

네트워크 용어집


이 네트워크 용어집에서는 **Brother** 기기의 고급 네트워크 기능과 함께 일반적인 네트워킹 및 일반 용어에 대한 설명이 제공됩니다 .

지원되는 프로토콜 및 네트워크 기능은 사용 중인 모델에 따라 다릅니다 . 지원되는 기능 및 네트워크 프로토콜을 확인하려면 부속된 *네트워크 사용자 설명서*를 참조하십시오 . 최신 설명서를 다운로드하려면 **Brother Solutions Center**(<http://solutions.brother.com/>) 를 방문하십시오 .

Brother Solutions Center 에서 기기의 최신 드라이버 및 유틸리티를 다운로드하거나 , **FAQ** 및 문제 해결 요령을 읽어보거나 , 특수한 인쇄 솔루션에 대해 알아볼 수도 있습니다 .

표기법

본 사용자 가이드에서는 다음과 같은 아이콘을 사용합니다 .

 참고	참고는 발생할 수 있는 상황에 대처하는 방법에 대해 설명하거나 다른 기능과 함께 조작하는 방법에 대한 요령을 제공합니다 .
---	--

중요 사항

- 본 제품은 구입한 나라에서만 사용하도록 승인되었습니다 . 본 제품을 구입한 나라가 아닌 다른 나라에서 사용하지 마십시오 . 해당 국가의 무선 통신 및 전원 규정에 위반될 수 있습니다 .
- 본 설명서에서 Windows® XP 는 Windows® XP Professional, Windows® XP Professional x64 Edition 및 Windows® XP Home Edition 을 나타냅니다 .
- 본 설명서에서 Windows Server® 2003 은 Windows Server® 2003 및 Windows Server® 2003 x64 Edition 을 나타냅니다 .
- 본 설명서에서 Windows Server® 2008 은 Windows Server® 2008 및 Windows Server® 2008 R2 를 나타냅니다 .
- 본 설명서에서 Windows Vista® 는 Windows Vista® 의 모든 Edition 을 나타냅니다 .
- 본 설명서에서 Windows® 7 은 Windows® 7 의 모든 Edition 을 나타냅니다 .
- 다른 설명서를 다운로드하려면 Brother Solutions Center(<http://solutions.brother.com/>) 를 방문하고 해당 모델 페이지에서 설명서를 클릭하십시오 .

목차

1	네트워크 연결 및 프로토콜 유형	1
	네트워크 연결 유형.....	1
	유선 네트워크 연결 예	1
	프로토콜	3
	TCP/IP 프로토콜 및 기능	3
	기타 프로토콜	6
2	네트워크에 대한 기기 구성	7
	IP 주소, 서브넷 마스크 및 게이트웨이	7
	IP 주소	7
	서브넷 마스크	8
	게이트웨이 (및 라우터)	8
	IEEE 802.1x 인증	9
3	무선 네트워크 용어 및 개념	11
	네트워크 지정	11
	SSID(Service Set Identifier) 및 채널	11
	보안 용어	11
	인증 및 암호화	11
	개인 무선 네트워크를 위한 인증 및 암호화 방법	12
	기업 무선 네트워크를 위한 인증 및 암호화 방법	13
4	Windows® 추가 네트워크 설정	15
	추가 네트워크 설정 유형	15
	Web Services(Windows Vista® 및 Windows® 7) 를 사용할 때의 네트워크 인쇄 설치	15
	수직 페어링 (Windows® 7) 사용 시 인프라 모드에 대한 네트워크 인쇄 설치	17
5	보안 용어 및 개념	19
	보안 기능	19
	보안 용어	19
	보안 프로토콜	20
	전자 메일 송신 및 수신을 위한 보안 방법	21
A	부록 A	22
	서비스 사용	22
	IP 주소를 설정하는 다른 방법 (고급 사용자 및 관리자).....	22
	DHCP 를 사용하여 IP 주소 구성	22
	RARP 를 사용하여 IP 주소 구성	23
	BOOTP 를 사용하여 IP 주소 구성	24

APIPA 를 사용하여 IP 주소 구성	25
ARP 를 사용하여 IP 주소 구성	25
TELNET 콘솔을 사용하여 IP 주소 구성	26

B 색인

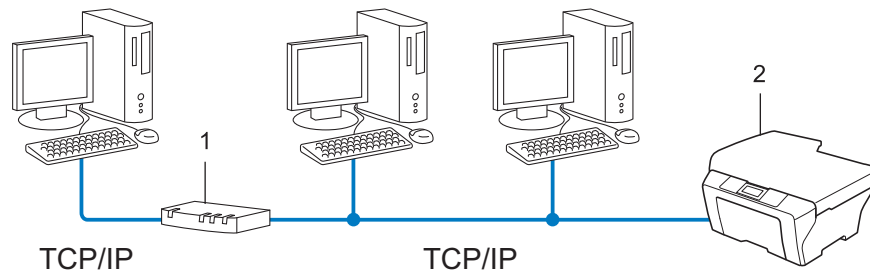
28

네트워크 연결 유형

유선 네트워크 연결 예

TCP/IP 를 사용한 피어 투 피어 인쇄

피어 투 피어 환경에서는 각 컴퓨터가 각 장치에 데이터를 직접 송신 및 수신합니다. 파일 액세스 또는 기기 공유를 제어하는 중앙 서버가 없습니다.



