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.

Версия 0

RUS

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

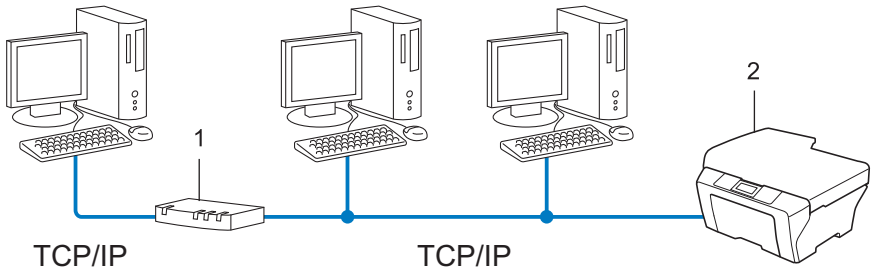
1 Типы сетевых подключений и протоколов

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, контролирующий общий доступ к файлам и устройствам.



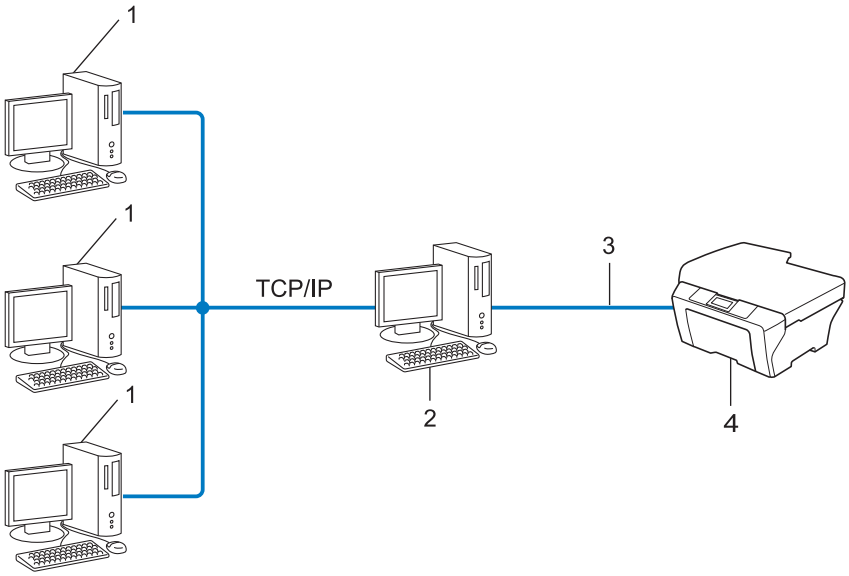
1 Маршрутизатор

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 стандартизованные 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/.

2 Настройка устройства для работы в сети

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.

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 шифрованного 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.

3 Термины и понятия, используемые в беспроводных сетях

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 802.1x.

При необходимости использования устройства в беспроводной сети, поддерживающей стандарт IEEE 802.1x, 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 попакетное 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, “WSLAN” (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.

- CKIP

  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)

4 Дополнительные параметры сети в ОС Windows®

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 **DPInst.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) [XXXXXXXXXXXX] (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.

5 Термины и понятия, относящиеся к безопасности

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.

A Приложение A

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)
BRNxxxxxxxxxxx	Бинарный протокол TCP/IP
BRNxxxxxxxxxxx_AT	Служба PostScript® для Macintosh
POSTSCRIPT_P1	Служба PostScript® (переключает PJL-совместимый аппарат в режим PostScript®)

(Где “xxxxxxxxxxx” – 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 A

255.255.0.0 для сетей класса B

255.255.255.0 для сетей класса C

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

B Указатель

W

А

Б

К

М

О

П

Р

С

Т

Ц

Ш