

Мрежови речник


В този Мрежови речник ще намерите основна информация за разширени мрежови характеристики на устройствата Brother и общи мрежови и често използвани термини.

Поддържаните протоколи и мрежови функции са различни в зависимост от модела, който използвате. За да разберете какви функции и мрежови протоколи се поддържат, вижте *Ръководство за мрежовия потребител*, който сме предоставили. За да изтеглите най-новото ръководство, моля, посетете Brother Solutions Center на адрес (<http://solutions.brother.com/>).

Можете да изтеглите най-новите драйвери и помощни програми за устройството, да прочетете често задаваните въпроси и съветите за отстраняване на неизправности или да научите за специални печатни решения от Brother Solutions Center.

Дефиниции на бележките

Ние използваме следната икона в Ръководството на потребителя:

 Забележка	Бележките ви казват какво да направите в дадена ситуация или ви дават полезни съвети за това как съответната операция работи с други функции.
--	---

ВАЖНА БЕЛЕЖКА

- Вашият продукт е одобрен за употреба само в държавата, в която е закупен. Не използвайте този продукт извън държавата, в която е закупен, тъй като това може да наруши разпоредбите относно безжичните телекомуникации и електроенергията на тази държава.
- Windows® XP в документа означава Windows® XP Professional, Windows® XP Professional x64 Edition и Windows® XP Home Edition.
- Windows Server® 2003 в документа означава Windows Server® 2003 и Windows Server® 2003 x64 Edition.
- Windows Server® 2008 в документа означава Windows Server® 2008 и Windows Server® 2008 R2.
- Windows Vista® в документа означава всички издания на Windows Vista®.
- Windows® 7 в документа означава всички издания на Windows® 7.
- Моля, посетете Brother Solutions Center на адрес <http://solutions.brother.com/> и щракнете върху Ръководства на страницата на Вашия модел, за да изтеглите останалите ръководства.

Съдържание

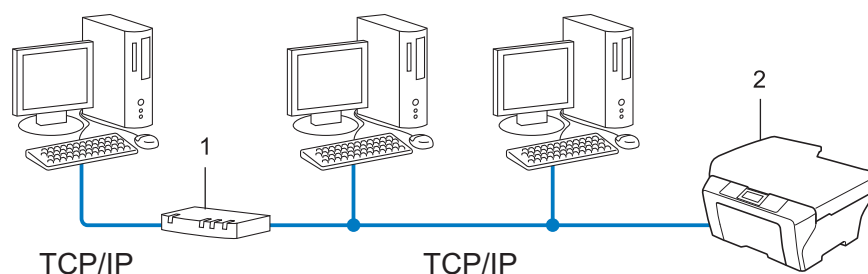
1	Видове мрежови връзки и протоколи	1
	Видове мрежови връзки	1
	Пример за жична мрежова връзка	1
	Протоколи	3
	TCP/IP протоколи и функционалност	3
	Друг протокол	6
2	Конфигурирайте Вашето устройство за мрежова работа	7
	IP адреси, маски на подмрежата и Gateway	7
	IP адрес	7
	Маска на подмрежата	8
	Gateway (и маршрутизатор)	8
	IEEE 802.1x Authentication	9
3	Условия и концепции на безжичните мрежи	11
	Посочване на Вашата мрежа	11
	SSID (идентификатор на обслужващ комплект) и канали	11
	Термини, свързани със сигурността	11
	Удостоверяване и шифроване	11
	Методи за удостоверяване и шифроване за лична безжична мрежа	11
	Методи за удостоверяване и шифроване за фирмена безжична мрежа	13
4	Допълнителни настройки на мрежата от Windows®	14
	Видове допълнителни настройки на мрежата	14
	Инсталиране на разпечатване в мрежа, когато използвате Web Services (Windows Vista® и Windows® 7)	14
	Инсталиране на разпечатване в мрежа за инфраструктурен режим, когато използвате Vertical Pairing (Windows® 7)	16
5	Термини и концепции, свързани със сигурността	18
	Функции за сигурност	18
	Термини, свързани със сигурността	18
	Протоколи за сигурност	19
	Методи за сигурност при изпращане и получаване на електронна поща	20
A	Приложение A	21
	Използване на услуги	21
	Други начини за конфигуриране на IP адреса (за напреднали потребители и администратори) ..	21
	Използване на DHCP за конфигуриране на IP адреса	21
	Използване на RARP за конфигуриране на IP адреса	22
	Използване на BOOTP за конфигуриране на IP адреса	23
	Използване на APIPA за конфигуриране на IP адреса	23
	Използване на ARP за конфигуриране на IP адреса	24
	Използване на TELNET конзола за конфигуриране на IP адреса	25

Видове мрежови връзки

Пример за жична мрежова връзка

Peer-to-Peer печат чрез TCP/IP

В Peer-to-Peer среда, всеки компютър изпраща и получава данни директно до всяко устройство. Няма централен сървър, контролиращ достъпа до файлове или споделени устройства.