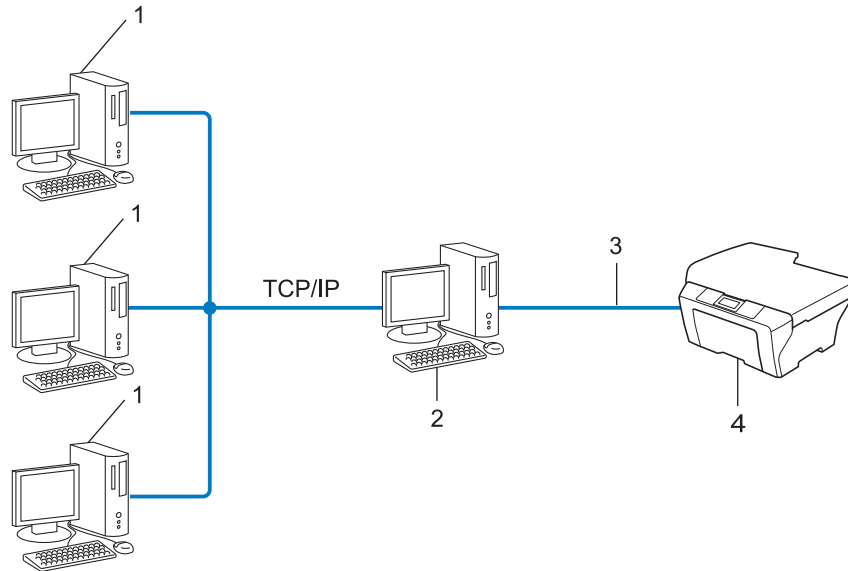
1 라우터

2 네트워크 기기 (본 기기)

- 2 대 또는 3 대의 컴퓨터로 구성된 소규모 네트워크의 경우 네트워크 공유 인쇄 방식보다 구성하기 쉬운 피어 투 피어 인쇄 방식을 권장합니다. 2 페이지의 *네트워크 공유 인쇄*를 참조하십시오.
- 각 컴퓨터에서 TCP/IP 프로토콜을 사용해야 합니다.
- Brother 기기는 적합한 IP 주소 구성이 필요합니다.
- 라우터를 사용하는 경우 컴퓨터 및 Brother 기기에 게이트웨이 주소를 구성해야 합니다.

네트워크 공유 인쇄

네트워크 공유 환경에서 각 컴퓨터는 중앙에서 제어되는 컴퓨터를 통해 데이터를 송신합니다. 이 유형의 컴퓨터를 "서버" 또는 "인쇄 서버" 라고도 부릅니다. 서버의 작업은 모든 인쇄 작업을 제어하는 것입니다.



- 1 클라이언트 컴퓨터
- 2 " 서버 " 또는 " 인쇄 서버 " 라고도 함
- 3 TCP/IP, USB 또는 병렬 (사용 가능한 경우)
- 4 네트워크 기기 (본 기기)

- 대규모 네트워크에서는 네트워크 공유 인쇄 환경을 권장합니다 .
- " 서버 " 또는 " 인쇄 서버 " 에서는 TCP/IP 인쇄 프로토콜을 사용해야 합니다 .
- Brother 기기를 USB 또는 서버의 병렬 인터페이스를 통해 연결하지 않은 경우 Brother 기기가 적합한 IP 주소로 구성되어 있어야 합니다 .

프로토콜

TCP/IP 프로토콜 및 기능

프로토콜은 네트워크에서 데이터를 전송하기 위한 일련의 표준화된 규칙의 집합입니다. 프로토콜을 사용하면 네트워크에 연결된 리소스에 액세스할 수 있습니다.

Brother 기기에서 사용되는 인쇄 서버는 TCP/IP(Transmission Control Protocol/Internet Protocol) 프로토콜을 지원합니다.

TCP/IP 는 인터넷 및 전자 메일과 같은 통신에 사용되는 가장 일반적인 프로토콜입니다. 이 프로토콜은 Windows®, Windows Server®, Mac OS X 및 Linux® 와 같은 거의 모든 운영 체제에서 사용할 수 있습니다. Brother 기기에서는 다음과 같은 TCP/IP 프로토콜을 사용할 수 있습니다.



참고

- HTTP 인터페이스(웹 브라우저)를 사용하여 프로토콜 설정을 구성할 수 있습니다. (*네트워크 사용자 설명서*를 참조하십시오.)
- Brother 기기에서 지원하는 프로토콜을 확인하려면 *네트워크 사용자 설명서*를 참조하십시오.
- 지원되는 보안 프로토콜에 대한 자세한 내용은 20 페이지의 *보안 프로토콜*을 참조하십시오.

DHCP/BOOTP/RARP

DHCP/BOOTP/RARP 프로토콜을 사용하면 IP 주소를 자동으로 구성할 수 있습니다.



참고

DHCP/BOOTP/RARP 프로토콜을 사용하려면 네트워크 관리자에게 문의하십시오.

APIPA

기기의 제어판 (LCD 모델의 경우) 또는 BRAdmin 소프트웨어를 사용하여 IP 주소를 직접 지정하지 않거나, DHCP/BOOTP/RARP 서버를 사용하여 자동으로 IP 주소를 지정하지 않으면 APIPA(Automatic Private IP Addressing) 프로토콜이 169.254.1.0 에서 169.254.254.255 사이의 IP 주소를 자동으로 지정합니다.

ARP

Address Resolution Protocol 은 IP 주소를 TCP/IP 네트워크의 MAC 주소에 매핑합니다.

DNS 클라이언트

Brother 인쇄 서버는 DNS(Domain Name System) 클라이언트 기능을 지원합니다 . 이 기능은 인쇄 서버가 DNS 이름을 사용하여 다른 장치와 통신할 수 있게 해줍니다 .

NetBIOS 이름 확인

Network Basic Input/Output System 이름 확인을 사용하면 네트워크 연결 중에 NetBIOS 이름을 사용하여 다른 장치의 IP 주소를 가져올 수 있습니다 .

