

Glosario de red

En este Glosario de red encontrará información básica acerca de las funciones de red avanzadas de los equipos Brother junto con información general acerca de la conexión de redes y los términos más comunes.

Los protocolos admitidos y las funciones de red varían en función del modelo que se utilice. Para saber qué funciones y protocolos de red son compatibles, consulte la *Guía del usuario en red* que le suministramos. Si desea descargar el manual más reciente, visite el Brother Solutions Center en (<http://solutions.brother.com/>).

Asimismo, puede descargar los controladores y utilidades más recientes para su equipo, leer las preguntas más frecuentes y los consejos de la sección de solución de problemas u obtener información acerca de soluciones de impresión especiales en el Brother Solutions Center.

Definiciones de las notas

A lo largo de esta Guía del usuario se utiliza el siguiente icono:

 Nota	Las notas le indican cómo responder a una situación que surja o le proporcionan sugerencias sobre el funcionamiento con otras características.
--	--

NOTA IMPORTANTE

- Su producto sólo está aprobado para su uso en el país donde se ha realizado la compra. No utilice este producto fuera del país donde se ha realizado la compra, ya que podría infringir la normativa eléctrica y de las comunicaciones inalámbricas de ese país.
- Windows[®] XP en este documento representa Windows[®] XP Professional, Windows[®] XP Professional x64 Edition y Windows[®] XP Home Edition.
- Windows Server[®] 2003 en este documento representa Windows Server[®] 2003 y Windows Server[®] 2003 x64 Edition.
- Windows Server[®] 2008 en este documento representa Windows Server[®] 2008 y Windows Server[®] 2008 R2.
- Windows Vista[®] en este documento representa todas las ediciones de Windows Vista[®].
- Windows[®] 7 en este documento representa todas las ediciones de Windows[®] 7.
- Visite el Brother Solutions Center en <http://solutions.brother.com/> y haga clic en Manuales en su página de modelos para descargar los otros manuales.

Tabla de contenido

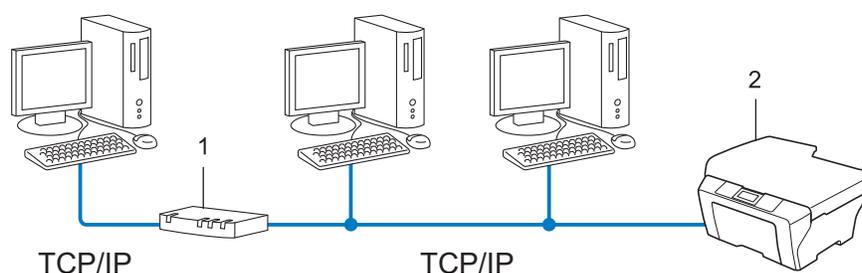
1	Tipos de conexiones de red y protocolos	1
	Tipos de conexión de red	1
	Ejemplo de conexión de red cableada	1
	Protocolos.....	3
	Protocolos TCP/IP y funciones.....	3
	Otro protocolo.....	6
2	Configuración del equipo para una red	7
	Direcciones IP, máscaras de subred y puertas de acceso.....	7
	Dirección IP	7
	Máscara de subred.....	8
	Puerta de acceso (y enrutador).....	8
	Autenticación IEEE 802.1x	9
3	Términos y conceptos relativos a redes inalámbricas	11
	Especificación de la red.....	11
	SSID (Identificador de conjunto de servicios) y canales	11
	Términos de seguridad.....	11
	Autenticación y encriptación	11
	Métodos de autenticación y encriptación para una red inalámbrica personal.....	12
	Métodos de autenticación y encriptación para una red inalámbrica corporativa.....	13
4	Configuración de red adicional desde Windows®	15
	Tipos de configuración de red adicional.....	15
	Instalación de Impresión en red cuando utilice los Web Services (Windows Vista® y Windows® 7).....	15
	Instalación de impresión en red para el modo Infraestructura cuando utilice Vertical Pairing (Emparejamiento vertical) (Windows® 7).....	17
5	Términos y conceptos relativos a la seguridad	18
	Funciones de seguridad	18
	Terminología de seguridad.....	18
	Protocolos de seguridad.....	19
	Métodos de seguridad para el envío y la recepción de correos electrónicos.....	20
A	Apéndice A	21
	Utilización de servicios	21
	Otras formas de establecer la dirección IP (para usuarios avanzados y administradores).....	21
	Uso de DHCP para configurar la dirección IP	21
	Uso de RARP para configurar la dirección IP	22
	Uso de BOOTP para configurar la dirección IP.....	23
	Uso de APIPA para configurar la dirección IP.....	23
	Uso de ARP para configurar la dirección IP	24
	Uso de la consola TELNET para configurar la dirección IP	25

Tipos de conexión de red

Ejemplo de conexión de red cableada

Impresión punto a punto mediante TCP/IP

En un entorno punto a punto, cada ordenador envía y recibe datos directamente hacia y desde cada dispositivo. No existe un servidor central que controle el acceso a los archivos o el uso compartido de los equipos.