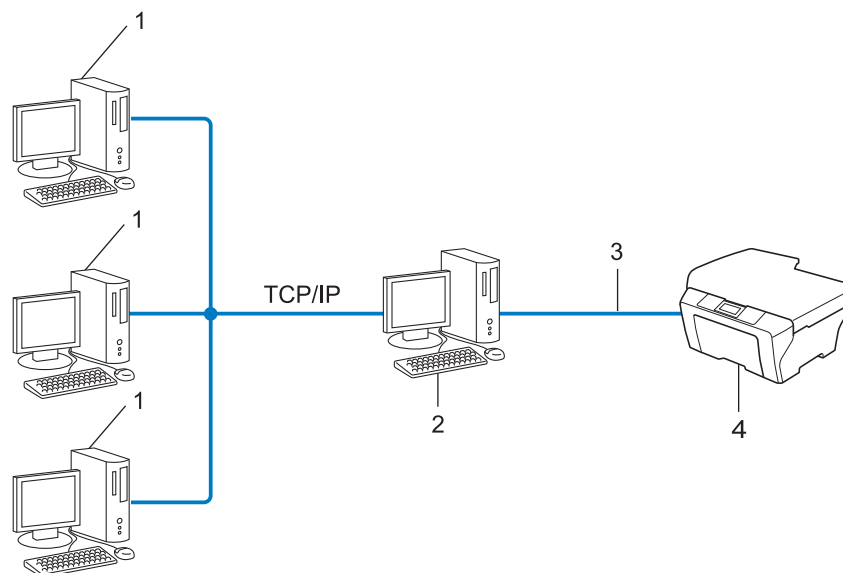
1 Маршрутизатор

2 Мрежово устройство (Вашето устройство)

- В по-малка мрежа от 2-3 компютъра препоръчваме метод на печатане Peer-to-Peer, тъй като се конфигурира по-лесно от метода за отпечатване в споделена мрежа. Вижте *Печат в споделена мрежова среда* на стр. 2.
- Всеки компютър трябва да използва TCP/IP протокола.
- Устройството Brother се нуждае от подходяща конфигурация на IP адрес.
- Ако използвате маршрутизатор, адресът на шлюза трябва да бъде конфигуриран на компютрите и устройството Brother.

Печат в споделена мрежова среда

В споделена мрежова среда всеки компютър изпраща данни чрез централно контролиран компютър. Този тип компютър често се нарича "сървър" или "сървър за печат". Неговата задача е да контролира разпечатването на всички задания за печат.



- 1 Клиентски компютър
- 2 Познат също и като "сървър" или "сървър за печат"
- 3 TCP/IP, USB или паралелен (при наличност)
- 4 Мрежово устройство (Вашето устройство)

- При по-голяма мрежа препоръчваме печатане в среда на споделена мрежа.
- "Сървърът" или "сървърът за печат" трябва да използват TCP/IP протокол за печат.
- Устройството Brother трябва да има конфигуриран собствен IP адрес, освен ако устройството не е споделено чрез USB или паралелен интерфейс в сървъра.

Протоколи

TCP/IP протоколи и функционалност

Протоколите са стандартизирани комплекси от правила за пренос на данни в мрежа. Протоколите позволяват на потребителите да получат достъп до свързани чрез мрежата ресурси.

Сървър за печат, използван при това устройство на Brother, поддържа TCP/IP (Transmission Control Protocol/Internet Protocol) протокол.

TCP/IP е най-популярният набор от протоколи, използвани за комуникационни схеми като интернет и електронна поща. Този протокол може да се използва в почти всички операционни системи като Windows®, Windows Server®, Mac OS X и Linux®. Това устройство на Brother разполага със следните TCP/IP протоколи.



Забележка

- Можете да конфигурирате настройките на протоколите чрез използване на HTTP интерфейс (уеб браузър). (Вижте *Ръководство за мрежовия потребител*.)
 - За да разберете какви протоколи използва Вашето устройство, вижте *Ръководство за мрежовия потребител*.
 - Информация за поддържаните протоколи за сигурност прочетете в *Протоколи за сигурност* на стр. 19.
-

DHCP/BOOTP/RARP

С използването на протоколите DHCP/BOOTP/RARP, IP адресът може да бъде автоматично конфигуриран.



Забележка

За използване на протоколите DHCP/BOOTP/RARP, моля, свържете с вашия мрежови администратор.

APIPA

Ако не зададете IP адрес ръчно (с помощта на контролния панел (за LCD модели) на устройството или софтуера BRAdmin) или автоматично (чрез сървър DHCP/BOOTP/RARP), протоколът за автоматично частно IP адресиране (APIPA) автоматично ще зададе IP адрес в диапазона от 169.254.1.0 до 169.254.254.255.

ARP

Протоколът Address Resolution извършва преобразуване на IP адрес в MAC адрес в TCP/IP мрежа.

DNS клиент

Печатният сървър на Brother поддържа клиентската функция Domain Name System (DNS). Тази функция позволява на сървъра за печат да комуникира с други устройства, като използва своето DNS име.

Разрешаване на имена в NetBIOS

Разрешаването на имена в мрежова базова система вход/изход ви дава възможност да получите IP адреса на другото устройство с помощта на неговото NetBIOS име по време на мрежовата връзка.

WINS

Услугата за интернет имена на Windows е услуга за предоставяне на информация за разрешаване на имена в NetBIOS чрез обединяване на IP адрес и NetBIOS име, което е в локалната мрежа.

LPR/LPD

Често използвани протоколи за печат в TCP/IP мрежа.

SMTP клиент

Клиентът SMTP (Протокол за стандартен пренос на поща) се използва за изпращане на електронна поща през интернет или интранет.

Custom Raw Port (по подразбиране е Port 9100)

Друг често използван протокол за печат в TCP/IP мрежа. Той дава възможност за интерактивен пренос на данни.

IPP

Протоколът за печатане през интернет (IPP версия 1.0) позволява директното разпечатване на документи на всяко достъпно устройство през интернет.



Забележка

За протокол IPPS вижте *Протоколи за сигурност* на стр. 19.

mDNS

mDNS позволява на сървър за печат на Brother да се самоконфигурира автоматично за работа в Mac OS X Simple Network конфигурирана система.

TELNET

Протоколът TELNET Ви позволява да управлявате отдалечените мрежови устройства в TCP/IP мрежа от Вашия компютър.

SNMP

Протоколът Simple Network Management (SNMP) се използва за управление на мрежови устройства, включващи компютри, маршрутизатори и готови мрежови устройства на Brother. Сървърът за печат на Brother поддържа SNMPv1, SNMPv2c и SNMPv3.