WINS

Windows Internet Name Service 는 로컬 네트워크에 있는 IP 주소 및 NetBIOS 이름을 통합하여 NetBIOS 이름 확인을 위한 정보를 제공하는 서비스입니다 .

LPR/LPD

TCP/IP 네트워크에서 일반적으로 사용되는 인쇄 프로토콜입니다 .

SMTP 클라이언트

SMTP(Simple Mail Transfer Protocol) 클라이언트는 인터넷 또는 인트라넷을 통해 전자 메일을 송신하기 위해 사용됩니다 .

Custom Raw Port(기본값 : Port 9100)

TCP/IP 네트워크에서 일반적으로 사용되는 또 다른 인쇄 프로토콜입니다 . 대화식 데이터 전송을 지원합니다 .

IPP

Internet Printing Protocol(IPP 버전 1.0) 은 인터넷을 통해 액세스 가능한 기기에 직접 문서를 인쇄할 수 있게 해줍니다 .



참고

IPPS 프로토콜에 대해서는 20 페이지의 *보안 프로토콜*을 참조하십시오 .

mDNS

mDNS 는 Mac OS X Simple Network Configured 시스템에서 작동할 수 있도록 Brother 인쇄 서버가 자동으로 구성되도록 합니다 .

TELNET

TELNET 프로토콜은 컴퓨터에서 TCP/IP 네트워크의 원격 네트워크 장치를 제어할 수 있게 해줍니다 .

SNMP

SNMP(Simple Network Management Protocol) 는 컴퓨터 , 라우터 및 Brother 네트워크에 사용할 수 있는 기기를 포함하여 네트워크 장치를 관리하기 위해 사용됩니다 . Brother 인쇄 서버는 SNMPv1, SNMPv2c 및 SNMPv3 를 지원합니다 .



참고

SNMPv3 프로토콜에 대해서는 20 페이지의 *보안 프로토콜*을 참조하십시오 .

LLMNR

LLMNR(Link-Local Multicast Name Resolution) 프로토콜은 네트워크에 DNS(Domain Name System) 서버가 없는 경우 주변 컴퓨터의 이름을 확인합니다 . LLMNR Responder 기능은 Windows Vista® 및 Windows® 7 과 같은 LLMNR Sender 기능이 있는 컴퓨터를 사용할 때 IPv4 또는 IPv6 환경에서 모두 작동합니다 .

Web Services

Web Services 프로토콜은 Windows Vista® 또는 Windows® 7 사용자가 네트워크 폴더에서 기기 아이콘을 마우스 오른쪽 버튼으로 클릭하여 Brother 프린터 드라이버를 설치할 수 있게 해줍니다 . (15 페이지의 *Web Services(Windows Vista® 및 Windows® 7) 를 사용할 때의 네트워크 인쇄 설치*을 참조하십시오 .) Web Services 는 또한 컴퓨터에서 기기의 현재 상태를 확인할 수 있게 해줍니다 .

HTTP

HTTP 프로토콜은 웹 서버와 웹 브라우저 사이에 데이터를 전송하는 데 사용됩니다 .



참고

HTTPS 프로토콜에 대해서는 20 페이지의 *보안 프로토콜*을 참조하십시오 .

FTP(FTP 로 스캔 기능용)

FTP(File Transfer Protocol) 는 Brother 기기가 네트워크 또는 인터넷 상에서 로컬 FTP 서버에 흑백 또는 컬러 문서를 직접 스캔할 수 있게 해줍니다 .

SNTP

Simple Network Time Protocol 은 TCP/IP 네트워크에서 컴퓨터 시간을 동기화하기 위해 사용됩니다 . 웹 기반 관리 (웹 브라우저) 를 사용하여 **SNTP** 설정을 구성할 수 있습니다 . (자세한 내용은 *네트워크 사용자 설명서*를 참조하십시오 .)

CIFS

Common Internet File System 은 컴퓨터가 Windows[®] 에서 파일 및 프린터를 공유하는 표준 방법입니다 .

LDAP

LDAP(Lightweight Directory Access Protocol) 는 Brother 기기가 LDAP 서버에서 팩스 번호 및 전자 메일 주소와 같은 정보를 검색할 수 있게 해줍니다 .

IPv6

IPv6 은 차세대 인터넷 프로토콜입니다 . IPv6 프로토콜에 대한 자세한 내용을 보려면 <http://solutions.brother.com/> 에서 사용 중인 기기에 대한 모델 페이지를 참조하십시오 .

기타 프로토콜

LLTD

LLTD(Link Layer Topology Discovery) 프로토콜은 Windows Vista[®]/Windows[®] 7 네트워크 맵에서 Brother 기기를 쉽게 찾을 수 있게 해줍니다 . 본 Brother 기기는 쉽게 구분 가능한 아이콘 및 노드 이름으로 표시됩니다 . 이 프로토콜의 기본 설정은 OFF 입니다 . 웹 기반 관리 (웹 브라우저) (*네트워크 사용자 설명서* 참조) 및 **BRAdmin Professional 3** 유틸리티 소프트웨어를 사용하여 LLTD 를 활성화할 수 있습니다 . **BRAdmin Professional 3** 를 다운로드 하려면 <http://solutions.brother.com/> 에서 해당 모델의 다운로드 페이지를 방문하십시오 .

IP 주소 , 서브넷 마스크 및 게이트웨이

네트워크에 연결된 TCP/IP 환경에서 기기를 사용하려면 IP 주소 및 서브넷 마스크를 구성해야 합니다 . 인쇄 서버에 지정하는 IP 주소는 호스트 컴퓨터와 동일한 논리적 네트워크에 있어야 합니다 . 그렇지 않으면 서브넷 마스크와 게이트웨이 주소를 적절히 구성해야 합니다 .

