

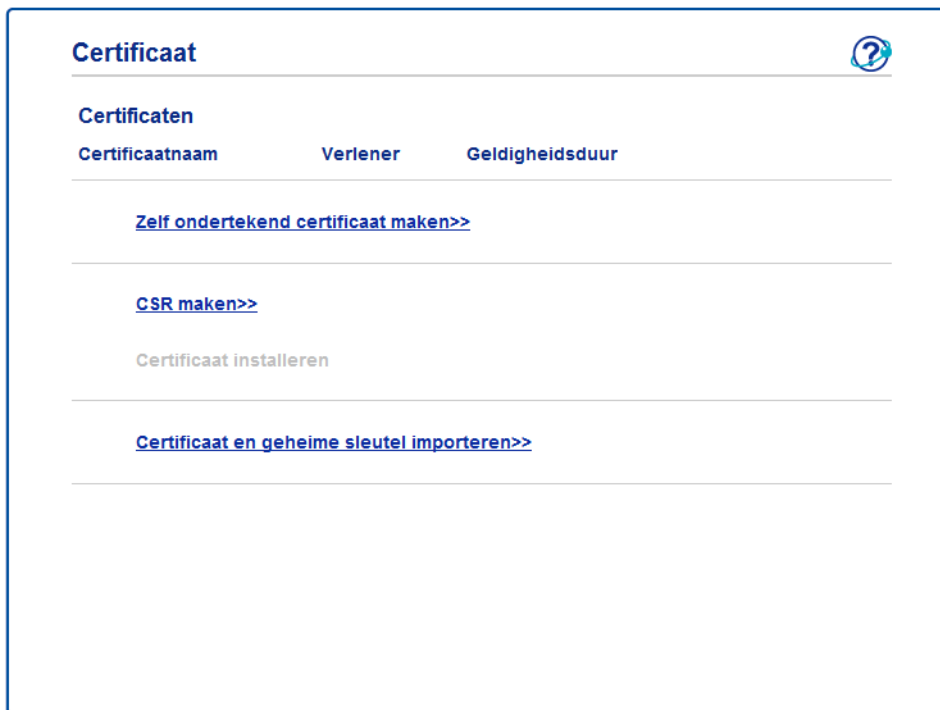
OPMERKING

- Als u gebruik wilt maken van SSL/TLS-communicatie, raden we u aan eerst uw systeembeheerder te contacteren.
 - Wanneer u de fabrieksinstellingen herstelt van de afdrukserver, worden het geïnstalleerde certificaat en de geïnstalleerde private sleutel gewist. Als u hetzelfde certificaat en dezelfde private sleutel wilt behouden na het herstellen van de fabrieksinstellingen op de afdrukserver, dient u deze vóór het herstellen te exporteren en nadien opnieuw te installeren. (Zie *Het door uzelf ondertekende certificaat, het certificaat uitgevaardigd door een CA en de geheime sleutel exporteren* ►► pagina 71.)
-

Een certificaat configureren met Beheer via een webbrowser

Deze functie kan alleen worden geconfigureerd via Beheer via een webbrowser. Volg deze stappen om de pagina voor het configureren van een certificaat te openen met Beheer via een webbrowser.

- 1 Start uw webbrowser.
- 2 Voer "http://IP-adres van de machine/" in de adresregel van uw browser (waarbij "IP-adres van de machine" staat voor het IP-adres van de machine of de naam van de afdrukserver).
 - Bijvoorbeeld: http://192.168.1.2/
- 3 Er dient standaard geen wachtwoord te worden ingevoerd. Als u voordien een wachtwoord hebt ingesteld, voert u dit in en drukt u op .
- 4 Klik op **Netwerk**.
- 5 Klik op **Beveiliging**.
- 6 Klik op **Certificaat**.
- 7 U kunt de certificaatinstellingen configureren op onderstaand scherm.



Certificaat 

Certificaten

Certificaatnaam	Verlener	Geldigheidsduur
Zelf ondertekend certificaat maken>>		
CSR maken>>		
Certificaat installeren		
Certificaat en geheime sleutel importeren>>		

OPMERKING

- De functies die uitgeschakeld zijn en waarop u niet kunt klikken, zijn niet beschikbaar.
- Raadpleeg de helptekst in Beheer via een webbrowser voor meer informatie over het configureren.

Een certificaat aanmaken en installeren

Schema voor het stap voor stap aanmaken en installeren van een certificaat



6

Een certificaat dat door uzelf is ondertekend aanmaken en installeren

- 1 Klik op **Zelf ondertekend certificaat maken** op de pagina **Certificaat**.
- 2 Voer een **Algemene naam** en een **Geldigheidsdatum** in.

OPMERKING

- De lengte van de **Algemene naam** moet minder dan 64 tekens bedragen. Voer een identifier in zoals een IP-adres, naam van een knooppunt of domeinnaam die u zult gebruiken om toegang te krijgen tot deze machine via SSL/TLS-communicatie. De naam van het knooppunt wordt standaard weergegeven.
- Een waarschuwing wordt weergegeven als u het IPPS- of HTTPS-protocol gebruikt en een andere naam in de URL invoert dan de **Algemene naam** die werd gebruikt voor het certificaat door uzelf ondertekend.

- 3 U kunt de instellingen **Algoritme van openbare sleutel** en **Digest-algoritme** selecteren in de keuzelijst. De standaardinstellingen zijn **RSA (2048-bits)** voor **Algoritme van openbare sleutel** en **SHA256** voor **Digest-algoritme**.
- 4 Klik op **Indienen**.

- 5 Het certificaat door uzelf ondertekend is met succes aangemaakt en opgeslagen in het geheugen van uw machine.
Om SSL/TLS-communicatie te kunnen gebruiken, moet het certificaat dat u zelf hebt ondertekend eveneens op uw computer worden geïnstalleerd. Raadpleeg *Het certificaat door uzelf ondertekend installeren op uw computer* >> pagina 65 voor meer informatie hierover.

Een CSR aanmaken

- 1 Klik op **CSR maken** op de pagina **Certificaat**.
- 2 Voer een **Algemene naam** en uw informatie in, zoals **Organisatie**.

OPMERKING

- Het is aan te raden dat het hoofdcertificaat van de CA reeds geïnstalleerd is op de computer voor u de CSR aanmaakt.
- De lengte van de **Algemene naam** moet minder dan 64 tekens bedragen. Voer een identicator in zoals een IP-adres, naam van een knooppunt of domeinnaam die u zult gebruiken om toegang te krijgen tot deze printer via SSL/TLS-communicatie. De naam van het knooppunt wordt standaard weergegeven. De **Algemene naam** is vereist.
- Een waarschuwing wordt weergegeven als u een andere naam in de URL invoert dan de openbare naam die werd gebruikt voor het certificaat.
- De lengte van de **Organisatie**, de **Organisatorische eenheid**, de **Plaats** en de **Provincie** moet minder dan 64 tekens bevatten.
- De **Land/Regio** moet een landcode zijn die voldoet aan ISO 3166 en bestaat uit twee tekens.
- Als u X.509v3-certificaatextensie configureert, selecteert u het vakje **Uitgebreide partitie configureren** en kiest u vervolgens **Automatisch (IPv4 registreren)** of **Handmatig**.

- 3 U kunt de instellingen **Algoritme van openbare sleutel** en **Digest-algoritme** selecteren in de keuzelijst. De standaardinstellingen zijn **RSA (2048-bits)** voor **Algoritme van openbare sleutel** en **SHA256** voor **Digest-algoritme**.
- 4 Klik op **Indienen**.
- 5 Wanneer de inhoud van de CSR verschijnt, klikt u op **Opslaan** om het CSR-bestand op te slaan op uw computer.

6 De CSR is aangemaakt.

OPMERKING

- Volg het beleid van uw CA inzake de methode om een CSR te sturen naar uw CA.
- Als u gebruik maakt van Basis-CA van onderneming van Windows Server® 2003/2008/2012, raden wij u aan de **Webserver** te gebruiken als certificaatsjabloon voor het aanmaken van het cliëntcertificaat voor veilig beheer. Als u een cliëntcertificaat aanmaakt voor een IEEE 802.1x-omgeving met EAP-TLS-verificatie, raden wij u aan **Gebruiker** te gebruiken als certificaatsjabloon. Meer informatie vindt u op de SSL-communicatiepagina van de bovenste pagina voor uw model op <http://solutions.brother.com/>.

Het certificaat installeren op uw machine

Wanneer u een certificaat ontvangt van een CA, volgt u onderstaande stappen om het te installeren op de afdrukserver.

OPMERKING

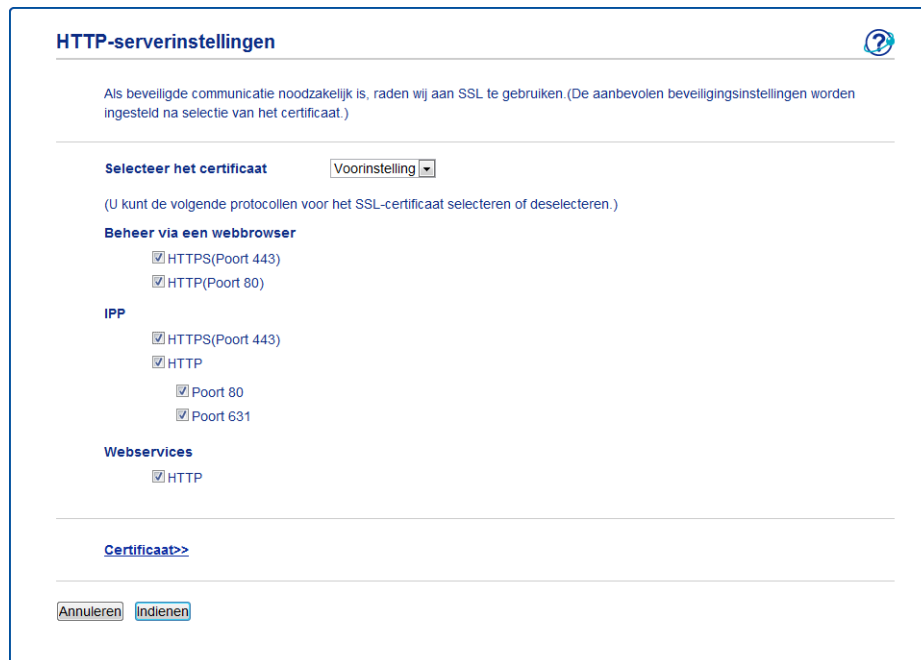
Alleen een certificaat die uitgevaardigd is met de CSR van deze machine kan worden geïnstalleerd. Als u een andere CSR wilt aanmaken, dient u ervoor te zorgen dat het certificaat geïnstalleerd is voor u een andere CSR aanmaakt. Maak een andere CSR aan na het installeren van het certificaat op de machine. Doet u dit niet, dan zal de CSR die u hebt aangemaakt vóór de installatie ongeldig zijn.

- 1 Klik op **Certificaat installeren** op de pagina **Certificaat**.
- 2 Specificeer het bestand van het certificaat dat werd uitgevaardigd door een CA en klik daarna op **Indienen**.
- 3 Het certificaat is nu met succes aangemaakt en opgeslagen in het geheugen van uw machine. Om SSL/TLS-communicatie te kunnen gebruiken, moet het hoofdcertificaat van de CA eveneens op uw computer worden geïnstalleerd. Neem contact op met uw netwerkbeheerder voor de installatie.

Het certificaat kiezen

Zodra u het certificaat hebt geïnstalleerd, volgt u onderstaande stappen om het certificaat te kiezen dat u wilt gebruiken.

- 1 Klik op **Netwerk**.
- 2 Klik op **Protocol**.
- 3 Klik op **HTTP-serverinstellingen** en kies vervolgens het certificaat uit het keuzemenu **Selecteer het certificaat**.



The screenshot shows the 'HTTP-serverinstellingen' (HTTP server settings) window. At the top, there is a header with the title 'HTTP-serverinstellingen' and a help icon. Below the header, a message states: 'Als beveiligde communicatie noodzakelijk is, raden wij aan SSL te gebruiken. (De aanbevolen beveiligingsinstellingen worden ingesteld na selectie van het certificaat.)'. The main section is titled 'Selecteer het certificaat' and includes a dropdown menu currently set to 'Voorinstelling'. A note below says: '(U kunt de volgende protocollen voor het SSL-certificaat selecteren of deselecteren.)'. There are three sections of checkboxes: 'Beheer via een webbrowser' with 'HTTPS(Poort 443)' and 'HTTP(Poort 80)' checked; 'IPP' with 'HTTPS(Poort 443)', 'HTTP', 'Poort 80', and 'Poort 631' checked; and 'Webservices' with 'HTTP' checked. At the bottom, there is a link 'Certificaat>>' and two buttons: 'Annuleren' and 'Indienen'.

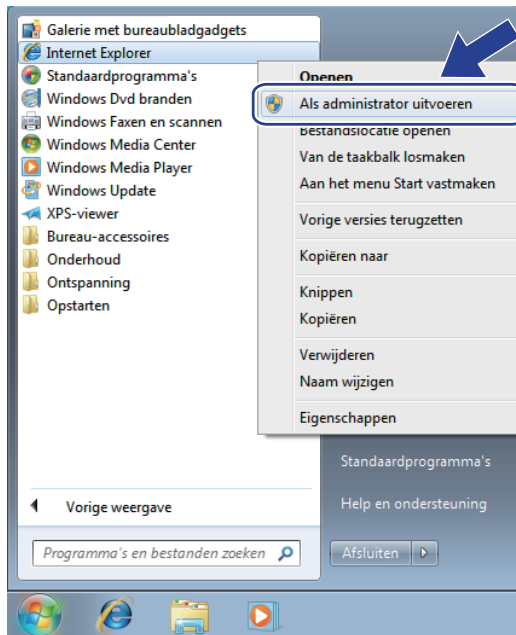
Het certificaat door uzelf ondertekend installeren op uw computer

OPMERKING

- De volgende stappen zijn voor Windows® Internet Explorer®. Als u gebruik maakt van een andere webbrowser, dient u de helptekst van die webbrowser te raadplegen.
- U moet beheerderrechten hebben om het door uzelf ondertekende certificaat te installeren.