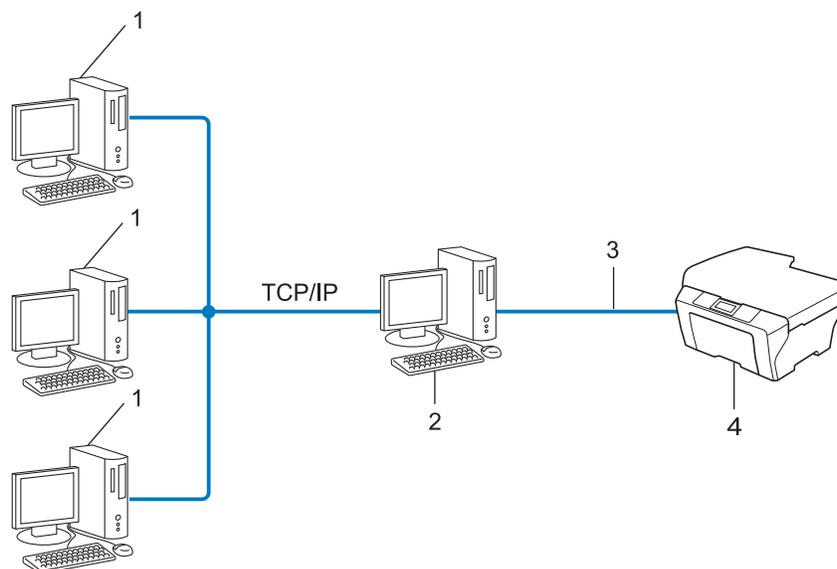
1 Enrutador

2 Equipo de red (su equipo)

- En una red pequeña de 2 ó 3 ordenadores, recomendamos el método de impresión punto a punto, ya que es más sencillo de configurar que el método de impresión compartida de red. Consulte *Impresión compartida de red* en la página 2.
- Cada ordenador debe utilizar el protocolo TCP/IP.
- El equipo Brother necesita la configuración de una dirección IP apropiada.
- Si está utilizando un enrutador, debe configurar la dirección de la puerta de acceso en los ordenadores y en el equipo Brother.

Impresión compartida de red

En un entorno compartido de red, cada ordenador envía datos a través de un sistema controlado de modo central. Este tipo de ordenador se suele denominar “Servidor” o “Servidor de impresión”. Su trabajo consiste en controlar la impresión de todos los trabajos de impresión.



1 Ordenador cliente

2 También conocido como “Servidor” o “Servidor de impresión”

3 TCP/IP, USB o paralelo (si hay disponible)

4 Equipo de red (su equipo)

- En una red mayor, recomendamos un entorno de impresión compartida de red.
- El “servidor” o “servidor de impresión” debe utilizar el protocolo de impresión TCP/IP.
- El equipo Brother necesita tener configurada una dirección IP apropiada, a menos que se conecte a través de la interfaz USB o paralelo en el servidor.

Protocolos

Protocolos TCP/IP y funciones

Los protocolos son los conjuntos de reglas estandarizadas para transmitir datos en una red. Los protocolos permiten a los usuarios obtener acceso a recursos conectados a la red.

El servidor de impresión utilizado en este equipo Brother es compatible con el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol).

TCP/IP es el conjunto de protocolos más difundido que se utiliza en telecomunicaciones como, por ejemplo, Internet y el correo electrónico. Este protocolo se puede utilizar en casi todos los sistemas operativos, como Windows®, Windows Server®, Mac OS X y Linux®. Los siguientes protocolos TCP/IP están disponibles en el equipo Brother.



Nota

- Puede configurar los parámetros del protocolo mediante la interfaz HTTP (navegador web). (Consulte la *Guía del usuario en red*).
 - Para saber qué protocolos admite su equipo Brother, consulte la *Guía del usuario en red*.
 - Para obtener información acerca de los protocolos de seguridad admitidos, consulte *Protocolos de seguridad* en la página 19.
-

DHCP/BOOTP/RARP

Al usar los protocolos DHCP/BOOTP/RARP se configura automáticamente la dirección IP.



Nota

Para utilizar los protocolos DHCP/BOOTP/RARP, póngase en contacto con su administrador de red.

APIPA

Si no asigna una dirección IP manualmente (mediante el panel de control del equipo (para los modelos con pantalla LCD) o el software BRAdmin) o automáticamente (mediante un servidor DHCP/BOOTP/RARP), el protocolo de direccionamiento automático de direcciones IP privadas (APIPA) asignará automáticamente una dirección IP del intervalo entre 169.254.1.0 y 169.254.254.255.

ARP

Address Resolution Protocol (Protocolo de resolución de direcciones) lleva a cabo la asignación de una dirección IP a una dirección MAC en una red TCP/IP.

Cliente DNS

El servidor de impresión Brother es compatible con la función de cliente Sistema de nombres de dominio (DNS). Esta función permite que el servidor de impresión se comunice con otros dispositivos utilizando su nombre DNS.

Resolución de nombres NetBIOS

La resolución de nombres del sistema básico de entrada y salida de red permite obtener la dirección IP del otro dispositivo mediante su nombre NetBIOS durante la conexión de red.

WINS

El servicio de nombres de Internet de Windows es un servicio que proporciona información para la resolución de nombres NetBIOS mediante la consolidación de una dirección IP y un nombre NetBIOS que se encuentra en la red local.

LPR/LPD

Protocolos de impresión que se utilizan frecuentemente en una red TCP/IP.

Cliente SMTP

El cliente SMTP (Simple Mail Transfer Protocol) se utiliza para enviar mensajes de correo electrónico a través de Internet o de una intranet.

Custom Raw Port (el puerto predeterminado es el Puerto 9100)

Otro protocolo de impresión que se utiliza frecuentemente en una red TCP/IP. Este protocolo permite la transmisión de datos interactiva.

IPP

El protocolo Internet Printing Protocol (IPP versión 1.0) le permite imprimir documentos directamente en cualquier equipo disponible a través de Internet.



Nota

Para obtener información acerca del protocolo IPPS, consulte *Protocolos de seguridad* en la página 19.

mDNS

mDNS permite que el servidor de impresión Brother se configure automáticamente para trabajar en un sistema de configuración simple de red Mac OS X.

TELNET

El protocolo TELNET le permite controlar los dispositivos de red remotos en una red TCP/IP desde su ordenador.

SNMP

El Protocolo simple de administración de redes (SNMP) se utiliza para administrar los dispositivos de red como ordenadores, enrutadores y equipos Brother preparados para la red. El servidor de impresión Brother admite los protocolos SNMPv1, SNMPv2c y SNMPv3.



Nota

Para obtener información acerca del protocolo SNMPv3, consulte *Protocolos de seguridad* en la página 19.