IP 주소

IP 주소는 네트워크에 연결된 각 장치를 식별하는 일련의 숫자입니다 . IP 주소는 점으로 구분된 네 개의 숫자로 구성됩니다 . 각 숫자는 0 부터 255 까지입니다 .

■ 예 : 소규모 네트워크에서는 일반적으로 마지막 숫자를 변경합니다 .

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

IP 주소가 인쇄 서버에 지정된 방식 :

네트워크에 DHCP/BOOTP/RARP 서버가 있으면 인쇄 서버가 해당 서버에서 IP 주소를 자동으로 가져옵니다 .

참고

소규모 네트워크에서는 DHCP 서버가 라우터가 될 수도 있습니다 .

DHCP, BOOTP 및 RARP 에 대한 자세한 내용은

22 페이지의 *DHCP 를 사용하여 IP 주소 구성* 를 참조하십시오 .

24 페이지의 *BOOTP 를 사용하여 IP 주소 구성* .

23 페이지의 *RARP 를 사용하여 IP 주소 구성* .

DHCP/BOOTP/RARP 서버가 없으면 APIPA(Automatic Private IP Addressing) 프로토콜이 169.254.1.0 부터 169.254.254.255 까지의 IP 주소를 자동으로 지정합니다 . APIPA 에 대한 자세한 내용은 25 페이지의 *APIPA 를 사용하여 IP 주소 구성* 를 참조하십시오 .

서브넷 마스크

서브넷 마스크는 네트워크 통신을 제한합니다 .

■ 예 : 컴퓨터 1 이 컴퓨터 2 에 데이터 전송

- 컴퓨터 1

IP 주소 : 192.168.1.2

서브넷 마스크 : 255.255.255.000

- 컴퓨터 2

IP 주소 : 192.168.1.3

서브넷 마스크 : 255.255.255.000

서브넷 마스크에 0 이 있으면 이 주소 부분에서 통신하는 데 제한이 없습니다 . 위 예에서는 192.168.1.x 로 시작하는 IP 주소가 있는 모든 장치와 통신할 수 있음을 나타냅니다 . (여기서 x 는 0 부터 255 까지의 숫자입니다 .)

게이트웨이 (및 라우터)

게이트웨이는 다른 네트워크로의 진입점으로 사용되어 네트워크를 통해 전송된 데이터를 정확한 대상에 송신하는 네트워크 지점입니다 . 라우터는 게이트웨이에 도착하는 데이터의 목적지를 확인합니다 . 대상이 외부 네트워크에 있는 경우 라우터가 데이터를 외부 네트워크로 전송합니다 . 네트워크가 다른 네트워크와 통신할 경우 게이트웨이 IP 주소를 구성해야 할 수 있습니다 . 게이트웨이 IP 주소를 모를 경우 네트워크 관리자에게 문의하십시오 .

IEEE 802.1x 인증

IEEE 802.1x 는 인증되지 않은 네트워크 장치가 유선 및 무선 네트워크에 액세스하는 것을 제한하는 IEEE 표준입니다 . Brother 기기 (요청자) 는 사용자의 액세스 포인트 (인증자) 를 통해 RADIUS 서버 (인증 서버) 에 인증 요청을 보냅니다 . RADIUS 서버에서 요청을 확인한 다음 본 기기가 네트워크에 액세스할 수 있습니다 .

인증 방법

■ LEAP(무선 네트워크용)

Cisco LEAP(Light Extensible Authentication Protocol) 는 Cisco Systems, Inc. 에서 개발된 기술로 사용자 ID 및 암호를 사용하여 인증을 수행합니다 .

■ EAP-FAST

EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secured Tunnel) 는 Cisco Systems, Inc. 에서 개발된 기술로 , 사용자 ID 및 암호를 사용하여 인증을 수행하고 대칭 키 알고리즘을 사용하여 터널링된 인증 프로세스를 구현합니다 .

Brother 기기는 다음과 같은 내부 인증을 지원합니다 .

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

■ EAP-MD5(유선 네트워크용)

EAP-MD5(Extensible Authentication Protocol-Message digest algorithm 5) 는 사용자 ID 및 암호를 사용하여 시도 - 응답 (challenge-response) 인증을 수행합니다 .

■ PEAP

PEAP(Protected Extensible Authentication Protocol) 는 Microsoft Corporation, Cisco Systems 및 RSA Security 에서 개발되었습니다 . PEAP 는 클라이언트와 인증 서버 간에 암호화 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 터널을 만들어 사용자 ID 및 암호를 전송합니다 . PEAP 는 서버와 클라이언트 사이에 상호 인증을 제공합니다 .

Brother 기기는 다음과 같은 내부 인증을 지원합니다 .

- PEAP/MS-CHAPv2
- PEAP/GTC

■ EAP-TTLS

EAP-TTLS(Extensible Authentication Protocol Tunneled Transport Layer Security) 는 Funk Software 및 Certicom 에서 개발되었습니다 . EAP-TTLS 는 PEAP 에 대해 비슷한 암호화 SSL 터널을 만들어서 클라이언트와 인증 서버 사이에 사용자 ID 와 암호를 전송합니다 . EAP-TTLS 는 서버와 클라이언트 사이에 상호 인증을 제공합니다 .

Brother 기기는 다음과 같은 내부 인증을 지원합니다 .

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

■ EAP-TLS

EAP-TLS(Extensible Authentication Protocol Transport Layer Security) 에는 클라이언트와 인증 서버 모두에서 디지털 인증서 인증을 요구합니다 .

네트워크 지정

SSID(Service Set Identifier) 및 채널

SSID 및 채널을 구성하여 연결하려는 무선 네트워크를 지정해야 합니다.