Voor gebruikers van Windows Vista®, Windows® 7 en Windows Server® 2008 met beheerdersbevoegdheden

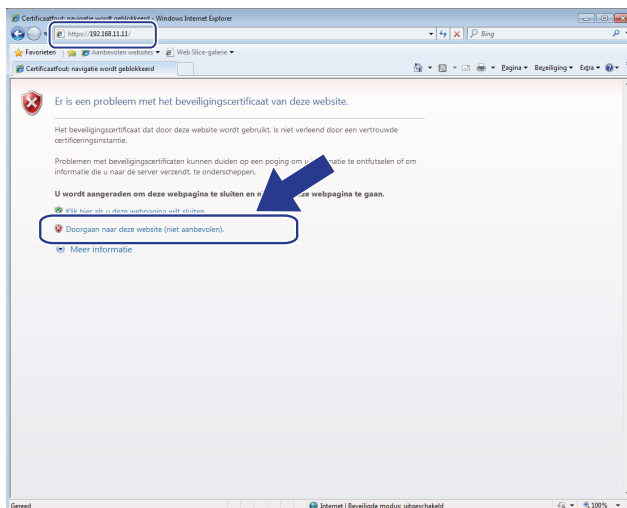
- 1 Klik op de knop  en selecteer **Alle programma's**.
- 2 Klik met de rechtermuisknop op **Internet Explorer** en klik daarna op **Als administrator uitvoeren**.



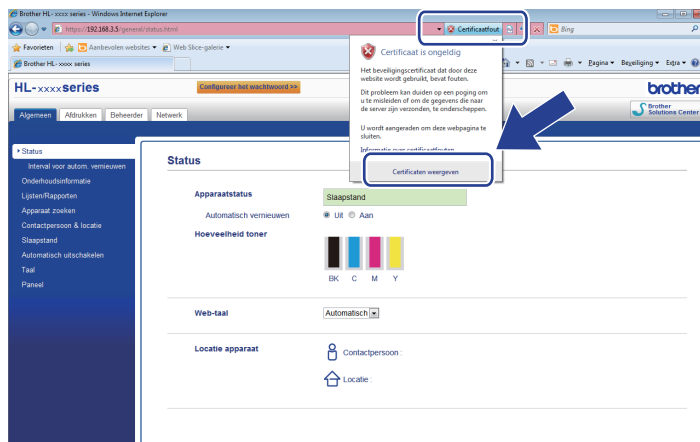
OPMERKING

Als het scherm **Gebruikersaccountbeheer** wordt weergegeven,
(Windows Vista®) Klik op **Doorgaan (Toestaan)**.
(Windows® 7/Windows® 8) Klik op **Ja**.

- 3 Typ "https://IP-adres van machine/" in uw browser om toegang te krijgen tot uw machine (hierbij staat "IP-adres van machine" voor het IP-adres van de machine of de naam van het knooppunt die u hebt gekozen voor het certificaat).
Klik vervolgens op **Doorgaan naar deze website (niet aanbevolen)**..



- 4 Klik op **Certificaatfout** en klik daarna op **Certificaten weergeven**. Voor de rest van de instructies dient u de stappen te volgen vanaf stap 4 bij *Voor gebruikers van Windows® XP en Windows Server® 2003* ➤➤ pagina 67.



Voor gebruikers van Windows® XP en Windows Server® 2003

- 1 Start uw webbrowser.
- 2 Typ "https://IP-adres van machine/" in uw browser om toegang te krijgen tot uw machine (hierbij staat "IP-adres van machine" voor het IP-adres of de naam van het knooppunt die u hebt gekozen voor het certificaat).
- 3 Wanneer het dialoogvenster met de veiligheidswaarschuwing verschijnt, voert u één van de volgende handelingen uit:
 - Klik op **Doorgaan naar deze website (niet aanbevolen)**.. Klik op **Certificaatfout** en klik daarna op **Certificaten weergeven**.
 - Als het volgende dialoogvenster verschijnt, klikt u op **Certificaat weergeven**.



- 4 Klik op **Certificaat installeren...** op het tabblad **Algemeen**.



- 5 Wanneer de **Wizard Certificaat importeren** verschijnt, klikt u op **Volgende**.
- 6 U dient een locatie te specificeren om het certificaat te installeren. We raden u aan om **Alle certificaten in het onderstaande archief opslaan** te kiezen en vervolgens te klikken op **Bladeren....**



- 7 Kies **Vertrouwde basiscertificeringsinstanties** en klik vervolgens op **OK**.

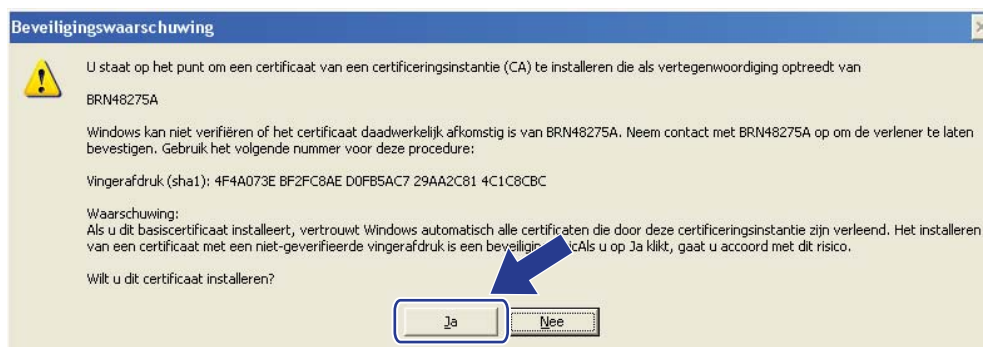


8 Klik op **Volgende**.



9 Klik op **Voltooien**.

10 Druk op **Ja** als de vingerafdruk (duimafdruk) correct is.



OPMERKING

De vingerafdruk (duimafdruk) wordt afgedrukt op het netwerkconfiguratierapport (zie *Het netwerkconfiguratierapport afdrukken* ►► pagina 41).

11 Klik op **OK**.

12 Het certificaat dat u zelf hebt ondertekend, is geïnstalleerd op uw computer en de SSL/TLS-communicatie is beschikbaar.

Het certificaat en de geheime sleutel importeren en exporteren

U kunt het certificaat en de private sleutel opslaan op de machine en deze beheren via importeren en exporteren.

Het door uzelf ondertekende certificaat, het certificaat uitgevaardigd door een CA en de geheime sleutel importeren

- 1 Klik op **Certificaat en geheime sleutel importeren** op de pagina **Certificaat**.
- 2 Geef het bestand op dat u wilt importeren.
- 3 Voer het wachtwoord in als het bestand versleuteld is en klik daarna op **Indienen**.
- 4 Het certificaat en de private sleutel zijn met succes geïmporteerd in uw machine.
Om SSL/TLS-communicatie te kunnen gebruiken, moet het hoofdcertificaat van de CA eveneens op uw computer worden geïnstalleerd. Neem contact op met uw netwerkbeheerder voor de installatie.

Het door uzelf ondertekende certificaat, het certificaat uitgevaardigd door een CA en de geheime sleutel exporteren

- 1 Klik op **Exporteren** weergegeven bij **Certificaten** op de pagina **Certificaat**.
- 2 Voer het wachtwoord in als u het bestand wil versleutelen.

OPMERKING

Als een leeg wachtwoord wordt gebruikt, wordt er geen versleuteling toegepast.

- 3 Voer het wachtwoord nogmaals in ter bevestiging en klik daarna op **Indienen**.
- 4 Geef de locatie op waar u het bestand wilt opslaan.
- 5 Het certificaat en de private sleutel zijn geëxporteerd naar uw computer.

OPMERKING

U kunt het bestand dat u hebt geëxporteerd ook importeren.

Een CA-certificaat importeren en exporteren

U kunt een CA-certificaat opslaan op de machine via importeren en exporteren.

Een CA-certificaat importeren

- 1 Klik op **CA-certificaat** op de pagina **Beveiliging**.
- 2 Klik op **CA-certificaat importeren** en kies het certificaat. Klik op **Indienen**.

Een CA-certificaat exporteren

- 1 Klik op **CA-certificaat** op de pagina **Beveiliging**.
- 2 Selecteer het certificaat dat u wilt exporteren en klik op **Exporteren**. Klik op **Indienen**.
- 3 Klik op **Opslaan** om de bestemmingsmap te kiezen.
- 4 Kies de bestemming waar u het geëxporteerde certificaat wilt opslaan en sla vervolgens het certificaat op.

Meerdere certificaten beheren

Met deze functie voor meerdere certificaten kunt u alle certificaten beheren die u hebt geïnstalleerd met Beheer via een webbrowser. Na het installeren van een certificaat kunt u op de pagina **Certificaat** zien welke certificaten geïnstalleerd zijn en vervolgens de inhoud van elk certificaat bekijken, het certificaat verwijderen of het exporteren. Raadpleeg *Een certificaat configureren met Beheer via een webbrowser* >> pagina 60 voor informatie over het raadplegen van de pagina **Certificaat**. Met de Brother-machine kunt u tot drie door uzelf ondertekende certificaten of tot drie certificaten uitgevaardigd door een CA opslaan. U kunt de opgeslagen certificaten toepassen om gebruik te maken van het HTTPS/IPPS-protocol of IEEE 802.1x-verificatie.

U kunt eveneens tot vier CA-certificaten opslaan om gebruik te maken van IEEE 802.1x-verificatie en SSL voor SMTP/POP3.

Wij raden u aan een certificaat minder op te slaan en de laatste vrij te houden voor het oplossen van problemen met vervallen certificaten. Als u bijvoorbeeld een CA-certificaat wilt opslaan, slaat u drie certificaten op en houdt u één opslag als back-up. Als het certificaat opnieuw moet worden uitgevaardigd, bijvoorbeeld wanneer het vervallen is, kunt u een nieuw certificaat importeren naar de back-up en vervolgens het vervallen certificaat verwijderen, om configuratiefouten te vermijden.

OPMERKING

- Wanneer u het HTTPS/IPPS-protocol of IEEE 802.1x gebruikt, moet u selecteren welk certificaat u gebruikt.
- Wanneer u SSL gebruikt voor SMTP-communicatie, hoeft u geen certificaat te selecteren. Het noodzakelijke certificaat wordt automatisch geselecteerd.

Uw netwerkmachine veilig beheren met SSL/TLS

Om uw netwerkmachine veilig te kunnen beheren, dient u de beheerprogramma's met beveiligingsprotocols te gebruiken.

Veilig beheer met Beheer via een webbrowser

Wij raden u aan het HTTPS-protocol te gebruiken voor een veilig beheer. Om deze protocollen te kunnen gebruiken, dient u de volgende machine-instellingen door te voeren.

OPMERKING

Het HTTPS-protocol is standaard ingeschakeld.

U kunt de HTTPS-protocolinstellingen en het certificaat wijzigen via het scherm Beheer via een webbrowser door te klikken op **Netwerk**, **Protocol** en vervolgens **HTTP-serverinstellingen**.

6

- 1 Start uw webbrowser.
- 2 Typ "http://IP-adres van machine/" in uw browser. (Als u het aangemaakte certificaat gebruikt, typ "http://openbare naam/" in uw browser. "Algemene naam" is de algemene naam die u hebt toegewezen aan het certificaat, zoals een IP-adres, een naam van een knooppunt of een domeinnaam. Raadpleeg *Certificaten gebruiken ter beveiliging van de machine* ►► pagina 58 voor meer informatie over het toewijzen van een openbare naam aan het certificaat.)
 - Bijvoorbeeld:
http://192.168.1.2/ (als de algemene naam het IP-adres van de machine is)
- 3 Er dient standaard geen wachtwoord te worden ingevoerd. Als u voordien een wachtwoord hebt ingesteld, voert u dit in en drukt u op .
- 4 U krijgt nu toegang tot de machine via HTTPS.
Als u het SNMPv3-protocol gebruikt, dient u onderstaande stappen te volgen.

OPMERKING

U kunt de SNMP-instellingen ook wijzigen met BRAdmin Professional 3.

- 5 Klik op **Netwerk**.
- 6 Klik op **Protocol**.

- 7 Zorg ervoor dat de **SNMP**-instelling geactiveerd is en klik vervolgens op **Geavanceerde instellingen** bij **SNMP**.
- 8 U kunt de SNMP-instellingen configureren op onderstaand scherm.

SNMP

Status Ingeschakeld

SNMP-gebruiksmodus

- ☒ Toegang lezen/schrijven SNMP v1/v2c
- ☐ Toegang lezen/schrijven SNMPv3 en alleen lezen v1/v2c
- ☐ Toegang lezen/schrijven SNMPv3

Instellingen SNMP v1/v2c-modus

- ☒ Netwerkbeheer inschakelen met oudere versies van BRAdmin

Er zijn drie **SNMP**-verbindingsmodi.

