов, таких как многостраничные документы с текстом и большими рисунками, возможно, следует выбрать проводную сеть Ethernet для более быстрой передачи данных или подключение USB для повышения общей скорости печати.

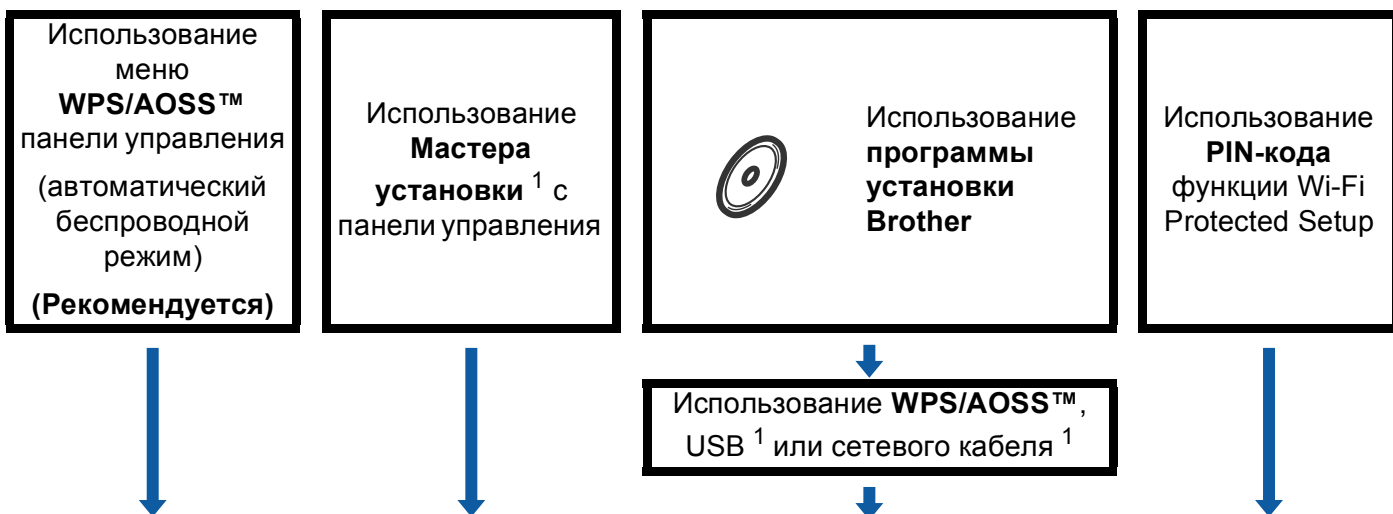
- Хотя аппарат Brother может использоваться как в проводной, так и в беспроводной сети, одновременно может использоваться только один способ подключения.
- Перед настройкой параметров беспроводной связи необходимо знать имя сети: (SSID, ESSID) и сетевой ключ. При использовании корпоративной беспроводной сети также необходимо знать идентификатор пользователя и пароль.

Пошаговая схема настройки конфигурации беспроводной сети Для режима инфраструктуры

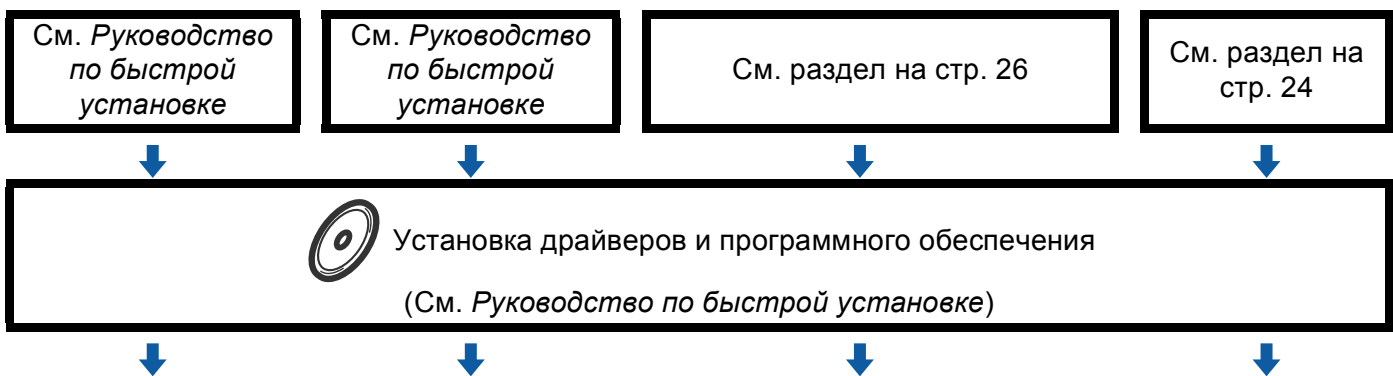
1 Проверьте свою сетевую среду. См. раздел на стр. 11.



2 Проверьте способ настройки беспроводной сети. См. раздел на стр. 12.



3 Настройте аппарат для работы в беспроводной сети. См. раздел на стр. 16.

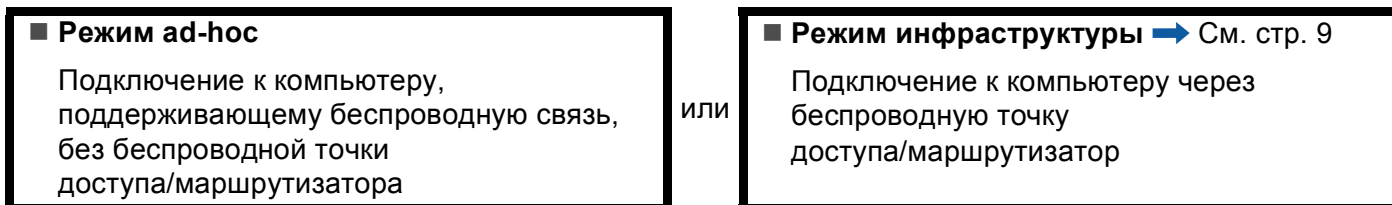


¹ Поддержка IEEE 802.1x

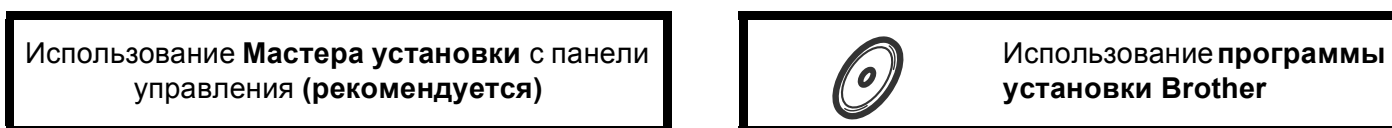
ОК! Настройка параметров беспроводной сети и установка драйвера принтера завершены.

Для режима ad-hoc

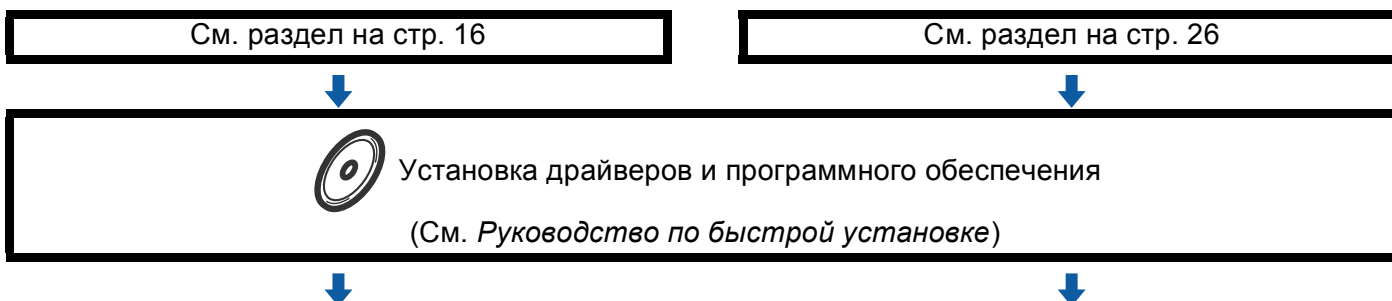
- 1 Проверьте свою сетевую среду. См. раздел на стр. 11.



- 2 Проверьте способ настройки беспроводной сети. См. раздел на стр. 12.



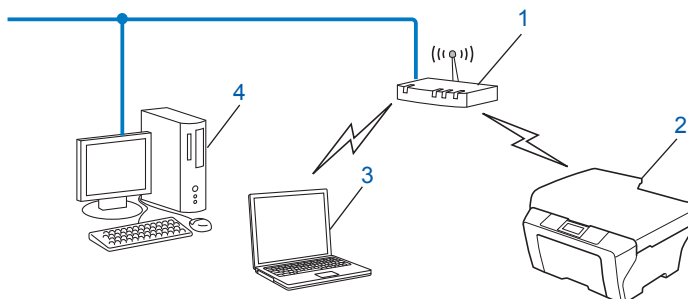
- 3 Настройте аппарат для работы в беспроводной сети. См. раздел на стр. 16.



- OK! Настройка параметров беспроводной сети и установка драйвера принтера завершены.

Проверьте свою сетевую среду

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



1 Беспроводная точка доступа/маршрутизатор ¹

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

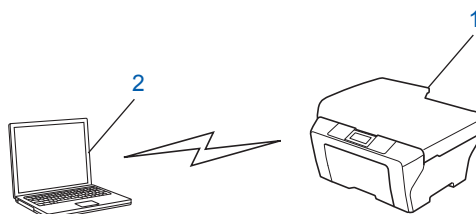
2 Беспроводное сетевое устройство (используемый аппарат)

3 Компьютер, поддерживающий беспроводное подключение, соединенный с беспроводной точкой доступа/маршрутизатором

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

Подключение к компьютеру, поддерживающему беспроводную связь, без беспроводной точки доступа/маршрутизатора в сети (режим ad-hoc)

В сети этого типа отсутствует центральная беспроводная точка доступа/маршрутизатор. Все беспроводные клиенты обмениваются данными непосредственно друг с другом. Когда беспроводной аппарат Brother (данный аппарат) подключен к сети, он получает все задания на печать непосредственно с компьютера, передающего данные печати.



1 Беспроводное сетевое устройство (используемый аппарат)

2 Компьютер, поддерживающий беспроводное подключение



Примечание

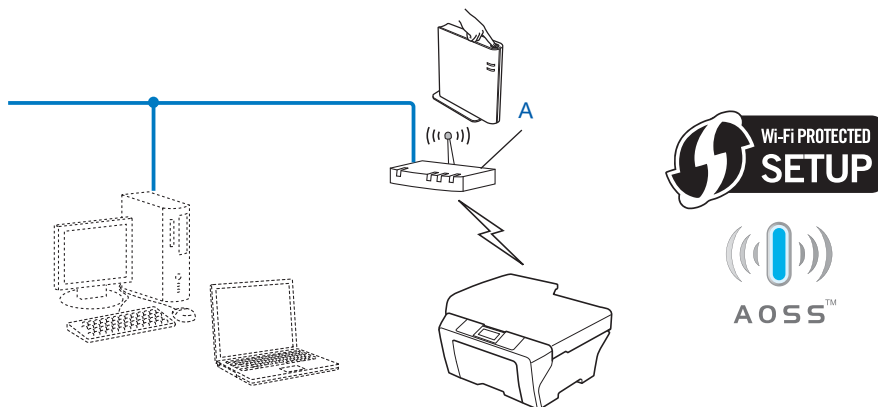
Беспроводное сетевое подключение для продуктов Windows Server® в режиме ad-hoc не гарантируется.

Проверьте способ настройки беспроводной сети

Существует четыре способа для настройки аппарата для работы в беспроводной сети. Используйте WPS/AOSS™ в меню панели управления (рекомендуется), мастер настройки с панели управления, программу установки Brother на компакт-диске или вариант с использованием ПИН-кода функции Wi-Fi Protected Setup. Порядок настройки зависит от сетевой среды.

Настройка аппарата с помощью WPS или AOSS™ в меню панели управления для работы в беспроводной сети (автоматический беспроводной режим, только режим инфраструктуры) (рекомендуется)

Рекомендуется использовать WPS или AOSS™ в меню панели управления для настройки параметров беспроводной сети, если беспроводная точка доступа/маршрутизатора (A) поддерживает функцию Wi-Fi Protected Setup (WPS¹) или AOSS™.



¹ Настройка нажатием клавиши

Настройка с помощью мастера установки панели управления аппарата для работы в беспроводной сети

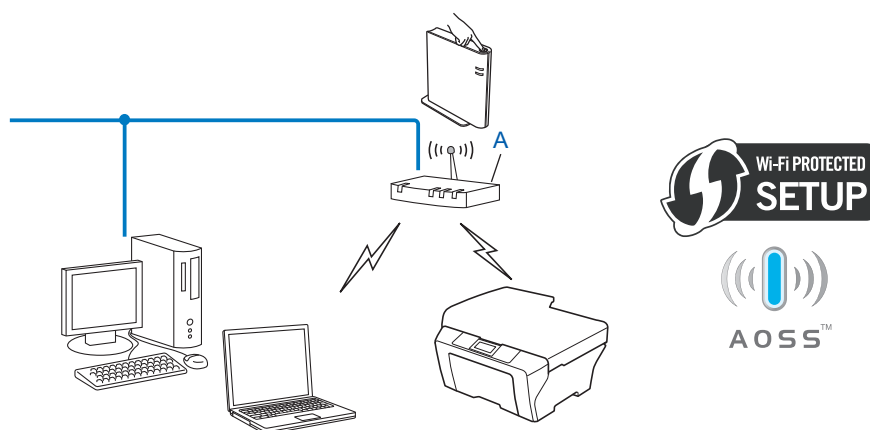
Для настройки параметров беспроводной сети рекомендуется использовать панель управления аппарата. С помощью функции Мастер уст-ки панели управления можно с легкостью подключить аппарат Brother к используемой беспроводной сети. **Перед продолжением установки необходимо узнать настройки беспроводной сети.**

Настройка с использованием находящейся на компакт-диске программы установки Brother, предназначенной для настройки беспроводного сетевого аппарата

Можно также использовать программу установки Brother с компакт-диска, прилагаемого к аппарату. На экран будут выводиться инструкции, после выполнения которых можно будет использовать беспроводной сетевой аппарат Brother. **Перед продолжением установки необходимо узнать настройки беспроводной сети.**

Настройка с использованием автоматического беспроводного режима

Если беспроводная точка доступа/маршрутизатор (A) поддерживает функцию Wi-Fi Protected Setup (PBC¹) или AOSS™, данный аппарат можно легко настроить, даже не зная параметры беспроводной сети, с помощью программы установки Brother.

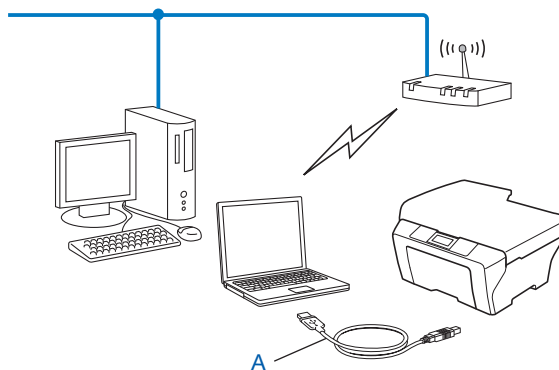


¹ Настройка нажатием клавиши

Настройка с временным использованием кабеля USB или сетевого кабеля

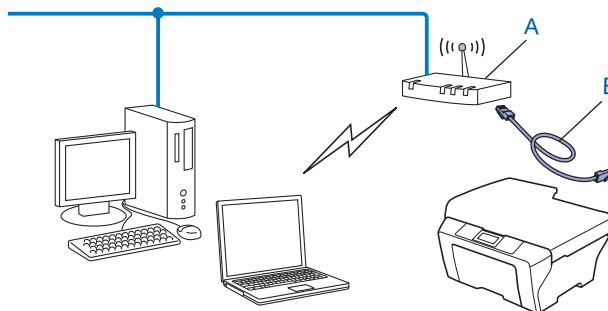
Можно временно использовать кабель USB или сетевой кабель для настройки аппарата Brother этим способом.

- Можно дистанционно настроить аппарат с компьютера, подключенного к сети, с помощью кабеля USB (A)¹.



¹ Можно настроить параметры беспроводной связи, временно подключив аппарат к проводному или беспроводному компьютеру с помощью кабеля USB.