■ SSID

각 무선 네트워크에는 고유한 네트워크 이름이 있으며, 기술적으로는 이를 **SSID** 또는 **ESSID(Extended Service Set Identifier)** 라고 합니다. **SSID** 는 32 바이트 이하의 값으로 액세스 포인트에 지정됩니다. 무선 네트워크에 연결하려는 무선 네트워크 장치는 액세스 포인트와 일치해야 합니다. 액세스 포인트 및 무선 네트워크 장치는 **SSID** 정보가 있는 무선 패킷 (비콘이라고 함) 을 정기적으로 전송합니다. 무선 네트워크 장치에서 비콘이 수신된 경우 부근에서 무선 신호가 수신되는 무선 네트워크를 식별해낼 수 있습니다.

■ 채널

무선 네트워크에는 채널이 사용됩니다. 각 무선 채널은 서로 다른 주파수를 사용합니다. 무선 네트워크를 사용할 때 사용 가능한 채널 수는 최대 14 개입니다. 하지만 많은 국가에서 사용 가능한 채널 수를 제한하고 있습니다.

보안 용어

인증 및 암호화

대부분의 무선 네트워크에는 몇 가지 보안 설정이 사용됩니다. 이러한 보안 설정은 인증 (네트워크에서 장치를 식별하는 방법) 및 암호화 (네트워크에 전송되는 데이터의 암호화 방법) 를 정의합니다. **Brother** 무선 기기를 구성할 때 이러한 옵션을 올바르게 지정하지 않으면 무선 네트워크에 연결할 수 없습니다. 따라서 이러한 옵션을 구성할 때 주의가 필요합니다. **Brother** 무선 기기가 지원하는 인증 및 암호화 방법을 보려면 *네트워크 사용자 설명서*에서 해당 정보를 참조하십시오.

개인 무선 네트워크를 위한 인증 및 암호화 방법

개인 무선 네트워크는 IEEE 802.1x 지원 없이 가정 내 무선 네트워크에서 기기를 사용하는 것과 같은 소규모 네트워크입니다 .

IEEE 802.1x 지원 무선 네트워크에서 기기를 사용하려면 13 페이지의 *기업 무선 네트워크를 위한 인증 및 암호화 방법*을 참조하십시오 .

인증 방법

■ 오픈 시스템

무선 장치가 인증 없이도 네트워크에 액세스할 수 있도록 허용됩니다 .

■ 공유 키

미리 정의된 보안 키는 무선 네트워크에 액세스하는 모든 장치에서 공유됩니다 .

Brother 무선 기기는 미리 정의된 키로 WEP 키를 사용합니다 .

■ WPA-PSK/WPA2-PSK

Brother 무선 기기를 WPA-PSK 용 TKIP 또는 WPA-PSK 및 WPA2-PSK 용 AES(WPA-Personal) 를 사용하여 액세스 포인트와 연결할 수 있게 해주는 Wi-Fi Protected Access Pre-shared Key(WPA-PSK/WPA2-PSK) 를 지원합니다 .

암호화 방법

■ 없음

암호화 방법이 사용되지 않습니다 .

■ WEP

WEP(Wired Equivalent Privacy) 을 사용하여 보안 키로 데이터를 송수신합니다 .

■ TKIP

TKIP(Temporal Key Integrity Protocol) 는 메시지 무결성 검사 및 키 재입력 메커니즘을 혼합한 사전 패킷 키를 제공합니다 .

■ AES

AES(Advanced Encryption Standard) 는 Wi-Fi® 에서 인증된 강력한 암호화 표준입니다 .

네트워크 키

■ 오픈 시스템 /WEP 공유 키

이 키는 ASCII 또는 16 진수 형식으로 입력해야 하는 64 비트 또는 128 비트 값입니다 .

- 64(40) 비트 ASCII:

5 자의 텍스트 문자를 사용합니다 . 예 : "WLAN"(대소문자 구분)

- 64(40) 비트 16 진수 :

10 자릿수의 16 진수 데이터를 사용합니다 . 예 : "71f2234aba"

- 128(104) 비트 ASCII:

13 자의 텍스트 문자를 사용합니다 . 예 : "Wirelesscomms"(대소문자 구분)

- 128(104) 비트 16 진수 :

26 자릿수의 16 진수 데이터를 사용합니다 . 예 : "71f2234ab56cd709e5412aa2ba"

■ WPA-PSK/WPA2-PSK 및 TKIP 또는 AES

길이가 8 자 이상 , 최대 63 자인 PSK(Pre-Shared Key) 를 사용합니다 .

기업 무선 네트워크를 위한 인증 및 암호화 방법

기업 무선 네트워크는 IEEE 802.1x 지원을 포함하여 업무용 기업 무선 네트워크에서 기기를 사용하는 것과 같은 대규모 네트워크입니다 . IEEE 802.1x 지원 무선 네트워크에서 기기를 구성한 경우 다음 인증 및 암호화 방법을 사용할 수 있습니다 .

인증 방법

■ LEAP

LEAP 는 9 페이지의 *LEAP(무선 네트워크용)* 를 참조하십시오 .

■ EAP-FAST

EAP-FAST 는 9 페이지의 *EAP-FAST* 를 참조하십시오 .

■ PEAP

PEAP 는 9 페이지의 *PEAP* 를 참조하십시오 .

■ EAP-TTLS

EAP-TTLS 는 10 페이지의 *EAP-TTLS* 를 참조하십시오 .

■ EAP-TLS

EAP-TLS 는 10 페이지의 *EAP-TLS* 를 참조하십시오 .

암호화 방법

■ TKIP

TKIP 는 12 페이지의 *TKIP* 를 참조하십시오 .

■ AES

AES 는 12 페이지의 *AES* 를 참조하십시오 .