LLMNR

El protocolo Link-Local Multicast Name Resolution (LLMNR) resuelve los nombres de los ordenadores vecinos si la red no dispone de un servidor DNS (Sistema de nombres de dominio). La función Respondedor LLMNR funciona en entornos IPv4 o IPv6 cuando se utiliza un ordenador que incluye la función Emisor LLMNR como, por ejemplo, en Windows Vista® y Windows® 7.

Web Services

El protocolo Web Services permite que los usuarios de Windows Vista® o Windows® 7 puedan instalar el controlador de impresora Brother al hacer clic con el botón derecho en el icono del equipo desde la carpeta **Red**. (Consulte *Instalación de Impresión en red cuando utilice los Web Services (Windows Vista® y Windows® 7)* en la página 15). Los Web Services también le permiten comprobar el estado actual del equipo desde su ordenador.

HTTP

El protocolo HTTP se utiliza para transmitir los datos entre un servidor web y un navegador web.



Nota

Para obtener información acerca del protocolo HTTPS, consulte *Protocolos de seguridad* en la página 19.

FTP (Para la función Escanear a FTP)

El Protocolo de transferencia de archivos (FTP) permite al equipo Brother escanear documentos en blanco y negro o en color directamente a un servidor FTP ubicado localmente en la red o en Internet.

SNTP

El protocolo Simple Network Time Protocol se utiliza para sincronizar los relojes del ordenador en una red TCP/IP. Puede realizar la configuración de SNTP mediante el uso de Administración basada en Web (navegador web). (Para obtener más información, consulte la *Guía del usuario en red*).

CIFS

El sistema Common Internet File System es el modo estándar mediante el cual los usuarios de los ordenadores comparten archivos e impresoras en Windows®.

LDAP

El protocolo Lightweight Directory Access Protocol (LDAP) permite que el equipo Brother busque información como, por ejemplo, números de fax y direcciones de correo electrónico desde un servidor LDAP.

IPv6

IPv6 es el protocolo de Internet de próxima generación. Si desea obtener más información sobre el protocolo IPv6, visite la página de modelos y busque el equipo que está utilizando en <http://solutions.brother.com/>.

Otro protocolo

LLTD

El protocolo Link Layer Topology Discovery (LLTD) le permite ubicar fácilmente su equipo Brother en el **Mapa de red** de Windows Vista® o Windows® 7. Su equipo Brother se mostrará con un icono distintivo y el nombre del nodo. De forma predeterminada, este protocolo está desactivado. Puede activar el protocolo LLTD mediante el uso de Administración basada en Web (navegador web) (Consulte la *Guía del usuario en red*) y la utilidad BRAdmin Professional 3. Visite la página de descarga correspondiente a su modelo en el sitio <http://solutions.brother.com/> para descargar BRAdmin Professional 3.

Direcciones IP, máscaras de subred y puertas de acceso

Para utilizar el equipo en un entorno de red TCP/IP, debe configurar su dirección IP y la máscara de subred. La dirección IP que asigne al servidor de impresión debe estar en la misma red lógica que los hosts. Si no es así, debe configurar adecuadamente la máscara de subred y la dirección de la puerta de acceso.

Dirección IP

Una dirección IP es una serie de números que identifican cada dispositivo conectado a una red. Una dirección IP se compone de cuatro números separados por puntos. Cada número está comprendido entre 0 y 255.

■ Ejemplo: en una red pequeña, normalmente cambiaría el número final.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

Cómo se asigna la dirección IP a su servidor de impresión:

Si dispone de un servidor DHCP/BOOTP/RARP en su red, el servidor de impresión obtendrá la dirección IP automáticamente desde dicho servidor.



Nota

En redes más pequeñas, el servidor DHCP puede ser asimismo el enrutador.

Para obtener más información sobre DHCP, BOOTP y RARP, consulte:

Uso de DHCP para configurar la dirección IP en la página 21.

Uso de BOOTP para configurar la dirección IP en la página 23.

Uso de RARP para configurar la dirección IP en la página 22.

Si no dispone de un servidor DHCP/BOOTP/RARP, el protocolo Automatic Private IP Addressing (APIPA) asignará automáticamente una dirección IP del intervalo entre 169.254.1.0 y 169.254.254.255. Para obtener más información acerca de APIPA, consulte *Uso de APIPA para configurar la dirección IP* en la página 23.

Máscara de subred

Las máscaras de subred restringen la comunicación en red.

■ Ejemplo: el Ordenador 1 puede comunicarse con el Ordenador 2

- Equipo 1

Dirección IP: 192.168. 1. 2

Máscara de subred: 255.255.255.000

- Equipo 2

Dirección IP: 192.168. 1. 3

Máscara de subred: 255.255.255.000

Cuando el 0 se encuentra en la Máscara de subred, no existe ningún límite de comunicación en esta parte de la dirección. El ejemplo anterior significa que podemos comunicarnos con cualquier dispositivo cuya dirección IP empiece por 192.168.1.x. (donde x. son números comprendidos entre 0 y 255).

Puerta de acceso (y enrutador)

Una puerta de acceso es un punto de la red que actúa como una entrada a otra red y envía datos transmitidos a través de la red a un destino exacto. El enrutador sabe dónde dirigir los datos que llegan a la puerta de acceso. Si un destino se localiza en una red externa, el enrutador transmite los datos a la red externa. Si su red se comunica con otras redes, puede necesitar configurar la dirección IP de la puerta de acceso. Si no conoce la dirección IP de la puerta de acceso, póngase en contacto con el administrador de red.

Autenticación IEEE 802.1x

IEEE 802.1x es un estándar IEEE para redes cableadas e inalámbricas que limita el acceso desde los dispositivos de red no autorizados. Su equipo Brother (solicitante) envía una solicitud de autenticación a un servidor RADIUS (servidor de autenticaciones) a través de su punto de acceso (autenticador). Una vez que el servidor RADIUS haya verificado la solicitud, su equipo podrá acceder a la red.