■ **Toegang lezen/schrijven SNMP v1/v2c**

In deze modus gebruikt de afdrukserver versie 1 en versie 2c van het SNMP-protocol. In deze modus kunt u alle Brother-toepassingen gebruiken. Deze modus is echter niet veilig omdat de gebruiker niet wordt geverifieerd en de gegevens niet worden versleuteld.

■ **Toegang lezen/schrijven SNMPv3 en alleen lezen v1/v2c**

In deze modus gebruikt de afdrukserver de lezen/schrijven-toegang van versie 3 en de alleen-lezen-toegang van versie 1 en versie 2c van het SNMP-protocol.

OPMERKING

Wanneer u de modus **Toegang lezen/schrijven SNMPv3 en alleen lezen v1/v2c** gebruikt, is het mogelijk dat sommige Brother-toepassingen (bv. BRAdmin Light) die gebruik maken van de afdrukserver niet correct werken omdat deze de alleen-lezen-toegang van versie 1 en versie 2c toelaten. Als u alle toepassingen wilt gebruiken, dient u de modus **Toegang lezen/schrijven SNMP v1/v2c** te gebruiken.

■ **Toegang lezen/schrijven SNMPv3**

In deze modus gebruikt de afdrukserver versie 3 van het SNMP-protocol. Gebruik deze modus als u de afdrukserver veilig wilt beheren.

OPMERKING

- Let op het volgende wanneer u de modus **Toegang lezen/schrijven SNMPv3** gebruikt.
 - U kunt de afdrukserver alleen beheren via BRAdmin Professional 3 of Beheer via een webbrowser.
 - Behalve BRAdmin Professional 3 worden alle toepassingen die gebruik maken van SNMPv1/v2c geweerd. Gebruik de modus **Toegang lezen/schrijven SNMPv3 en alleen lezen v1/v2c** of **Toegang lezen/schrijven SNMP v1/v2c** om het gebruik van SNMPv1/v2c-toepassingen toe te staan.
 - Raadpleeg de helptekst in Beheer via een webbrowser voor nadere informatie.
-

Veilig beheer met BRAdmin Professional 3 (Windows®)

Als u het programma BRAdmin Professional 3 veilig wilt gebruiken, dient u de onderstaande stappen te volgen

- Wij raden u ten stelligste aan de recentste versie van BRAdmin Professional 3 te gebruiken die u kunt downloaden op <http://solutions.brother.com/>. Als u een oudere versie van BRAdmin ¹ gebruikt voor het beheren van de machines van Brother, is de gebruikersverificatie niet veilig.
- Als u wilt verhinderen dat oudere versies van BRAdmin ¹ toegang krijgen tot de machine, moet u Beheer via een webbrowser gebruiken om de toegang door oudere versies van BRAdmin ¹ uitschakelen in de **Geavanceerde instellingen** van **SNMP** op de pagina **Protocol**. (Zie *Veilig beheer met Beheer via een webbrowser* ►► pagina 74.)
- Als u BRAdmin Professional 3 en Beheer via een webbrowser samen gebruikt, dient u Beheer via een webbrowser te gebruiken met het HTTPS-protocol.
- Als u een gemengde groep van oudere afdrukservers ² en afdrukservers met BRAdmin Professional 3 beheert, dan raden wij u aan om in elke groep een ander wachtwoord te gebruiken. Zo garandeert u dat de beveiliging op de nieuwe afdrukservers wordt gehandhaafd.

¹ BRAdmin Professional ouder dan ver. 2.80, BRAdmin Light voor Macintosh ouder dan ver. 1.10

² NC-2000 series, NC-2100p, NC-3100h, NC-3100s, NC-4100h, NC-5100h, NC-5200h, NC-6100h, NC-6200h, NC-6300h, NC-6400h, NC-8000, NC-100h, NC-110h, NC-120w, NC-130h, NC-140w, NC-8100h, NC-9100h, NC-7100w, NC-7200w, NC-2200w

Documenten veilig afdrukken met SSL/TLS

Om documenten veilig met het IPP-protocol af te drukken, kunt u het IPPS-protocol gebruiken.

De IPPS-instellingen met een webbrowser configureren:

- 1 Klik op **Netwerk** op de webpagina van de machine en klik vervolgens op **Protocol**. Als het selectievakje **IPP** al is aangevinkt, gaat u verder met stap 6.
- 2 Vink het selectievakje **IPP** aan en klik vervolgens op **Indienen**.
- 3 Herstart de machine om de configuratie te activeren.
- 4 Klik op **Netwerk** op de webpagina van de machine en klik vervolgens op **Protocol**.
- 5 Klik op **HTTP-serverinstellingen**.
- 6 Vink het selectievakje **HTTPS(Port443)** aan en klik vervolgens op **Indienen**.
- 7 Herstart de machine om de configuratie te activeren.

OPMERKING

Communicatie via IPPS kan geen ongeoorloofde toegang tot de afdrukserver voorkomen.

Een e-mail veilig

Configuratie met behulp van Beheer via een webbrowser

U kunt het beveiligd verzenden van e-mails met gebruikersverificatie of het verzenden van e-mails met SSL/TLS configureren op het scherm van Beheer via een webbrowser.

- 1 Start uw webbrowser.
- 2 Voer "http://IP-adres van de machine/" in de adresregel van uw browser (waarbij "IP-adres van de machine" staat voor het IP-adres van de machine of de naam van de afdrukserver).
 - Bijvoorbeeld: http://192.168.1.2/
- 3 Er dient standaard geen wachtwoord te worden ingevoerd. Als u voordien een wachtwoord hebt ingesteld, voert u dit in en drukt u op ➡.
- 4 Klik op **Netwerk**.
- 5 Klik op **Protocol**.
- 6 Klik op **Geavanceerde instellingen** van **POP3/SMTP** en zorg ervoor dat de status van **POP3/SMTP** **Ingeschakeld** is.
- 7 Op deze pagina kunt u de instellingen van **POP3/SMTP** configureren.

OPMERKING

- Raadpleeg de helptekst in Beheer via een webbrowser voor nadere informatie.
- U kunt tevens bevestigen of de e-mailinstellingen juist zijn door na het configureren een teste-mail te verzenden.
- Als u de POP3/SMTP-serverinstellingen niet kent, neemt u contact op met uw systeembeheerder of internetprovider voor meer informatie.

- 8 Klik na het configureren op **Indienen**. Het dialoogvenster "Configuratie van uitgaande e-mail testen" verschijnt.
- 9 Volg de instructies op het scherm als u met de huidige instellingen wilt testen.

Een e-mail verzenden met gebruikersverificatie

Deze machine ondersteunt de methodes POP voor SMTP en SMTP-AUTH voor het verzenden van e-mails via een e-mailserver waarvoor gebruikersverificatie is vereist. Deze methoden voorkomen dat onbevoegde gebruikers toegang tot de e-mailserver krijgen. Voor het configureren van de instellingen kunt u Beheer via een webbrowser of BRAdmin Professional 3 gebruiken. U kunt de methodes POP voor SMTP en SMTP-AUTH gebruiken voor waarschuwingen per e-mail.

E-mailserverinstellingen

De instellingen van SMTP-verificatie moeten overeenkomen met de methode die wordt gebruikt door uw e-mailserver. Vraag uw netwerkbeheerder of internetprovider (ISP) om de juiste configuratie van de e-mailserver.

U zult ook **SMTP-VERIF** bij **Verificatiemethode SMTP-server** moeten aanvinken om verificatie van de SMTP-server te activeren.

SMTP-instellingen

- U kunt het SMTP-poortnummer met Beheer via een webbrowser wijzigen. Dit komt van pas wanneer uw ISP (Internet Service Provider) de service "Outbound Port 25 Blocking (OP25B)" implementeert.
- Wanneer u in plaats van het SMTP-poortnummer een specifiek nummer gebruikt dat uw ISP gebruikt voor de SMTP-server (bijvoorbeeld poort 587), kunt u via de SMTP-server een e-mail versturen.
- U kunt zowel POP voor SMTP als SMTP-VERIF gebruiken, maar wij raden u aan SMTP-VERIF te kiezen.
- Als u POP voor SMTP als de SMTP-serververificatiemethode kiest, dan moet u de POP3-instellingen configureren. U kunt indien nodig ook de methode APOP gebruiken.

Een e-mail veilig verzenden met behulp van SSL/TLS

Deze machine ondersteunt de methodes SSL/TLS voor het verzenden van een e-mail via een e-mailserver waarvoor beveiligde SSL/TLS-communicatie vereist is. Voor het verzenden van e-mail via een e-mailserver die gebruik maakt van SSL/TLS-communicatie, dient u SMTP over SSL/TLS of POP3 over SSL/TLS correct te configureren.

Servercertificaat verifiëren

- Als u SSL of TLS selecteert voor **SMTP over SSL/TLS** of **POP3 over SSL/TLS**, wordt het vakje **Servercertificaat verifiëren** automatisch aangevinkt om het servercertificaat te verifiëren.
 - Voor u het servercertificaat verifieert, moet u het CA-certificaat importeren dat werd verstrekt door de CA die het servercertificaat heeft ondertekend. Vraag uw netwerkbeheerder of internetprovider (ISP) om bevestiging dat het importeren van een CA-certificaat nodig is. Raadpleeg *Een CA-certificaat importeren en exporteren* ►► pagina 72 voor het importeren van het certificaat.
 - Als u het servercertificaat niet wilt verifiëren, vinkt u **Servercertificaat verifiëren** uit.

Poortnummer

- Als u SSL of TLS selecteert, wordt de waarde bij **SMTP-poort** of **POP3-poort** gewijzigd om overeen te stemmen met het protocol. Als u het poortnummer handmatig wilt wijzigen, voert u het poortnummer in nadat u **SMTP over SSL/TLS** of **POP3 over SSL/TLS** hebt gekozen.
- U moet de POP3/SMTP-communicatiemethode configureren zodat deze overeenstemt met de e-mailserver. Voor meer informatie over de instellingen van de e-mailserver, contacteert u uw netwerkbeheerder of internetprovider.

In de meeste gevallen zijn de volgende instellingen vereist voor de beveiligde webmailservices:

(SMTP)

SMTP-poort: 587

Verificatiemethode SMTP-server: SMTP-AUTH

SMTP over SSL/TLS: TLS

(POP3)

POP3-poort: 995

POP3 over SSL/TLS: SSL

IEEE 802.1x-verificatie gebruiken

U kunt IEEE 802.1x-verificatie configureren voor een bedraad of draadloos netwerk.

Configuratie van IEEE 802.1x-verificatie via Beheer via een webbrowser

Als u IEEE 802.1x-verificatie configureert voor een bedraad of draadloos netwerk met behulp van Beheer via een webbrowser, volgt u de instructies.

U kunt de IEEE 802.1x-verificatie ook configureren met:

(Bedraad netwerk)

- BRAdmin Professional 3

(Draadloos netwerk)

- De wizard voor de draadloze instellingen via het bedieningspaneel (Zie *De machine voor een draadloos Enterprise-netwerk configureren* >> pagina 23 voor meer informatie.)
- De wizard voor de draadloze instellingen op de cd-rom (zie *Draadloze configuratie via tijdelijk gebruik van een USB-kabel (aanbevolen)* >> pagina 12 voor meer informatie.)
- BRAdmin Professional 3

OPMERKING

- Als u de machine configureert met behulp van EAP-TLS-verificatie, moet u het clientcertificaat uitgevaardigd door een CA installeren voor u de configuratie start. Neem contact op met uw netwerkbeheerder voor het clientcertificaat. Als u meer dan één certificaat hebt geïnstalleerd, raden wij aan dat u het certificaat noteert dat u wilt gebruiken. Raadpleeg *Certificaten gebruiken ter beveiliging van de machine* >> pagina 58 voor meer informatie over het installeren van het certificaat.
- Voor u het servercertificaat verifieert, moet u het CA-certificaat importeren dat werd verstrekt door de CA die het servercertificaat heeft ondertekend. Vraag uw netwerkbeheerder of internetprovider (ISP) om bevestiging dat het importeren van een CA-certificaat nodig is. Raadpleeg *Een CA-certificaat importeren en exporteren* >> pagina 72 voor meer informatie over het importeren van het certificaat.
- Raadpleeg *Certificaten gebruiken ter beveiliging van de machine* >> pagina 58 voor meer informatie over elk certificaat.

- 1 Start uw webbrowser.
- 2 Voer "http://IP-adres van de machine/" in de adresregel van uw browser (waarbij "IP-adres van de machine" staat voor het IP-adres van de machine of de naam van de afdrukserver).
 - Bijvoorbeeld: http://192.168.1.2/

OPMERKING

- Als u een domeinnaamsysteem gebruikt of een naam NetBIOS inschakelt, kunt u een andere naam invoeren zoals "GedeeldePrinter" in plaats van het IP-adres.

- Bijvoorbeeld: `http://GedeeldePrinter/`

Als u een naam NetBIOS inschakelt, kunt u eveneens de naam van het knooppunt gebruiken.

- Bijvoorbeeld: `http://brnxxxxxxxxxxxxx/`

De naam NetBIOS kunt u vinden in het netwerkconfiguratierapport (zie *Het netwerkconfiguratierapport afdrukken* ►► pagina 41).

- Bij gebruik van Macintosh krijgt u eenvoudig toegang tot het systeem voor Beheer via een webbrowser door in het scherm **Status Monitor** gewoon op het symbool van de machine te klikken. Voor meer informatie: ►► Gebruikershandleiding.