■ CKIP

Cisco Systems, Inc. 에서 개발한 LEAP 용 원본 키 무결성 프로토콜입니다 .

사용자 ID 및 암호

다음 보안 방법들에서는 64 자 미만의 사용자 ID 와 32 자 미만의 암호가 사용됩니다 .

■ LEAP

■ EAP-FAST

■ PEAP

■ EAP-TTLS

■ EAP-TLS(사용자 ID 용)

추가 네트워크 설정 유형

추가 네트워크 설정을 구성하려는 경우 다음 기능들을 사용할 수 있습니다.

- Web Services(Windows Vista® 및 Windows® 7)
- 수직 페어링 (Windows® 7)

참고

호스트 컴퓨터 및 기기가 동일 서브넷에 있는지 또는 라우터가 두 장치 간에 데이터를 전송하도록 올바르게 구성되었는지 확인합니다.

Web Services(Windows Vista® 및 Windows® 7) 를 사용할 때의 네트워크 인쇄 설치

Web Services 기능을 사용하면 네트워크에 연결된 기기 정보를 모니터링할 수 있습니다. 또한 프린터 아이콘에서 프린터 드라이버 설치가 활성화되고 Web Services 포트 (WSD 포트) 가 만들어집니다.

참고

- 이 설정을 구성하려면 먼저 기기에서 IP 주소를 구성해야 합니다.
- Windows Server® 2008 의 경우 Print Services 를 설치해야 합니다.
- 프린터 지원만 웹 서비스로 설치됩니다.

- 1 설치 CD-ROM 을 삽입합니다.
- 2 CD-ROM 드라이브 /install/driver/gdi/32 또는 64 을 선택합니다.
- 3 언어를 선택한 다음 **DPIinst.exe** 을 두 번 클릭합니다.


참고

사용자 계정 컨트롤 화면이 표시되면,
(Windows Vista®) 허용을 클릭합니다.
(Windows® 7) 예를 클릭합니다.

4 (Windows Vista®)

를 클릭한 다음 **네트워크**를 선택합니다.

(Windows® 7)

, **제어판**, **네트워크 및 인터넷** 및 **네트워크 컴퓨터 및 장치 보기**를 차례로 클릭합니다.

5 기기의 **Web Services** 이름이 프린터 아이콘과 함께 표시됩니다. 설치하려는 기기를 마우스 오른쪽 단추로 클릭합니다.

 **참고**

Brother 시스템에 대한 **Web Services** 이름은 모델 이름과 기기의 **MAC** 주소 (이더넷 주소)입니다 (예 : Brother MFC-XXXX(모델 이름) [XXXXXXXXXXXXX](MAC 주소 / 이더넷 주소)).

6 풀다운 메뉴에서 **설치**를 클릭합니다.


수직 페어링 (Windows® 7) 사용 시 인프라 모드에 대한 네트워크 인쇄 설치

Windows® 수직 페어링은 수직 페어링을 지원하는 무선 기기가 Wi-Fi Protected Setup 및 웹 서비스 기능의 PIN 방식을 사용하여 인프라 네트워크에 연결할 수 있도록 허용하는 기술입니다. 또한 이 기술로 장치 추가 화면에 있는 프린터 아이콘에서 프린터 드라이버 설치가 가능합니다.

인프라 모드일 경우 기기를 무선 네트워크에 연결한 다음 이 기능을 사용하여 프린터 드라이버를 설치할 수 있습니다. 아래 단계를 따르십시오.

참고

- 기기의 Web Services 기능을 OFF로 설정한 경우 다시 ON으로 설정해야 합니다. Brother 기기의 기본 Web Services 설정은 ON입니다. 웹 기반 관리 (웹 브라우저) 또는 BRAdmin Professional 3를 사용하여 Web Services 설정을 변경할 수 있습니다.
- WLAN 액세스 포인트 / 라우터에 Windows® 7 호환성 로고가 포함되어 있는지 확인하십시오. 호환성 로고가 있는지 확실하지 않으면 해당 액세스 포인트 / 라우터 제조업체에 문의하십시오.
- 컴퓨터에 Windows® 7 호환성 로고가 포함되는지 확인합니다. 호환성 로고가 있는지 확실하지 않으면 컴퓨터 제조업체에 문의하십시오.
- 무선 NIC(네트워크 인터페이스 카드)를 사용하여 무선 네트워크를 구성하는 경우 무선 NIC에 Windows® 7 호환성 로고가 포함되어 있는지 확인하십시오. 자세한 내용은 무선 NIC 제조업체에 문의하십시오.
- Windows® 7 컴퓨터를 레지스트라로 사용하려면 컴퓨터를 미리 네트워크에 등록해야 합니다. WLAN 액세스 포인트 / 라우터에 부속된 설명서를 참조하십시오.

- 1 기기를 켭니다.
- 2 Wi-Fi Protected Setup(PIN 방식)에서 기기를 설정합니다.
PIN 방식으로 기기를 설정하는 방법은 *네트워크 사용자 설명서*에서 Wi-Fi Protected Setup(PIN 방식) 무선 구성을 참조하십시오.
- 3  버튼을 클릭한 다음 장치 및 프린터를 클릭합니다.
- 4 장치 및 프린터 대화 상자에서 장치 추가를 선택합니다.
- 5 기기를 선택하고 기기에 표시된 PIN을 입력합니다.

- ⑥ 연결하려는 인프라 네트워크를 선택하고 다음을 클릭합니다 .
- ⑦ 기기가 **장치 및 프린터** 대화 상자에 표시되면 무선 구성 및 프린터 드라이버 설치가 성공적으로 완료된 것입니다 .

보안 기능

보안 용어

■ CA(인증 기관)

CA 는 디지털 인증서 (특히 X.509 인증서) 를 발행하고 인증서 내의 데이터 항목 간 구속력을 보증하는 기관입니다 .