Métodos de autenticación

■ LEAP (Para redes inalámbricas)

Cisco Systems, Inc. ha desarrollado el protocolo Cisco LEAP (Protocolo ligero de autenticación extensible), que utiliza identificaciones de usuario y contraseñas para la autenticación.

■ EAP-FAST

Cisco Systems, Inc. ha desarrollado el protocolo EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunnel), que utiliza identificaciones de usuario y contraseñas para la autenticación, así como algoritmos de clave simétrica para obtener un proceso de autenticación de túnel.

El equipo Brother admite las siguientes autenticaciones internas:

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

■ EAP-MD5 (Para redes cableadas)

El protocolo EAP-MD5 (Extensible Authentication Protocol-Message digest algorithm 5) utiliza identificaciones de usuario y contraseñas para una autenticación basada en cuestiones y respuestas.

■ PEAP

Microsoft Corporation, Cisco Systems y RSA Security han desarrollado el protocolo PEAP (Protected Extensible Authentication Protocol). El protocolo PEAP crea un túnel encriptado por SSL (Secure Socket Layer, capa de sockets seguros)/TLS (Transport Layer Security, seguridad de la capa de transporte) entre un cliente y un servidor de autenticación, para enviar una identificación de usuario y una contraseña. El protocolo PEAP crea una autenticación mutua entre el servidor y el cliente.

El equipo Brother admite las siguientes autenticaciones internas:

- PEAP/MS-CHAPv2
- PEAP/GTC

■ EAP-TTLS

Funk Software y Certicom han desarrollado el protocolo EAP-TTLS (Extensible Authentication Protocol Tunneled Transport Layer Security). El protocolo EAP-TTLS crea un túnel encriptado por SSL similar al que crea el protocolo PEAP, entre un cliente y un servidor de autenticación, para enviar una identificación de usuario y una contraseña. El protocolo EAP-TTLS crea una autenticación mutua entre el servidor y el cliente.

El equipo Brother admite las siguientes autenticaciones internas:

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

■ EAP-TLS

El protocolo EAP-TLS (Extensible Authentication Protocol Transport Layer Security) requiere una autenticación mediante certificado digital tanto del cliente como del servidor de autenticación.

Especificación de la red

SSID (Identificador de conjunto de servicios) y canales

Es necesario que configure el SSID y un canal para especificar la red inalámbrica a la que desea conectar.

■ SSID

Cada red inalámbrica tiene su propio nombre de red y se conoce técnicamente como SSID o ESSID (Identificador de conjunto de servicios ampliado). El SSID tiene un valor de 32 bytes o menos y está asignado al punto de acceso. Los dispositivos de red inalámbrica que desee asociar a la red inalámbrica deben tener el mismo punto de acceso. El punto de acceso y los dispositivos de red inalámbrica envían regularmente paquetes inalámbricos (conocidos como baliza) que tienen la información SSID. Cuando su dispositivo de red inalámbrica recibe una baliza, puede identificar la red inalámbrica que esté lo suficientemente cerca para que las ondas de radiofrecuencia alcancen su dispositivo.

■ Canales

Las redes inalámbricas emplean canales. Cada canal inalámbrico tiene una frecuencia diferente. En una red inalámbrica se pueden utilizar hasta 14 canales diferentes. Sin embargo, en muchos países el número de canales disponibles está restringido.

Términos de seguridad

Autenticación y encriptación

La mayoría de las redes inalámbricas utilizan algún tipo de configuración de seguridad. Estas configuraciones de seguridad definen la autenticación (el modo en que el dispositivo en sí se identifica en la red) y la encriptación (el modo en que los datos se cifran a medida que se envían por la red). **Si no especifica correctamente estas opciones cuando realice la configuración de su equipo inalámbrico Brother, este no podrá conectarse a la red inalámbrica.** En cualquier caso, debe prestar atención cuando configure estas opciones. Consulte la información de la *Guía del usuario en red* para ver los métodos de autenticación y encriptación que admite su equipo inalámbrico Brother.

Métodos de autenticación y encriptación para una red inalámbrica personal

Una red inalámbrica personal es una red pequeña, por ejemplo, si utiliza su equipo en una red inalámbrica doméstica, sin compatibilidad con el estándar IEEE 802.1x.

Si desea utilizar su equipo en una red inalámbrica compatible con el estándar IEEE 802.1x, consulte *Métodos de autenticación y encriptación para una red inalámbrica corporativa* en la página 13.

Métodos de autenticación

■ Sistema abierto

Se permite el acceso a la red a dispositivos inalámbricos sin ninguna autenticación.

■ Clave compartida

Todos los dispositivos que acceden a la red inalámbrica comparten una clave predeterminada secreta.

El equipo inalámbrico Brother utiliza la clave WEP como clave predeterminada.

■ WPA-PSK/WPA2-PSK

Activa una clave precompartida de acceso protegido Wi-Fi (WPA-PSK/WPA2-PSK), que permite al equipo inalámbrico Brother asociarse con puntos de acceso mediante TKIP para WPA-PSK o AES para WPA-PSK y WPA2-PSK (WPA-Personal).

Métodos de encriptación

■ Ninguna

No se utiliza ningún método de encriptación.

■ WEP

Al utilizar WEP (Privacidad equivalente a cableado), los datos se transmiten y se reciben con una clave segura.

■ TKIP

El protocolo TKIP (Temporal Key Integrity Protocol) proporciona una clave por paquete que mezcla una comprobación de integridad de mensajes y un mecanismo que vuelve a crear claves.

■ AES

El protocolo AES (Advanced Encryption Standard) es un potente estándar de encriptación autorizado por Wi-Fi®.

Clave de red

■ Sistema abierto/Clave compartida con WEP

Esta clave consiste en un valor de 64 bits o 128 bits que debe introducirse en formato ASCII o hexadecimal.

- ASCII de 64 (40) bits:

Utiliza 5 caracteres de texto, por ejemplo, “WSLAN” (distingue entre mayúsculas y minúsculas).