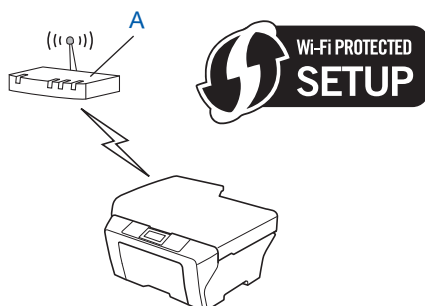
- Если в одной сети присутствует концентратор или маршрутизатор Ethernet с беспроводной точкой доступа (A), можно временно подключить концентратор или маршрутизатор к аппарату с помощью сетевого кабеля (B). Он позволяет дистанционно настроить аппарат с компьютера, подключенного к сети.



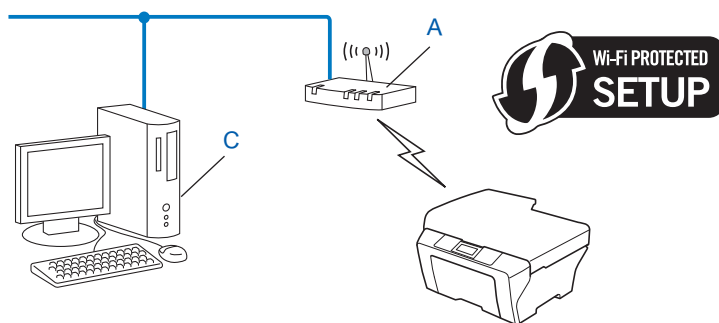
Настройка с помощью PIN-кода функции Wi-Fi Protected Setup для работы в беспроводной сети (только режим инфраструктуры)

Если точка беспроводного доступа/маршрутизатор (A) поддерживает функцию Wi-Fi Protected Setup, настройку можно выполнить также с использованием PIN-кода функции Wi-Fi Protected Setup.

- Подключение, когда беспроводная точка доступа/маршрутизатор (A) используется как регистратор¹.



- Соединение, при котором другое устройство (C), например компьютер, используется в качестве регистратора¹.



¹ Регистратор – это устройство, управляющее беспроводной ЛВС.

Настройка аппарата для работы в беспроводной сети (Для режима инфраструктуры и режима ad-hoc)

❗ ВАЖНАЯ ИНФОРМАЦИЯ

- Если требуется подключить аппарат Brother к компьютерной сети, рекомендуется предварительно обратиться к системному администратору. **Перед продолжением установки необходимо узнать настройки беспроводной сети.**
- Если параметры беспроводной связи данного аппарата уже настраивались, для повторной настройки этих параметров необходимо сбросить настройки сети ЛВС. Нажмите **Меню, 7, 0**, чтобы выбрать **Сброс сет.наст.**, клавишу **1**, чтобы выбрать **Сброс**, после чего нажмите **1** для выбора **Да**, чтобы принять изменения. Аппарат автоматически перезапускается.

Настройка аппарата с помощью WPS или AOSS™ в меню панели управления для работы в беспроводной сети (автоматический беспроводной режим)

Если беспроводная точка доступа/маршрутизатор поддерживает функцию Wi-Fi Protected Setup (WPS¹) или AOSS™, данный аппарат можно легко настроить, даже не зная параметры беспроводной сети. На панели управления аппарата Brother предусмотрено меню WPS/AOSS™. Для получения дополнительной информации см. *Руководство по быстрой установке*.

¹ Настройка нажатием клавиши

Использование Мастера установки с панели управления

Можно настроить аппарат Brother с помощью функции **Мастер уст-ки**. Она расположена в меню **Сеть** на панели управления аппарата.

- 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. *Руководство по быстрой установке*.
 - Если в настройках беспроводной точки доступа/маршрутизатора передача имени SSID запрещена, см. раздел *Настройка аппарата, если отключена передача идентификатора SSID* на стр. 17.
- При настройке аппарата для работы в беспроводной сети с поддержкой стандарта IEEE 802.1x см. раздел *Настройка аппарата для работы в корпоративной беспроводной сети* на стр. 20.
- При настройке аппарата с помощью функции Wi-Fi Protected Setup (PIN-код) см. раздел *Использование PIN-кода функции Wi-Fi Protected Setup* на стр. 24.

Настройка аппарата, если отключена передача идентификатора SSID

- 1 Перед настройкой аппарата рекомендуется записать параметры беспроводной сети. Эта информация понадобится перед продолжением настройки.

Проверьте и запишите текущие значения параметров беспроводной сети.

Имя сети: (SSID / ESSID)

3

Режим обмена данными	Способ аутентификации	Режим шифрования	Сетевой ключ
Инфраструктура	Открытая система	WEP	—
		WEP	
	Общий ключ	WEP	
		WPA/WPA2-PSK	AES
Ad-hoc	Открытая система	TKIP ¹	
		WEP	

¹ Режим TKIP поддерживается только для WPA-PSK.

Пример:

Имя сети: (SSID / ESSID)
HELLO

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



Примечание

Если маршрутизатор использует шифрование WEP, введите ключ, который использовался в качестве первого ключа WEP. Аппарат Brother поддерживает только использование первого ключа WEP.

- 2 Нажмите клавишу **Меню**.
- 3 С помощью ▲ или ▼ выберите **Сеть**.
Нажмите клавишу **ОК**.
- 4 С помощью ▲ или ▼ выберите **Беспровод. сеть**.
Нажмите клавишу **ОК**.
- 5 С помощью ▲ или ▼ выберите **Мастер уст-ки**.
Нажмите клавишу **ОК**.
- 6 Когда отобразится индикация **Вкл. беспр. сеть?**, нажмите кнопку ▲ или ▼ для выбора **1. Вкл.**, а затем нажмите **ОК** для подтверждения.
Запустится мастер беспроводной настройки.
Для отмены нажмите **Стоп/Выход**.
- 7 Устройство производит поиск сети и отображает список доступных идентификаторов SSID.
Выберите **<Новый SSID>** с помощью ▲ или ▼.
Нажмите клавишу **ОК**.
- 8 Введите имя SSID. (Для получения информации о вводе текста см. раздел *Руководство по быстрой установке*.)
Нажмите клавишу **ОК**.
- 9 С помощью ▲ и ▼ выберите **Ad-hoc** или **Инфраструктура**, когда будет указано.
Нажмите клавишу **ОК**.
Выполните одно из следующих действий:
Если выбрано значение **Ad-hoc**, перейдите к шагу 11.
Если выбрано значение **Инфраструктура**, перейдите к шагу 10.
- 10 С помощью ▲ или ▼ выберите способ аутентификации, после чего нажмите клавишу **ОК**.
Выполните одно из следующих действий:
Если выбрано значение **Открытая система**, перейдите к шагу 11.
Если выбрано значение **Общий ключ**, перейдите к шагу 12.
Если выбрано значение **WPA/WPA2-PSK**, перейдите к шагу 13.
- 11 Выберите тип шифрования **Нет** или **WEP** с помощью кнопок ▲ и ▼, а затем нажмите **ОК**.
Выполните одно из следующих действий:
Если выбрано значение **Нет**, перейдите к шагу 15.
Если выбрано значение **WEP**, перейдите к шагу 12.
- 12 Введите ключ WEP, записанный в шаге 1. Нажмите клавишу **ОК**. Перейдите к шагу 15. (Для получения информации о вводе текста см. раздел *Руководство по быстрой установке*.)
- 13 С помощью ▲ или ▼ выберите тип шифрования, **TKIP** или **AES**. Нажмите клавишу **ОК**. Перейдите к шагу 14.

- 14 Введите ключ WPA, записанный в шаге 1, и нажмите **ОК**. Перейдите к шагу 15. (Для получения информации о вводе текста см. раздел *Руководство по быстрой установке*.)
- 15 Чтобы применить настройки, выберите **Да**. Для отмены выберите **Нет**.
Выполните одно из следующих действий:
Если выбрано значение **Да**, перейдите к шагу 16.
Если выбрано значение **Нет**, вернитесь к шагу 7.
- 16 Аппарат начинает подключение к выбранному беспроводному устройству.
- 17 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение **Подключена**.
Аппарат распечатает отчет о состоянии беспроводной сети. Если выполнить подключение не удалось, проверьте код ошибок на распечатанном отчете и см. раздел *Устранение неисправностей* в *Руководстве по быстрой установке*.



(Windows®)

Настройка беспроводной сети завершена. Если требуется продолжить установку драйверов и программного обеспечения, необходимого для работы с аппаратом, выберите в меню компакт-диска пункт Установить MFL-Pro Suite.

(Macintosh)

Настройка беспроводной сети завершена. Если требуется продолжить установку драйверов и программного обеспечения, необходимых для работы с аппаратом, выберите в меню компакт-диска пункт Start Here OSX (Запуск OSX).

Настройка аппарата для работы в корпоративной беспроводной сети

- 1 Перед настройкой аппарата рекомендуется записать параметры беспроводной сети. Эта информация понадобится перед продолжением настройки.

Проверьте и запишите текущие значения параметров беспроводной сети.

Имя сети: (SSID / ESSID)

3

Режим обмена данными	Способ 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 / ESSID)
HELLO

Режим обмена данными	Способ 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 перед началом настройки. Если установлено более одного сертификата, рекомендуется записать имя сертификата, который будет использоваться. Для получения информации об установке сертификата см. раздел *Использование сертификатов для защиты устройств* на стр. 69.
- 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 сетевому администратору.

- 2 Нажмите клавишу **Меню**.
- 3 С помощью ▲ или ▼ выберите *Сеть*.
Нажмите клавишу **ОК**.
- 4 С помощью ▲ или ▼ выберите *Беспровод. сеть*.
Нажмите клавишу **ОК**.
- 5 С помощью ▲ или ▼ выберите *Мастер уст-ки*.
Нажмите клавишу **ОК**.
- 6 Когда отобразится индикация *Вкл. беспр. сеть?*, нажмите кнопку ▲ или ▼ для выбора *1. Вкл.*, а затем нажмите **ОК** для подтверждения.
Запустится мастер беспроводной настройки.
Для отмены нажмите **Стоп/Выход**.
- 7 Устройство производит поиск сети и отображает список доступных идентификаторов 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 **ОК**. Перейдите к шагу 11.
Если в точке доступа отключена вещательная передача идентификатора SSID, необходимо вручную добавить требуемое имя SSID. Перейдите к шагу 8.
- 8 Выберите *<НОВЫЙ SSID>* с помощью ▲ или ▼.
Нажмите клавишу **ОК**. Перейдите к шагу 9.
- 9 Введите имя SSID. (Для получения информации о наборе текста см. *Руководство по быстрой установке*.)
Нажмите клавишу **ОК**. Перейдите к шагу 10.
- 10 С помощью кнопок ▲ и ▼ выберите *Инфраструктура*, когда будет указано.
Нажмите клавишу **ОК**.

- 11 С помощью ▲ или ▼ выберите способ аутентификации, после чего нажмите клавишу **ОК**.
Выполните одно из следующих действий:
Если выбрано значение LEAP, перейдите к шагу 17.
Если выбрано значение EAP-FAST, перейдите к шагу 12.
Если выбрано значение PEAP, перейдите к шагу 12.
Если выбрано значение EAP-TTLS, перейдите к шагу 12.
Если выбрано значение EAP-TLS, перейдите к шагу 13.
- 12 Выберите способ внутренней аутентификации NET, CHAP, MS-CHAP, MS-CHAPv2, GTC или PAP с помощью кнопок ▲ и ▼, а затем нажмите **ОК**.
Перейдите к шагу 13.



Примечание

В зависимости от способа аутентификации можно выбрать различные способы внутренней аутентификации.

- 13 Выберите тип шифрования TKIP или AES с помощью кнопок ▲ и ▼, а затем нажмите **ОК**.
Выполните одно из следующих действий:
Если способом аутентификации является EAP-TLS, перейдите к шагу 14.
При использовании других способов аутентификации перейдите к шагу 15.
- 14 На аппарате отобразится список доступных сертификатов клиента. Выберите сертификат и перейдите к шагу 15.
- 15 Выберите метод проверки подлинности Без проверки, ЦС или ЦС + идент.серв с помощью кнопок ▲ и ▼, а затем нажмите **ОК**.
Выполните одно из следующих действий:
Если выбрано значение ЦС + идент.серв, перейдите к шагу 16.
Если выбрано другое значение, перейдите к шагу 17.



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 защиты устройств* на стр. 69.

- 16 Введите идентификатор сервера. (Для получения информации о наборе текста см. *Руководство по быстрой установке*.) Перейдите к шагу 17.

- 17 Введите идентификатор пользователя, записанный в шаге 1. Нажмите клавишу **ОК**. (Для получения информации о наборе текста см. *Руководство по быстрой установке*.)
Выполните одно из следующих действий:
Если способом аутентификации является EAP-TLS, перейдите к шагу 19.
При использовании других способов аутентификации перейдите к шагу 18.
- 18 Введите пароль, записанный в шаге 1. Нажмите клавишу **ОК**. Перейдите к шагу 19.
- 19 Чтобы применить настройки, выберите **Да**. Для отмены выберите **Нет**.
Выполните одно из следующих действий:
Если выбрано значение **Да**, перейдите к шагу 20.
Если выбрано значение **Нет**, вернитесь к шагу 7.
- 20 Аппарат начинает подключение к выбранной беспроводной сети.
- 21 При успешном подключении беспроводного аппарата на дисплее отобразится сообщение **Подключена**.
Аппарат распечатает отчет о состоянии беспроводной сети. Если выполнить подключение не удалось, проверьте код ошибок на распечатанном отчете и см. раздел **Устранение неисправностей** в *Руководстве по быстрой установке*.



(Windows®)

Настройка беспроводной сети завершена. Если требуется продолжить установку драйверов и программного обеспечения, необходимого для работы с аппаратом, выберите в меню компакт-диска пункт **Установить MFL-Pro Suite.**

(Macintosh)

Настройка беспроводной сети завершена. Если требуется продолжить установку драйверов и программного обеспечения, необходимых для работы с аппаратом, выберите в меню компакт-диска пункт **Start Here OSX (Запуск OSX).**

Использование программы установки Brother с компакт-диска для настройки аппарата для работы в беспроводной сети

Для получения информации об установке см. раздел *Настройка параметров беспроводной сети с помощью программы установки Brother (для MFC-9560CDW)* на стр. 26.

Использование PIN-кода функции Wi-Fi Protected Setup

Если беспроводная точка доступа/маршрутизатор поддерживает функцию Wi-Fi Protected Setup (PIN-код), данный аппарат можно легко настроить. Вариант с использованием PIN-кода (личного идентификационного номера) – это один из способов подключения, разработанный 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 Wi-Fi Protected Setup см. в руководстве пользователя, прилагаемом к беспроводной точке доступа/маршрутизатору.



Примечание

На маршрутизаторах или точках доступа, поддерживающих функцию Wi-Fi Protected Setup, имеется указанный ниже символ.



- 1 С помощью кнопок **Меню**, **7**, **2**, **4**, чтобы выбрать WPS с PIN-код..
- 2 На ЖК-дисплее отображается 8-разрядный PIN-код, и аппарат в течение 5 мин производит поиск беспроводной точки доступа/маршрутизатора.
- 3 На компьютере, подключенном к сети, введите в браузере “http://IP-адрес точки доступа/”. (Где “IP-адрес точки доступа” – это IP-адрес устройства, используемого в качестве регистратора ¹) Перейдите на страницу настройки WPS (Wi-Fi Protected Setup) и введите PIN-код регистратора, отображавшийся на ЖКД в шаге 2, затем следуйте инструкциям на экране.

¹ Регистратором обычно является беспроводная точка доступа/маршрутизатор.



Примечание

Страницы настройки различаются в зависимости от марки беспроводной точки доступа/маршрутизатора. См. инструкции, прилагаемые к беспроводной точке доступа/беспроводному маршрутизатору.



Windows Vista®/Windows® 7

При использовании в качестве регистратора компьютера выполните следующие операции:




Примечание

- Чтобы использовать в качестве регистратора компьютер с ОС Windows Vista® или Windows® 7, сначала необходимо зарегистрировать его в сети. См. инструкции, прилагаемые к беспроводной точке доступа/беспроводному маршрутизатору.
- При использовании в качестве регистратора компьютера с ОС Windows® 7 можно установить драйвер принтера после настройки параметров беспроводной сети, следуя инструкциям на экране. При необходимости установки полного пакета драйверов и программного обеспечения следуйте инструкциям в *Руководство по быстрой установке*.