■ CSR(Certificate Signing Request)

CSR 은 인증서 발행을 신청하기 위해 신청자가 CA 에 전송하는 메시지입니다 . CSR 에는 신청자를 식별하는 정보 , 신청자가 생성한 공개 키 및 신청자의 디지털 서명이 포함됩니다 .

■ 인증서

인증서는 공개 키와 ID 를 바인딩하는 정보입니다 . 인증서는 공개 키가 특정 개인에게 속하는지를 확인하기 위해 사용할 수 있습니다 . 형식은 x.509 표준에 의해 정의됩니다 .

■ CA 인증서

CA 인증서는 CA(인증 기관) 자체를 식별하고 해당 개인 키를 소유하는 인증 체계입니다 . CA 인증서는 CA 에서 발행된 인증서를 확인합니다 .

■ 디지털 서명

디지털 서명은 암호화 알고리즘을 사용하여 계산되고 데이터 수신자가 서명을 사용해서 데이터의 진위성 및 무결성을 확인할 수 있는 방식으로 데이터 객체에 첨부되는 값입니다 .

■ 공개 키 암호 체계

공개 키 암호 체계는 알고리즘에 한 쌍의 키 (공개 키와 개인 키) 가 사용되고 알고리즘의 여러 단계에서 해당 쌍의 서로 다른 구성 요소가 사용되는 현대적인 암호화 기술 중 하나입니다 .

■ 공유 키 암호 체계

공유 키 암호 체계는 알고리즘의 두 가지 서로 다른 단계 (예 : 암호화 및 해독) 를 사용하는 암호화 관련 알고리즘의 한 갈래입니다 .

보안 프로토콜

참고

웹 기반 관리 (웹 브라우저) 를 사용하여 프로토콜 설정을 구성할 수 있습니다 . 자세한 내용은 *네트워크 사용자 설명서*를 참조하십시오 .

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

이 보안 통신 프로토콜은 보안 위협을 방지하기 위해 데이터를 암호화합니다 .

HTTPS

HTTP(Hyper Text Transfer Protocol) 에서 SSL 을 사용하는 인터넷 프로토콜입니다 .

IPPS

IPP(Internet Printing Protocol) 버전 1.0 에서 SSL 을 사용하는 인쇄 프로토콜입니다 .

SNMPv3

Simple Network Management Protocol 버전 3(SNMPv3) 는 네트워크 장치를 안전하게 관리하기 위한 사용자 인증 및 데이터 암호화를 제공합니다 .

전자 메일 송신 및 수신을 위한 보안 방법

참고

웹 기반 관리 (웹 브라우저) 를 사용하여 보안 방식 설정을 구성할 수 있습니다 . 자세한 내용은 *네트워크 사용자 설명서*를 참조하십시오 .

POP before SMTP(PbS)

클라이언트의 전자 메일을 전송하기 위한 사용자 인증 방식입니다 . 클라이언트는 전자 메일을 전송하기 전에 POP3 서버에 액세스하여 SMTP 서버를 사용할 수 있는 권한을 부여 받습니다 .

SMTP-AUTH(SMTP 인증)

SMTP-AUTH 는 SMTP(인터넷 전자 메일 전송 프로토콜) 의 확장 기술로서 발신자의 실제 ID 가 알려진 것인지 보장하는 인증 방식이 포함됩니다 .

APOP(Authenticated Post Office Protocol)

APOP 는 POP3(인터넷 수신 프로토콜) 의 확장 기술로서 클라이언트가 전자 메일을 수신할 때 암호를 암호화하는 인증 방식이 포함됩니다 .

SMTP over SSL

SMTP over SSL 기능은 SSL 을 사용하여 암호화된 전자 메일을 전송할 수 있게 해줍니다 .

POP over SSL

POP over SSL 기능은 SSL 을 사용하여 암호화된 전자 메일을 수신할 수 있게 해줍니다 .

서비스 사용

서비스는 Brother 인쇄 서버로 인쇄하려는 컴퓨터를 통해 액세스할 수 있는 리소스입니다. Brother 인쇄 서버는 다음과 같은 미리 정의된 서비스를 제공합니다 (사용 가능한 서비스 목록을 보려면 Brother 인쇄 서버 원격 콘솔에서 **SHOW SERVICE** 명령 실행). 지원되는 명령 목록을 보려면 명령 프롬프트에서 **HELP** 를 입력합니다.

서비스 (예)	정의
BINARY_P1	TCP/IP 바이너리
TEXT_P1	TCP/IP 텍스트 서비스 (각 라인 피드 다음에 캐리지 리턴 추가)
PCL_P1	PCL 서비스 (PJL 호환 기기를 PCL 모드로 전환)
BRNxxxxxxxxxxxx	TCP/IP 바이너리
BRNxxxxxxxxxxxx_AT	Macintosh 용 PostScript® 서비스
POSTSCRIPT_P1	PostScript® 서비스 (PJL 호환 기기를 PostScript® 모드로 전환)

"xxxxxxxxxxxx" 는 기기의 MAC 주소 (이더넷 주소)입니다.

IP 주소를 설정하는 다른 방법 (고급 사용자 및 관리자)

DHCP 를 사용하여 IP 주소 구성

DHCP(Dynamic Host Configuration Protocol) 는 IP 주소 할당을 위한 몇 가지 자동 메커니즘 중 하나입니다. 네트워크에 DHCP 서버가 있는 경우, 인쇄 서버가 DHCP 서버에서 IP 주소를 자동으로 가져오고 해당 이름을 모든 RFC 1001 및 1002 호환 동적 이름 서비스에 등록합니다.