- 3 Er dient standaard geen wachtwoord te worden ingevoerd. Als u voordien een wachtwoord hebt ingesteld, voert u dit in en drukt u op ➡.
- 4 Klik op **Netwerk**.
- 5 (Bedraad) Klik op **Bedraad** en selecteer vervolgens **Authenticatie 802.1x**.
(Draadloos) Klik op **Draadloos** en selecteer vervolgens **Draadloos (Bedrijf)**.
- 6 Nu kunt u de instellingen voor IEEE 802.1x-verificatie configureren.
 - Als u IEEE 802.1x-verificatie wilt inschakelen voor een bedraad netwerk, vinkt u **Ingeschakeld** aan voor **Status 802.1x vast** op de pagina **Authenticatie 802.1x**.
 - Zie *IEEE 802.1x-verificatie* ►► pagina 102 voor meer informatie over IEEE 802.1x-verificatie en de inwendige verificatiemethoden.
 - Als u EAP-TLS-verificatie gebruikt, moet u het clientcertificaat kiezen dat geïnstalleerd is (weergegeven met certificaatnaam) voor verificatie in de keuzelijst **Clientcertificaat**.
 - Als u EAP-FAST-, PEAP-, EAP-TTLS- of EAP-TLS-verificatie selecteert, kunt u de verificatiemethode kiezen uit de keuzelijst **Verificatie servercertificaat**. U kunt het servercertificaat verifiëren met behulp van het CA-certificaat dat vooraf werd geïmporteerd op de machine en dat werd verstrekt door de CA die het servercertificaat heeft ondertekend.

U kunt een van de volgende verificatiemethoden selecteren in de keuzelijst **Verificatie servercertificaat**.

■ **Geen verificatie**

Het servercertificaat kan altijd vertrouwd worden. De verificatie wordt niet uitgevoerd.

■ **CA-cert.**

De verificatiemethode voor het controleren van de CA-betrouwbaarheid van het servercertificaat, door gebruik te maken van het CA-certificaat dat werd verstrekt door de CA die het servercertificaat heeft ondertekend.

■ **CA-cert. + server-id**

De verificatiemethode voor het controleren van de openbare naam¹ van het servercertificaat, naast de CA-betrouwbaarheid van het servercertificaat.

¹ De verificatie van de openbare naam vergelijkt de openbare naam van het servercertificaat met de tekenreeks die geconfigureerd werd voor de **Server-id**. Voor u deze methode gebruikt, neemt u contact op met uw systeembeheerder voor de openbare naam van het servercertificaat en configureert u vervolgens **Server-id**.

7 Klik na het configureren op **Indienen**.
(Bedraad)

Na de configuratie sluit u uw machine aan op het netwerk met IEEE 802.1x-ondersteuning. Druk na een paar minuten het netwerkconfiguratie-rapport af om de **<Wired IEEE 802.1x> Status** te controleren (zie *Het netwerkconfiguratie-rapport afdrukken* ►► pagina 41.)

■ **Success**

De bedrade IEEE 802.1x-functie is ingeschakeld en de verificatie is gelukt.

■ **Failed**

De bedrade IEEE 802.1x-functie is ingeschakeld; de verificatie is echter mislukt.

■ **Off**

De bedrade IEEE 802.1x-functie is niet beschikbaar.

(Draadloos)

Het WLAN-rapport wordt kort na de configuratie automatisch afgedrukt. Controleer uw draadloze configuratie op het rapport. Raadpleeg *Het WLAN-rapport afdrukken* (voor HL-3140CW, HL-3150CDW en HL-3170CDW) ►► pagina 42.

Overzicht

In dit hoofdstuk wordt uitgelegd hoe algemene netwerkproblemen met de Brother-machine kunnen worden opgelost. Kunt u de oplossing voor het probleem niet in dit hoofdstuk vinden, kijk dan op het Brother Solutions Center: <http://solutions.brother.com/>.

Ga naar het Brother Solutions Center op <http://solutions.brother.com/> en klik op Handleidingen op de pagina voor uw model om de andere handleidingen te downloaden.

Het probleem vaststellen

Zorg ervoor dat de volgende items geconfigureerd zijn vooraleer u dit hoofdstuk leest.

Controleer eerst het volgende:
Het netsnoer is goed aangesloten en de Brother-machine is ingeschakeld.
Het toegangspunt (voor draadloos gebruik), de router of de hub is ingeschakeld en de linkknop knippert.
Alle beschermende verpakkingen zijn verwijderd van de Brother-machine.
De tonercartridges en de drumeenheid zijn goed geïnstalleerd.
Het bovendeksel en achterdeksel zijn goed gesloten.
Het papier is goed in de papierlade geplaatst.
(Voor bedrade netwerken) Een netwerkkabel is correct aangesloten op de Brother-machine en de router of hub.

Raadpleeg de onderstaande lijst en ga naar de pagina met de oplossing voor uw probleem

- Ik kan de configuratie van het draadloze netwerk niet voltooien. (Zie pagina 86.)
- De Brother-machine wordt niet gevonden op het netwerk tijdens de installatie van de printerdriver. (Zie pagina 87.)
- De Brother-machine kan niet afdrukken via het netwerk. (Zie pagina 88.)
- De Brother-machine wordt niet gevonden op het netwerk nadat deze met succes werd geïnstalleerd. (Zie pagina 88.)
- Ik gebruik beveiligingssoftware. (Zie pagina 91.)
- Ik wil controleren of mijn netwerkapparaten correct werken. (Zie pagina 92.)

Ik kan de configuratie van het draadloze netwerk niet voltooien.

Vraag	Interface	Oplossing
Mijn machine krijgt geen verbinding tijdens de draadloze instelling.	draadloos	Schakel uw draadloze router uit en daarna weer in. Probeer vervolgens de draadloze instellingen opnieuw te configureren.
Zijn uw beveiligingsinstellingen (SSID/netwerksleutel) correct?	draadloos	■ Controleer en kies indien nodig de correcte beveiligingsinstellingen. • Het is mogelijk dat de naam van de fabrikant of het modelnummer van het WLAN-toegangspunt/de WLAN-router wordt gebruikt als de standaardbeveiligingsinstellingen. • Raadpleeg de gebruiksaanwijzing van uw WLAN-toegangspunt/WLAN-router voor informatie over het vinden van de beveiligingsinstellingen. • Vraag hulp aan de fabrikant van uw WLAN-toegangspunt/WLAN-router of aan uw internetprovider of netwerkbeheerder. ■ Zie <i>Termen en concepten voor draadloze netwerken (voor HL-3140CW, HL-3150CDW en HL-3170CDW)</i> >> pagina 104 voor meer informatie over SSID en netwerksleutels.
Gebruikt u MAC-adresfiltering?	draadloos	Controleer of het MAC-adres van de Brother-machine toegestaan is in de filter. U kunt het MAC-adres vinden via het bedieningspaneel van de Brother-machine. (Zie <i>Functietabel en standaardinstellingen</i> >> pagina 43.)
Is de afgeschermdede modus geactiveerd op uw WLAN-toegangspunt/-router? (de SSID wordt niet verzonden)	draadloos	■ U moet de correcte SSID-naam of netwerksleutel handmatig invoeren. ■ Controleer de SSID-naam of de netwerksleutel in de gebruiksaanwijzing van uw WLAN-toegangspunt/-router en herconfigureer de draadloze netwerkinstellingen. (Raadpleeg <i>Uw machine configureren als de SSID niet wordt doorgegeven</i> >> pagina 20 voor meer informatie.)
Ik heb alle bovenstaande oplossingen gecontroleerd en geprobeerd, maar ik slaag er niet in de draadloze configuratie te voltooien. Kan ik nog iets anders proberen?	draadloos	Gebruik de Reparatietool voor netwerkaansluiting. Raadpleeg <i>De Brother-machine kan niet afdrukken via het netwerk. De Brother-machine wordt niet gevonden op het netwerk nadat deze met succes werd geïnstalleerd.</i> >> pagina 88.

De Brother-machine wordt niet gevonden op het netwerk tijdens de installatie van de printerdriver.

Vraag	Interface	Oplossing
Is uw machine verbonden met het netwerk en heeft het een geldig IP-adres?	bedraad/ draadloos	Druk het netwerkconfiguratierapport af en controleer dat Ethernet Link Status of Wireless Link Status op Link OK is ingesteld. Raadpleeg <i>Het netwerkconfiguratierapport afdrukken</i> >> pagina 41.
Gebruikt u beveiligingssoftware?	bedraad/ draadloos	■ Kies op het installatiedialogvenster om opnieuw te zoeken naar de Brother-machine. ■ Sta de toegang toe wanneer het waarschuwingsbericht van de beveiligingssoftware wordt weergegeven tijdens de installatie van de printerdriver. ■ Voor meer informatie over beveiligingssoftware, raadpleegt u <i>Ik gebruik beveiligingssoftware</i>. >> pagina 91.
Is uw Brother-machine te ver van het WLAN-toegangspunt/de WLAN-router geplaatst?	draadloos	Plaats de Brother-machine binnen een afstand van ongeveer 3,3 voet (1 meter) van het WLAN-toegangspunt/de WLAN-router bij het configureren van de draadloze netwerkinstellingen.
Bevinden er zich obstakels (muren, meubels enz.) tussen de machine en het WLAN-toegangspunt/de WLAN-router?	draadloos	Verplaats uw Brother-machine naar een ruimte zonder obstakels of dichterbij de buurt van het WLAN-toegangspunt/de WLAN-router.
Bevindt er zich een draadloze computer, Bluetooth-apparaat, magnetron of digitale draadloze telefoon in de buurt van de Brother-machine of het WLAN-toegangspunt/de WLAN-router?	draadloos	Verwijder alle apparaten uit de buurt van de Brother-machine of het WLAN-toegangspunt/de WLAN-router.

De Brother-machine kan niet afdrukken via het netwerk.

De Brother-machine wordt niet gevonden op het netwerk nadat deze met succes werd geïnstalleerd.

Vraag	Interface	Oplossing
Gebruikt u beveiligingssoftware?	bedraad/ draadloos	Raadpleeg <i>Ik gebruik beveiligingssoftware</i> . ►► pagina 91.
Wordt er een beschikbaar IP-adres toegewezen aan uw Brother-machine?	bedraad/ draadloos	■ (Windows®) Controleer het IP-adres en het subnetmasker met de Reparatiетool voor netwerkaansluiting. Gebruik de Reparatiетool voor netwerkaansluiting voor het repareren van de netwerkinstellingen van de Brother-machine. Deze tool zorgt ervoor dat het correcte IP-adres en subnetmasker toegewezen zijn. Contacteer uw netwerkbeheerder voor meer informatie over het gebruik van de Reparatiетool voor netwerkaansluiting, en volg daarna de onderstaande stappen: OPMERKING • (Windows® XP/XP Professional x64 Edition/Windows Vista®/Windows® 7/Windows® 8) U moet zich aanmelden als beheerder. • Zorg ervoor dat de Brother-machine ingeschakeld is en met hetzelfde netwerk is verbonden als uw computer.

De Brother-machine kan niet afdrukken via het netwerk.

De Brother-machine wordt niet gevonden op het netwerk nadat deze met succes werd geïnstalleerd. (Vervolg)

Vraag	Interface	Oplossing
Wordt er een beschikbaar IP-adres toegewezen aan uw Brother-machine? (vervolg)	bedraad/ draadloos	1 (Windows® XP, Windows Server® 2003/2008) Klik op de knop Start, Alle programma's, Bureau-accessoires en Windows Verkenner en vervolgens op Deze computer (Computer). (Windows Vista®/Windows® 7) Klik op de knop  en Computer. 2 Dubbelklik op Lokaal station (C:), Program Files of Program Files (x86) voor gebruikers van het 64 bit-OS, Browny02, Brother, BrotherNetTool.exe om het programma te starten. OPMERKING Als het scherm Gebruikersaccountbeheer verschijnt, kunt u via het venster verder gaan met de installatie. 3 Volg de instructies op het scherm. 4 Zorg ervoor dat u kunt afdrukken of scannen. OPMERKING Het Reparatietool voor netwerkaansluiting start automatisch als u het vakje Hulpprogramma voor verbindingsherstel inschakelen aanvinkt met behulp van Status Monitor. Klik met de rechtermuisknop op het scherm Status Monitor, klik op Opties, Details en klik vervolgens op het tabblad Diagnose. Dit wordt niet aangeraden wanneer de netwerkbeheerder het IP-adres heeft ingesteld op statisch, omdat dit automatisch het IP-adres zal wijzigen. Als het correcte IP-adres en subnetmasker nog steeds niet toegewezen zijn na het gebruik van de Reparatietool voor netwerkaansluiting, vraagt u meer informatie aan uw netwerkbeheerder of gaat u naar het Brother Solutions Center op http://solutions.brother.com/.

De Brother-machine kan niet afdrukken via het netwerk.

De Brother-machine wordt niet gevonden op het netwerk nadat deze met succes werd geïnstalleerd. (Vervolg)

Vraag	Interface	Oplossing
Is de vorige afdruktaak mislukt?	bedraad/ draadloos	■ Verwijder de mislukte afdruktaak uit de afdrukwachtrij van uw computer als deze nog steeds aanwezig is. ■ Dubbelklik op het printerpictogram in de volgende map en kies vervolgens Alle documenten annuleren in het menu Printer: (Windows® XP/Windows Server® 2003) Start en Printers en faxapparaten. (Windows Vista®)  Configuratiescherm, Hardware en geluiden en daarna Printers. (Windows® 7)  Apparaten en printers en daarna Printers en faxapparaten. (Windows Server® 2008) Start, Configuratiescherm en Printers.
Verbindt u de Brother-machine draadloos met het netwerk?	draadloos	■ Druk het WLAN-rapport af om de status van de draadloze verbinding te controleren. (Raadpleeg <i>Het WLAN-rapport afdrukken (voor HL-3140CW, HL-3150CDW en HL-3170CDW)</i> >> pagina 42 voor informatie over het afdrukken.) Als er een foutcode wordt vermeld op het afgedrukte WLAN-rapport: >> Installatiehandleiding: <i>Problemen oplossen</i>. ■ Raadpleeg <i>De Brother-machine wordt niet gevonden op het netwerk tijdens de installatie van de printerdriver</i>. >> pagina 87.
Ik heb alle bovenstaande oplossingen gecontroleerd en geprobeerd, maar de Brother-machine drukt niet af. Kan ik nog iets anders proberen?	bedraad/ draadloos	Verwijder de printerdriver en installeer deze opnieuw.