Забележка

За протокол SNMPv3 вижте *Протоколи за сигурност* на стр. 19.

LLMNR

Протоколът Link-Local Multicast Name Resolution (LLMNR) разрешава имената на съседни компютри, ако мрежата няма DNS (Система за наименование на домейни) сървър. Отговарящата функция на LLMNR работи в IPv4 или IPv6 среда, когато се използва компютър с изпращащата функция на LLMNR като Windows Vista® и Windows® 7.

Web Services

Протоколът Web Services позволява на потребителите на Windows Vista® или Windows® 7 да инсталират драйвера за принтера Brother, като щракнат с десен бутон върху иконата на устройството от папка **Мрежа**. (Вижте *Инсталиране на разпечатване в мрежа, когато използвате Web Services (Windows Vista® и Windows® 7)* на стр. 14.) Web Services позволяват и да проверите текущото състояние на устройството от компютъра.

HTTP

Протоколът HTTP се използва за пренос на данни между уеб сървър и уеб браузър.



Забележка

За протокол HTTPS вижте *Протоколи за сигурност* на стр. 19.

FTP (За функцията сканиране към FTP)

Протоколът File Transfer Protocol (FTP) позволява на устройството на Brother директно да сканира черно-бели или цветни документи към FTP сървър, разположен локално в мрежата или в интернет.

SNTP

Протоколът Simple Network Time се използва за синхронизиране на компютърните часовници в TCP/IP мрежа. Можете да конфигурирате настройките на SNTP с помощта на Уеб-базирано управление (уеб браузър). (За подробности, вижте *Ръководство за мрежовия потребител*.)

CIFS

Общата мрежова файлова система е стандартният способ, по който компютърните потребители споделят файлове и принтери под Windows®.

LDAP

Лекият протокол за достъп до справочници (LDAP) позволява на устройството Brother да търси информация, като факс номера и електронни адреси от LDAP сървър.

IPv6

IPv6 е следващото поколение интернет протокол. За повече информация за протокола IPv6, посетете страницата с моделите на устройството, което използвате, на адрес <http://solutions.brother.com/>.

Друг протокол

LLTD

Протоколът Link Layer Topology Discovery (LLTD) позволява лесно да откриете устройството на Brother в **Карта на мрежата** под Windows Vista®/Windows® 7. Устройството на Brother ще бъде показано с отличителна икона и име на възел. Фабричната настройка на този протокол е на Изключено. Можете да активирате LLTD с помощта на Уеб-базирано управление (уеб браузър) (Вижте *Ръководство за мрежовия потребител.*), и помощната програма BRAdmin Professional 3. Посетете страницата за файлове за изтегляне на адрес <http://solutions.brother.com/>, за да изтеглите BRAdmin Professional 3.

IP адреси, маски на подмрежата и Gateway

За да използвате устройството в TCP/IP мрежова среда, трябва да конфигурирате неговия IP адрес и маската на подмрежата. IP адресът, който ще зададете на сървъра за печат, трябва да бъде в същата логическа мрежа, в която са хост компютрите. Ако не е, трябва правилно да конфигурирате маската на подмрежата и адреса на шлюза.

IP адрес

Всеки IP адрес е поредица от числа, идентифициращи всяко свързано с мрежата устройство. Всеки IP адрес се състои от четири числа, разделени с точки. Всяко число е в порядъка от 0 до 255.

- Например: В малка по размер мрежа, обикновено можете да промените числата на последния сегмент.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

Как се задава IP адрес на вашия сървър за печат:

Ако във вашата мрежа имате DHCP/BOOTP/RARP сървър, сървърът за печат автоматично ще получи своя IP адрес от този сървър.



Забележка

В малки мрежи DHCP сървърът може да е и маршрутизаторът.

За повече информация относно DHCP, BOOTP и RARP, вижте *Използване на DHCP за конфигуриране на IP адреса* на стр. 21.
Използване на BOOTP за конфигуриране на IP адреса на стр. 23.
Използване на RARP за конфигуриране на IP адреса на стр. 22.

Ако нямате DHCP/BOOTP/RARP сървър, протоколът за автоматично частно IP адресиране (APIPA) автоматично ще зададе IP адрес в диапазона от 169.254.1.0 до 169.254.254.255. За повече информация относно APIPA, вижте *Използване на APIPA за конфигуриране на IP адреса* на стр. 23.

Маска на подмрежата

Маската на подмрежата ограничава комуникацията в мрежата.

■ Например: Компютър 1 може да комуникира с Компютър 2

- Компютър 1

IP адрес: 192.168. 1. 2

Маска на подмрежата: 255.255.255.000

- Компютър 2

IP адрес: 192.168. 1. 3

Маска на подмрежата: 255.255.255.000

Там където 0 е в маската на подмрежата, няма ограничения в комуникацията в тази част на адреса. В горния пример това означава, че можем да комуникираме с всяко устройство, което има IP адрес, започващ с 192.168.1.x. (където x. са числата от 0 до 255).

Gateway (и маршрутизатор)

Gateway е точка в мрежата, която действа като вход към друга мрежа и изпраща пренесените през мрежата данни до точна дестинация. Маршрутизаторът знае накъде да насочи данните, които пристигат в Gateway. Ако дестинацията се намира във външна мрежа, маршрутизаторът изпраща данните към външната мрежа. Ако вашата мрежа комуникира с други мрежи, може да се наложи да конфигурирате IP адреса на Gateway. Ако не знаете IP адреса на Gateway, обърнете се към администратора на мрежата.