- Hexadecimal de 64 (40) bits:

Utiliza 10 dígitos de datos hexadecimales, por ejemplo, “71f2234aba”.

- ASCII de 128 (104) bits:

Utiliza 13 caracteres de texto, por ejemplo, “Wirelesscomms” (distingue entre mayúsculas y minúsculas).

- Hexadecimal de 128 (104) bits:

Utiliza 26 dígitos de datos hexadecimales, por ejemplo, “71f2234ab56cd709e5412aa2ba”.

■ WPA-PSK/WPA2-PSK y TKIP o AES

Utiliza una clave precompartida (PSK) que tiene 8 o más caracteres de longitud, hasta un máximo de 63 caracteres.

Métodos de autenticación y encriptación para una red inalámbrica corporativa

Una red inalámbrica corporativa es una red extensa, por ejemplo, si utiliza su equipo en una red inalámbrica corporativa empresarial, compatible con el estándar IEEE 802.1x. Si configura su equipo en una red inalámbrica compatible con el estándar IEEE 802.1x, podrá utilizar los siguientes métodos de autenticación y encriptación.

Métodos de autenticación

■ LEAP

Para obtener información sobre el protocolo LEAP, consulte *LEAP (Para redes inalámbricas)* en la página 9.

■ EAP-FAST

Para obtener información sobre el protocolo EAP-FAST, consulte *EAP-FAST* en la página 9.

■ PEAP

Para obtener información sobre el protocolo PEAP, consulte *PEAP* en la página 9.

■ EAP-TTLS

Para obtener información sobre el protocolo EAP-TTLS, consulte *EAP-TTLS* en la página 10.

■ EAP-TLS

Para obtener información sobre el protocolo EAP-TLS, consulte *EAP-TLS* en la página 10.

Métodos de encriptación

- TKIP

Para obtener información sobre el protocolo TKIP, consulte *TKIP* en la página 12.

- AES

Para obtener información sobre el sistema AES, consulte *AES* en la página 12.

- CKIP

El protocolo de integridad de clave original para LEAP de Cisco Systems, Inc.

ID de usuario y contraseña

Los siguientes métodos de seguridad utilizan menos de 64 caracteres de longitud en la identificación de usuario y menos de 32 caracteres en la contraseña.

- LEAP

- EAP-FAST

- PEAP

- EAP-TTLS

- EAP-TLS (Para la ID de usuario)

Tipos de configuración de red adicional

Si desea configurar una configuración de red adicional, las siguientes funciones están disponibles para su uso.

- Web Services (Windows Vista® y Windows® 7)
- Vertical Pairing (Emparejamiento vertical) (Windows® 7)



Nota

Verifique que el host y el equipo se encuentran en la misma subred o que el enrutador está configurado correctamente para pasar los datos entre los dos dispositivos.

Instalación de Impresión en red cuando utilice los Web Services (Windows Vista® y Windows® 7)

La función Web Services le permite controlar la información del equipo que está conectado a la red. Asimismo, esto activa la instalación del controlador de impresora desde el icono de la impresora y se creará el puerto Web Services (puerto WSD).



Nota

- Debe configurar la dirección IP en su equipo antes de realizar esta configuración.
- Para Windows Server® 2008, debe instalar Print Services.
- Sólo se instala la asistencia de la impresora con servicios web.

- 1 Inserte el CD-ROM de instalación.
- 2 Elija su unidad de CD-ROM/**install/driver/gdi/32** o **64**.
- 3 Elija su idioma y, a continuación, haga doble clic en **DPIInst.exe**.



Nota

Si aparece la pantalla **Control de cuentas de usuario**,
(Windows Vista®) Haga clic en **Permitir**.
(Windows® 7) Haga clic en **Sí**.

- 4 (Windows Vista®)
Haga clic en , y a continuación, elija **Red**.
(Windows® 7)
Haga clic en , **Panel de control, Redes e Internet** y a continuación, en **Ver los equipos y dispositivos de red**.
- 5 Aparecerá el nombre de los Web Services del equipo con el icono de la impresora. Haga clic con el botón derecho en el equipo que desea instalar.



Nota

El nombre de los Web Services para el equipo Brother es el nombre del modelo y la dirección MAC (dirección Ethernet) del equipo (por ejemplo, Brother MFC-XXXX (nombre del modelo) [XXXXXXXXXXXX] (Dirección MAC/Dirección Ethernet)).

- 6 En el menú desplegable, haga clic en **Instalar**.

Instalación de impresión en red para el modo Infraestructura cuando utilice Vertical Pairing (Emparejamiento vertical) (Windows® 7)

Windows® Vertical Pairing (Emparejamiento vertical de Windows®) es una tecnología que permite que un equipo inalámbrico compatible con la función Vertical Pairing (Emparejamiento vertical) se conecte a la red Infraestructura mediante el Método PIN de Wi-Fi Protected Setup y la función servicios web. Esto también permite la instalación del controlador de impresora desde el icono de impresora que aparece en la pantalla **Agregar un dispositivo**.

Si se encuentra en modo Infraestructura, puede conectar su equipo a la red inalámbrica y, a continuación, instalar el controlador de impresora mediante esta función. Siga los pasos que se indican a continuación:



Nota

- Si ha establecido la función Web Services del equipo en No, debe volver a establecerla en Sí. La configuración predeterminada de Web Services para el equipo Brother es Sí. Puede cambiar la configuración de Web Services mediante el uso de Administración basada en Web (navegador web) o BRAdmin Professional 3.
- Asegúrese de que su punto de acceso/enrutador WLAN incluye el logotipo de compatibilidad con Windows® 7. Si no está seguro sobre el logotipo de compatibilidad que se requiere, póngase en contacto con el fabricante del punto de acceso o enrutador.
- Asegúrese que su ordenador incluye el logotipo de compatibilidad con Windows® 7. Si no está seguro sobre el logotipo de compatibilidad que se requiere, póngase en contacto con el fabricante de su ordenador.
- Si configura la red inalámbrica mediante una NIC inalámbrica externa (Tarjeta de interfaz de red), asegúrese que la NIC inalámbrica incluye el logotipo de compatibilidad con Windows® 7. Si desea obtener más información, póngase en contacto con el fabricante de su NIC inalámbrica.
- Para usar un ordenador con Windows® 7 como Registrador, tiene que registrarlo en su red de antemano. Consulte la instrucción suministrada con su punto de acceso/enrutador WLAN.