Ik gebruik beveiligingssoftware.

Vraag	Interface	Oplossing
Hebt u ervoor gekozen het dialoogvenster met de veiligheidswaarschuwing te accepteren tijdens de installatie van de printerdriver, het opstartproces van de applicatie of bij het gebruik van de functies voor afdrukken?	bedraad/ draadloos	Als u er niet voor hebt gekozen om het dialoogvenster met de veiligheidswaarschuwing te accepteren, is het mogelijk dat de firewallfunctie van uw beveiligingssoftware de toegang verhindert. Het is ook mogelijk dat bepaalde beveiligingssoftware de toegang blokkeert zonder een dialoogvenster met een veiligheidswaarschuwing weer te geven. Om de toegang toe te staan, raadpleegt u de gebruiksaanwijzing van uw beveiligingssoftware of neemt u contact op met de fabrikant.
Ik wil weten welk poortnummer ik nodig heb voor de instellingen van de beveiligingssoftware.	bedraad/ draadloos	De volgende poortnummers worden gebruikt voor Brother-netwerkfuncties: ■ Printen via het netwerk ¹ – Poortnummer 161 en 137 / Protocol UDP ■ BRAdmin Light ¹ – Poortnummer 161 / Protocol UDP ¹ Alleen Windows®. Voor meer informatie over het openen van de poort raadpleegt u de gebruiksaanwijzing van de beveiligingssoftware of neemt u contact op met de fabrikant.

Ik wil controleren of mijn netwerkapparaten correct werken.

Vraag	Interface	Oplossing
Is de Brother-machine, het toegangspunt/de router of de netwerkhub ingeschakeld?	bedraad/ draadloos	Zorg ervoor dat u alle instructies van <i>Controleer eerst het volgende:</i> ►► pagina 85 hebt gecontroleerd.
Waar kan ik de netwerkinstellingen van mijn Brother-machine vinden, zoals het IP-adres?	bedraad/ draadloos	Druk het netwerkconfiguratierapport af. Raadpleeg <i>Het netwerkconfiguratierapport afdrukken</i> ►► pagina 41.
Hoe kan ik de linkstatus van mijn Brother-machine controleren?	bedraad/ draadloos	Druk het netwerkconfiguratierapport af en controleer dat Ethernet Link Status of Wireless Link Status op Link OK is ingesteld. Raadpleeg <i>Het netwerkconfiguratierapport afdrukken</i> ►► pagina 41.
Kan ik de Brother-machine "pingen" vanaf mijn computer?	bedraad/ draadloos	Ping de Brother-machine vanaf uw computer via het IP-adres of de naam van het knooppunt. ■ Gelukt → Uw Brother-machine werkt correct en is verbonden met hetzelfde netwerk als uw computer. ■ Mislukt → Uw Brother-machine is niet verbonden met hetzelfde netwerk als uw computer. (Windows®) Contacteer uw netwerkbeheerder en gebruik de Reparatietool voor netwerkaansluiting om het IP-adres en het subnetmasker automatisch te herstellen. Raadpleeg (Windows®) <i>Controleer het IP-adres en het subnetmasker met de Reparatietool voor netwerkaansluiting</i>. bij <i>Wordt er een beschikbaar IP-adres toegewezen aan uw Brother-machine?</i> ►► pagina 88 voor meer informatie over de Reparatietool voor netwerkaansluiting.
Maakt de Brother-machine verbinding met het draadloze netwerk?	draadloos	Druk het WLAN-rapport af om de status van de draadloze verbinding te controleren. Voor meer informatie over het afdrukken, raadpleegt u <i>Het WLAN-rapport afdrukken (voor HL-3140CW, HL-3150CDW en HL-3170CDW)</i> ►► pagina 42. Als er een foutcode wordt vermeld op het afgedrukte WLAN-rapport: ►► Installatiehandleiding: <i>Problemen oplossen</i> .
Ik heb alle bovenstaande oplossingen gecontroleerd en geprobeerd, maar ik ervaar nog steeds problemen. Kan ik nog iets anders proberen?	draadloos	Raadpleeg de gebruiksaanwijzing van uw WLAN-toegangspunt/WLAN-router voor meer informatie over het vinden van de SSID en de netwerksleutel, en deze correct in te stellen. Raadpleeg <i>Zijn uw beveiligingsinstellingen (SSID/netwerksleutel) correct?</i> bij <i>Ik kan de configuratie van het draadloze netwerk niet voltooien.</i> ►► pagina 86 voor meer informatie over de SSID en de netwerksleutel.



Verklarende woordenlijst Netwerk

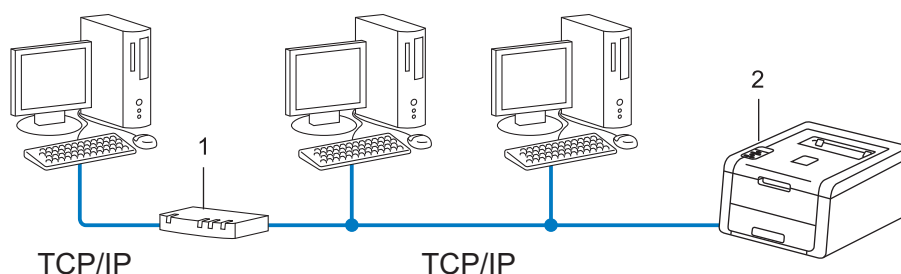
Typen netwerkverbindingen en protocollen	94
De machine configureren voor een netwerk	100
Termen en concepten voor draadloze netwerken (voor HL-3140CW, HL-3150CDW en HL-3170CDW)	104
Bijkomende netwerkinstellingen van Windows®	108
Beveiligingsvoorschriften en -concepten	111

Typen netwerkverbinding

Voorbeeld van een bedrade netwerkaansluiting

Peer-to-peer-afdrucken via TCP/IP

In een peer-to-peer-omgeving kan elke computer rechtstreeks gegevens uitwisselen met alle apparaten. Er is geen centrale server die toegang tot bestanden en het delen van printers beheert.



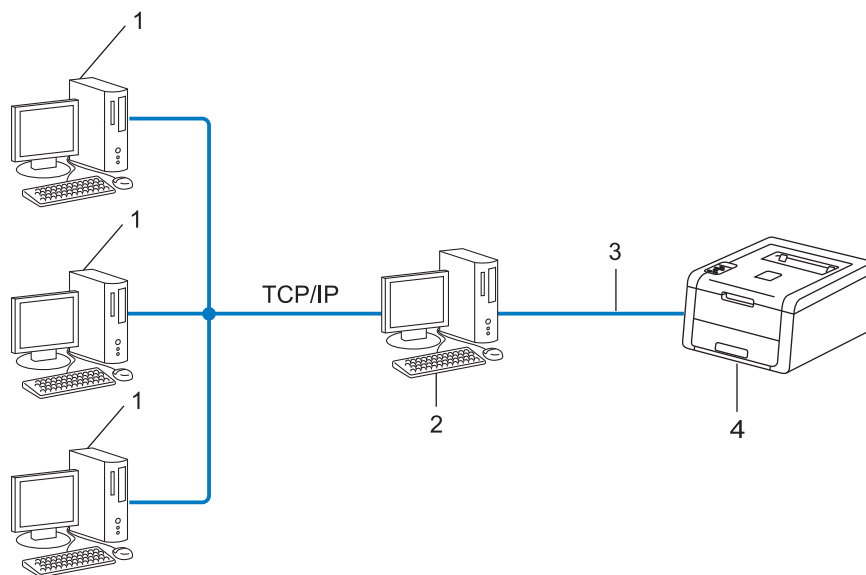
1 Router

2 Netwerkmachine (uw machine)

- In een kleiner netwerk van twee of drie computers bevelen wij de peer-to-peer-afdrukmethode aan, omdat peer-to-peer makkelijker is te configureren dan de op het netwerk gedeelde afdrukmethode. Raadpleeg *Op een netwerk gedeelde printer* >> pagina 95.
- Elke computer dient het TCP/IP-protocol te gebruiken.
- Voor de machine van Brother moet een geschikt IP-adres worden geconfigureerd.
- Als u een router gebruikt, moet het gateway-adres worden geconfigureerd op zowel de computers als de machine van Brother.

Op een netwerk gedeelde printer

In een gedeelde netwerkomgeving stuurt elke computer gegevens via een centraal beheerde computer. Een dergelijke computer wordt vaak een "server" of een "afdrukserver" genoemd. Hij beheert het afdrucken van alle taken.



1 Client-computer

2 Computer die "server" of "afdrukserver" wordt genoemd

3 TCP/IP, USB of parallel (waar beschikbaar)

4 Netwerkmachine (uw machine)

- In een groter netwerk bevelen wij de op het netwerk gedeelde afdrukmethode aan.
- De "server" of "afdrukserver" moet het TCP/IP-afdrukprotocol gebruiken.
- Voor de machine van Brother moet een geschikt IP-adres zijn geconfigureerd, tenzij de machine via de USB- of de parallelle interface op de server is aangesloten.

Protocollen

TCP/IP-protocollen en -functies

Protocollen zijn gestandaardiseerde sets regels volgens welke gegevens over een netwerk worden overdragen. Protocollen bieden de gebruiker toegang tot op het netwerk aangesloten apparaten.

De afdrukserver die met de Brother-machine wordt gebruikt, ondersteunt het TCP/IP-protocol (TCP/IP = Transmission Control Protocol/Internet Protocol).

TCP/IP is de populairste verzameling protocollen en wordt bijvoorbeeld gebruikt voor communicatie via internet en e-mail. Dit protocol kan met de meeste besturingssystemen worden gebruikt, zoals Windows[®], Windows Server[®], Mac OS X en Linux[®]. Op deze machine van Brother zijn de volgende TCP/IP-protocollen beschikbaar.

OPMERKING

- U kunt de protocolinstellingen configureren met de HTTP-interface (webbrowser). (Zie *De instellingen van de machine configureren met Beheer via een webbrowser* >> pagina 48.)
- Raadpleeg *Ondersteunde protocollen en beveiligingsfuncties* >> pagina 115 voor meer informatie over de protocollen die worden gebruikt door uw Brother-machine.
- Raadpleeg *Beveiligingsprotocollen* >> pagina 112 voor meer informatie over ondersteunde beveiligingsprotocollen.

DHCP/BOOTP/RARP

Bij gebruik van de protocollen DHCP/BOOTP/RARP kan het IP-adres automatisch worden geconfigureerd.

OPMERKING

Neem contact op met de netwerkbeheerder als u de DHCP/BOOTP/RARP-protocollen wilt gebruiken.

APIPA

Als u het IP-adres niet handmatig (met het bedieningspaneel van de machine of de software BRAdmin) of automatisch (met een DHCP/BOOTP/RARP-server) toewijst, zal het APIPA-protocol (APIPA = Automatic Private IP Addressing) automatisch een IP-adres toewijzen uit het bereik 169.254.1.0 tot 169.254.254.255.

ARP

Het Address Resolution Protocol koppelt een IP-adres aan een MAC-adres in een TCP/IP-netwerk.

DNS-client

De afdrukserver van Brother ondersteunt de DNS-clientfunctie (DNS = Domain Name System). Met deze functie kan de afdrukserver met gebruikmaking van zijn eigen DNS-naam met andere apparaten communiceren.

NetBIOS-naamresolutie

Met Network Basic Input/Output System name resolution kunt u tijdens de netwerkverbinding het IP-adres verkrijgen van het andere toestel op basis van zijn naam NetBIOS.

WINS

Windows® Internet Name Service is een informatieverstrekken dienst voor de NetBIOS-naamresolutie, waarbij een IP-adres en een naam NetBIOS in het lokale netwerk worden geconsolideerd.

LPR/LPD

Algemeen gebruikte afdrukprotocollen op TCP/IP-netwerken.

SMTP-client

De SMTP-client (SMTP = Simple Mail Transfer Protocol) wordt gebruikt om e-mails via het internet of intranet te versturen.

Custom Raw Port (Standaard is Poort 9100)

Nog een algemeen gebruikt afdrukprotocol op TCP/IP-netwerken. Hiermee is interactieve gegevensoverdracht mogelijk.

IPP

Het IPP (Internet Printing Protocol) stelt u in staat documenten via het internet rechtstreeks naar een beschikbare machine af te drukken.

OPMERKING

Raadpleeg *Beveiligingsprotocollen* ►► pagina 112 voor meer informatie over het IPPS-protocol.

mDNS

Met mDNS kan een afdrukserver van Brother zichzelf automatisch configureren, zodat hij in een Apple-systeem kan werken dat met de eenvoudige netwerkconfiguratie van Mac OS X is ingesteld.

TELNET

Het TELNET-protocol stelt u in staat om de netwerkapparaten op een TCP/IP-netwerk te bedienen via uw computer.

SNMP

Het SNMP (Simple Network Management Protocol) wordt gebruikt voor het beheren van netwerkapparaten zoals computers, routers en netwerkklare machines van Brother. De afdrukserver van Brother ondersteunt SNMPv1, SNMPv2c en SNMPv3.