IEEE 802.1x Authentication

IEEE 802.1x е IEEE стандарт за жична и безжична мрежа, която ограничава достъп от неупълномощени мрежови устройства. Вашето устройство Brother (молител) изпраща искане за удостоверяване до сървър RADIUS (сървър за удостоверяване) през Вашата точка за достъп (удостоверител). След като искането Ви бъде проверено от сървъра RADIUS, Вашето устройство може да получи достъп до мрежата.

Метод на удостоверяване

■ LEAP (За безжична мрежа)

Cisco LEAP (Лек разширяем протокол за удостоверяване) е разработен от Cisco Systems, Inc., който използва потребителска идентификация и парола за удостоверяване.

■ EAP-FAST

EAP-FAST (разширяем протокол за удостоверяване-гъвкаво удостоверяване през безопасен тунел) е разработен от Cisco Systems, Inc., който използва потребителска идентификация и парола за удостоверяване, и алгоритми на ключ за шифроване-разшифроване, за да се получи процес на удостоверяване по тунел.

Машината Brother поддържа следните вътрешни удостоверявания:

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

■ EAP-MD5 (За жична мрежа)

EAP-MD5 (разширяем протокол за удостоверяване-алгоритъм за представяне на съобщения в кратка форма 5) използва потребителска идентификация и парола за удостоверяване за удостоверяване чрез запитване-отговор.

■ PEAP

PEAP (защитен разширяем протокол за удостоверяване) е разработен от Microsoft Corporation, Cisco Systems и RSA Security. PEAP създава шифрован тунел SSL (Secure Sockets Layer) (Протокол за защита на информацията)/TLS (Transport Layer Security) (Протокол за защита на трафика на информация) между клиент и сървър за удостоверяване за изпращане на потребителска идентификация и парола. PEAP осигурява взаимно удостоверяване между сървъра и клиента.

Машината Brother поддържа следните вътрешни удостоверявания:

- PEAP/MS-CHAPv2
- PEAP/GTC

■ EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) (разширяем протокол за удостоверяване-протокол за защита на трафика на информация по тунел) е разработен от Funk Software и Certicom. EAP-TTLS създава подобен шифрован тунел SSL към PEAP между клиент и сървър за удостоверяване за изпращане на потребителска идентификация и парола. EAP-TTLS осигурява взаимно удостоверяване между сървъра и клиента.

Машината Brother поддържа следните вътрешни удостоверявания:

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

■ EAP-TLS

EAP-TLS ((Extensible Authentication Protocol Transport Layer Security) разширяем протокол за удостоверяване-протокол за защита на трафика на информация) изисква удостоверяване с цифров сертификат на клиентски сървър и сървър за удостоверяване.

Посочване на Вашата мрежа

SSID (идентификатор на обслужващ комплект) и канали

Трябва да конфигурирате SSID и един канал, за да зададете безжичната мрежа, с която искате да се свържете.

■ SSID

Всяка безжична мрежа има свое собствено уникално мрежово име и технически се характеризира като SSID или ESSID (идентификатор на разширен обслужващ комплект). SSID е с 32-байтова или по-малка стойност и е присвоен на точката за достъп. Безжичните мрежови устройства, които искате да свържете към безжичната мрежа, трябва да съответстват на точката за достъп. Точката за достъп и безжичните мрежови устройства изпращат безжични пакети (наричани навигационни), които съдържат SSID информацията. Когато Вашето безжично мрежово устройство получи навигационен пакет, можете да идентифицирате безжичната мрежа, която е достатъчно близо до радиовълните, достигащи до Вашето устройство.

■ Канали

Безжичните мрежи използват канали. Всеки безжичен канал е на различна честота. Има до 14 различни канала, които могат да бъдат използвани при употребата на безжична мрежа. При все това в много страни броят на наличните канали е ограничен.

Термини, свързани със сигурността

Удостоверяване и шифроване

Повечето безжични мрежи използват някакъв вид настройки за сигурност. Тези настройки за сигурност дефинират удостоверяването (как устройството идентифицира себе си в мрежата) и шифроването (как данните се шифроват при изпращането им в мрежата). **Ако не зададете правилно тези опции, когато конфигурирате Вашето безжично устройство Brother, то няма да може да се свърже с безжичната мрежа.** Поради това трябва да се внимава при конфигурирането на тези опции. Моля, вижте информацията в *Ръководство за мрежовия потребител*, за да разберете кои методи на удостоверяване и шифроване се поддържат от Вашето безжично устройство Brother.

Методи за удостоверяване и шифроване за лична безжична мрежа

Личната безжична мрежа е малка мрежа, например, когато използвате устройството си в безжична мрежа у дома, без да поддържа IEEE 802.1x.

Ако искате да използвате устройството си в безжична мрежа, която се поддържа от IEEE 802.1x, вижте *Методи за удостоверяване и шифроване за фирмена безжична мрежа* на стр. 13.

Методи на удостоверяване

■ Отворена система

На безжичните устройства се позволява достъп до мрежата без никакво удостоверяване.

■ Споделен ключ

Предварително определен таен ключ се споделя от всички устройства, които ще имат достъп до безжичната мрежа.

Устройството на Brother използва WEP ключа като предварително определения ключ.

■ WPA-PSK/WPA2-PSK

Активира Wi-Fi Protected Access Pre-shared key (WPA-PSK/WPA2-PSK), който позволява на безжичното устройство Brother да се свърже с точките за достъп посредством използването на TKIP за WPA-PSK или AES за WPA-PSK и WPA2-PSK (WPA-Personal).

Методи на шифроване

■ Никакъв

Не се използва метод на шифроване.

■ WEP

С използването на WEP (Wired Equivalent Privacy) данните се предават и приемат с ключ за защита.

■ TKIP

TKIP (Temporal Key Integrity Protocol) осигурява механизъм за смесване на ключовете, проверка на интегритета на съобщението и повторно отключване за всеки пакет.