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

- ④ При успешном подключении беспроводного аппарата на дисплее отобразится сообщение **Подключена**.
Аппарат распечатает отчет о состоянии беспроводной сети. Если выполнить подключение не удалось, проверьте код ошибок на распечатанном отчете и см. раздел *Устранение неисправностей* в *Руководстве по быстрой установке*.

 (Windows®)
Настройка беспроводной сети завершена. Если требуется продолжить установку драйверов и программного обеспечения, необходимого для работы с аппаратом, выберите в меню компакт-диска пункт Установить MFL-Pro Suite.

(Macintosh)

Настройка беспроводной сети завершена. Если требуется продолжить установку драйверов и программного обеспечения, необходимых для работы с аппаратом, выберите в меню компакт-диска пункт Start Here OSX (Запуск OSX).

Настройка параметров беспроводной сети с помощью программы установки Brother (для MFC-9560CDW)

Перед настройкой параметров беспроводной связи

! ВАЖНАЯ ИНФОРМАЦИЯ

- Приведенные ниже инструкции предназначены для установки аппарата Brother в сетевой среде с использованием программы установки Brother, находящейся на компакт-диске из комплекта поставки аппарата.
- Аппарат Brother можно также настроить с помощью WPS или AOSS™ на панели управления аппарата (рекомендуется). См. инструкции в прилагаемом *Руководстве по быстрой установке*.
- Если параметры беспроводной связи данного аппарата уже настраивались, для повторной настройки этих параметров необходимо сбросить настройки сети ЛВС. Нажмите **Меню, 7, 0**, чтобы выбрать **Сброс сет. наст.**, клавишу **1**, чтобы выбрать **Сброс**, после чего нажмите **1** для выбора **Да**, чтобы принять изменения. Аппарат автоматически перезапускается.
- 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 потребуются временно использовать кабель USB или кабель Ethernet (LAN).
- **Перед продолжением установки необходимо узнать настройки беспроводной сети.**
Обязательно запишите все текущие параметры, такие как SSID, аутентификация и шифрование используемой беспроводной сети. Если настройки неизвестны, обратитесь к сетевому администратору или производителю беспроводной точки доступа/маршрутизатора.

Настройка параметров беспроводной связи

- 1 Перед настройкой аппарата рекомендуется записать параметры беспроводной сети. Эта информация понадобится перед продолжением настройки.
Проверьте и запишите текущие значения параметров беспроводной сети.

Настройка частной беспроводной сети

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

Имя сети (SSID, ESSID)	Сетевой ключ

Пример:

Имя сети (SSID, ESSID)	Сетевой ключ
HELLO	12345678

Настройка корпоративной беспроводной сети

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

Имя сети: (SSID / ESSID)

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

Пример:

Имя сети: (SSID / ESSID)
HELLO

Режим обмена данными	Способ 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 перед началом настройки. Если установлено более одного сертификата, рекомендуется записать имя сертификата, который будет использоваться. Для получения информации об установке сертификата см. раздел *Использование сертификатов для защиты устройств* на стр. 69.
- 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 сетевому администратору.

- 2** Вставьте сопроводительный компакт-диск в дисковод для компакт-дисков.

(Windows®)

- 1 Автоматически откроется начальное окно.
Если откроется экран выбора модели, выберите имеющийся аппарат. Если откроется экран выбора языка, выберите требуемый язык.
- 2 Откроется главное меню установочного компакт-диска. Нажмите **Начальная установка**.

Примечание

- Если это окно не открывается, с помощью Проводника Windows® запустите программу Start.exe из корневой папки компакт-диска Brother.
- Если отображается экран **Контроль учетных записей пользователей**,
(Windows Vista®) щелкните **Разрешить**.
(Windows® 7) щелкните **Да**.

- 3** Нажмите **Мастер настройки беспроводной сети**.

(Macintosh)

- 1 Дважды щелкните значок **MFL-Pro Suite** на рабочем столе.
- 2 Дважды щелкните значок **Utilities** (Утилиты).
- 3 Дважды щелкните значок **Wireless Device Setup Wizard** (Мастер настройки беспроводного устройства).

- 3 Выберите **Да, моя точка доступа поддерживает WPS или AOSS, и я хочу их использовать.** или **Нет**, затем щелкните **Далее**.

При выборе **Нет** для настройки параметров беспроводной связи можно использовать четыре разных способа.

- Временное использование кабеля USB
- Временное использование кабеля Ethernet (LAN)
- Настройка вручную с помощью панели управления
- Использование режима ad-hoc



Примечание

При использовании режима ad-hoc выполните следующие действия.

- Если после изменения настроек беспроводной сети отображается сообщение с требованием перезагрузить компьютер, перезагрузите компьютер, затем вернитесь к шагу 2.
- Настройки беспроводной связи в компьютере можно временно изменить.

(Windows Vista® и Windows® 7)

- 1 Нажмите кнопку , а затем **Панель управления**.
- 2 Нажмите **Сеть и Интернет**, а затем щелкните значок **Центр управления сетями и общим доступом**.
- 3 Нажмите **Центр управления сетями и общим доступом**.
- 4 В списке отображается идентификатор SSID беспроводного аппарата. Выберите **SETUP**, а затем нажмите **Подключиться**.
- 5 (Только для Windows Vista®)
Нажмите **Все равно подключить**, затем **Заккрыть**.
- 6 (ОС Windows Vista®)
Нажмите **Просмотр состояния** в окне **Беспроводное сетевое соединение (SETUP)**.
- 7 (ОС Windows® 7)
Нажмите **Беспроводное сетевое соединение (SETUP)**.
- 8 Нажмите **Сведения...** и проверьте экран **Сведения о сетевом подключении**. Переход с IP-адреса 0.0.0.0 на IP-адрес 169.254.x.x на экране может занять несколько минут (где x.x. – числа от 1 до 254).

(Windows® XP SP2 или более поздней версии)

- 1 Нажмите **Пуск**, затем **Панель управления**.
- 2 Щелкните значок **Сеть и подключения к Интернету**.
- 3 Щелкните значок **Сетевые подключения**.
- 4 Выберите и нажмите правой кнопкой мыши **Беспроводное сетевое соединение**. Нажмите **Просмотреть доступные беспроводные сети**.
- 5 В списке отображается идентификатор SSID беспроводного принтера. Выберите **SETUP** и нажмите **Подключиться**.
- 6 Проверьте состояние **Беспроводное сетевое соединение**. Переход с IP-адреса 0.0.0.0 на IP-адрес 169.254.x.x на экране может занять несколько минут (где x.x. – числа от 1 до 254).

(Macintosh)

- 1 Щелкните значок состояния AirPort в строке меню.
- 2 Выберите **SETUP** (Настройка) из всплывающего меню.
- 3 Беспроводная сеть успешно подключена.

4 Для настройки параметров беспроводной связи следуйте инструкциям на экране.



Настройка беспроводной сети завершена. Если требуется продолжить установку драйверов и программного обеспечения, необходимых для работы с аппаратом, выберите в меню компакт-диска пункт Установить MFL-Pro Suite.

Меню “Сеть”

Настроить аппарат Brother для сети с определенной конфигурацией можно с помощью пунктов меню *Сеть* панели управления. (Для получения дополнительной информации об использовании панели управления см. *Руководство по основным функциям*.) Нажмите **Меню**, затем с помощью кнопок ▲ и ▼ выберите *Сеть*. Перейдите к пункту меню, который нужно настроить. (Для получения дополнительной информации о меню см. раздел *Таблица функций и заводские настройки* на стр. 38.)

Обратите внимание, что в комплект аппарата входит утилита BRAdmin Light, система управление через веб-интерфейс или программы удаленной настройки ¹, которые также можно использовать для настройки различных параметров сети. (См. раздел *Другие утилиты управления* на стр. 6.)

¹ Не поддерживается для модели DCP.

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 *Беспровод. сеть*.

Способ загрузки

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

Автоматический режим

В этом режиме аппарат будет сканировать сеть для поиска сервера DHCP. Если аппарат найдет сервер и сервер DHCP настроен для выделения IP-адреса, аппарат будет использовать IP-адрес, предоставленный сервером DHCP. Если сервер DHCP недоступен, то аппарат выполнит сканирование для поиска сервера BOOTP. Если сервер BOOTP доступен и правильно настроен, аппарат получит IP-адрес от сервера BOOTP. Если сервер BOOTP недоступен, аппарат выполнит сканирование для поиска сервера RARP. Если сервер RARP также не отвечает, IP-адрес задается с помощью протокола APIPA. После включения питания аппарату может потребоваться несколько минут для сканирования сети на наличие сервера.

Статический режим

В этом режиме IP-адрес устройства должен быть назначен вручную. После ввода назначенный IP-адрес будет зафиксирован.



Примечание

Если не требуется настраивать сервер печати с помощью DHCP, BOOTP или RARP, необходимо установить для параметра *Метод загрузки* значение *Статический*, чтобы сервер печати имел статический IP-адрес. Это предотвратит попытки сервера печати получить IP-адрес от какой-либо из этих систем. Чтобы изменить способ загрузки, используйте панель управления аппарата, утилиту BRAdmin Light, систему управления через веб-интерфейс или программу удаленной настройки.

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 сетевому администратору). Если выбран способ, отличный от *Статический*, аппарат определит свой IP-адрес с помощью протокола DHCP или BOOTP.

Выбранный по умолчанию IP-адрес аппарата, вероятно, будет несовместим со схемой номеров IP-адресов, которая используется в сети. Для получения IP-адреса сети, к которой будет подключен аппарат, обратитесь к сетевому администратору.

Маска подсети

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

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 сетевому администратору.

Имя хоста

Можно зарегистрировать имя аппарата в сети. Это имя часто называется именем NetBIOS; оно будет зарегистрировано сервером WINS в сети. Компания Brother рекомендует имя “BRNxxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxxx” – это MAC-адрес / адрес Ethernet аппарата.)

Конфигурация WINS

Этот параметр определяет, как аппарат получает IP-адрес сервера WINS.

Авто

Аппарат автоматически использует запрос DHCP для определения IP-адресов первичного и вторичного серверов WINS. Чтобы использовать эту функцию, для параметра СПОСОБ ЗАГР. должно быть установлено значение “Авто”.

Статический

Аппарат использует указанный IP-адрес для первичного и вторичного серверов WINS.

Сервер WINS

IP-адрес первичного сервера WINS

В этом поле указывается IP-адрес первичного сервера WINS (Windows® Internet Name Service). Если задано значение, отличное от нуля, аппарат отправит запрос на этот сервер для регистрации своего имени в Windows® Internet Name Service.

IP-адрес вторичного сервера WINS

В этом поле указывается IP-адрес вторичного сервера WINS. Этот адрес используется в качестве резервного адреса первичного сервера WINS. Если первичный сервер недоступен, аппарат может зарегистрироваться на вторичном сервере. Если задано значение, отличное от нуля, аппарат отправит запрос на этот сервер для регистрации своего имени в Windows® Internet Name Service. Если имеется первичный сервер WINS, но отсутствует вторичный сервер WINS, оставьте это поле незаполненным.

Сервер DNS

IP-адрес первичного сервера DNS

В этом поле указывается IP-адрес первичного сервера DNS (Domain Name System).

IP-адрес вторичного сервера DNS

В этом поле указывается IP-адрес вторичного сервера DNS. Этот адрес используется в качестве резервного адреса первичного сервера DNS. При отсутствии доступа к первичному серверу DNS аппарат обращается к вторичному серверу DNS. Если имеется первичный сервер DNS, но отсутствует вторичный сервер DNS, оставьте это поле незаполненным.

APIPA

Если установить значение **Вкл.**, то сервер печати будет автоматически выделять IP-адрес локальной связи в диапазоне (169.254.1.0 - 169.254.254.255), когда он не сможет получить IP-адрес выбранным способом загрузки. (См. раздел *Способ загрузки* на стр. 31.) При выборе значения **Выкл.**, если серверу печати не удастся получить IP-адрес с помощью выбранного способа загрузки, IP-адрес меняться не будет.

IPv6

Этот аппарат совместим с протоколом IPv6, протоколом Интернета следующего поколения. Если нужно использовать протокол IPv6, выберите **Вкл.** Значение по умолчанию для IPv6 – **Откл.** Для получения дополнительной информации о протоколе IPv6 посетите веб-сайт <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 установки для IPv6 значения **Вкл.** эта настройка будет применена к интерфейсам проводной и беспроводной ЛВС.

Ethernet (только для проводной сети)

Режим связи Ethernet. Значение “Авто” позволяет серверу печати работать в полно- или полудуплексном режиме 100BASE-TX, а также в полно- или полудуплексном режиме 10BASE-T посредством автоматического согласования.



Примечание

Если это значение задано неправильно, возможно, обмен данными с сервером печати не удастся выполнить.

Состояние (Для DCP-9055CDN, MFC-9460CDN и MFC-9465CDN)/Состояние проводного подключения (Для MFC-9560CDW)

В данном поле отображается текущее состояние проводной сети.

Мастер установки (только для беспроводной сети)

Мастер уст-ки помогает выполнить настройку беспроводной сети. (Для получения дополнительной информации см. *Руководство по быстрой установке* или раздел *Использование Мастера установки с панели управления* на стр. 16.)

WPS или AOSS™ (только для беспроводной сети)

Если беспроводная точка доступа/маршрутизатор поддерживает функцию Wi-Fi Protected Setup (WPS¹) или AOSS™ (автоматический беспроводной режим), данный аппарат можно легко настроить, даже не зная параметры беспроводной сети. (Для получения дополнительной информации см. *Руководство по быстрой установке* или раздел *Настройка аппарата с помощью WPS или AOSS™ в меню панели управления для работы в беспроводной сети (автоматический беспроводной режим)* на стр. 16.)

¹ Настройка нажатием клавиши

WPS с PIN-кодом (только для беспроводной сети)

Если беспроводная точка доступа/маршрутизатор поддерживает функцию Wi-Fi Protected Setup (PIN-код), данный аппарат можно легко настроить без использования компьютера. (Для получения дополнительной информации см. раздел *Использование PIN-кода функции Wi-Fi Protected Setup* на стр. 24.)

Состояние беспроводной сети (только для беспроводной сети)

Состояние

В данном поле отображается текущее состояние беспроводной сети.

Сигнал

В данном поле отображается текущий уровень сигнала беспроводной сети.

SSID

В данном поле отображается текущее значение SSID беспроводной сети. На дисплее отображаются до 32 символов имени SSID.

Режим связи

В данном поле отображается текущий режим связи беспроводной сети.

MAC-адрес

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

Установка значений по умолчанию (для модели MFC-9560CDW)

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* на стр. 36.

Проводное подключение (для модели MFC-9560CDW)

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

Беспроводное подключение (для MFC-9560CDW)

Если требуется использовать беспроводное сетевое подключение, задайте для параметра *В/пр. сеть* *вкл.* значение *Вкл.*.



Примечание

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

Установка нового значения по умолчанию для функции “Сканировать на FTP”

Можно выбрать используемый по умолчанию тип цветных файлов для функции “Сканировать на FTP”. (Для получения информации об использовании функции “Сканировать на FTP” см. раздел *Сетевое сканирование в Руководство по использованию программного обеспечения.*)

Установка нового значения по умолчанию для функции “Сканировать в сеть”

Можно задать цвет и тип файлов по умолчанию для функции “Сканировать в сеть”, чтобы выполнять сканирование документа непосредственно на сервер, поддерживающий протокол CIFS в локальной сети или сети Интернет. (Для получения информации о протоколе CIFS см. *Сетевая терминология.*) (Для получения информации об использовании функции “Сканировать в сеть” см. раздел *Сетевое сканирование в Руководство по использованию программного обеспечения.*)

Восстановление заводских настроек сети

Можно восстановить заводские параметры сервера печати (восстановление всей информации, такой как информация о пароле и IP-адресе).



Примечание

- Эта функция восстанавливает все заводские параметры проводной и беспроводной сети.
- Можно также восстановить заводские параметры сервера печати с помощью приложений BRAdmin или системы управления через веб-интерфейс. (Для получения дополнительной информации см. раздел *Другие утилиты управления* на стр. 6.)

- 1 Нажмите клавишу **Меню**.
- 2 С помощью ▲ или ▼ выберите **Сеть**.
Нажмите клавишу **ОК**.
- 3 С помощью ▲ или ▼ выберите **Сброс сет.наст.**
Нажмите клавишу **ОК**.
- 4 Нажмите клавишу **1**, чтобы выбрать **Сброс**.
- 5 Нажмите клавишу **1**, чтобы выбрать **Да** для перезагрузки.
- 6 Аппарат выполнит перезагрузку.