- 1 Encienda el equipo.
- 2 Establezca el equipo en Wi-Fi Protected Setup (Método PIN). Consulte la configuración inalámbrica de Wi-Fi Protected Setup (Método PIN) en la *Guía del usuario en red*, sobre cómo establecer el equipo en el Método PIN.
- 3 Haga clic en el botón  y, a continuación, seleccione **Dispositivos e impresoras**.
- 4 Seleccione **Agregar un dispositivo** en el cuadro de diálogo **Dispositivos e impresoras**.
- 5 Elija su equipo e introduzca el PIN indicado para él.
- 6 Seleccione la red Infraestructura a la que desea conectar y, a continuación, haga clic en **Siguiente**.
- 7 Cuando el equipo aparezca en el cuadro de diálogo **Dispositivos e impresoras**, la configuración inalámbrica y la instalación del controlador de impresora habrán finalizado correctamente.

Funciones de seguridad

Terminología de seguridad

■ CA (Certificate Authority, entidad de certificación)

Una CA es una entidad que emite certificados digitales (especialmente certificados X.509) y garantiza la vinculación de los elementos de datos de un certificado.

■ CSR (Certificate Signing Request, solicitud de firma de certificado)

CSR es un mensaje enviado desde un solicitante a una CA para solicitar la emisión de un certificado. La CSR contiene información que permite identificar al solicitante, la clave pública generada por este y su firma digital.

■ Certificado

Un certificado es la información que vincula una clave pública con una identidad. El certificado puede utilizarse para comprobar que una clave pública pertenece a un individuo. El formato viene definido por el estándar x.509.

■ Certificado CA (Certificate Authority, entidad de certificación)

Un Certificado CA es la certificación que identifica la propia CA (Certificate Authority, entidad de certificación) y es el propietario de sus claves privadas. Asimismo, verifica los certificados emitidos por la CA.

■ Firma digital

Una firma digital es un valor calculado con un algoritmo criptográfico y añadido a un objeto de datos para que cualquier destinatario de los datos pueda utilizar la firma para comprobar el origen y la integridad de los datos.

■ Sistema criptográfico de clave pública

Un sistema criptográfico de clave pública es una rama moderna de la criptografía en la que los algoritmos emplean un par de claves (una clave pública y una privada) y utilizan un componente diferente del par para los distintos pasos del algoritmo.

■ Sistema criptográfico de clave compartida

Un sistema criptográfico de clave compartida es una rama de la criptografía que implica la utilización de algoritmos que emplean la misma clave para dos pasos diferentes del algoritmo (como para el cifrado y el descifrado).

Protocolos de seguridad



Nota

Puede realizar la configuración del protocolo mediante el uso de Administración basada en Web (navegador web). Para obtener más información, consulte la *Guía del usuario en red*.

SSL (Secure Socket Layer, capa de sockets seguros)/TLS (Transport Layer Security, seguridad de la capa de transporte)

Estos protocolos de comunicación de seguridad cifran datos para prevenir amenazas de seguridad.

HTTPS

El protocolo de Internet que emplea HTTP (Hyper Text Transfer Protocol, protocolo de transferencia de hipertexto) es SSL.

IPPS

El protocolo de impresión que utiliza el Internet Printing Protocol (IPP versión 1.0) es SSL.

SNMPv3

El SNMPv3 (Simple Network Management Protocol versión 3, protocolo simple de administración de redes versión 3) ofrece autenticación de usuario y cifrado de datos para administrar dispositivos de red de manera segura.

Métodos de seguridad para el envío y la recepción de correos electrónicos



Nota

Puede realizar la configuración de los métodos de seguridad mediante el uso de Administración basada en Web (navegador web). Para obtener más información, consulte la *Guía del usuario en red*.

POP antes de SMTP (PbS)

Es el método de autenticación de usuarios para enviar correos electrónicos desde un cliente. El cliente recibe permiso para utilizar el servidor SMTP mediante el acceso al servidor POP3 antes de enviar el correo electrónico.

SMTP-AUTH (Autenticación SMTP)

SMTP-AUTH amplía el protocolo SMTP (el protocolo de envío de correo electrónico por Internet) para incluir un método de autenticación que asegure que se conoce la identidad real del remitente.

APOP (Authenticated Post Office Protocol)

APOP amplía el protocolo POP3 (el protocolo de recepción por Internet) para incluir un método de autenticación que encripta la contraseña cuando el cliente recibe correos electrónicos.

SMTP sobre SSL

La función SMTP sobre SSL permite el envío de correos electrónicos encriptados mediante SSL.

POP sobre SSL

La función POP sobre SSL permite la recepción de correos electrónicos encriptados mediante SSL.

Utilización de servicios

Un servicio es un recurso al que se puede acceder a través de ordenadores que desean imprimir en el servidor de impresión Brother. El servidor de impresión Brother proporciona los siguientes servicios predefinidos (realice un comando `SHOW SERVICE` en la consola remota del servidor de impresión Brother para ver una lista de los servicios disponibles): introduzca `HELP` cuando se le solicite un comando para obtener una lista de comandos admitidos.