■ AES

AES (Advanced Encryption Standard) е Wi-Fi® оторизираният сигурен стандарт за шифроване.

Мрежов ключ

■ Отворена система/Споделен ключ с WEP

Този ключ е 64-битова или 128-битова стойност, която трябва да бъде въведена в ASCII или шестнадесетичен формат.

- 64 (40) битова ASCII:

Използва 5 текстови знака, напр. "WLAN" (чувствителност към главни и малки букви).

- 64 (40) битова шестнадесетична:

Използва 10 цифри шестнадесетични данни, напр. "71f2234aba"

- 128 (104) битова ASCII:

Използва 13 текстови знака, напр. "Wirelesscomms" (чувствителност към главни и малки букви)

- 128 (104) битова шестнадесетична:

Използва 26 цифри шестнадесетични данни, напр. "71f2234ab56cd709e5412aa2ba"

■ WPA-PSK/WPA2-PSK и TKIP или AES

Използва Pre-Shared Key (PSK), който е с дължина 8 или повече знака, максимум 63 знака.

Методи за удостоверяване и шифроване за фирмена безжична мрежа

Фирмената безжична мрежа е голяма мрежа, например, когато използвате устройството си в служебна безжична мрежа с поддръжка на IEEE 802.1x. Ако конфигурирате устройството си в безжична мрежа, която се поддържа от IEEE 802.1x, можете да използвате следните методи за удостоверяване и шифроване.

Метод на удостоверяване

- LEAP

За LEAP, вижте *LEAP (За безжична мрежа)* на стр. 9.

- EAP-FAST

За EAP-FAST, вижте *EAP-FAST* на стр. 9.

- PEAP

За PEAP, вижте *PEAP* на стр. 9.

- EAP-TTLS

За EAP-TTLS, вижте *EAP-TTLS* на стр. 10.

- EAP-TLS

За EAP-TLS, вижте *EAP-TLS* на стр. 10.

Методи на шифроване

- TKIP

За TKIP, вижте *TKIP* на стр. 12.

- AES

За AES, вижте *AES* на стр. 12.

- SKIP

Оригиналният Key Integrity Protocol за LEAP от Cisco Systems Inc.

Потребителска идентификация и парола

Следните методи за сигурност използват потребителска идентификация с дължина по-малко от 64 знака и парола с дължина по-малко от 32 знака.

- LEAP

- EAP-FAST

- PEAP

- EAP-TTLS

- EAP-TLS (За потребителска идентификация)

Видове допълнителни настройки на мрежата

Можете да използвате следните функции, ако искате да конфигурирате допълнителни настройки на мрежата.

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



Забележка

Проверете дали хост компютърът и устройството са в една и съща подмрежа или дали маршрутизаторът е правилно конфигуриран за преноса на данни между двете устройства.

Инсталиране на разпечатване в мрежа, когато използвате Web Services (Windows Vista® и Windows® 7)

Функцията Web Services Ви позволява да следите информацията за устройството, което е свързано с мрежата. Това дава възможност и за инсталиране на драйвера на принтера от иконата на принтера и ще се създаде порта Web Services (WSD порт).



Забележка

- Преди да конфигурирате тази настройка, трябва да конфигурирате IP адреса на Вашето устройство.
- За Windows Server® 2008 трябва да инсталирате Print Services.
- С уеб услугите се инсталира само поддръжка на принтера.



1 Поставете инсталационния CD-ROM диск.



2 Изберете CD-ROM устройството/install/driver/gdi/32 или 64.



3 Изберете Вашия език, а след това щракнете двукратно върху **DPIInst.exe**.



Забележка


Ако се появи екранът **Управление на потребителските акаунти**,

(Windows Vista®) Щракнете върху **Позволи**.


(Windows® 7) Щракнете върху **Да**.



4 (Windows Vista®)

Щракнете върху , след което изберете **Мрежа**.

(Windows® 7)

Щракнете върху , **Контролен панел, Мрежа и интернет**, а след това **Преглед на компютри в мрежата и устройства**.

- 5 Заедно с иконата на принтера ще се появи името Web Services на устройството. Щракнете с десен бутон върху устройството, което желаете да инсталирате.



Забележка

Наименованието Web Services на устройството на Brother е наименованието на модела, а MAC адреса (Ethernet адреса) на устройството (напр., Brother MFC-XXXX (име на модела) [XXXXXX]) (MAC адрес / Ethernet адрес).

- 6 От падащото меню щракнете върху **Инсталирай**.

Инсталиране на разпечатване в мрежа за инфраструктурен режим, когато използвате Vertical Pairing (Windows® 7)


Windows® Vertical Pairing е технология, която позволява на Вашето безжично устройство, поддържано от Vertical Pairing, да се свързва с Вашата инфраструктурна мрежа с помощта на PIN метода на Wi-Fi Protected Setup и функцията за уеб услуги. Това дава възможност и за инсталиране на драйвера на принтера от иконата на принтера, която е на екрана **Добавяне на устройство**.

Ако сте в инфраструктурен режим, можете да свържете устройството си с безжичната мрежа, а след това да инсталирате драйвера за принтера с помощта на тази функция. Изпълнете следните стъпки:



Забележка

- Ако сте настроили функцията Web Services на Вашето устройство на Off, трябва да го върнете на On. Настройката по подразбиране на Web Services за устройството Brother е On. Можете да промените настройката на Web Services с помощта на Уеб-базирано управление (уеб браузър) или BRAdmin Professional 3.
- Уверете се, че точката за достъп/маршрутизаторът на Вашата WLAN включва графичния знак за съвместимост на Windows® 7. Ако не сте сигурни за графичния знак за съвместимост, обърнете се към производителя на Вашата точка за достъп/маршрутизатора.
- Уверете се, че Вашият компютър включва графичния знак за съвместимост на Windows® 7. Ако не сте сигурни за графичния знак за съвместимост, обърнете се към производителя на Вашия компютър.
- Ако конфигурирате безжична мрежа с помощта на външна безжична NIC (Network Interface Card) (мрежова интерфейсна карта), уверете се, че безжичната NIC включва графичния знак за съвместимост на Windows® 7. За повече информация се обърнете към производителя на Вашата NIC.
- За да използвате компютър с Windows® 7 като Registrar (регистратор), трябва да го регистрирате предварително във Вашата мрежа. Вижте инструкцията към Вашата точка за достъп/маршрутизатор на WLAN.