5

Печать Списка конфигурации сети



Примечание

Имя узла: имя узла отображается в списке конфигурации сети. По умолчанию используется имя узла “BRNxxxxxxxxxxxx” для проводной сети или “BRWxxxxxxxxxxxx” для беспроводной сети. (“xxxxxxxxxxxx” – это MAC-адрес / адрес Ethernet аппарата.)

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

- 1 Нажмите клавишу **Меню**.
- 2 (Для моделей MFC) С помощью кнопок ▲ и ▼ выберите **Печать отчетов**.
(Для моделей DCP) С помощью кнопок ▲ и ▼ выберите **Инф. об уст-ве**.
Нажмите клавишу **ОК**.
- 3 С помощью ▲ или ▼ выберите **Сетев. конфиг..**
Нажмите клавишу **ОК**.
- 4 Нажмите **Ч/б Старт** или **Цвет Старт**.



Примечание

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

Печать отчета о состоянии беспроводной сети (для MFC-9560CDW)

Отчет WLAN можно распечатать отчет о состоянии беспроводной сети. Если выполнить беспроводное подключение не удалось, проверьте код ошибок на распечатанном отчете и см. раздел Устранение неисправностей в *Руководстве по быстрой установке*.

- 1 Нажмите клавишу **Меню**.
- 2 С помощью ▲ или ▼ выберите **Печать отчетов**.
Нажмите клавишу **ОК**.
- 3 С помощью ▲ или ▼ выберите **Отчет WLAN**.
Нажмите клавишу **ОК**.
- 4 Нажмите **Ч/Б Старт** или **Цвет Старт**.

Таблица функций и заводские настройки

DCP-9055CDN, MFC-9460CDN и MFC-9465CDN

Заводские настройки выделены жирным шрифтом и звездочкой.

Главное меню	Подменю	Пункты меню	Опции	
4. Сеть (DCP-9055CDN) 7. Сеть (MFC-9460CDN и MFC-9465CDN)	1. TCP/IP	1. Метод загрузки	Авто* Статический RARP BOOTP DHCP (При выборе значения Авто, RARP, BOOTP или DHCP появится запрос на введение количества попыток получения IP-адреса аппаратом.)	
		2. IP-адрес	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000] * ¹	
		3. Маска подсети	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000] * ¹	
		4. Шлюз	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000] *	
		5. Имя хоста	BRNxxxxxxxxxxxxxx (не более 32 символов)	
		6. Конфиг. WINS	Авто* Статический	
		7. Сервер WINS	Первичный	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000] *
			Вторичный	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000] *
		8. Сервер DNS	Первичный	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000] *
			Вторичный	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000] *
9. APIPA	Вкл.* Выкл.			

Главное меню	Подменю	Пункты меню	Опции
4. Сеть (DCP-9055CDN) 7. Сеть (MFC-9460CDN и MFC-9465CDN) (продолжение)	1. TCP/IP (продолжение)	0. IPv6	Вкл. Откл.*
	2. Ethernet	—	Авто* 100В-FD 100В-HD 10В-FD 10В-HD
	3. Состояние	—	Активна 100В-FD Активна 100В-HD Активна 10В-FD Активна 10В-HD Неактивна
	4. MAC-адрес	—	—
	5. Скан. на FTP	—	Цвет 100 т/д* Цвет 200 т/д Цвет 300 т/д Цвет 600 т/д Серый 100 т/д Серый 200 т/д Серый 300 т/д Ч/Б 200 т/д Ч/Б 200x100 т/д

Главное меню	Подменю	Пункты меню	Опции
4 . Сеть (DCP-9055CDN) 7 . Сеть (MFC-9460CDN и MFC-9465CDN) (продолжение)	6.Скан.на сервер	—	Цвет 100 т/д* (Если выбран вариант “Цвет”) Цвет 200 т/д PDF* Цвет 300 т/д PDF/A Цвет 600 т/д Secure PDF Серый 100 т/д Подписанный PDF Серый 200 т/д JPEG Серый 300 т/д XPS Ч/Б 200 т/д (Если выбран вариант “Серый”) Ч/Б 200x100 т/д PDF* PDF/A Secure PDF Подписанный PDF JPEG XPS (Если выбран вариант “Ч/Б”) PDF* PDF/A Secure PDF Подписанный PDF TIFF
	0.Сброс сет.наст	—	1 . Сброс
	—	—	2 . Выход

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

MFC-9560CDW

Главное меню	Подменю	Пункты меню		Опции
7. Сеть	1. Проводная сеть	1. TCP/IP	1. Метод загрузки	Авто* Статический RARP BOOTP DHCP (При выборе значения Авто, RARP, BOOTP или DHCP появится запрос на введение количества попыток получения IP-адреса аппаратом.)
			2. IP-адрес	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]* ¹
			3. Маска подсети	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]* ¹
			4. Шлюз	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
			5. Имя хоста	BRNxxxxxxxxxxxxxx (не более 32 символов)
			6. Конфиг. WINS	Авто* Статический
			7. Сервер WINS	Первичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
				Вторичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
			8. Сервер DNS	Первичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
				Вторичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
9. APIPA	Вкл.* Выкл.			
0. IPv6	Вкл. Откл.*			

Главное меню	Подменю	Пункты меню		Опции	
7. Сеть (продолжение)	1. Проводная сеть (продолжение)	2. Ethernet	—	Авто* 100В-FD 100В-HD 10В-FD 10В-HD	
		3. Сост. пров. сети	—	Активна 100В-FD Активна 100В-HD Активна 10В-FD Активна 10В-HD Неактивна Провод. сеть откл	
		4. MAC-адрес	—	—	
		5. Настр. по умч.	—	1. Сброс 2. Выход	
		6. Пров. сеть вкл.	—	Вкл.* Откл.	
		2. Беспровод. сеть	1. TCP/IP	1. Метод загрузки	—
	2. IP-адрес			—	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]* ¹
	3. Маска подсети			—	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]* ¹
	4. Шлюз			—	[000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
	5. Имя хоста			—	BRWxxxxxxxxxxxxx (не более 32 символов)
	6. Конфиг. WINS			—	Авто Статический

Главное меню	Подменю	Пункты меню	Опции	
7. Сеть (продолжение)	2. Беспровод. сеть (продолжение)	1. TCP/IP (продолжение)	7. Сервер WINS	Первичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
				Вторичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
			8. Сервер DNS	Первичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
				Вторичный [000-255] . [000-255] . [000-255] . [000-255] [000] . [000] . [000] . [000]*
			9. APIPA	Вкл.* Выкл.
			0. IPv6	Вкл. Откл.*
		2. Мастер уст-ки	1. Вкл. 2. Откл.	—
		3. WPS/AOSS	1. Вкл. 2. Откл.	—
		4. WPS с PIN-код.	1. Вкл. 2. Откл.	—
		5. Статус WLAN	1. Состояние	Активна (11b) Активна (11g) Пров. сеть актив Беспр. сеть откл AOSS активен Сбой соединения
			2. Сигнал	Сильный Средний Слабый Нет
			3. SSID	—
			4. Режим связи	Ad-hoc Инфраструктура
		6. MAC-адрес	—	—

Главное меню	Подменю	Пункты меню		Опции
7. Сеть (продолжение)	2. Беспровод. сеть (продолжение)	7. Настр. по умч.	—	1. Сброс 2. Выход
		8. Б/пр. сеть вкл.	—	1. Вкл. 2. Откл.
	3. Скан. на FTP	—	Цвет 100 т/д* Цвет 200 т/д Цвет 300 т/д Цвет 600 т/д Серый 100 т/д Серый 200 т/д Серый 300 т/д Ч/Б 200 т/д Ч/Б 200x100 т/д	(Если выбран вариант “Цвет”) PDF* PDF/A Secure PDF Подписанный PDF JPEG XPS (Если выбран вариант “Серый”) PDF* PDF/A Secure PDF Подписанный PDF JPEG XPS (Если выбран вариант “Ч/Б”) PDF* PDF/A Secure PDF Подписанный PDF TIFF

Главное меню	Подменю	Пункты меню		Опции
7. Сеть (продолжение)	4. Скан. на сервер	—	Цвет 100 т/д* Цвет 200 т/д Цвет 300 т/д Цвет 600 т/д Серый 100 т/д Серый 200 т/д Серый 300 т/д Ч/Б 200 т/д Ч/Б 200x100 т/д	(Если выбран вариант “Цвет”) PDF* PDF/A Secure PDF Подписанный PDF JPEG XPS (Если выбран вариант “Серый”) PDF* PDF/A Secure PDF Подписанный PDF JPEG XPS (Если выбран вариант “Ч/Б”) PDF* PDF/A Secure PDF Подписанный PDF TIFF
		0. Сброс сет. наст	—	1. Сброс
	—	—	2. Выход	

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

Обзор

Используйте стандартный веб-браузер для изменения настроек аппарата с помощью протокола HTTP (Hyper Text Transfer Protocol). С помощью веб-браузера можно получить доступ к следующим пунктам настройки аппарата.

- Информация о состоянии аппарата
- Изменение элементов конфигурации факса, таких как параметры общей настройки, адресной книги и удаленного факса
- Изменение сетевых параметров, например информации TCP/IP.
- Настройка защитной блокировки функций 2.0
- Настройка функции “Сохранение журнала в сети”
- Настроить функцию “Сканировать на FTP”
- Настройка функции “Сканировать в сеть”
- Информация о версии программного обеспечения аппарата и сервера печати
- Изменение сведений о конфигурации сети и аппарата



Примечание

Рекомендуется использовать Microsoft® Internet Explorer® 6.0 (или более поздней версии) или Firefox 3,0 (или более поздней версии) для Windows® и Safari 3,0 (или более поздней версии) для Macintosh. Проследите за тем, чтобы в используемом браузере всегда были разрешены JavaScript и Cookies. Любой другой веб-браузер должен быть совместим с HTTP 1.0 и HTTP 1.1.

В сети должен использоваться протокол TCP/IP, на сервере печати и компьютере необходимо запрограммировать действующий IP-адрес.

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

Используйте стандартный веб-браузер для изменения настроек принтера с помощью протокола HTTP (Hyper Text Transfer Protocol).



Примечание

При выполнении настроек с помощью системы управления через веб-интерфейс в целях интернет-безопасности рекомендуется использовать протокол HTTPS. Чтобы включить протокол HTTPS, см. раздел *Безопасное управление сетевым аппаратом с помощью SSL/TLS* на стр. 61.

- 1 Запустите веб-браузер.
- 2 Введите “http://IP-адрес аппарата/” в браузере (где “IP-адрес аппарата” – это IP-адрес аппарата).
 - Пример:
`http://192.168.1.2/`



Примечание

- При использовании системы доменных имен (DNS) или включении имени NetBIOS вместо IP-адреса можно ввести другое название, например Shared_Printer.

- Пример:

```
http://Shared_Printer/
```

При включении имени NetBIOS можно также использовать имя узла.

- Пример:

```
http://brnxxxxxxxxxxxxxx/
```

Имя NetBIOS отображается в списке конфигурации сети. (Для получения информации о печати списка конфигурации сети см. раздел *Печать Списка конфигурации сети* на стр. 36.)

- При использовании компьютера Macintosh можно легко воспользоваться системой управления через веб-интерфейс. Для этого щелкните значок аппарата на экране **Status Monitor**. Для получения дополнительной информации см. *Руководство по использованию программного обеспечения*.

3 Нажмите **Конфигурация сети**.

4 Введите имя пользователя и пароль. Имя пользователя по умолчанию – “**admin**”, пароль по умолчанию – “**access**”.

5 Нажмите **ОК**.

6 Теперь параметры сервера печати можно изменять.



Примечание

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

Информация о пароле

Система управления через веб-интерфейс предлагает два уровня доступа с использованием паролей. Пользователи могут получить доступ к **Общие настройки**, **Параметры факса**, **Параметры копирования**, **Параметры печати** и **Прямой интерф. с USB**. По умолчанию для пользователей используется имя “**user**” (с учетом регистра) и пароль “**access**”.

Администраторы имеют доступ ко всем параметрам. Для входа в качестве администратора используется имя “**admin**” (с учетом регистра) и пароль по умолчанию “**access**”.

Защитная блокировка функций 2.0

Защитная блокировка функций 2.0 от компании Brother поможет сохранить денежные средства и увеличить уровень безопасности путем ограничения функций, доступных на используемом 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 только авторизованные пользователи смогут воспользоваться ими.

С помощью системы управления через веб-интерфейс или утилиты BRAdmin Professional 3 можно настроить и изменить следующие параметры защитной блокировки функций 2.0.

- Печать с ПК ¹
- Прямая печать через USB ²
- Копирование
- Цветная печать
- Макс. число страниц
- Отправка факса ²
- Прием факса ²
- Сканирование
- Счетчик страниц

¹ Если выполняется регистрация имен пользователей компьютера, можно ограничить печать с компьютера, не используя вводимый пользователем пароль. Для получения дополнительной информации см. раздел *Ограничение печати с компьютера с помощью имени пользователя компьютера* на стр. 50.

² Только для моделей, поддерживающих данную функцию.

Настройка параметров защитной блокировки функций 2.0 с помощью системы управления через веб-интерфейс (веб-браузер)

Основная настройка

- 1 Нажмите **Настройки администратора** на веб-странице аппарата, после чего нажмите **Защитная блокировка функций**.
- 2 Выберите **Вкл.** в **Блокировка функций**.



Примечание

Чтобы настроить защитную блокировку функций через встроенный веб-сервер, необходимо ввести пароль администратора (четырёхзначное число). Если требуется изменить параметры, настроенные ранее с помощью панели управления на аппарате, сначала нужно ввести пароль в поле **Пароль администратора**.

- 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 Для функций, которые нужно ограничить, снимите флажок **Печать** или **Другие**. Если нужно настроить максимальное количество страниц, установите флажок **Вкл.** в столбце **Макс. число страниц**, после чего введите значение в поле **Макс..** После этого нажмите **Отправить**.
- 5 Если нужно ограничить печать с компьютера с помощью имени пользователя компьютера, нажмите **Ограничение печати с ПК по имени пользователя** и выполните настройку параметров. (См. раздел *Ограничение печати с компьютера с помощью имени пользователя компьютера* на стр. 50.)

Сканирование при использовании защитной блокировки функций 2.0

Защитная блокировка функций 2.0 позволяет администратору ограничивать число пользователей, которым разрешено выполнять сканирование. Если функция сканирования отключена для режима общего доступа, сканирование смогут выполнять только те пользователи, для которых установлены флажки в поле Сканирование. Чтобы запустить сканирование с панели управления аппарата, пользователю потребуется ввести PIN-код для входа в режим сканирования. Чтобы запустить сканирование со своего компьютера пользователю с ограниченным доступом также потребуется ввести PIN-код на панели управления аппарата, прежде чем он сможет выполнить сканирование с компьютера. Если не ввести PIN-код на панели управления аппарата, при попытке выполнить сканирование на компьютере пользователя появится сообщение об ошибке.

Ограничение печати с компьютера с помощью имени пользователя компьютера

После настройки этого параметра аппарат сможет выполнять аутентификацию по имени пользователя компьютера для разрешения задания на печать с зарегистрированного компьютера.

- 1 Нажмите **Ограничение печати с ПК по имени пользователя**. Откроется экран **Ограничение печати с ПК по имени пользователя**.
- 2 Выберите **Вкл.** в **Ограничение печати с ПК**.
- 3 Выберите для каждого имени номер идентификатора, заданный в **Идентификатор/Имя** в шаге 3 в *Основная настройка*, в раскрывающемся списке **Идентификатор**, после чего введите имя пользователя компьютера в поле **Имя пользователя**.
- 4 Нажмите **Отправить**.



Примечание

- Если требуется ограничить печать с компьютера для группы, установите одинаковый номер идентификатора для каждого имени компьютера, который должен находиться в группе.
- Если используется имя компьютера, убедитесь в том, что в драйвере принтера установлен флажок **Использовать имя пользователя компьютера**. Для получения дополнительной информации о драйвере принтера см. раздел *Руководство по использованию программного обеспечения*.
- Защитная блокировка функций не поддерживает драйвер BR-Script для печати.

Настройка режима общего доступа

Можно задать режим общего доступа, чтобы указать функции, доступные для общего использования. В режиме общего доступа пользователям не требуется вводить пароль для использования функций, которые сделаны доступными для этого режима.

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

Другие функции

Для защитной блокировки функций 2.0 можно настроить следующие элементы.

■ 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

После сброса счетчика аппарат сохраняет подсчитанное количество страниц.