OPMERKING

Raadpleeg *Beveiligingsprotocollen* ►► pagina 112 voor meer informatie over het SNMPv3-protocol.

LLMNR

Het LLMNR-protocol (Link-Local Multicast Name Resolution) zet de namen van naburige computers om als het netwerk geen DNS-server (Domeinnaamsysteem) heeft. De functie LLMNR Responder werkt in zowel de IPv4- als IPv6-omgeving bij gebruik van een computer die over de functie LLMNR Sender beschikt, zoals een computer met Windows Vista®, Windows® 7 en Windows® 8.

Web Services

Met het protocol Web Services kunnen gebruikers van Windows Vista®, Windows® 7 of Windows® 8 de afdrukdrivers installeren door met de rechtermuisknop te klikken op het symbool van de machine vanuit de map **Netwerk**. (Zie *Drivers installeren die gebruikt worden voor afdrukken via Web Services* (Windows Vista®, Windows® 7 en Windows® 8) ►► pagina 108.) Met Web Services kunt u bovendien vanaf uw computer de huidige status van de machine controleren.

HTTP

Het HTTP-protocol wordt gebruikt voor het versturen van gegevens tussen een webserver en een webbrowser.

OPMERKING

Raadpleeg *Beveiligingsprotocollen* ►► pagina 112 voor meer informatie over het HTTPS-protocol.

SNTP

Het Simple Network Time Protocol wordt gebruikt om computerklokken op een TCP/IP-netwerk te synchroniseren. U kunt de SNTP-instellingen configureren met Beheer via een webbrowser. (Zie *Het SNTP-protocol configureren met Beheer via een webbrowser* ►► pagina 52 voor meer informatie.)

CIFS

Het Common Internet File System is de standaardmanier waarop pc-gebruikers bestanden en printers delen in Windows®.

IPv6

IPv6 is het internetprotocol van de nieuwe generatie. Kijk voor meer informatie over het IPv6-protocol op de modelpagina van de machine die u gebruikt op <http://solutions.brother.com/>.

IP-adressen, subnetmaskers en gateways

Als u de machine in een genetwerkte TCP/IP-omgeving wilt gebruiken, moet u het IP-adres en het subnetmasker configureren. Het IP-adres dat u toewijst aan de afdrukserver, moet zich op hetzelfde logische netwerk bevinden als uw hostcomputers. Is dit niet het geval, dan moeten het subnetmasker en gateway-adres worden geconfigureerd.

IP-adres

Een IP-adres is een reeks cijfers die elk apparaat identificeert dat op het netwerk is aangesloten. Een IP-adres bestaat uit vier nummers die door punten van elkaar worden gescheiden. Elk nummer ligt tussen de 0 en 255.

■ Voorbeeld: in een klein netwerk zou u normaal gesproken het laatste cijfer wijzigen.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

Hoe het IP-adres aan de afdrukserver wordt toegewezen:

Als u een DHCP/BOOTP/RARP-server in uw netwerk hebt, zal de afdrukserver het IP-adres automatisch via deze server ontvangen.

OPMERKING

Op kleinere netwerken kan de DHCP-server ook de router zijn.

Raadpleeg de volgende pagina's voor informatie over DHCP, BOOTP en RARP:

DHCP gebruiken voor het configureren van het IP-adres >> pagina 116.

BOOTP gebruiken voor het configureren van het IP-adres >> pagina 118.

RARP gebruiken voor het configureren van het IP-adres >> pagina 117.

Als er geen DHCP/BOOTP/RARP-server beschikbaar is, zal het APIPA-protocol (Automatic Private IP Addressing) automatisch een IP-adres toewijzen binnen het bereik 169.254.1.0 tot 169.254.254.255.

Raadpleeg *APIPA gebruiken voor het configureren van het IP-adres* >> pagina 118 voor meer informatie over APIPA.

Subnetmasker

Subnetmaskers beperken de netwerkcommunicatie.

■ Voorbeeld: computer 1 kan communiceren met computer 2

- Computer 1

IP-adres: 192.168.1.2

Subnetmasker: 255.255.255.000

- Computer 2

IP-adres: 192.168.1.3

Subnetmasker: 255.255.255.000

Wanneer er een 0 voorkomt in het subnetmasker, betekent dit dat er geen limiet bestaat voor communicatie op dit deel van het adres. In het bovenstaande voorbeeld betekent dit dat we kunnen communiceren met alle apparaten die een IP-adres hebben dat begint met 192.168.1.x. (x. staat voor een nummer tussen 0 en 255).

Gateway (en router)

Een gateway is een netwerkpunt dat fungeert als een ingang naar een ander netwerk en dat gegevens die via het netwerk worden doorgegeven naar de juiste bestemming stuurt. De router weet waarheen gegevens die via de gateway binnenkwamen, geleid moeten worden. Als een bestemming zich op een extern netwerk bevindt, geeft de router gegevens aan het externe netwerk door. Wanneer uw netwerk met andere netwerken communiceert, zult u wellicht ook het IP-adres van de gateway moeten configureren. Als u het IP-adres van de gateway niet kent, kunt u dit bij uw netwerkbeheerder opvragen.

IEEE 802.1x-verificatie

IEEE 802.1x is een IEEE-standaard voor bedrade en draadloze netwerken die de toegang van onbevoegde netwerkapparaten verhindert. Uw Brother-machine (aanvrager) verstuurt een verificatieaanvraag naar een RADIUS-server (verificatieserver) via uw toegangspunt (verificator). Nadat uw aanvraag werd geverifieerd door de RADIUS-server, krijgt uw machine toegang tot het netwerk.

Verificatiemethoden

■ LEAP (voor draadloos netwerk)

Cisco Systems, Inc. heeft Cisco LEAP (Lightweight Extensible Authentication Protocol) ontwikkeld dat gebruik maakt van een gebruikersidentificatie en wachtwoord voor de verificatie.

■ EAP-FAST

Cisco Systems, Inc. heeft EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling) ontwikkeld dat gebruik maakt van een gebruikersidentificatie en wachtwoord voor de verificatie, en van symmetrische sleutelalgoritmes voor het verkrijgen van een getunneld verificatieproces.

De Brother-machine ondersteunt de volgende inwendige verificatiemethoden:

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

■ EAP-MD5 (voor bedraad netwerk)

EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) maakt gebruik van een gebruikersidentificatie en een wachtwoord voor vraag-antwoordverificatie.

■ PEAP

PEAP (Protected Extensible Authentication Protocol) werd ontwikkeld door Microsoft Corporation, Cisco Systems en RSA Security. PEAP creëert een versleutelde SSL (Secure Sockets Layer)/TLS (Transport Layer Security)-tunnel tussen een client en een verificatieserver voor het verzenden van een gebruikersidentificatie en wachtwoord. PEAP zorgt voor een wederzijdse verificatie tussen de server en de client.

De machine van Brother ondersteunt de volgende inwendige verificatiemethoden:

- PEAP/MS-CHAPv2
- PEAP/GTC

■ EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) werd ontwikkeld door Funk Software en Certicom. EAP-TTLS creëert een gelijkaardige versleutelde SSL-tunnel als bij PEAP tussen een client en een verificatieserver voor het verzenden van een gebruikersidentificatie en wachtwoord. EAP-TTLS zorgt voor een wederzijdse verificatie tussen de server en de client.

De machine van Brother ondersteunt de volgende inwendige verificatiemethoden:

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

■ EAP-TLS

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) vereist verificatie van het digitale certificaat bij zowel een client als een verificatieserver.

Termen en concepten voor draadloze netwerken (voor HL-3140CW, HL-3150CDW en HL-3170CDW)

Uw netwerk specificeren

SSID (Service Set Identifier) en kanalen

U moet de SSID en een kanaal configureren om aan te geven met welk draadloos netwerk u verbinding wilt maken.

■ SSID

Elk draadloos netwerk heeft een eigen, unieke netwerknaam; in technische termen wordt dit SSID genoemd. De SSID is een waarde van 32 bytes of minder en wordt toegewezen aan de toegangspoort. De draadloze netwerkapparaten die u aan het draadloze netwerk wilt toewijzen, moeten compatibel zijn met de toegangspoort. De toegangspoort en de draadloze netwerkapparaten verzenden regelmatig draadloze packets (ook wel beacons genoemd), die de SSID-gegevens bevatten. Wanneer uw draadloze netwerkapparaat een beacon ontvangt, kunt u draadloze netwerken identificeren die voldoende dichtbij zijn om er een verbinding mee te maken.

■ Kanalen

Draadloze netwerken gebruiken kanalen. Elk draadloos kanaal zit op een andere frequentie. Bij gebruik van een draadloos netwerk kunnen maximaal 14 kanalen worden gebruikt. In vele landen is echter slechts een beperkt aantal kanalen beschikbaar.

Beveiligingsvoorschriften

Verificatie en versleuteling

De meeste draadloze netwerken gebruiken bepaalde beveiligingsinstellingen. Deze beveiligingsinstellingen bepalen de verificatie (de manier waarop het apparaat zich bij het netwerk bekend maakt) en de versleuteling (de manier waarop de gegevens worden versleuteld wanneer deze over het netwerk worden verstuurd). **Als u tijdens het configureren van de draadloze Brother-machine bij deze opties een fout maakt, kan het apparaat geen verbinding met het draadloos netwerk maken.** Deze opties moeten derhalve zorgvuldig worden geconfigureerd. Raadpleeg *Ondersteunde protocollen en beveiligingsfuncties* >> pagina 115 om te zien welke verificatie- en versleutelingsmethoden deze draadloze machine van Brother ondersteunt.

Verificatie- en versleutelingsmethoden voor een persoonlijk draadloos netwerk

Een persoonlijk draadloos netwerk is een klein netwerk, zoals een draadloos thuisnetwerk, zonder IEEE 802.1x-ondersteuning.

Raadpleeg *Verificatie- en versleutelingsmethoden voor een draadloos Enterprise-netwerk* ►► pagina 106 als u de machine wilt gebruiken in een draadloos netwerk met IEEE 802.1x-ondersteuning.

Verificatiemethoden

■ Open systeem

Draadloze apparaten worden zonder enige verificatie op het netwerk toegelaten.

■ Gedeelde sleutel

Alle apparaten die toegang tot het draadloze netwerk hebben, delen een geheime, vooraf gedefinieerde sleutel.

De draadloze machine van Brother gebruikt de WEP-sleutel als vooraf gedefinieerde sleutel.

■ WPA-PSK/WPA2-PSK

Activeert een Wi-Fi Protected Access™ Pre-shared key (WPA-PSK/WPA2-PSK), waarmee de draadloze machine van Brother met behulp van TKIP voor WPA-PSK of AES voor WPA-PSK en WPA2-PSK (WPA-Personal) verbinding kan maken met toegangspunten.

Versleutelingsmethoden

■ Geen

Er wordt geen versleuteling gebruikt.

■ WEP

Met WEP (Wired Equivalent Privacy) worden de gegevens met een beveiligde sleutel verzonden en ontvangen.

■ TKIP

TKIP (Temporal Key Integrity Protocol) is in principe een sleutelcombinatie per pakket, met een combinatie van berichtintegriteitscontrole en een vernieuwingsmechanisme voor de sleutels.

■ AES

AES (Advanced Encryption Standard) biedt een krachtigere gegevensbescherming door gebruik te maken van een versleuteling met symmetrische sleutel.

OPMERKING

- IEEE 802.11n biedt geen ondersteuning voor WEP of TKIP voor de versleutelingsmethode.
- Als u verbinding wilt maken met uw draadloos netwerk via IEEE 802.11n, raden wij u aan te opteren voor AES.

Netwerksleutel

■ Open systeem/Gedeelde sleutel met WEP

Deze sleutel is een waarde van 64 bit of 128 bit die moet worden ingevoerd in een ASCII-formaat of een hexadecimaal formaat.

- 64 (40) bits ASCII:

Gebruikt 5 teksttekens. Bijvoorbeeld "WSLAN" (hoofdlettergevoelig)

- 64 (40) bits hexadecimaal:

Gebruikt 10 hexadecimale tekens, bijvoorbeeld "71f2234aba"

- 128 (104) bits ASCII:

Gebruikt 13 teksttekens. Bijvoorbeeld "Wirelesscomms" (hoofdlettergevoelig)

- 128 (104) bits hexadecimaal:

Gebruikt 26 hexadecimale tekens, bijvoorbeeld "71f2234ab56cd709e5412aa2ba"

■ WPA-PSK/WPA2-PSK en TKIP of AES

Maakt gebruik van een Pre-Shared Key (PSK) van meer dan 8 tekens en maximaal 63 tekens lang.

Verificatie- en versleutelingsmethoden voor een draadloos Enterprise-netwerk

Een draadloos Enterprise-netwerk is een groot netwerk, bijvoorbeeld wanneer u de machine in een draadloos bedrijfsnetwerk gebruikt, met IEEE 802.1x-ondersteuning. Als u de machine configureert in een draadloos netwerk met IEEE 802.1x-ondersteuning, kunt u de volgende verificatie- en versleutelingsmethoden gebruiken.

10

Verificatiemethoden

■ LEAP

Raadpleeg *LEAP (voor draadloos netwerk)* ►► pagina 102 voor LEAP.

■ EAP-FAST

Raadpleeg *EAP-FAST* ►► pagina 102 voor EAP-FAST.

■ PEAP

Raadpleeg *PEAP* ►► pagina 102 voor PEAP.

■ EAP-TTLS

Raadpleeg *EAP-TTLS* ►► pagina 103 voor EAP-TTLS.