- 1 Включете Вашето устройство.
- 2 Настройте устройството на Wi-Fi Protected Setup (PIN метод).
Вижте безжично конфигуриране на Wi-Fi Protected Setup (PIN метод) в *Ръководство за мрежовия потребител* за това как да настроите устройството си на PIN метода.
- 3 Щракнете върху бутона , а след това върху **Устройства и принтери**.
- 4 Изберете **Добавяне на устройство** от диалога **Устройства и принтери**.
- 5 Изберете Вашето устройство и въведете PIN, който е посочило Вашето устройство.
- 6 Изберете инфраструктурната мрежа, към която искате да се свържете, и след това щракнете върху **Напред**.

- 7 Когато устройството Ви се появи в диалога **Устройства и принтери**, безжичното конфигуриране и инсталирането на драйвера на принтера са приключили успешно.

Функции за сигурност

Термини, свързани със сигурността

■ СО (Сертифициращ орган)

СО е юридическо лице, което издава цифрови сертификати (по-специално, сертификати X.509) и отговаря за обвързването на данните в сертификата.

■ ЗПС (Заявка за подписване на сертификат)

ЗПС е съобщение, изпратено до СО от кандидат за издаване на сертификат. ЗПС съдържа информация за кандидата, публичния ключ, генериран от кандидата, и цифровия подпис на кандидата.

■ Сертификат

Сертификатът е информацията, която обвързва публичен ключ със самоличност. Сертификатът може да се използва за удостоверяване, че публичен ключ принадлежи на някое лице. Форматът се определя от стандарта x.509.

■ Сертификат на СО

Сертификат на СО е сертифицирането, което идентифицира самия СО (Сертифициращ орган) и притежава личния му ключ. Той проверява сертификат, издаден от СО.

■ Цифров подпис

Цифровият подпис е величина, изчислена с криптографски алгоритъм и прикрепена към обект от данни по такъв начин, че всеки получател на данните може да използва подписа за удостоверяване на произхода и истинността на данните.

■ Криptosистема с публичен ключ

Криptosистемата с публичен ключ е съвременен клон на криптографията, в който в алгоритмите се използва двойка ключове (публичен ключ и личен ключ) и различен компонент на двойката за различните стъпки на алгоритъма.

■ Криptosистема със споделен ключ

Криptosистемата със споделен ключ е клон на криптографията за алгоритми, в които се използва един и същ ключ за две различни стъпки на алгоритъма (например, като шифроване и разшифроване).

Протоколи за сигурност



Забележка

Можете да конфигурирате настройките на протокола с помощта на Уеб-базирано управление (уеб браузър). За подробности, вижте *Ръководство за мрежовия потребител*.

SSL (Secure Socket Layer) (Протокол за защита на информацията)/ TLS (Transport Layer Security) (Протокол за защита на трафика на информация)

Тези протоколи за сигурност на комуникацията шифроват данните за предпазване от заплахи за сигурността.

HTTPS

В интернет протокола "Протокол за трансфер на хипер-текст" (HTTP) се използва SSL.

IPPS

В интернет протокола "Протокол за печатане през интернет" (IPP версия 1.0) се използва SSL.

SNMPv3

Протоколът Simple Network Management, версия 3 (SNMPv3) осигурява удостоверяване на потребителя и шифроване на данни за сигурност в управлението на мрежови устройства.

Методи за сигурност при изпращане и получаване на електронна поща



Забележка

Можете да конфигурирате настройките на методите за сигурност с помощта на Уеб-базирано управление (уеб браузър). За подробности, вижте *Ръководство за мрежовия потребител*.

POP преди SMTP (PbS)

Метод за удостоверяване на потребителя при изпращане на електронна поща от клиент. Клиентът получава разрешение да използва SMTP сървър чрез достъп до POP3 сървър преди изпращането на електронно писмо.

SMTP-AUTH (SMTP удостоверяване)

SMTP-AUTH разширява SMTP (протокола за изпращане на електронни писма в интернет), за да включи метод на удостоверяване, който осигурява разкриване на истинската самоличност на изпращача.

APOP (Протокол на удостоверена поща)

APOP разширява POP3 (протокола за получаване в интернет), за да включи метод на удостоверяване, който шифрова паролата при получаване на електронно писмо от клиента.

SMTP по SSL

Функцията SMTP по SSL дава възможност за изпращане на шифрована електронна поща с помощта на SSL.

POP по SSL

Функцията POP по SSL дава възможност за получаване на шифрована електронна поща с помощта на SSL.

Използване на услуги

Услуга е ресурс, достъпен за компютри, които желаят да печатат на сървъра за печат Brother. Сървърът за печат Brother осигурява следните предварително зададени услуги (изпълнете команда ПОКАЗВАНЕ НА УСЛУГА в дистанционната конзола на сървъра за печат на Brother за преглед на списък с налични услуги): Въведете ПОМОЩ в командния ред за списък с поддържани команди.