■ Настройки авт. сброса счетчиков

Во время работы аппарата можно установить автоматический сброс счетчиков страниц, настроив временной интервал на основании ежедневных, еженедельных или ежемесячных настроек.

Синхронизация с сервером SNTP

SNTP является протоколом для синхронизации времени, используемого аппаратом для аутентификации, с сервером времени SNTP (не того времени, которое отображается на ЖКД аппарата). Можно установить регулярную синхронизацию аппарата со всемирным координированным временем (UTC), предоставляемым с сервера времени SNTP.



Примечание

Данная функция недоступна в некоторых странах.

- 1 Нажмите **Конфигурация сети**, а затем **Настроить протокол**.
- 2 Для включения параметра установите флажок **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).
 - **Порт первичного сервера SNTP, Порт вторичного сервера SNTP**

Введите номер порта (1 – 65535).

■ Интервал синхронизации

Введите интервал времени в часах, по прошествии которого будет производиться синхронизация с сервером (1 – 168 часов).



Примечание

- Для синхронизации времени, используемого аппаратом, с сервером времени SNTP, необходимо настроить параметр **Дата и время**. Нажмите **Настройка даты и времени**, а затем настройте параметр **Дата и время** на экране **Общие настройки**. Настроить дату и время можно также с помощью панели управления аппарата.

Дата и время

Дата	<input type="text" value="5"/> / <input type="text" value="18"/> / <input type="text" value="2011"/>
Время	<input type="text" value="5"/> : <input type="text" value="05"/>
Часовой пояс	<input type="text" value="UTC-xxxx"/> ▾
Летнее время: авто	<input checked="" type="radio"/> Выкл. <input type="radio"/> Вкл.
<input type="checkbox"/> Синхронизация с SNTP-сервером	

*Для синхронизации параметра "Дата и время" с вашим SNTP-сервером необходимо настроить параметры SNTP-сервера.

[Настройка SNTP](#)

- Установите флажок **Синхронизация с SNTP-сервером**. Необходимо также убедиться, что установлены правильные настройки часового пояса. Выберите разницу во времени между вашей местностью и временем UTC в раскрывающемся списке **Часовой пояс**. Например, часовой пояс для Восточного времени в США и Канаде обозначается UTC-05:00.

■ 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 CIFS ¹. Можно сохранить идентификатор, тип задания печати, название задания печати, дату, время, число напечатанных страниц и цветных страниц ² 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.

² Только для моделей, поддерживающих данную функцию.

В журнал печати сохраняются следующие функции печати.

- Задания печати с компьютера
- Прямая печать через USB (только для моделей, поддерживающих данную функцию)
- Копирование
- Принятый факс (только для моделей, поддерживающих данную функцию)



Примечание

- Функция “Сохранение журнала в сети” поддерживает аутентификацию **Kerberos** и **NTLMv2**.
Для выполнения аутентификации необходимо настроить протокол SNTP (сетевой сервер времени) или установить дату, время и часовой пояс .
- При сохранении файла на сервер для него можно установить тип **TXT** или **CSV**.

Настройка параметров сохранения журнала в сети с помощью системы управления через веб-интерфейс (веб-браузер)

- 1 Нажмите **Настройки администратора** на веб-странице аппарата, после чего нажмите **Сохранение журнала печати в сеть**.
- 2 Выберите **Вкл.** в **Журнал печати**.
- 3 С помощью веб-браузера можно настроить следующие параметры.
 - **Адрес хоста**
Адрес хоста – это имя хоста сервера CIFS. Введите адрес хоста (например, 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 по умолчанию, является NTLMv2.

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

Параметры Дата и время и SNTP можно настроить с помощью системы управления через веб-интерфейс.

Настроить Дата и время можно также с помощью панели управления аппарата.

- **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 для использования только аутентификации Kerberos.
- **NTLMv2:** выберите значение NTLMv2, чтобы использовать только аутентификацию NTLMv2.

■ 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, example.com) (не более 64 символов) или IP-адрес (например, 192.168.56.189).

- 4 С помощью параметра **Состояние подключения** можно проверить состояние последнего журнала. Для получения дополнительной информации см. раздел *Сообщения об ошибках* на стр. 56.
- 5 Нажмите **Отправить** для применения параметров.

Настройка обнаружения ошибки

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.



Примечание

Даже при выборе значения **Отменить печать** аппарат будет печатать принятые факсы.