Servicio (Ejemplo)	Definición
BINARY_P1	Servicio binario TCP/IP
TEXT_P1	Servicio de texto TCP/IP (añade un retorno de carro después de cada línea)
PCL_P1	Servicio PCL (conmuta el equipo compatible con PjL al modo PCL)
BRNxxxxxxxxxxxx	Servicio binario TCP/IP
BRNxxxxxxxxxxxx_AT	Servicio PostScript® para Macintosh
POSTSCRIPT_P1	Servicio PostScript® (conmuta el equipo compatible con PjL al modo PostScript®)

Donde “xxxxxxxxxxxx” es la dirección MAC del equipo (dirección Ethernet).

Otras formas de establecer la dirección IP (para usuarios avanzados y administradores)

Uso de DHCP para configurar la dirección IP

El protocolo Dynamic Host Configuration Protocol (DHCP) es uno de los diversos mecanismos automatizados para la asignación de direcciones IP. Si dispone de un servidor DHCP en la red, el servidor de impresión obtendrá de forma automática su dirección IP desde el servidor DHCP y registrará el nombre con cualquier servicio de nombres dinámico que cumpla con las normas RFC 1001 y 1002.



Nota

Si no desea que el servidor de impresión se configure a través de DHCP, BOOTP o RARP, deberá establecer la opción Método de arranque como Estático para que el servidor de impresión tenga una dirección IP estática. Esto evitará que el servidor de impresión intente obtener una dirección IP desde cualquiera de estos sistemas. Para cambiar el Método de arranque, utilice el menú de red del panel de control del equipo (para los modelos con pantalla LCD), las aplicaciones BRAdmin, la Configuración remota o Administración basada en Web (navegador web).

Uso de RARP para configurar la dirección IP

La dirección IP del servidor de impresión Brother se puede configurar mediante la utilidad Reverse ARP (RARP) del host. Se realiza mediante la edición del archivo `/etc/ethers` (si no existe este archivo, puede crearlo) con una entrada como la indicada a continuación:

```
00:80:77:31:01:07    BRN008077310107 (o BRW008077310107 para una red inalámbrica)
```

Donde la primera entrada es la dirección MAC (dirección Ethernet) del servidor de impresión y la segunda entrada es el nombre del servidor de impresión (el nombre debe coincidir con el que se introdujo en el archivo `/etc/hosts`).

Si el centinela RARP todavía no se está ejecutando, inícielo (en función del sistema, el comando puede ser `rarpd`, `rarpd -a`, `in.rarpd -a` o un comando parecido; escriba `man rarpd` o consulte la documentación del sistema para obtener información adicional). Para comprobar que el centinela RARP se está ejecutando en un sistema basado en UNIX de Berkeley, escriba el siguiente comando:

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

Para sistemas basados en UNIX de AT&T, escriba:

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

El servidor de impresión Brother tomará la dirección IP del centinela RARP cuando se encienda el equipo.

Uso de BOOTP para configurar la dirección IP

BOOTP es una alternativa al comando RARP que tiene la ventaja de permitir la configuración de la máscara de subred y de la puerta de acceso. Para poder utilizar BOOTP para configurar la dirección IP, asegúrese de que BOOTP está instalado y activo en el host (debe aparecer en el archivo `/etc/services` en el host como un servicio real; escriba `man bootpd` o consulte la documentación del sistema para obtener más información). BOOTP se inicia normalmente a través del archivo `/etc/inetd.conf`, de manera que deberá activarlo eliminando la “#” situada delante de la entrada de `bootp` en dicho archivo. Por ejemplo, una entrada BOOTP típica en el archivo `/etc/inetd.conf` podría ser:

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

En función del sistema, esta entrada puede aparecer como “bootps” en lugar de “bootp”.



Nota

Para poder activar BOOTP, simplemente utilice un editor para eliminar “#” (si no aparece el carácter “#”, significa que BOOTP ya está activado). A continuación, edite el archivo de configuración de BOOTP (normalmente denominado `/etc/bootptab`) e introduzca el nombre, el tipo de red (1 para Ethernet), la dirección MAC (dirección Ethernet) y la dirección IP, la máscara de subred y la puerta de acceso del servidor de impresión. Lamentablemente, el formato exacto para realizar esta acción no es estándar, de manera que deberá consultar la documentación del sistema para determinar cómo introducir esta información (muchos sistemas UNIX disponen de ejemplos de plantillas en el archivo `bootptab` que se pueden utilizar como referencia). Algunos ejemplos de entradas típicas de `/etc/bootptab` son: (“BRN” a continuación es “BRW” para una red inalámbrica).

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

y:

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

Algunas implementaciones de software del host de BOOTP no responderán a las solicitudes de BOOTP si no se ha incluido un nombre de archivo de descarga en el archivo de configuración. Si éste es el caso, cree un archivo nulo en el host y especifique el nombre de este archivo y su ruta en el archivo de configuración.

De la misma forma que con el comando RARP, el servidor de impresión cargará su dirección IP desde el servidor BOOTP al encender la impresora.

Uso de APIPA para configurar la dirección IP

El servidor de impresión Brother admite el protocolo de direccionamiento automático de direcciones IP privadas (APIPA). Con APIPA, los clientes DHCP configuran automáticamente una dirección IP y una máscara de subred cuando no hay ningún servidor DHCP disponible. El dispositivo selecciona su propia dirección IP en el intervalo de direcciones entre 169.254.1.0 y 169.254.254.255. La máscara de subred se establece automáticamente en 255.255.0.0 y la puerta de acceso en 0.0.0.0.

El protocolo APIPA está activado de forma predeterminada. Si desea desactivar el protocolo APIPA, puede hacerlo mediante el panel de control panel del equipo (para los modelos con pantalla LCD), BRAdmin Light o Administración basada en Web (navegador web).

Uso de ARP para configurar la dirección IP

Si no puede utilizar la aplicación BRAdmin y su red no utiliza un servidor DHCP, puede utilizar también el comando ARP. El comando ARP está disponible en sistemas Windows® que tengan instalado TCP/IP, así como en sistemas UNIX. Para utilizar ARP, escriba el siguiente comando en el símbolo del sistema:

```
arp -s direccionip direccionethernet  
ping direccionip
```

Donde `direccionethernet` es la dirección MAC (dirección Ethernet) del servidor de impresión y `direccionip` es la dirección IP del servidor de impresión. Por ejemplo:

■ Sistemas Windows®

Los sistemas Windows® requieren el carácter de guión “-” entre cada dígito de la dirección MAC (dirección Ethernet).