■ EAP-TLS

Raadpleeg *EAP-TLS* ►► pagina 103 voor EAP-TLS.

Versleutelingsmethoden

- TKIP

Raadpleeg *TKIP* >> pagina 105 voor TKIP.

- AES

Raadpleeg *AES* >> pagina 105 voor AES.

- CKIP

Het oorspronkelijke Key Integrity Protocol voor LEAP van Cisco Systems, Inc.

Gebruikersidentificatie en wachtwoord

De volgende beveiligingsmethoden maken gebruik van een gebruikersidentificatie van minder dan 64 tekens en een wachtwoord van minder dan 32 tekens.

- LEAP

- EAP-FAST

- PEAP

- EAP-TTLS

- EAP-TLS (voor gebruikersidentificatie)

Types bijkomende netwerkinstellingen

De volgende functies kunnen worden gebruikt als u bijkomende netwerkinstellingen wilt configureren.

- Web Services voor afdrukken (Windows Vista®, Windows® 7 en Windows® 8)
- Verticaal koppelen (Windows® 7 en Windows® 8)

OPMERKING

Controleer of de hostcomputer en de machine zich ofwel op hetzelfde subnet bevinden, of dat de router foutloos is geconfigureerd, zodat gegevensuitwisseling tussen deze twee apparaten mogelijk is.

Drivers installeren die gebruikt worden voor afdrukken via Web Services (Windows Vista®, Windows® 7 en Windows® 8)

Met de functie Web Services kunt u machines op het netwerk opvolgen. Dit vereenvoudigt eveneens het driverinstallatieproces. Drivers die gebruikt worden voor afdrukken via Web Services kunnen geïnstalleerd worden door met de rechtermuisknop te klikken op het printerpictogram op de computer. De Web Services-poort (WSD-poort) van de computer wordt automatisch aangemaakt.

OPMERKING

- Zorg dat u een IP-adres op de machine hebt geconfigureerd alvorens u deze instelling doorvoert.
- Voor Windows Server® 2008/2012 moet u Print Services installeren.

- 1 Plaats de installatie-cd-rom.
- 2 Selecteer uw cd-rom-station/**install/driver/gdi/32_64**.
- 3 Dubbelklik op **dpinst86.exe** of **dpinst64.exe**.

OPMERKING

Als het scherm **Gebruikersaccountbeheer** wordt weergegeven:

(Windows Vista®) Klik op **Toestaan**.

(Windows® 7/Windows® 8) Klik op **Ja**.

4 (Windows Vista®)

Klik op  en selecteer vervolgens **Netwerk**.

(Windows® 7)

Klik op , **Configuratiescherm, Netwerk en internet** en vervolgens op **Computers en apparaten in het netwerk weergeven**.

- 5** De Web Services-naam van de machine wordt samen met het printerpictogram weergegeven. Klik met de rechtermuisknop op de machine die u wilt installeren.

OPMERKING

De Web Services-naam voor de Brother-machine is de modelnaam en het MAC-adres (ethernetadres) van uw machine (bv. Brother HL-XXXX (modelnaam) [XXXXXXXXXXXX] (MAC-adres / ethernetadres)).

- 6** Klik in het keuzemenu op **Installeren**.

De installatie van drivers die gebruikt worden voor afdrukken ongedaan maken via Web Services (Windows Vista®, Windows® 7 en Windows® 8)

Om Web Services te verwijderen van een computer, volgt u de onderstaande instructies.

1 (Windows Vista®)

Klik op  en selecteer vervolgens **Netwerk**.

(Windows® 7)

Klik op , **Configuratiescherm, Netwerk en internet** en vervolgens op **Computers en apparaten in het netwerk weergeven**.

- 2** De Web Services-naam van de machine wordt samen met het printerpictogram weergegeven. Klik met de rechtermuisknop op de machine die u wilt verwijderen.

- 3** Klik in het keuzemenu op **Verwijderen**.

Installatie voor Printen via het netwerk voor infrastructuurmodus bij gebruik van Vertical Pairing (Windows® 7 en Windows® 8)

Windows® Vertical Pairing is een technologie waarmee u uw machine die Vertical Pairing ondersteunt, kunt verbinden met uw infrastructuurnetwerk met behulp van de PIN-methode van WPS en de functie Web Services. Hiermee kunt u ook de printerdriver installeren via het pictogram van de printer op het scherm **Een apparaat toevoegen**.

Als de infrastructuurmodus geactiveerd is, kunt u de machine aansluiten op het draadloze netwerk en vervolgens de printerdriver installeren via deze functie. Volg de onderstaande stappen:

OPMERKING

- Als Web Services uitgeschakeld is op de machine, dient u dit weer in te schakelen. De Web Services voor de machine van Brother zijn standaard ingeschakeld. U kunt de instellingen voor Web Services wijzigen met Beheer via een webbrowser of BRAdmin Professional 3.
- Zorg ervoor dat uw WLAN-toegangspunt/-router gemarkeerd is met het compatibiliteitslogo voor Windows® 7 of Windows® 8. Contacteer voor vragen over het compatibiliteitslogo de fabrikant van uw toegangspunt/router.
- Zorg ervoor dat uw computer gemarkeerd is met het compatibiliteitslogo voor Windows® 7 of Windows® 8. Contacteer voor vragen over het compatibiliteitslogo de fabrikant van uw computer.
- Als u uw draadloos netwerk configureert via een externe draadloze NIC (Network Interface Card), dient u zich ervan te vergewissen dat de draadloze NIC gemarkeerd is met het compatibiliteitslogo voor Windows® 7 of Windows® 8. Neem contact op met de fabrikant van uw draadloze NIC voor meer informatie.
- Wanneer u een computer met Windows® 7 of Windows® 8 wilt gebruiken als een registrar, moet u deze eerst registreren op het netwerk. Raadpleeg hiervoor de instructies geleverd bij uw WLAN-toegangspunt/-router.

11

- 1 Schakel uw machine in.
- 2 Zet uw machine op WPS-modus (PIN-methode).
Uw machine configureren voor gebruik van de PIN-methode
Raadpleeg *Configuratie met behulp van de PIN-methode van WPS (Wi-Fi Protected Setup)*
➤➤ pagina 29.
- 3 Klik op de knop  en vervolgens op **Apparaten en printers**.
- 4 Kies **Een apparaat toevoegen** in het dialoogvenster **Apparaten en printers**.
- 5 Kies uw machine en voer de PIN in die uw machine heeft aangeduid.
- 6 Selecteer het infrastructuurnetwerk waarmee u verbinding wilt maken en klik op **Volgende**.
- 7 Wanneer uw machine wordt weergegeven in het dialoogvenster **Apparaten en printers**, zijn de draadloze configuratie en de installatie van de printerdriver gelukt.

Beveiligingsfuncties

Beveiligingsvoorschriften

■ CA (Certificate Authority)

Een CA is een entiteit die digitale certificaten uitvaardigt (vooral X.509-certificaten) en instaat voor de binding tussen de data-items in een certificaat.

■ CSR (Certificate Signing Request)

Een CSR is een bericht dat wordt verzonden van een verzoeker naar een CA om een certificaat aan te vragen. De CSR bevat informatie over de verzoeker, de openbare sleutel aangemaakt door de verzoeker en de digitale handtekening van de verzoeker.

■ Certificaat

Een certificaat is de informatie die een openbare sleutel bindt aan een identiteit. Het certificaat kan worden gebruikt om na te gaan of een openbare sleutel toebehoort aan een bepaald individu. Het formaat wordt gedefinieerd door de x.509-standaard.

■ CA-certificaat

Een CA-certificaat is een certificatie die de CA (Certificate Authority) zelf identificeert en de private sleutel ervan bevat. Het verifieert een certificaat dat werd uitgevaardigd door de CA.

■ Digitale handtekening

Een digitale handtekening is een waarde die wordt berekend via een cryptografisch algoritme en wordt toegevoegd aan een gegevensobject zodat om het even welke ontvanger van deze gegevens de handtekening kan gebruiken om de oorsprong en de integriteit van de gegevens na te gaan.

■ Cryptosysteem met openbare sleutel

Een cryptosysteem met openbare sleutel is een moderne tak van de cryptografie waarbij de algoritmes gebruik maken van twee sleutels (een openbare en een private sleutel) en waarbij een verschillende sleutel wordt gebruikt voor verschillende stappen in het algoritme.

■ Cryptosysteem met gedeelde sleutel

Een cryptosysteem met gedeelde sleutel is een tak van de cryptografie waarbij algoritmes worden gebruikt die dezelfde sleutel gebruiken voor twee verschillende stappen in het algoritme (zoals versleuteling en ontsleuteling).

Beveiligingsprotocollen

SSL (Secure Socket Layer) / TLS (Transport Layer Security)

Deze communicatiebeveiligingsprotocollen versleutelen gegevens om beveiligingsbedreigingen te voorkomen.

HTTPS

De versie van het internetprotocol Hyper Text Transfer Protocol (HTTP) dat SSL gebruikt.

IPPS

De versie van het afdrukprotocol IPP (Internet Printing Protocol) dat SSL gebruikt.

SNMPv3

Het SNMPv3 (Simple Network Management Protocol version 3) zorgt voor gebruikersverificatie en gegevensversleuteling om netwerkapparaten veilig te kunnen beheren.

Beveiligingsmethoden voor verzenden van e-mail

OPMERKING

U kunt de beveiligingsmethoden configureren met Beheer via een webbrowser. Raadpleeg *De instellingen van de machine configureren met Beheer via een webbrowser* >> pagina 48 voor meer informatie.

POP voor SMTP (PbS)

De gebruikersverificatiemethode wanneer e-mail via een client wordt verzonden. De client krijgt toestemming om de SMTP-server te gebruiken door toegang te krijgen tot de POP3-server alvorens de e-mail te verzenden.

SMTP-VERIF (SMTP-verificatie)

SMTP-AUTH is een uitbreiding van SMTP (het internetprotocol voor het verzenden van e-mail) en omvat tevens een verificatiemethode die verzekert dat de ware identiteit van de afzender bekend is.

APOP (Authenticated Post Office Protocol)

APOP is een uitbreiding van POP3 (het internetprotocol voor het ontvangen van e-mail) en omvat een verificatiemethode die het wachtwoord versleutelt wanneer de client e-mail ontvangt.

SMTP over SSL

De functie SMTP over SSL maakt het mogelijk versleutelde e-mails te versturen via SSL.

POP over SSL

De functie POP over SSL maakt het mogelijk versleutelde e-mails te ontvangen via SSL.



Bijlagen

Bijlage A	115
Bijlage B	116

Ondersteunde protocollen en beveiligingsfuncties

Interface	Ethernet ¹	10BASE-T, 100BASE-TX
	Draadloos ²	IEEE 802.11b/g/n (infrastructuurmodus/ad-hocmodus) IEEE 802.11g/n (Wi-Fi Direct)
Netwerk (algemeen)	Protocol (IPv4)	ARP, RARP, BOOTP, DHCP, APIPA (Auto IP), WINS/NetBIOS-naamresolutie, DNS Resolver, mDNS, LLMNR responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP-server, TELNET-server, HTTP/HTTPS-server, TFTP-client en -server, SMTP-client, SNMPv1/v2c/v3, ICMP, Web Services (Print), CIFS-client, SNTP-client
	Protocol (IPv6)	NDP, RA, DNS resolver, mDNS, LLMNR responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP-server, TELNET-server, HTTP/HTTPS-server, TFTP-client en -server, SMTP-client, SNMPv1/v2c/v3, ICMPv6, Web Services (Print), CIFS-client, SNTP-client
Netwerk (beveiliging)	Bedraad ¹	SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
	Draadloos ²	WEP 64/128 bit, WPA-PSK (TKIP/AES), WPA2-PSK (AES), SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
E-mail (beveiliging)	Bedraad ¹ en draadloos ²	APOP, POP voor SMTP, SMTP-AUTH, SSL/TLS (SMTP/POP)
Netwerk (draadloos) ²	Draadloze certificatie	Licentie Wi-Fi-certificatiemarkering (WPA™/WPA2™ - Enterprise, Personal), licentie identificatiemarkering Wi-Fi Protected Setup™ (WPS), AOSS-logo, Wi-Fi CERTIFIED™ Wi-Fi Direct™

¹ Voor HL-3150CDN, HL-3150CDW en HL-3170CDW

² Voor HL-3140CW, HL-3150CDW en HL-3170CDW

Services gebruiken

Een service is een bron die beschikbaar is voor computers die willen afdrukken op de afdrukserver van Brother. De afdrukserver van Brother biedt de volgende voorgedefinieerde services (voer de opdracht SHOW SERVICE uit op de remote console van de Brother-afdrukserver om een lijst van beschikbare services op te vragen): Typ `HELP` bij de opdrachtprompt voor een overzicht van ondersteunde opdrachten.

Service (voorbeeld)	Definitie
BINARY_P1	TCP/IP binair
TEXT_P1	Tekstservice van TCP/IP (voegt aan het einde van elke regel een regelterugloop toe)
PCL_P1	PCL-service (zet de PjL-compatibele machine in PCL-modus)
BRNxxxxxxxxxxxx	TCP/IP binair
BRNxxxxxxxxxxxx_AT ¹	PostScript®-service voor Macintosh
POSTSCRIPT_P1 ¹	PostScript®-service (zet de PjL-compatibele machine in PostScript®-modus)

Waar "xxxxxxxxxxxx" het MAC-adres (ethernetadres) van uw machine is.