■ 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 и цветных 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 (Network), "Doc01.doc","user01", 25/01/2009, 14:21:32, 10,10
2,Print (Network), "Doc02.doc","user01", 25/01/2009, 14:45:30, ?, ?
3,Print(USB), "Report01.els", "Mike", 25/01/2009, 15:20:30, 13, 10
4,<ERROR>, ?, ?, ?, ?, ?, ?
5,Print (Network), "Doc03.doc","user01", 25/01/2009, 16:12:50, 40, 10
```

(1)

(2)

- 2 Нажмите **Отправить** для применения параметров.

Сообщения об ошибках

Состояние ошибки можно проверить на ЖКД аппарата, а **Состояние подключения** с помощью системы управления через веб-интерфейс.

■ Тайм-аут сервера

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

Если параметр **Настройка аутентификации** установлен неправильно, появится сообщение. Убедитесь, что выполнены следующие условия.

- Имя пользователя ¹ и пароль установлены правильно в параметрах аутентификации.

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

- Проверьте, что время сервера файла журнала совпадает со временем сервера SNTP или значениями параметров **Дата и время**.
- Проверьте, что параметры сервера времени SNTP настроены правильно и время сервера совпадает со временем, используемым для аутентификации с помощью протоколов Kerberos или NTLMv2. Если сервер SNTP отсутствует, убедитесь, что параметры **Дата и время** и **Часовой пояс** установлены правильно с помощью системы управления через веб-интерфейс или панели управления, так что аппарат синхронизирует время сервера аутентификации.

■ Ошибка доступа к файлу

Данное сообщение появляется, если не удается получить доступ к целевой папке. Убедитесь, что выполнены следующие условия.

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

■ Неверная дата и время

Данное сообщение появляется, если аппарат не получает время с сервера времени SNTP. Убедитесь, что выполнены следующие условия.

- Проверьте, что параметры доступа к времени SNTP установлены правильно с помощью системы управления через веб-интерфейс.
- Если SNTP-сервер не используется, убедитесь, что дата и время, установленные с помощью панели управления совпадает со временем, используемым сервером аутентификации.



Примечание

При выборе параметра **Отменить печать** в системе управления через веб-интерфейс сообщение `Ошиб. дост. к журн` будет отображаться на ЖКД в течение 60 секунд.

Использование функции “Сохранение журнала в сети” с защитной блокировкой функций 2.0

Если включена защитная блокировка функций 2.0, имена зарегистрированных пользователей для функций копирования, приема факсов и прямой печати через USB (при наличии) будут записаны с помощью функции “Сохранение журнала в сети”.

Пример пользователей, записанных в журнал печати с защитной блокировкой функций 2.0:

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

Изменение параметров функции “Сканировать на FTP” с помощью веб-браузера

С помощью функции “Сканировать на FTP” можно отсканировать документ непосредственно на сервер FTP в локальной сети или сети Интернет.

Для получения дополнительной информации о функции “Сканировать на FTP” см. раздел Сетевое сканирование в *Руководстве по использованию программного обеспечения*.

1 Нажмите **Настройки администратора** на веб-странице MFC-XXXX (или DCP-XXXX), после чего нажмите **Настройки скан. на FTP/сервер**.

2 Можно выбрать, какие номера профилей (1 – 10) использовать для настроек функции “Сканировать на FTP”.

Помимо семи стандартных имен файлов в **Создайте опред.польз.имя файла** можно сохранить два определяемые пользователем имени файлов, которые можно использовать для создания профиля сервера FTP. В каждое из двух полей можно ввести не более 15 символов. После настройки нажмите **Отправить**.

3 Нажмите **Профиль сканир. на FTP/сервер** на стр. **Настройки администратора**. Теперь с помощью веб-браузера можно настроить и изменить следующие параметры функции “Сканировать на FTP”.

- **Имя профиля** (не более 15 символов)
- **Адрес хоста** (адрес сервера FTP)
- **Имя пользователя**
- **Пароль**
- **Папка сохранения**
- **Имя файла**
- **Разрешение**
- **Тип файла**
- **Размер файла**
- **Пассивный режим**
- **Номер порта**

Для **Пассивный режим** можно задать значение **Выкл.** или **Вкл.** в зависимости от параметров сервера FTP и сетевого брандмауэра. По умолчанию для этого параметра установлено значение **Вкл.**, кроме того, можно изменить номер порта, используемый для доступа к серверу FTP. По умолчанию установлен порт 21. В большинстве случаев для этих двух параметров можно оставить значения по умолчанию.



Примечание

Функция “Сканировать на FTP” доступна, если профили сервера FTP настроены с помощью системы управления через веб-интерфейс.

Изменение параметров функции “Сканировать в сеть” с помощью веб-браузера

С помощью функции “Сканировать в сеть” можно отсканировать документы непосредственно в общую папку на сервере CIFS в локальной сети или сети Интернет. (Для получения дополнительной информации о протоколе CIFS см. брошюру *Сетевая терминология*). Чтобы включить протокол CIFS, установите флажок для **CIFS** в **Настроить протокол** со страницы **Конфигурация сети**.

Для получения дополнительной информации о функции “Сканировать в сеть” см. раздел Сетевое сканирование в *Руководстве по использованию программного обеспечения*.



Примечание

Функция “Сканировать в сеть” поддерживает аутентификацию Kerberos и NTLMv2.

Для выполнения аутентификации необходимо настроить протокол SNTP (сетевой сервер времени) или установить дату, время и часовой пояс.

- 1 Нажмите **Настройки администратора** на веб-странице MFC-XXXX (или DCP-XXXX), после чего нажмите **Настройки скан. на FTP/сервер**.
- 2 Можно выбрать, какие номера профилей (1 – 10) использовать для настроек функции “Сканировать в сеть”.
Помимо семи стандартных имен файлов в **Создайте опред.польз.имя файла** можно сохранить два определяемые пользователем имени файлов, которые можно использовать для создания профиля функции “Сканировать в сеть”. В каждое из двух полей можно ввести не более 15 символов.
После настройки нажмите **Отправить**.
- 3 Нажмите **Профиль сканир. на FTP/сервер** на стр. **Настройки администратора**.
Теперь с помощью веб-браузера можно настроить и изменить следующие параметры функции “Сканировать в сеть”.
 - **Имя профиля** (не более 15 символов)
 - **Адрес хоста**
 - **Папка сохранения**
 - **Имя файла**
 - **Разрешение**
 - **Тип файла**
 - **Размер файла**
 - **Использ.PIN для аутентификации**
 - **PIN-код**
 - **Метод аутентификации**
 - **Имя пользователя**
 - **Пароль**
 - **Адрес сервера Kerberos**



Примечание

Функция “Сканировать в сеть” доступна, если профили сетевых серверов настроены с помощью системы управления через веб-интерфейс.

Обзор

На сегодняшний день имеется множество угроз безопасности для используемой сети и данным, которые по ней передаются. Данный аппарат Brother оснащен некоторыми из последних протоколов безопасности и шифрования данных, разработанных на сегодняшний день. Эти функции поддержки сети могут быть интегрированы в общий план безопасности сети, что поможет обеспечить безопасность данных и предотвратить неавторизованный доступ к аппарату. В этой главе описывается настройка таких функций.

Можно настроить следующие функции безопасности.

- Безопасное управление сетевым аппаратом с помощью SSL/TLS (см. *Безопасное управление сетевым аппаратом с помощью SSL/TLS* на стр. 61).
- Безопасное управление сетевым аппаратом с помощью протокола SNMPv3 (см. *Безопасное управление с помощью системы управления через веб-интерфейс (веб-браузер)* на стр. 61 или *Безопасное управление с использованием утилиты BRAdmin Professional 3 (Windows®)* на стр. 68).
- Безопасная печать документов по протоколу SSL/TLS (см. *Безопасная печать документов по протоколу SSL/TLS* на стр. 63).
- Безопасная отправка и получение электронной почты (см. *Безопасная отправка и получение электронной почты* на стр. 64).
- Использование аутентификации IEEE 802.1x (см. *Использование аутентификации IEEE 802.1x* на стр. 66).
- Безопасное управление с использованием утилиты BRAdmin Professional 3 (Windows®) (см. *Безопасное управление с использованием утилиты BRAdmin Professional 3 (Windows®)* на стр. 68).
- Сертификат для безопасного управления (см. *Использование сертификатов для защиты устройств* на стр. 69).
- Управление несколькими сертификатами (см. *Управление несколькими сертификатами* на стр. 78).



Примечание

Рекомендуется отключить протоколы Telnet, FTP и TFTP. Доступ к аппарату с использованием этих протоколов не является безопасным. (Для получения информации о настройке параметров протокола см. раздел *Настройка параметров аппарата с помощью системы управления через веб-интерфейс (веб-браузер)* на стр. 46.) Если отключить FTP, функция “Сканировать на FTP” будет также отключена.

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 (веб-браузер)

Для безопасного управления рекомендуется использовать протокол HTTPS и SNMPv3. Чтобы использовать протокол HTTPS, необходимо настроить следующие параметры аппарата.

- На аппарате должны быть установлены самоподписанный сертификат или сертификат, выданный ЦС, а также секретный ключ. (Для получения информации об установке сертификата и ключа безопасности см. в разделе *Использование сертификатов для защиты устройств* на стр. 69.)
- Протокол HTTPS должен быть включен. Для включения протокола HTTPS выберите установленный сертификат в раскрывающемся списке на странице **Настройки сервера HTTP** в **Система управления через веб-интерфейс** на странице **Настроить протокол**, а затем включите параметр **Используется связь SSL (порт 443)**. (Для получения информации о доступе к странице **Настроить протокол** см. раздел *Настройка параметров аппарата с помощью системы управления через веб-интерфейс (веб-браузер)* на стр. 46.)

- 1 Запустите веб-браузер.
- 2 Введите в браузере "https://стандартное имя/". (Где "стандартное имя" – это стандартное имя, назначенное сертификату, такое как IP-адрес, имя узла или имя домена. О назначении стандартного имени для сертификата см. раздел *Использование сертификатов для защиты устройств* на стр. 69.)
 - Пример:

https://192.168.1.2/ (если стандартным именем является IP-адрес принтера)
- 3 Теперь имеется доступ к аппарату с помощью протокола HTTPS.

Рекомендуется использовать безопасное управление (SNMPv3) вместе с протоколом HTTPS.

Если используется протокол SNMPv3, следуйте описанным ниже действиям.

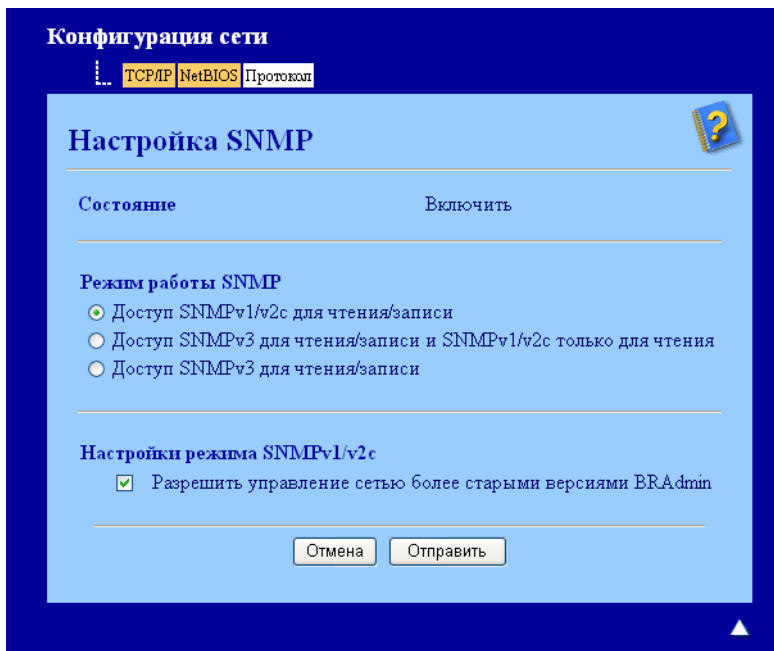


Примечание

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

- 4 Нажмите **Конфигурация сети**.
- 5 Введите имя пользователя и пароль. По умолчанию используется имя пользователя "**admin**", и пароль "**access**".
- 6 Нажмите **ОК**.
- 7 Нажмите **Настроить протокол**.

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



Существует три режима соединения **SNMP**.

■ **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 утилит BRAdmin Professional 3, Web BRAdmin или системы управления через веб-интерфейс.
- Рекомендуется использовать безопасную связь SSL (HTTPS).
- Будет ограничено использование всех приложений, в которых используется протокол SNMPv1/v2c за исключением утилит BRAdmin Professional 3 и Web BRAdmin. Чтобы разрешить использование приложений SNMPv1/v2c, используйте режим **Доступ SNMPv3 для чтения/записи и SNMPv1/v2c только для чтения** или **Доступ SNMPv1/v2c для чтения/записи**.

■ 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 2c 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 2c. Если требуется использовать все приложения, используйте режим **Доступ SNMPv1/v2c для чтения/записи**.

■ Доступ SNMPv1/v2c для чтения/записи

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



Примечание

Для получения дополнительной информации обратитесь к справке системы управления через веб-интерфейс.

Безопасная печать документов по протоколу SSL/TLS

Для безопасной печати документов по Интернету можно использовать протокол IPPS.



Примечание

- Соединение с использованием протокола IPPS не может предотвратить несанкционированный доступ к серверу печати.
- Протокол IPPS поддерживается в ОС Windows® 2000/XP, Windows Vista®, Windows® 7 и Windows Server® 2003/2008.

Чтобы использовать протокол IPPS, необходимо настроить следующие параметры аппарата.

- На аппарате должны быть установлены самозаверяющий сертификат или сертификат, выданный ЦС, а также секретный ключ. Для получения информации об установке сертификата и секретного ключа см. раздел *Использование сертификатов для защиты устройств* на стр. 69.
- Протокол IPPS должен быть включен. Для включения протокола IPPS выберите установленный сертификат в раскрывающемся списке на странице **Настройки сервера HTTP в IPP** на странице **Настроить протокол**, а затем включите параметр **Используется связь SSL (порт 443)**. Для получения информации о доступе к стр. **Настроить протокол** см. раздел *Настройка параметров аппарата с помощью системы управления через веб-интерфейс (веб-браузер)* на стр. 46.

Безопасная отправка и получение электронной почты

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

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

- 1 Запустите веб-браузер.
- 2 Введите “http://IP-адрес принтера/” в браузере (где “IP-адрес принтера” – это IP-адрес принтера).
 - Пример:
http://192.168.1.2/
- 3 Нажмите **Конфигурация сети**.
- 4 Введите имя пользователя и пароль. По умолчанию используется имя пользователя “admin”, и пароль “access”.
- 5 Нажмите **ОК**.
- 6 Нажмите **Настроить протокол**.
- 7 Нажмите **Дополнительные параметры** в **POP3/SMTP** и убедитесь, что для параметра **POP3/SMTP** установлено значение **Включить**.
- 8 На этой странице можно настроить параметры **POP3/SMTP**.



Примечание

- Для получения дополнительной информации обратитесь к справке системы управления через веб-интерфейс.
- Можно подтвердить правильность параметров электронной почты после их настройки, отправив тестовое сообщение электронной почты.

- 9 После настройки нажмите **Отправить**. Отобразится диалоговое окно настройки отправки и получения тестового сообщения электронной почты.
- 10 При необходимости выполнения теста с текущими параметрами следуйте инструкциям, отображаемым на экране.

Отправка электронной почты с аутентификацией пользователя

Данный аппарат поддерживает методы авторизации “POP перед использованием SMTP” и SMTP-AUTH для отправки электронной почты через сервер электронной почты, поддерживающий аутентификацию пользователей. Использование этих способов позволяет предотвратить доступ к серверу электронной почты неавторизованных пользователей. Для настройки этих параметров можно воспользоваться системой управления через веб-интерфейс, утилитой BRAdmin Professional 3 и Web BRAdmin. Для уведомлений и отчетов по электронной почте можно использовать методы авторизации “POP перед использованием SMTP” и SMTP-AUTH.

Параметры сервера электронной почты

Необходимо, чтобы метод аутентификации SMTP совпадал с методом аутентификации, используемым сервером электронной почты. По вопросам настройки сервера электронной почты обратитесь к сетевому администратору или поставщику услуг Интернета.

Необходимо также проверить **SMTP-AUTH** раздела **Способ проверки подлинности на сервере SMTP**, чтобы включить аутентификацию сервера SMTP.

Параметры SMTP

- Изменить номер порта SMTP можно с помощью системы управления через веб-интерфейс. Это может быть полезно, если ISP (Internet Service Provider – поставщик услуг Интернета) использует службу “Блокирование исходящего порта 25 (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 имеется возможность использовать как “POP перед использованием SMTP”, так и SMTP-AUTH, рекомендуется выбрать SMTP-AUTH.
- При выборе POP перед SMTP в качестве способа идентификации сервера SMTP необходимо настроить параметры POP3. При необходимости можно также использовать метод APOP.

Безопасная отправка и получение электронной почты с помощью SSL/TLS