Услуга (Пример)	Дефиниция
BINARY_P1	TCP/IP binary
TEXT_P1	TCP/IP текстова услуга (добавя връщане в началото след всеки нов ред)
PCL_P1	PCL услуга (превключва съвместимото с PJL устройство в PCL режим)
BRNxxxxxxxxxxxx	TCP/IP binary
BRNxxxxxxxxxxxx_AT	PostScript® услуга за Macintosh
POSTSCRIPT_P1	PostScript® услуга (превключва PJL-съвместимото устройство в PostScript® режим)

Където “xxxxxxxxxxxx” е MAC адресът (Ethernet адрес) на Вашата машина.

Други начини за конфигуриране на IP адреса (за напреднали потребители и администратори)

Използване на DHCP за конфигуриране на IP адреса

Протоколът за динамично конфигуриране на хостове (DHCP) е един от няколко автоматизирани механизми за разпределяне на IP адреси. Ако във вашата мрежа имате DHCP сървър, сървърът за печат автоматично ще получи своя IP адрес от DHCP сървъра и ще регистрира наименованието си към всички RFC 1001 и 1002-съвместими услуги за динамични наименования.



Забележка

Ако не желаете да конфигурирате сървъра за печат чрез DHCP, BOOTP или RARP, трябва да настроите метода на първоначално зареждане на статичен, за да има сървърът за печат статичен IP адрес. Това ще попречи на сървъра за печат да се опита да получи IP адрес от която и да било от тези системи. За промяна на метода на зареждане, използвайте менюто Мрежа на контролния панел на устройството (при LCD модели), приложенията BRAdmin, дистанционната настройка или уеб базирано управление (уеб браузър).

Използване на RARP за конфигуриране на IP адреса

IP адресът на сървър за печат Brother може да бъде конфигуриран с използването на помощното средство Reverse ARP (RARP) на хост компютъра. Това се прави с редактиране на `/etc/ethers` файла (ако този файл не съществува, можете да го създадете) със запис, подобен на следния:

```
00:80:77:31:01:07 BRN008077310107 (или BRW008077310107 за безжична мрежа)
```

Където първият запис е MAC адреса (Ethernet адреса) на сървъра за печат, а вторият запис е наименованието на сървъра за печат (наименованието трябва да бъде същото като въведеното в `/etc/hosts` файла).

Ако RARP даемон още не е включен, стартирайте го (в зависимост от системата, командата може да бъде `rarpd`, `rarpd -a`, `in.rarpd -a` или нещо друго; напишете `man rarpd` или направете справка в системната документация за допълнителна информация). За да проверите дали работи RARP даемон в базирана върху Berkeley UNIX система, напишете следната команда:

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

За базирани на AT&T UNIX системи, напишете:

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

Сървър за печат на Brother ще получи IP адреса от RARP даемон, когато се включи устройството.

Използване на BOOTP за конфигуриране на IP адреса

BOOTP е алтернатива на RARP, която има предимството да позволява конфигуриране на маската на подмрежата и шлюза. За да използвате BOOTP за конфигуриране на IP адреса, уверете се, че BOOTP е инсталиран и работи на Вашия хост компютър (той трябва да се появи във файла `/etc/services` на Вашия хост като реална услуга; напишете `man bootpd` или направете справка в документацията на Вашата система). BOOTP обикновено се стартира чрез `/etc/inetd.conf` файла, така че може би трябва да го активирате, като отстраните “#” пред `bootp` записа във файла. Например, един типичен `bootp` запис в `/etc/inetd.conf` файла би бил:

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

В зависимост от системата този запис може да е наречен “bootps”, вместо “bootp”.



Забележка

За активирането на BOOTP, просто използвайте редактор, за да изтриете “#” (ако няма “#”, то BOOTP вече е активиран). След това редактирайте файла за конфигуриране на BOOTP (обикновено `/etc/bootptab`) и въведете името, типа мрежа (1 за Ethernet), MAC адрес (Ethernet адрес) и IP адреса, маска на подмрежата и шлюз на сървъра за печат. За съжаление, точният формат за това не е стандартизиран, така че ще трябва да направите справка със системната документация, за да определите как да въведете тази информация (много UNIX системи също имат шаблонни примери в `bootptab` файла, които можете да използвате за справка). Някои примери на типични `/etc/bootptab` записи включват: (“BRN” по-долу е “BRW” за безжична мрежа.)

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

и:

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

Определени внедрявания на BOOTP хост софтуер няма да реагират на BOOTP заявки, ако не сте включили наименование на файл за изтегляне в конфигурационния файл. Ако случаят е такъв, просто създайте празен файл на хоста и посочете наименованието на този файл и пътя до него в конфигурационния файл.

Както при RARP, сървърът за печат ще зареди своя IP адрес от BOOTP сървъра при включване на устройството.

Използване на APIPA за конфигуриране на IP адреса

Печатният сървър на Brother поддържа протокол за автоматично задаване на частен адрес Automatic Private IP Addressing (APIPA). С APIPA, DHCP клиентите автоматично конфигурират IP адрес и маска на подмрежа, когато DHCP сървърът не е достъпен. Устройството избира собствен IP адрес в порядъка 169.254.1.0 до 169.254.254.255. Маската на подмрежата автоматично се настройва на 255.255.0.0, а адресът на Gateway става 0.0.0.0.

По подразбиране APIPA протоколът е активиран. Ако искате да деактивирате APIPA протокола, можете да го деактивирате през контролния панел на устройството (при LCD модели), BRAdmin Light или уеб-базирано управление (уеб браузър).