¹ Voor HL-3170CDW

Andere manieren om het IP-adres in te stellen (voor geavanceerde gebruikers en beheerders)

DHCP gebruiken voor het configureren van het IP-adres

DHCP (Dynamic Host Configuration Protocol) is een van de geautomatiseerde mechanismen die gebruikt worden voor het toewijzen van een IP-adres. Als u een DHCP-server in uw netwerk hebt, zal de afdrukserver het IP-adres automatisch via de DHCP-server ontvangen en de naam registreren bij een met RFC 1001 en 1002 compatibele dynamische naamservice.

OPMERKING

Als u de afdrukserver niet via DHCP wilt configureren, dient u de Boot Method in te stellen op statisch, zodat de afdrukserver een statisch IP-adres heeft. Zo wordt voorkomen dat de afdrukserver probeert om een IP-adres van een van deze systemen te krijgen. U kunt de opstartmethode wijzigen met het bedieningspaneelmenu Netwerk van de machine, met BRAdmin of met Beheer via een webbrowser.

RARP gebruiken voor het configureren van het IP-adres

Voor u het IP-adres configureert met behulp van RARP, dient u de Boot Method van de machine in te stellen op RARP. U kunt de opstartmethode wijzigen met het bedieningspaneelmenu Netwerk van de machine, met BRAdmin of met Beheer via een webbrowser.

Het IP-adres van de afdrukserver van Brother kunt u configureren met de functie Reverse ARP (RARP) op uw hostcomputer. Daarvoor bewerkt u het bestand `/etc/ethers` (als dit bestand niet bestaat, kunt u het aanmaken) met een ingang gelijkaardig aan het volgende:

```
00:80:77:31:01:07    BRN008077310107 (of BRW008077310107 voor een draadloos netwerk)
```

De eerste ingang is het MAC-adres (ethernetadres) van de afdrukserver en de tweede ingang is de naam van de afdrukserver (deze naam moet dezelfde zijn als de naam die u hebt gebruikt in het bestand `/etc/hosts`).

Als de RARP-daemon nog niet draait, start u deze nu op (afhankelijk van uw systeem is de opdracht `rarpd`, `rarpd -a`, `in.rarpd -a` of een andere opdracht; typ `man rarpd` of raadpleeg de bij uw systeem geleverde documentatie voor meer informatie). Als u bij een systeem op basis van Berkeley UNIX wilt controleren of de RARP-daemon draait, typt u de onderstaande opdracht:

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

Bij systemen op basis van AT&T UNIX typt u:

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

De afdrukserver van Brother ontvangt het IP-adres van de RARP-daemon nadat de machine is opgestart.

BOOTP gebruiken voor het configureren van het IP-adres

Voor u het IP-adres configureert met behulp van BOOTP, dient u de Boot Method van de machine in te stellen op BOOTP. U kunt de opstartmethode wijzigen met het bedieningspaneelmenu Netwerk van de machine, met BRAdmin of met Beheer via een webbrowser.

BOOTP is een alternatief voor RARP. Het voordeel van BOOTP is dat ook het subnetmasker en de gateway geconfigureerd kunnen worden. Als u BOOTP wilt gebruiken voor het configureren van het IP-adres, moet BOOTP op uw hostcomputer geïnstalleerd en geactiveerd zijn (het moet in het bestand `/etc/services` op uw host als een echte service verschijnen; voer `man bootpd` in of raadpleeg de met uw systeem meegeleverde documentatie voor meer informatie). BOOTP wordt meestal opgestart via het bestand `/etc/inetd.conf` en u kunt dit activeren door `"#"` te verwijderen dat in dit bestand voor de ingang `bootp` staat. Een typische `bootp`-ingang in het bestand `/etc/inetd.conf` kan er bijvoorbeeld als volgt uitzien:

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

Afhankelijk van het systeem kan deze ingang `"bootps"` heten in plaats van `"bootp"`.

OPMERKING

Voor het activeren van BOOTP gebruikt u een tekstverwerkingsprogramma om `"#"` te verwijderen (staat er geen `"#"`, dan is BOOTP reeds geactiveerd). Bewerk nu het BOOTP-configuratiebestand (doorgaans `/etc/bootptab`) en voer de naam in, het netwerktype (1 voor Ethernet), MAC-adres (ethernetadres) en het IP-adres, het subnetmasker en de toegangspoort van de afdrukserver. Helaas kan de indeling van deze gegevens afwijken, en het is derhalve zaak dat u de met uw systeem meegeleverde documentatie raadpleegt om te zien hoe u deze informatie invoert (vele UNIX-systemen hebben templates in het bestand `bootptab` die u als voorbeeld kunt gebruiken). Enkele voorbeelden van een doorsnee `/etc/bootptab` ingang zijn: ("`BRN`" hieronder moet u voor een draadloos netwerk vervangen door `"BRW"`.)

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

en:

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

Bepaalde implementaties van BOOTP-hostsoftware reageren alleen op BOOTP-verzoeken als u in het configuratiebestand een download-bestandsnaam hebt opgenomen. In dat geval maakt u gewoon een leeg bestand op de host en specificeert u de bestandsnaam en zijn pad in het configuratiebestand.

Net als bij RARP, zal de afdrukserver zijn IP-adres bij de BOOTP-server opvragen zodra de machine wordt aangezet.

APIPA gebruiken voor het configureren van het IP-adres

De afdrukserver van Brother ondersteunt het APIPA-protocol (Automatic Private IP Addressing). Met APIPA zullen DHCP-clients automatisch een IP-adres en subnetmasker configureren als er geen DHCP-server beschikbaar is. Het apparaat kiest een eigen IP-adres van 169.254.1.0 t/m 169.254.254.255. Het subnetmasker wordt automatisch ingesteld op 255.255.0.0 en het gateway-adres wordt ingesteld op 0.0.0.0.

Standaard is het APIPA-protocol ingeschakeld. Als u het APIPA-protocol wilt uitschakelen, kunt u dit via het bedieningspaneel van de machine, via BRAdmin Light of via Beheer via een webbrowser.

ARP gebruiken voor het configureren van het IP-adres

Als u BRAdmin niet kunt gebruiken en het netwerk geen DHCP-server gebruikt, kunt u ook de opdracht ARP gebruiken. De ARP-opdracht is beschikbaar op Windows[®]-systemen waarop TCP/IP is geïnstalleerd, en op UNIX-systemen. Als u ARP wilt gebruiken, voert u de onderstaande opdracht in:

```
arp -s ipaddress ethernetaddress  
ping ipadres
```

Waar `ethernetadres` het MAC-adres (`ethernetadres`) van de afdrukserver is en `ipadres` het IP-adres van de afdrukserver is. Bijvoorbeeld:

■ Windows[®]-systemen

Op Windows[®]-systemen moet u het koppelteken "-" tussen ieder teken van het MAC-adres (`ethernetadres`) plaatsen.

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

■ UNIX/Linux-systemen

Op UNIX- en Linux-systemen moet u een dubbele punt ":" plaatsen tussen ieder cijfer van het MAC-adres (`ethernetadres`).

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

OPMERKING

Om de opdracht `arp -s` te kunnen gebruiken, dient u zich op hetzelfde Ethernetsegment te bevinden (met andere woorden, er mag zich geen router bevinden tussen de afdrukserver en het besturingssysteem).

Wanneer er een router tussen zit, kunt u BOOTP of andere methoden uit dit hoofdstuk gebruiken om het IP-adres in te voeren. Als uw beheerder heeft geconfigureerd dat het systeem IP-adressen verstrekt met gebruikmaking van BOOTP, DHCP of RARP, kan de afdrukserver van Brother een IP-adres van een van deze systemen ontvangen. In dat geval hoeft u de opdracht ARP niet te gebruiken. De opdracht ARP werkt slechts één keer. Nadat u de opdracht ARP hebt gebruikt om het IP-adres van de Brother-afdrukserver te configureren, kunt u de opdracht ARP om veiligheidsredenen niet meer gebruiken om dat adres te wijzigen. De afdrukserver zal alle pogingen tot wijziging van het IP-adres negeren. Als u het IP-adres weer wilt wijzigen, dient u Beheer via een webbrowser of TELNET (met de opdracht SET IP ADDRESS) te gebruiken, of moet u de standaardinstellingen van de afdrukserver herstellen (waarna u de opdracht ARP weer kunt gebruiken).

TELNET-console gebruiken voor het configureren van het IP-adres

U kunt ook de opdracht TELNET gebruiken om het IP-adres te wijzigen.

TELNET biedt een doeltreffende methode om het IP-adres van de machine te wijzigen. Er moet echter reeds een geldig IP-adres in de afdrukserver zijn geprogrammeerd.

Typ TELNET <opdrachtregel> bij de opdrachtprompt van de systeemprompt, waar <opdrachtregel> het IP-adres van de afdrukserver is. Wanneer er verbinding is gemaakt, drukt u op Return of Enter om de prompt "#" te openen. Voer het wachtwoord "access" in (het wachtwoord verschijnt niet op het scherm).

U wordt om een gebruikersnaam gevraagd. Voer bij deze prompt een willekeurige naam in.

Nu verschijnt de prompt Local>. Typ SET IP ADDRESS ipadres, waar ipadres het IP-adres is dat u aan de afdrukserver wilt toewijzen (vraag uw netwerkbeheerder welk IP-adres u kunt gebruiken).

Bijvoorbeeld:

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

U stelt nu het subnetmasker in door SET IP SUBNET subnetmasker te typen, waar subnetmasker het subnetmasker is dat u aan de afdrukserver wilt toewijzen (vraag uw netwerkbeheerder welk subnetmasker u kunt gebruiken). Bijvoorbeeld:

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

Als u geen subnetten gebruikt, moet u een van de onderstaande subnetmaskers gebruiken:

255.0.0.0 voor klasse A netwerken

255.255.0.0 voor klasse B netwerken

255.255.255.0 voor klasse C netwerken

Het netwerktype kan worden aangeduid met de linkergroep cijfers in uw IP-adres. De waarde van deze groep kan variëren van 1 t/m 127 voor klasse A netwerken (bijvoorbeeld 13.27.7.1), 128 t/m 191 voor klasse B netwerken (bijvoorbeeld 128.10.1.30), en 192 t/m 255 voor klasse C netwerken (bijvoorbeeld 192.168.1.4).

Als u een gateway (router) hebt, voert u het adres daarvan in met de opdracht SET IP ROUTER routeradres, waar routeradres het IP-adres van de gateway is die u aan de afdrukserver wilt toewijzen. Bijvoorbeeld:

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

Typ SET IP METHOD STATIC om de methode voor IP-toegang op statisch in te stellen.

Om te controleren of u de juiste IP-informatie hebt ingevoerd, typt u SHOW IP.

Typ EXIT of druk op Ctrl-D (m.a.w. houd de Ctrl-toets ingedrukt en typ "D") om deze remote console sessie af te sluiten.

A

Ad-hocmodus	11, 32
AES	105
AOSS™	27, 38
APIPA	37, 96, 118
APOP	113
ARP	96, 119

B

Bedieningspaneel	35
Beheer via een webbrowser	2, 7, 74
Beveiligingsvoorschriften	111
BINARY_P1	116
BOOTP	96, 118
BRAdmin Light	2, 4
BRAdmin Professional 3	2, 7, 77
BRNxxxxxxxxxxxx	116
BRNxxxxxxxxxxxx_AT	116
BRPrint Auditor	8

C

CA	111
CA-certificaat	111
Certificaat	58, 111
CIFS	99
CKIP	107
Cryptosysteem met gedeelde sleutel	111
Cryptosysteem met openbare sleutel	111
CSR	111
Custom Raw Port	97

D

DHCP	96, 116
Digitale handtekening	111
DNS-client	97
Draadloos netwerk	9, 104

E

EAP-FAST	102
EAP-MD5	102
EAP-TLS	103
EAP-TTLS	103
Encryptie	105
Ethernet	38

F

Fabrieksinstellingen	40
----------------------------	----

G

Gateway	37
Gedeelde sleutel	105

H

HTTP	47, 98
HTTPS	74, 112

I

IEEE 802.1x	14, 17, 102
Infrastructuurmodus	10
IP Boot-pogingen	37
IP-adres	37, 100
IPP	97
IPPS	78, 112
IPv6	37, 99

K

Kanalen	104
---------------	-----

L

LEAP	102
LLMNR	98
LPR/LPD	97

M

MAC-adres	5, 6, 7, 39, 41, 109, 116, 117, 118, 119
mDNS	97

N

NetBIOS-naamresolutie	97
Netwerk, gedeelde printer	95
Netwerkconfiguratie rapport	41
Netwerkinstellingen resetten	40
Netwerksleutel	106

O

Ondersteunde protocollen en beveiligingsfuncties	115
Open systeem	105

P

PBC	27, 38
PCL_P1	116
PEAP	102
Peer-to-Peer	94
PIN-methode	29, 38
POP over SSL	113
POP voor SMTP	80, 113
Port 9100	97
POSTSCRIPT_P1	116
Protocol	96

R

RARP	96, 117
Reparatietool voor netwerkaansluiting	88
RFC 1001	116

S

Service	116
SMTP over SSL	113
SMTP-client	97
SMTP-VERIF	80, 113
SNMP	98
SNMPv3	74, 112
SNTP	99
SSID	104
SSL/TLS	58, 112
Status Monitor	2
Subnetmasker	37, 101

T

TCP/IP	36, 43, 44, 45, 96
TELNET	98, 120
TEXT_P1	116
TKIP	105

V

Verificatie	105
Verticaal koppelen	2, 108

W

Web Services	98, 108, 109
WEP	105
WINS	97
Wizard Driver installeren	2
WLAN-rapport	42, 90, 92
WPA-PSK/WPA2-PSK	105
WPS (Wi-Fi Protected Setup)	27, 29, 38