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

7

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 **Проверять сертификат сервера** для проверки подлинности сертификата сервера.
 - Перед проверкой подлинности сертификата сервера необходимо импортировать сертификат ЦС, выданный тем ЦС, который подписал сертификат сервера. Для получения сертификата ЦС обратитесь к системному администратору. Для получения информации об импорте сертификата см. раздел *Импорт и экспорт сертификата ЦС* на стр. 79.
 - 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 сервера электронной почты. Для получения подробной информации о параметрах сервера электронной почты обратитесь к сетевому администратору или поставщику услуг Интернета. 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.

Для использования аутентификации IEEE 802.1x необходимо установить сертификат, выданный ЦС. При необходимости импорта сертификата ЦС обратитесь к сетевому администратору или к поставщику услуг Интернета. (Для получения информации об установке сертификата см. раздел *Использование сертификатов для защиты устройств* на стр. 69.)

Настройка аутентификации IEEE 802.1x с помощью системы управления через веб-интерфейс (веб-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 беспроводной настройки на панели управления (для получения дополнительной информации см. раздел *Настройка аппарата для работы в корпоративной беспроводной сети* на стр. 20.)
- Мастер беспроводной настройки на компакт диске (для получения дополнительной информации см. раздел *Настройка параметров беспроводной сети с помощью программы установки Brother (для MFC-9560CDW)* на стр. 26.)
- BRAdmin Professional 3



Примечание

- Если выполняется настройка аппарата, использующего аутентификацию EAP-TLS, необходимо установить сертификат клиента перед началом настройки. Если установлено более одного сертификата, рекомендуется записать сертификат, который будет использоваться. Для получения информации об установке сертификата см. раздел *Использование сертификатов для защиты устройств* на стр. 69.
- Перед проверкой подлинности сертификата сервера необходимо импортировать сертификат ЦС, выданный тем ЦС, который подписал сертификат сервера. Для получения сертификата ЦС обратитесь к системному администратору. Для получения информации об импорте сертификата см. раздел *Импорт и экспорт сертификата ЦС* на стр. 79.
- Для получения дополнительной информации о каждом сертификате см. раздел *Использование сертификатов для защиты устройств* на стр. 69.

- 1 Запустите веб-браузер.
- 2 Введите “http://IP-адрес аппарата/” в браузере (где “IP-адрес аппарата” – это IP-адрес аппарата).
 - Пример:
http://192.168.1.2/



Примечание

- При использовании системы доменных имен (DNS) или включении имени NetBIOS вместо IP-адреса можно ввести другое название, например Shared_Printer.

- Пример:

`http://Shared_Printer/`

При включении имени NetBIOS можно также использовать имя узла.

- Пример:

`http://brnxxxxxxxxxxxxxx/`

Имя NetBIOS отображается в списке конфигурации сети. (Для получения информации о печати списка конфигурации сети см. раздел *Печать Списка конфигурации сети* на стр. 36.)

- При использовании компьютера Macintosh можно легко воспользоваться системой управления через веб-интерфейс. Для этого щелкните значок аппарата на экране **Status Monitor**. Для получения дополнительной информации см. *Руководство по использованию программного обеспечения*.

3 Нажмите **Конфигурация сети**.

4 Введите имя пользователя и пароль. Имя пользователя по умолчанию – “**admin**”, пароль по умолчанию – “**access**”.

5 Нажмите **ОК**.

6 (Проводная сеть) Нажмите **Настройка проводной сети 802.1x**.
(Беспроводная сеть) Нажмите **Настройка беспроводной связи**, а затем выберите вкладку **Предприятие**.

7 Теперь можно настраивать параметры аутентификации IEEE 802.1x.

- Если необходимо включить аутентификацию IEEE 802.1x для проводной сети, установите флажок **Включить** для **Состояние проводной сети 802.1x** на странице **Настройка проводной сети 802.1x**.

- Для получения дополнительной информации об аутентификации IEEE 802.1x и о методах внутренней аутентификации см. *Сетевая терминология*.

- При использовании аутентификации EAP-TLS необходимо в раскрывающемся 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 раскрывающемся 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 раскрывающемся списке **Проверка сертификата сервера** можно выбрать следующие методы проверки подлинности.

- **Без проверки**

Сертификату сервера всегда можно доверять. Проверка подлинности не производится.

- **Серт. ЦС**

Метод проверки надежности сертификата сервера с помощью ЦС 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 **Идентификатор сервера**. Перед использованием данного метода обратитесь к системному администратору для получения информации о стандартном имени сертификата сервера, а затем настройте параметр **Идентификатор сервера**.

8 После настройки нажмите **Отправить**.

(Проводная сеть)

После настройки подключите аппарат к сети, поддерживающей стандарт IEEE 802.1x. Через несколько минут напечатайте список конфигурации сети для проверки параметра **<Wired IEEE 802.1x> Status**. (для получения информации о печати списка конфигурации сети с помощью имеющегося сервера печати см. раздел *Печать Списка конфигурации сети* на стр. 36.)

■ 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)

Сразу после настройки будет напечатан Отчет WLAN. Проверьте настройку беспроводной сети по отчету. См. раздел *Печать отчета о состоянии беспроводной сети (для MFC-9560CDW)* на стр. 37.

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

Для безопасного использования утилиты BRAdmin Professional 3 необходимо соблюдать условия, приведенные ниже.

- Рекомендуется использовать самую последнюю версию утилиты BRAdmin Professional 3 или Web BRAdmin, которую можно загрузить по адресу <http://solutions.brother.com/>. При использовании устаревшей версии утилиты BRAdmin ¹ для управления аппаратами Brother аутентификация пользователя не будет достаточно безопасной.
- При необходимости ограничения доступа к аппарату с помощью более ранних версий утилиты BRAdmin ¹ необходимо отключить доступ с помощью более ранних версий утилиты BRAdmin ¹ в параметре **Дополнительные параметры** раздела **SNMP** на странице **Настроить протокол** с помощью системы управления через веб-интерфейс. (См. раздел *Безопасное управление с помощью системы управления через веб-интерфейс (веб-браузер)* на стр. 61.)
- При одновременном использовании утилиты BRAdmin Professional 3 и системы управления через веб-интерфейс используйте систему управления через веб-интерфейс с протоколом HTTPS. (См. раздел *Безопасное управление с помощью системы управления через веб-интерфейс (веб-браузер)* на стр. 61.)

- При управлении смешанной группой серверов печати более ранних моделей² и серверами печати с помощью программы BRAdmin Professional рекомендуется использовать для каждой группы отдельный пароль. Таким образом поддерживается безопасность на новых серверах печати.

- ¹ BRAdmin Professional более ранних версий, чем версия 2.80, Web BRAdmin более ранних версий, чем версия 1.40, BRAdmin Light для Macintosh более ранних версий, чем версия 1.10
- 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

Использование сертификатов для защиты устройств

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.

- Соединение по протоколу SSL/TLS
- Аутентификация IEEE 802.1x
- Соединение по протоколу SSL для SMTP/POP3

Аппарат Brother поддерживает следующие сертификаты.

- 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 сертификатов. (См. раздел *Создание и установка сертификата* на стр. 71.)

- Сертификат от ЦС

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

- С использованием CSR (Запрос о подписи сертификата) от данного сервера печати. (См. раздел *Создание запроса на подпись сертификата (CSR)* на стр. 76.)
- С импортированием сертификата и секретного ключа. (См. раздел *Импорт и экспорт сертификата и секретного ключа* на стр. 77.)

- 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* на стр. 79.)



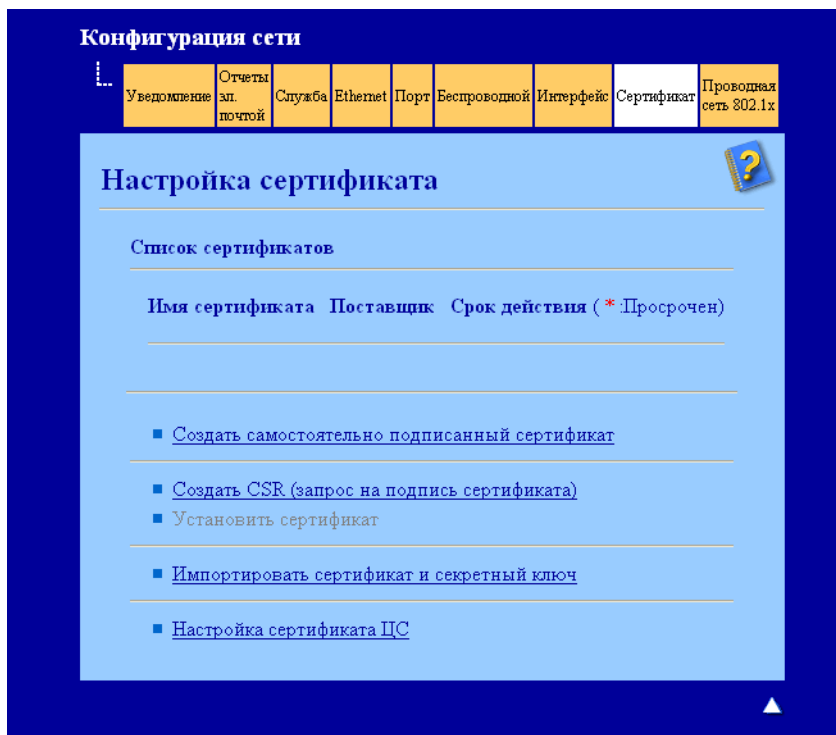
Примечание

- 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 самозаверяющего сертификата, сертификата, выданного ЦС, и секретного ключа* на стр. 78.)

Настройка сертификата с помощью системы 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 (веб-браузер), выполните следующие действия.

- 1 Запустите веб-браузер.
- 2 Введите “http://IP-адрес принтера/” в браузере (где “IP-адрес принтера” – это IP-адрес принтера).
 - Пример:
http://192.168.1.2/
- 3 Нажмите **Конфигурация сети**.
- 4 Введите имя пользователя и пароль. По умолчанию используется имя пользователя “**admin**”, и пароль “**access**”.
- 5 Нажмите **ОК**.
- 6 Нажмите **Настройка сертификата**.
- 7 С помощью экрана, приведенного ниже, можно настроить параметры сертификата.

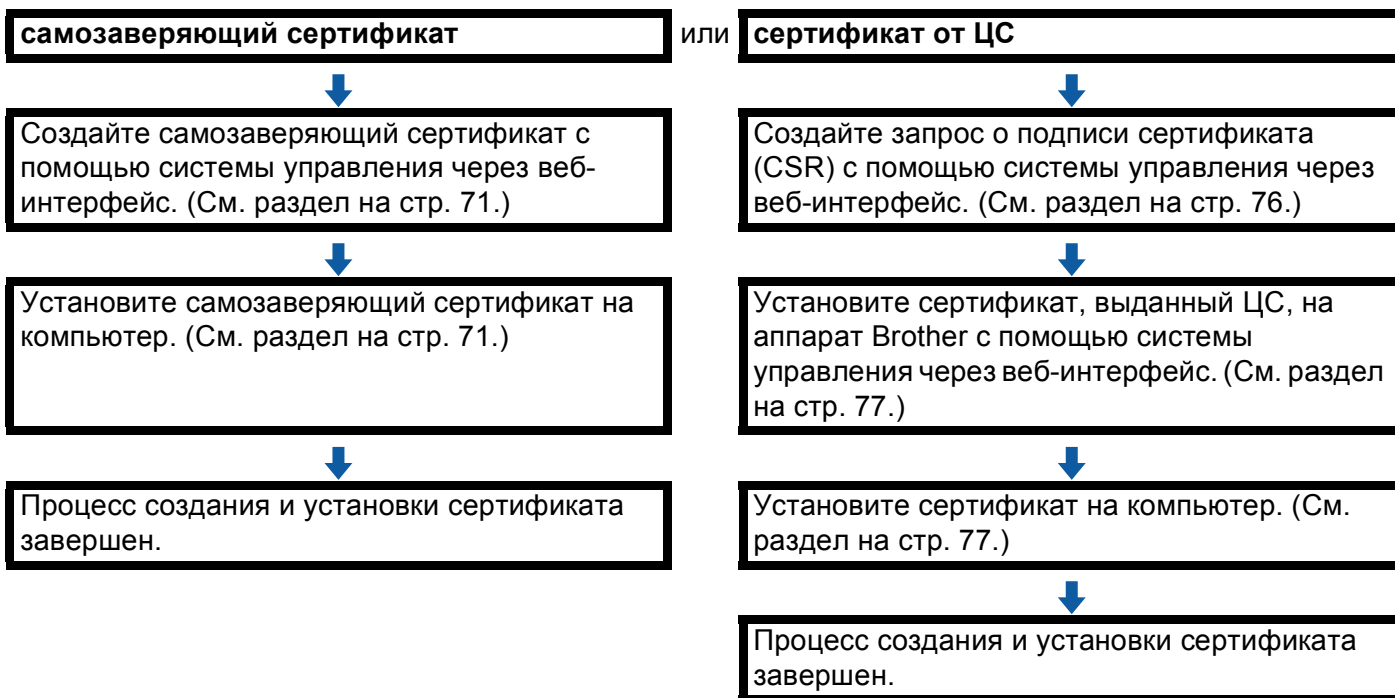


Примечание

- 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. **Настройка сертификата**.
- 2 Введите **Общее название** и **Срок действия**, а затем нажмите **Отправить**.

Примечание

- Длина **Общее название** не должна превышать 64 байта. 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 Создание и установка самозаверяющего сертификата в память аппарата завершена успешно. Чтобы использовать соединение по протоколу SSL/TLS, на компьютере необходимо установить самозаверяющий сертификат. Перейдите к следующему разделу.

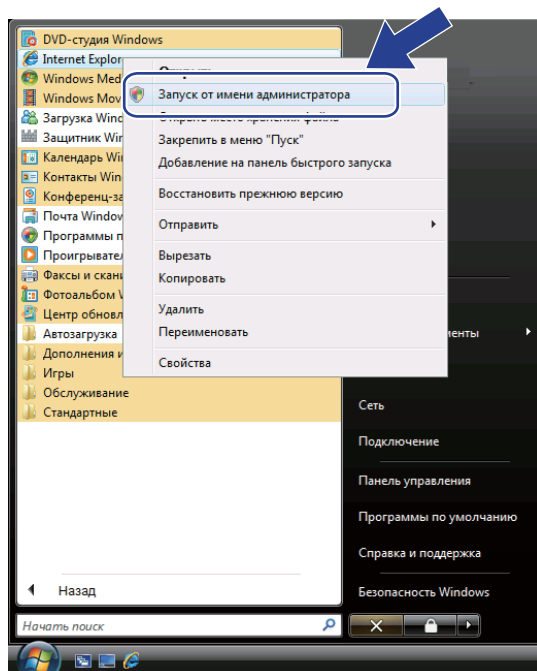
Установка самозаверяющего сертификата на компьютер

Примечание

При работе в программе Microsoft® Internet Explorer® необходимо выполнить следующие шаги. При использовании другого веб-браузера следует обратиться к справке этого браузера.

Для пользователей ОС Windows Vista®, Windows® 7 и Windows Server® 2008 с правами администратора

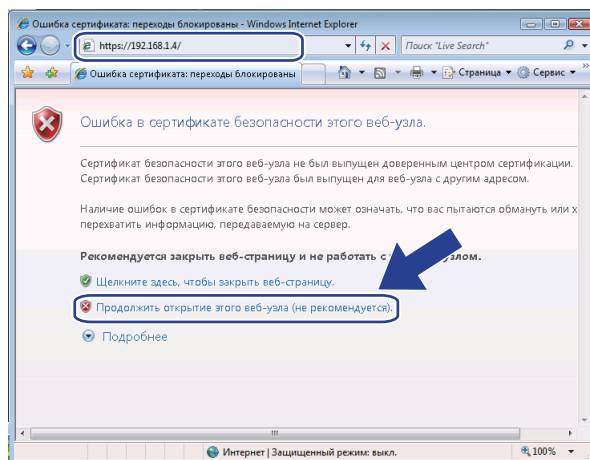
- 1 Нажмите кнопку  и выберите **Все программы**.
- 2 Нажмите правой кнопкой мыши **Internet Explorer**, а затем выберите **Запуск от имени администратора**.



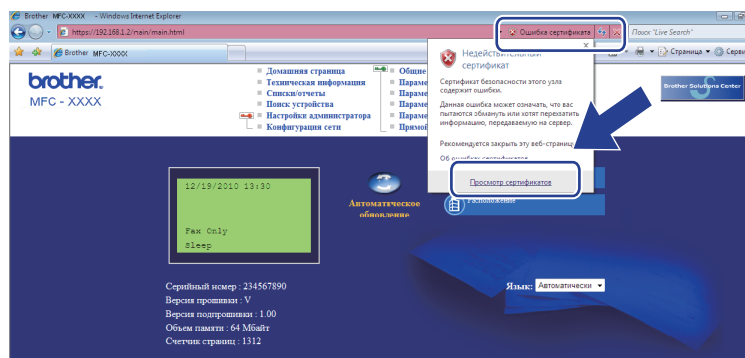
Примечание

Если отобразится экран **Контроль учетных записей пользователей**,
(Windows Vista®) нажмите **Продолжить (Разрешить)**.
(Windows® 7) нажмите **Да**.

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

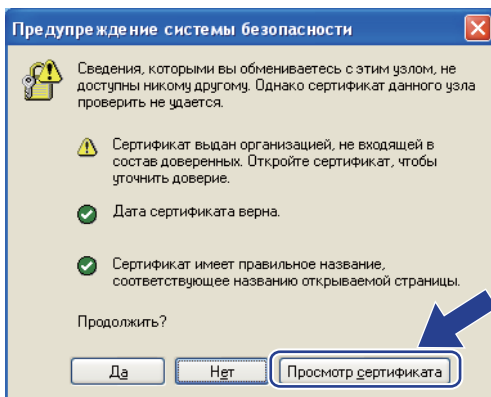


- 4 Нажмите **Ошибка сертификата**, а затем **Просмотр сертификатов**. Чтобы выполнить остальные инструкции, выполните шаги с 4 в *Для пользователей Windows® 2000/XP и Windows Server® 2003* на стр. 74.

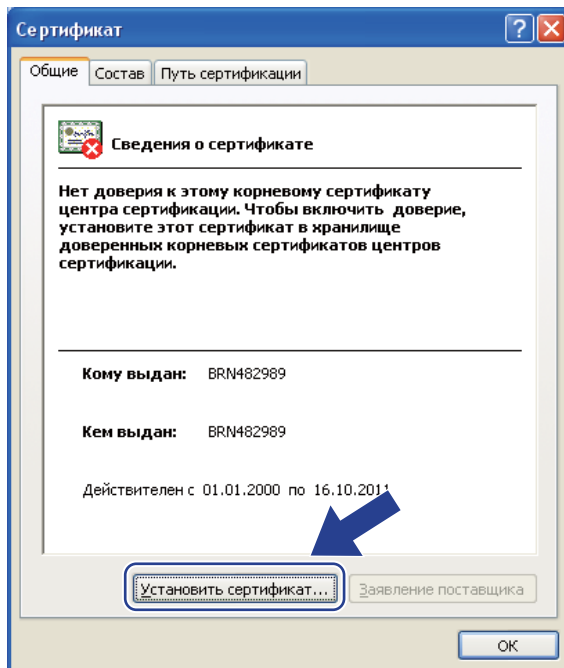


Для пользователей Windows® 2000/XP и Windows Server® 2003

- 1 Запустите веб-браузер.
- 2 Чтобы получить доступ к аппарату, введите в браузере “https://IP-адрес принтера/” (где “IP-адрес принтера” — это IP-адрес или имя узла, назначенное для сертификата).
- 3 В появившемся диалоговом окне нажмите **Просмотр сертификата**.

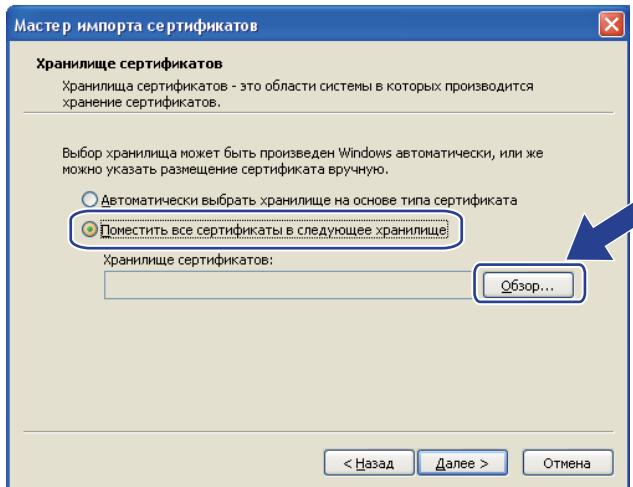


- 4 Нажмите **Установить сертификат...** на вкладке **Общие**.

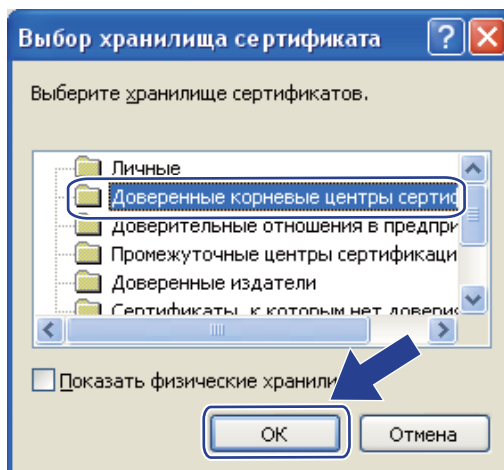


- 5 Когда отобразится **Мастер импорта сертификатов**, нажмите **Далее**.

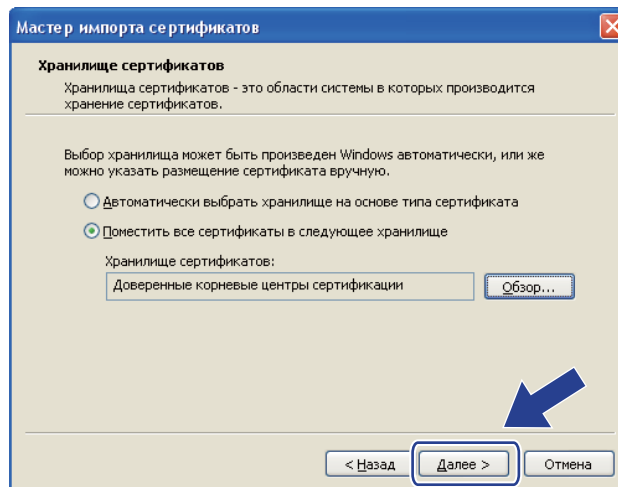
- 6 Выберите **Поместить все сертификаты в следующее хранилище**, а затем нажмите **Обзор...**



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

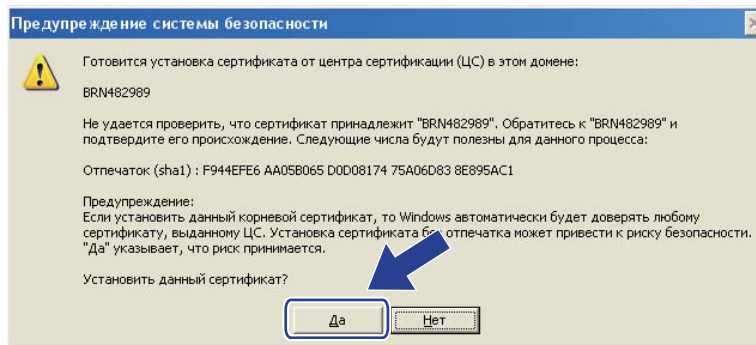


- 8 Нажмите **Далее**.



- 9 Нажмите **Готово**.

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



 **Примечание**

Отпечаток пальца (отпечаток большого пальца) печатается в списке конфигурации сети. (Для получения информации о печати списка конфигурации сети см. раздел *Печать Списка конфигурации сети* на стр. 36.)

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

Создание запроса на подпись сертификата (CSR)

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

 **Примечание**

- Перед созданием запроса на подпись сертификата рекомендуется установить на компьютере корневой сертификат, полученный от ЦС.
- Длина **Общее название** не должна превышать 64 байта. Введите идентификатор, такой как IP-адрес, имя узла или имя домена, чтобы использовать его при доступе к принтеру через связь SSL/TLS. По умолчанию отображается имя узла. Требуется **Общее название**.
- При вводе адреса URL, отличного от стандартного имени, которое было использовано для заполнения сертификата, будет отображаться всплывающее сообщение.
- Длина **Организация**, **Подразделение**, **Город/район** и **Страна/регион** не должна превышать 64 байта.
- 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 **Настройка дополнительного раздела**, а затем выберите **Авто** или **Вручную**.

- 3 При отображении содержания запроса на подпись сертификата нажмите **Сохранить**, чтобы сохранить файл запроса на своем компьютере.

- 4 Запрос на подпись сертификата создан.

Примечание

- Чтобы отправить запрос на подпись сертификата в центр сертификатов, выполните соответствующие указания своего ЦС.
- Если используется Enterprise root CA операционной системы Windows Server® 2003/2008, то при создании сертификата клиента для обеспечения безопасного управления рекомендуется использовать для шаблона сертификата **Веб-сервер**. При создании сертификата клиента для окружения 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. **Настройка сертификата**.
- 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 сетевому администратору.

Импорт и экспорт сертификата и секретного ключа

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

Импорт самоподписанного сертификата, сертификата, выданного ЦС, и секретного ключа

- 1 Нажмите **Импортировать сертификат и секретный ключ** на стр. **Настройка сертификата**.
- 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 сертификат, полученный из ЦС. Чтобы получить консультацию по его установке, обратитесь к сетевому администратору.

Экспорт самоподписанного сертификата, сертификата, выданного ЦС, и секретного ключа

- 1 Нажмите **Экспорт** рядом с **Список сертификатов** на странице **Настройка сертификата**.
- 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.

7

Управление несколькими сертификатами

Функция управления несколькими сертификатами позволяет управлять каждым сертификатом, установленным с помощью системы управления через веб-интерфейс. После установки сертификатов можно видеть, какие сертификаты установлены со страницы **Настройка сертификата**, а затем просмотреть содержимое каждого сертификата, удалить и или экспортировать сертификат. Для получения информации о доступе к стр. **Настройка сертификата** см. раздел *Настройка сертификата с помощью системы управления через веб-интерфейс* на стр. 70. Аппарат Brother позволяет хранить до четырех самоподписанных сертификатов или до четырех сертификатов, выданных ЦС. Сохраненные сертификаты можно задействовать для использования протокола HTTPS/IPPS, аутентификации IEEE 802.1x или PDF с цифровой подписью.

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 HTTPS/IPPS, IEEE 802.1x или PDF с цифровой подписью необходимо выбрать сертификат, который будет использоваться.

Импорт и экспорт сертификата ЦС

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

Импорт сертификата ЦС

- 1 Нажмите **Настройка сертификата ЦС** на стр. **Настройка сертификата**.
- 2 Нажмите **Импорт сертификата ЦС**. Нажмите **Отправить**.

Экспорт сертификата ЦС

- 1 Нажмите **Настройка сертификата ЦС** на стр. **Настройка сертификата**.
- 2 Выберите сертификат, который требуется экспортировать, и нажмите **Экспорт**. Нажмите **Отправить**.

Обзор

В этой главе рассказывается об устранении возможных проблем сети, с которыми можно столкнуться при эксплуатации аппарата Brother. Если после прочтения этой главы возникшая проблема не будет решена, посетите 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.

Определение проблемы

Перед чтением этой главы выполните следующие действия.

Сначала проверьте следующее:
Кабель питания подсоединен правильно и аппарат Brother включен.
Точка доступа (для беспроводных сетей), маршрутизатор или концентратор включены и мигает кнопка связи.
Вся защитная упаковка снята с аппарата.
Тонер-картриджи и узел фотобарабана установлены правильно.
Передняя и задняя крышки плотно закрыты.
Бумага правильно вставлена в лоток для бумаги.
(Для проводных сетей) Сетевой кабель надежно подсоединен к аппарату Brother и маршрутизатору или концентратору.

Перейдите на страницы решения проблем, указанные ниже

- Не удается завершить настройку параметров беспроводной сети. (См. раздел на стр. 81.)
- Аппарат Brother не обнаружен в сети при установке MFL-Pro Suite. (См. раздел на стр. 82.)
- Не удается выполнить операции печати или сканирования с помощью аппарата Brother по сети. (См. раздел на стр. 82.)
- Аппарат Brother не обнаружен в сети даже после успешной установки. (См. раздел на стр. 82.)
- Используется программное обеспечение системы безопасности. (См. раздел на стр. 86.)
- Необходимо проверить надлежащее функционирование используемых сетевых устройств. (См. раздел на стр. 86.)

Не удается завершить настройку параметров беспроводной сети.

Вопрос	Интерфейс	Решение
Параметры безопасности (SSID/сетевой ключ) настроены правильно?	беспроводная сеть	<ul style="list-style-type: none"> ■ Проверьте еще раз и выберите правильные параметры безопасности. <ul style="list-style-type: none"> • В качестве настроек по безопасности по умолчанию могут быть использованы название компании производителя или номер модели беспроводной точки доступа/маршрутизатора. • Для получения информации о том, как найти настройки безопасности см. инструкции, прилагаемые к беспроводной точке доступа/маршрутизатору. • Обратитесь к производителю беспроводной точки доступа/маршрутизатора или сетевому администратору или провайдеру Интернета. ■ Для получения информации о SSID и сетевом ключе см. разделы, посвященные SSID, сетевому ключу и каналам в <i>Сетевая терминология</i>.
Фильтрация MAC-адресов используется?	беспроводная сеть	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</i> на стр. 38.)
Беспроводная точка доступа/маршрутизатор работает в скрытом режиме? (передача SSID запрещена)	беспроводная сеть	<ul style="list-style-type: none"> ■ Вручную правильно введите имя SSID или сетевой ключ. ■ Проверьте имя SSID или сетевой ключ в инструкциях, прилагаемых к беспроводной точке доступа/маршрутизатору, и заново выполните настройку параметров беспроводной сети. (Для получения дополнительной информации см. раздел <i>Настройка аппарата, если отключена передача идентификатора SSID</i> на стр. 17.)
Указанные процедуры были выполнены, однако настройку параметров беспроводной сети не удается завершить. Есть ли еще какие-то способы решения данной проблемы?	беспроводная сеть	Используйте программу для исправления сетевого подключения. См. раздел <i>Не удается выполнить операции печати или сканирования с помощью аппарата Brother по сети. Аппарат Brother не обнаружен в сети даже после успешной установки.</i> на стр. 82.

Аппарат Brother не обнаружен в сети при установке MFL-Pro Suite.

Вопрос	Интерфейс	Решение
Программное обеспечение системы безопасности используется?	проводная/ беспроводная сеть	<ul style="list-style-type: none"> ■ В диалоговом окне программы установки выполните поиск аппарата Brother еще раз. ■ При установке MFL-Pro Suite при отображении предупредительного сообщения программное обеспечение системы безопасности следует разрешить доступ. ■ Для получения дополнительной информации о программном обеспечении системы безопасности см. раздел <i>Программное обеспечение системы безопасности используется</i> на стр. 86.
Аппарат Brother расположен слишком далеко от беспроводной точки доступа/маршрутизатора?	беспроводная сеть	Расположите аппарат Brother на расстоянии 3,3 фута (1 метр) от беспроводной точки доступа/маршрутизатора при настройке параметров беспроводной сети.
Между беспроводной точкой доступа/маршрутизатором и аппаратом есть какие-либо препятствия (стены или мебель, например)?	беспроводная сеть	Переместите аппарат Brother в место без препятствий или ближе к беспроводной точке доступа/маршрутизатору.
Рядом с аппаратом Brother или беспроводной точкой доступа/маршрутизатором находится компьютер, использующий беспроводную сеть, или устройство с поддержкой технологии Bluetooth, микроволновая печь или цифровой беспроводной телефон?	беспроводная сеть	Уберите эти устройства от аппарата Brother или беспроводной точки доступа/маршрутизатора.


Не удается выполнить операции печати или сканирования с помощью аппарата Brother по сети.

Аппарат Brother не обнаружен в сети даже после успешной установки.

Вопрос	Интерфейс	Решение
Программное обеспечение системы безопасности используется?	проводная/ беспроводная сеть	См. раздел <i>Программное обеспечение системы безопасности используется</i> на стр. 86.




Не удается выполнить операции печати или сканирования с помощью аппарата Brother по сети.

Аппарат Brother не обнаружен в сети даже после успешной установки. (продолжение)

Вопрос	Интерфейс	Решение
Для аппарата Brother назначен доступный IP-адрес?	проводная/ беспроводная сеть	<p>■ Проверьте IP-адрес и маску подсети</p> <p>Убедитесь, что IP-адреса и маски подсети компьютера и аппарата Brother верны и расположены в одной сети. Для получения дополнительной информации о проверке IP-адреса и маски подсети обратитесь к сетевому администратору или посетите веб-сайт Brother Solutions Center по адресу http://solutions.brother.com/.</p> <p>■ (Windows®)</p> <p>Проверьте IP-адрес и маску подсети с помощью программы для исправления сетевого подключения.</p> <p>Для решения проблем, связанных с настройкой параметров беспроводной сети аппарата Brother, используйте программу для исправления сетевого подключения. Программа назначит верный IP-адрес и маску подсети.</p> <p>Для получения информации об использовании программы для исправления сетевого подключения обратитесь к сетевому администратору и выполните следующие действия:</p> <p> Примечание</p> <ul style="list-style-type: none"> • (Windows® 2000 Professional/XP/XP Professional x64 Edition/Windows Vista®/Windows® 7) Необходимо войти в систему с полномочиями администратора. • Убедитесь, что аппарат Brother включен и подключен по сети к компьютеру.

Не удается выполнить операции печати или сканирования с помощью аппарата Brother по сети.

Аппарат Brother не обнаружен в сети даже после успешной установки. (продолжение)

Вопрос	Интерфейс	Решение
<p>Для аппарата Brother назначен доступный IP-адрес? (продолжение)</p>	<p>проводная/ беспроводная сеть</p>	<p>1 (Windows® 2000/XP, Windows Server® 2003/2008) Нажмите кнопку Пуск, Все программы (Программы для Windows® 2000), Стандартные и Проводник, а затем Мой 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 отобразится экран Контроль учетных записей пользователей, (Windows Vista®) нажмите Продолжить. (Windows® 7) нажмите Да.</p> <p>3 Следуйте выводимым на экран инструкциям.</p> <p>4 Распечатайте список конфигурации сети для установления причин неполадок.</p> <p> Примечание</p> <p>Программа для исправления сетевого подключения 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. Не рекомендуется, чтобы сетевой администратор устанавливал статический IP-адрес, так как при этом IP-адрес автоматически изменится.</p> <p>Если верные IP-адрес и маска подсети не назначены даже после использования программы для исправления сетевого подключения, для получения информации обратитесь к сетевому администратору или посетите веб-сайт Brother Solutions Center по адресу http://solutions.brother.com/.</p>

Не удается выполнить операции печати или сканирования с помощью аппарата Brother по сети.

Аппарат Brother не обнаружен в сети даже после успешной установки. (продолжение)

Вопрос	Интерфейс	Решение
<p>Предыдущее задание печати не было выполнено?</p>	<p>проводная/ беспроводная сеть</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): <p>(ОС Windows® 2000) Пуск, Настройка и затем Принтеры.</p> <p>(ОС Windows® XP) Пуск и Принтеры и факсы.</p> <p>(ОС Windows Vista®)  Панель управления, Оборудование и звук и затем Принтеры.</p> <p>(ОС Windows® 7)  Панель управления, Оборудование и звук, Устройства и принтеры и затем Принтеры и факсы.</p>
<p>Подключение аппарата Brother к сети выполняется с помощью беспроводной сети?</p>	<p>беспроводная сеть</p>	<ul style="list-style-type: none"> ■ Для определения состояния беспроводного подключения распечатайте Отчет WLAN. (Для получения информации о печати см. раздел <i>Печать отчета о состоянии беспроводной сети (для MFC-9560CDW)</i> на стр. 37.) При обнаружении кода ошибки на Отчет WLAN см. раздел Устранение неисправностей в <i>Руководстве по быстрой установке</i>. ■ См. раздел <i>Аппарат Brother не обнаружен в сети при установке MFL-Pro Suite</i> на стр. 82.
<p>Указанные процедуры были выполнены, однако с помощью аппарата Brother все еще не удается выполнить операции печати/сканирования. Есть ли еще какие-то способы решения данной проблемы?</p>	<p>проводная/ беспроводная сеть</p>	<p>Удалите MFL-Pro Suite и установите его снова.</p>

Программное обеспечение системы безопасности используется.

Вопрос	Интерфейс	Решение
Был ли разрешен доступ при отображении диалогового окна с предупредительным сообщением при установке MFL-Pro Suite, запуске приложений или использовании операций печати/сканирования?	проводная/ беспроводная сеть	Если доступ не был разрешен на диалоговом окне с предупредительным сообщением, функция брандмауэра программного обеспечения системы безопасности может блокировать доступ. Некоторое программное обеспечение системы безопасности может блокировать доступ без отображения диалогового окна с предупредительным сообщением. Для получения информации о том, как разрешить доступ, см. справку программного обеспечения системы безопасности или обратитесь к производителю.
Необходимо узнать номер порта для настройки параметров программного обеспечения для защиты компьютера.	проводная/ беспроводная сеть	Сетевыми функциями Brother используются следующие порты. <ul style="list-style-type: none"> ■ Сетевое сканирование → порт 54925 / протокол UDP ■ Прием ПК-факса → порт 54926 / протокол UDP ■ Сетевое сканирование/печать, прием ПК-факса, удаленная настройка → порт 137 / протокол UDP ■ BRAdmin Light → порт 161 / протокол UDP Для получения дополнительной информации об открытии портов см. справку программного обеспечения для защиты компьютера или обратитесь к производителю.

Необходимо проверить надлежащее функционирование используемых сетевых устройств.

Вопрос	Интерфейс	Решение
Аппарат Brother, точка доступа/маршрутизатор или сетевой концентратор включены?	проводная/ беспроводная сеть	Убедитесь, что соблюдены все инструкции в разделе <i>Сначала проверьте следующее</i> : на стр. 80.
Как можно узнать сетевые параметры аппарата Brother, например IP-адрес?	проводная/ беспроводная сеть	Напечатайте список конфигурации сети. См. раздел <i>Печать Списка конфигурации сети</i> на стр. 36.
Как можно узнать состояние подключения аппарата Brother?	проводная/ беспроводная сеть	Напечатайте список конфигурации сети и убедитесь что для параметра Ethernet Link Status или Wireless Link Status установлено значение Link OK . Если в параметре Link Status отображается значение Link DOWN или Failed To Associate , начните заново с раздела <i>Сначала проверьте следующее</i> : на стр. 80.

Необходимо проверить надлежащее функционирование используемых сетевых устройств. (продолжение)

Вопрос	Интерфейс	Решение
Можно ли проверить работу аппарата Brother с помощью команды ping с компьютера?	проводная/ беспроводная сеть	<p>Проверьте работу аппарата Brother с помощью команды ping, используя IP-адрес или имя узла.</p> <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 сетевому администратору и используйте программу для исправления сетевого подключения, чтобы автоматически исправить IP-адрес и маску подсети. Для получения дополнительной информации о программе для исправления сетевого подключения см. (Windows®) <i>Проверьте IP-адрес и маску подсети с помощью программы для исправления сетевого подключения.</i> в вопросе <i>Для аппарата Brother назначен доступный IP-адрес?</i> на стр. 83.</p> <p>(Macintosh) Убедитесь, что IP-адрес и маска подсети установлены правильно. См. <i>Проверьте IP-адрес и маску подсети</i> в вопросе <i>Для аппарата Brother назначен доступный IP-адрес?</i> на стр. 83.</p>
Аппарат Brother подключен к беспроводной сети?	беспроводная сеть	<p>Для определения состояния беспроводного подключения распечатайте Отчет WLAN. (Для получения информации о печати см. <i>Печать отчета о состоянии беспроводной сети (для MFC-9560CDW)</i> на стр. 37. Если напечатанный Отчет WLAN содержит код ошибки, см. раздел Устранение неисправностей в <i>Руководстве по быстрой установке</i>.</p>
Проверены все вышеперечисленные варианты решения, но проблемы все равно остаются. Есть ли еще какие-то способы решения данной проблемы?	проводная/ беспроводная сеть	<p>См. инструкции, прилагаемые к беспроводной точке доступа/беспроводному маршрутизатору, чтобы узнать SSID и сетевой ключ и установить правильные значения для них. Для получения дополнительной информации о SSID и сетевом ключе см. <i>Параметры безопасности (SSID/сетевой ключ) настроены правильно?</i> в вопросе <i>Не удается завершить настройку параметров беспроводной сети.</i> на стр. 81.</p>

Поддерживаемые протоколы и сетевые функции

Интерфейс	Ethernet	10/100BASE-TX
	Беспроводная сеть ¹	IEEE802.11b/g (режим инфраструктуры / режим ad-hoc)
Сеть (стандартные функции)	Протокол (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, клиент и сервер FTP, сервер TELNET, сервер HTTP/HTTPS, клиент и сервер TFTP, клиент SMTP, SNMPv1/v2c/v3, ICMP, передатчик LLTD, веб-службы (печать), клиент CIFS, клиент SNTF
	Протокол (IPv6)	NDP, RA, преобразователь адресов DNS, mDNS, передатчик LLMNR, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, клиент и сервер FTP, сервер TELNET, сервер HTTP/HTTPS, клиент и сервер TFTP, клиент SMTP, SNMPv1/v2c/v3, ICMPv6, передатчик LLTD, веб-службы (печать), клиент CIFS, клиент SNTF
Сеть (функции безопасности)	Проводная сеть	APOP, POP перед использованием SMTP, SMTP-AUTH, SSL/TLS (IPPS, HTTPS, SMTP, POP), SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
	Беспроводная сеть ¹	WEP 64/128 бит, WPA-PSK (TKIP/AES), WPA2-PSK (AES), APOP, POP перед использованием SMTP, SMTP-AUTH, SSL/TLS (IPPS, HTTPS, SMTP, POP), SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
Сеть (беспроводные функции)¹	Сертификация беспроводной сети	Лицензия на использование знака сертификации Wi-Fi, лицензия на использование знака идентификации Wi-Fi Protected Setup (WPS), логотип AOSS

¹ Для модели MFC-9560CDW

В

Указатель

A

AOSS™ 12, 13, 16, 34
APIPA 33

B

BRAdmin Light 1, 3
BRAdmin Professional 3 1, 6, 68
Brother Solutions Center 4, 6
BRPrint Auditor 7

E

Ethernet 34

H

HTTPS 61
Hyper Text Transfer Protocol 6

I

IEEE 802.1x 16, 26, 27
IP адрес 32
IPPS 63
IPv6 33

M

MAC-адрес 4, 5, 6, 32, 35, 36

P

PBC 12, 13, 16, 34
PIN-код 15, 24, 34
POP перед использованием SMTP 64

S

SMTP-AUTH 64
SNMPv3 61
SSL/TLS 69
Status Monitor 2

T

TCP/IP 31

V

Vertical Pairing (метод беспроводного подключения) 2

W

Web BRAdmin 1, 7
Wi-Fi Protected Setup 12, 13, 16, 24, 34

Б

Беспроводная сеть 8

В

Веб-браузер (HTTP) 6
Восстановление заводских настроек сети 36

З

Заводские настройки 36

И

Имя хоста 32

К

Конфигурация WINS 32

М

Маска подсети 32
Мастер развертывания драйверов 2

О

Операционные системы 1
Отчет WLAN 37, 85, 87

П

Панель управления 3
Программа для исправления сетевого подключения 83
Программа установки Brother 12, 13

Р

Режим ad-hoc	10, 11
Режим инфраструктуры	9, 11

С

Сервер DNS	33
Сервер WINS	32
Сертификат	69
Система управления через веб-интерфейс (веб-браузер)	1, 6, 61
Список конфигурации сети	36

Т

Технические характеристики	88
----------------------------------	----

У

Удаленная настройка	1
---------------------------	---

Ш

Шлюз	32
------------	----