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

■ Sistemas UNIX/Linux

Normalmente, los sistemas UNIX y Linux requieren el carácter de dos puntos “:” entre cada dígito de la dirección MAC (dirección Ethernet).

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



Nota

Debe encontrarse en el mismo segmento Ethernet (es decir, no puede haber un enrutador entre el servidor de impresión y el sistema operativo) para utilizar el comando `arp -s`.

Si hay un enrutador, deberá utilizar BOOTP u otros métodos descritos en este capítulo para introducir la dirección IP. Si el administrador ha configurado el sistema para entregar direcciones IP utilizando BOOTP, DHCP o RARP, el servidor de impresión Brother podrá recibir una dirección IP desde cualquiera de estos sistemas de asignación de direcciones IP. En este caso, no tendrá que utilizar el comando ARP. El comando ARP sólo funciona una vez. Por razones de seguridad, una vez que se ha logrado configurar con éxito la dirección IP de un servidor de impresión Brother mediante el comando ARP, no se puede volver a utilizar este comando para modificar la dirección. El servidor de impresión ignorará cualquier intento de modificación. Si desea cambiar de nuevo la dirección IP, utilice Administración basada en Web (navegador web) o TELNET (mediante el comando SET IP ADDRESS), o restaure los valores de fábrica del servidor de impresión (de esta forma podrá volver a utilizar el comando ARP).

Uso de la consola TELNET para configurar la dirección IP

También puede servirse del comando TELNET para cambiar la dirección IP.

TELNET es un eficaz método para cambiar la dirección IP del equipo. Pero es necesario que haya una dirección IP válida ya programada en el servidor de impresión.

Escriba `TELNET <línea de comando>` en el símbolo de sistema, donde `<línea de comando>` es la dirección IP del servidor de impresión. Cuando esté conectado, pulse la tecla Retorno o Intro para obtener el símbolo "#". Introduzca la contraseña "**access**" (la contraseña no aparecerá en la pantalla).

Se le solicitará un nombre de usuario. Introduzca cualquier cosa en respuesta a esta solicitud.

Aparecerá el símbolo de sistema `Local>`. Escriba `SET IP ADDRESS direccionip`, donde `direccionip` es la dirección IP que desea asignar al servidor de impresión (consulte al administrador de la red cuáles son las direcciones IP que puede utilizar). Por ejemplo:

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

Debe introducir la máscara de subred mediante la entrada `SET IP SUBNET subnet mask`, donde `subnet mask` es la máscara de subred que desea asignar al servidor de impresión (consulte al administrador de la red cuál es la máscara de subred que debe utilizar). Por ejemplo:

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

Si no tiene ninguna subred, utilice una de las siguientes máscaras de subred predeterminadas:

255.0.0.0 para redes de clase A

255.255.0.0 para redes de clase B

255.255.255.0 para redes de clase C

El grupo de dígitos más a la izquierda de la dirección IP pueden identificar el tipo de red. El valor de este grupo va desde 1 hasta 127 para redes de clase A (por ej., 13.27.7.1), desde 128 hasta 191 para redes de clase B (por ej., 128.10.1.30) y desde 192 hasta 255 para redes de clase C (por ej., 192.168.1.4).

Si dispone de una puerta de acceso (enrutador), introduzca su dirección con el comando `SET IP ROUTER direccionenrutador`, donde `direccionenrutador` es la dirección IP de la puerta de acceso que desea asignar al servidor de impresión. Por ejemplo:

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

Escriba `SET IP METHOD STATIC` para establecer el método de configuración de acceso IP como estático.

Para verificar que ha introducido correctamente la información IP, escriba `SHOW IP`.

Escriba `EXIT` o Ctrl-D (o sea, mantenga pulsada la tecla Control y pulse la letra "D") para finalizar la sesión de consola remota.

A

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

B

BINARY_P1	21
BOOTP	3, 23
BRNxxxxxxxxxxxx	21
BRNxxxxxxxxxxxx_AT	21

C

CA	18
Canales	11
Certificado	18
Certificado CA	18
CIFS	6
CKIP	14
Clave compartida	12
Clave de red	13
Ciente DNS	4
Ciente SMTP	4
CSR	18
Custom Raw Port	4

D

DHCP	3, 21
Dirección IP	7
Dirección MAC	16, 21, 22, 23, 24

E

EAP-FAST	9
EAP-MD5	9
EAP-TLS	10
EAP-TTLS	10
Encriptación	12

F

Firma digital	18
FTP	5

H

HTTP	5
HTTPS	19

I

IEEE 802.1x	9
Impresión compartida de red	2
Impresión en red	15
Impresión TCP/IP	15
IPP	4
IPPS	19
IPv6	6

L

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

M

Máscara de subred	8
mDNS	4

P

PCL_P1	21
PEAP	9
POP antes de SMTP	20
POP sobre SSL	20
POSTSCRIPT_P1	21
Protocolo	3
Puerto 9100	4
Punto a punto	1

R

RARP	3, 22
Red inalámbrica	11
Resolución de nombres NetBIOS	4
RFC 1001	21

S

Servicios	21
Sistema abierto	12
Sistema criptográfico de clave compartida	18
Sistema criptográfico de clave pública	18
SMTP sobre SSL	20
SMTP-AUTH	20
SNMP	5
SNMPv3	19
SNTP	6
SSID	11
SSL/TLS	19

T

TCP/IP	3
TELNET	5, 25
Terminología de seguridad	18
TEXT_P1	21
TKIP	12

V

Vertical Pairing (Emparejamiento vertical)	15
--	----

W

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