Използване на ARP за конфигуриране на IP адреса

Ако не можете да използвате приложението BRAdmin и вашата мрежа не използва DHCP сървър, можете да използвате и командата ARP. Командата ARP е достъпна от Windows® системи, които имат инсталиран TCP/IP, както и от UNIX системи. За да използвате ARP, в командния ред въведете следната команда:

```
arp -s ipaddress ethernetaddress
```

```
ping ipaddress
```

Където `ethernetaddress` е MAC адрес (Ethernet адрес) на сървъра за печат, а `ipaddress` е IP адресът на печатния сървър. Например:

■ Windows® системи

Windows® системите изискват знака типе “-” между всяка цифра от MAC адреса (Ethernet адреса).

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

```
ping 192.168.1.2
```

■ UNIX/Linux системи

Обикновено UNIX и Linux системите изискват знака двоеточие “:” между всяка цифра на MAC адреса (Ethernet адреса).

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

```
ping 192.168.1.2
```



Забележка

Трябва да бъдете в същия Ethernet сегмент (т.е. не може да има маршрутизатор между сървъра за печат и операционната система), за да използвате командата `arp -s`.

Ако има маршрутизатор, можете да използвате BOOTP или другите описани в тази глава методи, за да въведете IP адреса. Ако вашият администратор е конфигурирал системата да задава IP адреси чрез BOOTP, DHCP или RARP, сървърът за печат на Brother може да получи IP адрес от всяка от тези раздаващи IP адреси системи. В който случай няма нужда да използвате командата ARP. Командата ARP работи само веднъж. От съображения за сигурност, след като успешно сте конфигурирали IP адреса на сървъра за печат на Brother чрез командата ARP, повече не можете да използвате ARP командата, за да промените адреса. Сървърът за печат ще игнорира всички опити за това. Ако желаете отново да промените IP адреса, използвайте уеб базирано управление (уеб браузър), TELNET (чрез командата SET IP ADDRESS) или фабричната инициализация на сървъра за печат (което ще ви позволи отново да използвате ARP командата).

Използване на TELNET конзола за конфигуриране на IP адреса

Можете да използвате командата TELNET за промяна на IP адреса.

TELNET е ефективен метод за промяна на IP адреса на устройството. Но в сървъра за печат вече трябва да е програмиран валиден IP адрес.

Напишете TELNET <command line> в командния ред на системния промпт, където <command line> е IP адреса на сървъра за печат. Когато сте се свързали, натиснете клавиша Return или Enter, за да получите “#” промпт. Въведете паролата “access” (паролата няма да се появи на екрана).

Ще ви бъде поискано име на потребител. Там напишете каквото и да е.

Тогава ще получите Local> промпта. Напишете SET IP ADDRESS ipaddress, където ipaddress е желаният IP адрес, който искате да зададете на сървъра за печат (проверете при мрежовия администратор какъв IP адрес да използвате). Например:

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

Сега ще трябва да зададете маска на подмрежата, като напишете SET IP SUBNET subnet mask, където subnet mask е желаната маска на подмрежата, която искате да зададете на сървъра за печат (проверете при мрежовия администратор каква маска на подмрежата да използвате). Например:

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

Ако нямате никакви подмрежи, използвайте някоя от следните фабрични маски на подмрежата:

255.0.0.0 за мрежи клас А

255.255.0.0 за мрежи клас В

255.255.255.0 за мрежи клас С

Най-лявата група цифри от вашия IP адрес може да определи какъв тип мрежа имате. Стойността на тази група е от порядъка от 1 до 127 за мрежи от клас А (напр., 13.27.7.1), от 128 до 191 за мрежи от клас В (напр., 128.10.1.30) и от 192 до 255 за мрежи от клас С (напр., 192.168.1.4).

Ако имате Gateway (маршрутизатор), въведете неговия адрес с командата SET IP ROUTER routeraddress, където routeraddress е желаният IP адрес на Gateway, който искате да зададете на сървъра за печат. Например:

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

Напишете SET IP METHOD STATIC, за да настроите метода на конфигурация на достъпа до IP на статичен.

За да проверите дали сте въвели информацията за IP правилно, напишете SHOW IP.

Напишете EXIT или Ctrl-D (т.е., задръжте натиснат клавиша control и напишете “D”) за приключване на сесията на дистанционната конзола.

В

Индекс

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	5
CKIP	13
Custom Raw Port	4

D

DHCP	3, 21
DNS клиент	3

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
IP адрес	7
IPP	4
IPPS	19
IPv6	5

L

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

M

MAC адреса	24
MAC адресът	15, 21, 22, 23, 24
mDNS	4

P

PCL_P1	21
PEAP	9
Peer-to-Peer (Равноправен достъп)	1
POP по SSL	20
POP преди SMTP	20
Port 9100	4
POSTSCRIPT_P1	21

R

RARP	3, 22
RFC 1001	21

S

SMTP клиент	4
SMTP по SSL	20
SMTP-AUTH	20
SNMP	4
SNMPv3	19
SNTP	5
SSID	11
SSL/TLS	19

T

TCP/IP	3
TELNET	4, 25
TEXT_P1	21
TKIP	12

V

Vertical Paring	14
-----------------------	----

W

Web Services	5, 14
WEF	12
WINS	4
WPA-PSK/WPA2-PSK	12

Б

Безжична мрежа	11
----------------------	----

З

ЗПС	18
-----------	----

К

Канали	11
Криптосистема с публичен ключ	18
Криптосистема със споделен ключ	18

М

Маска на подмрежата	8
Мрежов ключ	12

О

Отворена система	12
------------------------	----

П

Печат в споделена мрежова среда	2
Печат през TCP/IP	14
Протокол	3

Р

Разпечатване в мрежа	14
Разрешаване на имена в NetBIOS	4

С

Сертификат	18
Сертификат на СО	18
СО	18
Споделен ключ	12

Т

Термини, свързани със сигурността	18
---	----

У

Удостоверяване	12
Услуга	21

Ц

Цифров подпис	18
---------------------	----

Ш

Шифроване	12
-----------------	----