참고

DHCP, BOOTP 또는 RARP 를 통하지 않고 인쇄 서버를 구성하려면 인쇄 서버가 정적 IP 주소를 갖도록 부팅 방법을 정적으로 설정해야 합니다. 이로써 인쇄 서버가 이러한 시스템에서 IP 주소를 획득하지 못하게합니다. 부팅 방법을 변경하려면 기기 제어판의 네트워크 메뉴 (LCD 모델의 경우), BRAdmin 응용 프로그램, 원격 설정 또는 웹 기반 관리 (웹 브라우저) 를 사용하십시오.

RARP 를 사용하여 IP 주소 구성

Brother 인쇄 서버의 IP 주소는 호스트 컴퓨터에서 리버스 ARP(RARP) 기능을 사용하여 구성할 수 있습니다. 이렇게 하려면 다음과 같은 항목으로 /etc/ethers 파일 (이 파일이 존재하지 않으면 생성할 수 있음)을 편집합니다.

```
00:80:77:31:01:07    BRN008077310107( 또는 무선 네트워크의 경우
BRW008077310107)
```

여기에서 첫 번째 항목은 인쇄 서버의 MAC 주소 (이더넷 주소)이고 두 번째 항목은 인쇄 서버의 이름입니다 (이름은 /etc/hosts 파일에 입력한 것과 같은 이름이어야 함).

RARP 데몬이 아직 실행 중이 아니면 데몬을 시작합니다 (명령은 시스템에 따라 rarpd, rarpd -a, in.rarpd -a 또는 다른 명령일 수 있습니다. 추가 정보를 보려면 man rarpd 를 입력하거나 시스템 설명서를 참조하십시오). RARP 데몬이 Berkeley UNIX 기반 시스템에서 실행 중인지 확인하려면 다음 명령을 입력합니다.

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

AT&T UNIX 기반 시스템의 경우 다음 명령을 입력합니다.

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

Brother 인쇄 서버는 기기 전원이 켜지면 RARP 데몬에서 IP 주소를 가져옵니다.

BOOTP 를 사용하여 IP 주소 구성

BOOTP 는 RARP 의 대안으로서 서브넷 마스크 및 게이트웨이를 구성할 수 있는 이점이 있습니다 . BOOTP 를 사용하여 IP 주소를 구성하려면 BOOTP 가 설치되어 있고 호스트 컴퓨터에서 실행 중인지 확인합니다 (호스트의 /etc/services 파일에 실제 서비스로 표시되어 있어야 합니다 . 자세한 내용을 보려면 man bootpd 를 입력하거나 시스템 설명서를 참조하십시오) . BOOTP 는 일반적으로 /etc/inetd.conf 파일을 통해 시작되므로 해당 파일의 bootp 항목 앞에서 "#" 을 제거하여 사용하도록 설정해야 합니다 . 예를 들어 일반적인 /etc/inetd.conf 파일의 bootp 항목은 다음과 같습니다 .

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

시스템에 따라 이 항목은 "bootp" 대신 "bootps" 로 호출할 수 있습니다 .



참고

BOOTP 를 활성화하려면 편집기를 사용하여 "#" 을 삭제만 하면 됩니다 ("#" 이 없으면 BOOTP 가 활성화됩니다) . 그런 다음 BOOTP 구성 파일을 편집하고 (일반적으로 /etc/bootptab) 인쇄 서버의 이름 , 네트워크 유형 (이더넷의 경우 1) , MAC 주소 (이더넷 주소) 및 IP 주소 , 서브넷 마스크 및 게이트웨이를 입력합니다 . 이를 위한 정확한 형식이 표준화되지 않았기 때문에 시스템 설명서를 참조하여 이 정보를 입력할 방법을 결정해야 합니다 (많은 UNIX 시스템에는 참조용으로 사용할 수 있는 템플릿 예가 bootptab 파일에 포함되어 있습니다) . 일반적인 /etc/bootptab 항목 예로는 다음이 포함됩니다 (아래의 "BRN" 은 무선 네트워크용 "BRW" 입니다 .).

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

및 :

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

구성 파일에 다운로드 파일 이름을 포함하지 않은 경우 특정 BOOTP 호스트 소프트웨어 구현에서는 BOOTP 요청에 응답하지 않습니다 . 이 경우에는 호스트에 Null 파일을 만들고 이 파일의 이름과 경로를 구성 파일에 지정합니다 .

RARP 에서와 같이 인쇄 서버는 기기 전원이 켜질 때 BOOTP 서버에서 해당 IP 주소를 로드합니다 .

APIPA 를 사용하여 IP 주소 구성

Brother 인쇄 서버는 APIPA(Automatic Private IP Addressing) 프로토콜을 지원합니다. APIPA 를 사용하면 DHCP 서버를 사용할 수 없는 경우 DHCP 클라이언트가 IP 주소 및 서브넷 마스크를 자동으로 구성합니다. 장치는 169.254.1.0 에서 169.254.254.255 까지의 범위 중에서 고유한 IP 주소를 선택합니다. 서브넷 마스크는 자동으로 255.255.0.0 으로 설정되고 게이트웨이 주소는 0.0.0.0 으로 설정됩니다.

APIPA 프로토콜은 기본적으로 활성화됩니다. APIPA 프로토콜을 비활성화하려면 기기 제어판 (LCD 모델의 경우), BRAdmin Light 또는 웹 기반 관리 (웹 브라우저) 를 사용하여 비활성화할 수 있습니다.

ARP 를 사용하여 IP 주소 구성

BRAdmin 응용 프로그램을 사용할 수 없고 네트워크에서 DHCP 서버를 사용하지 않는 경우, ARP 명령을 사용할 수도 있습니다. ARP 명령은 UNIX 시스템 뿐만 아니라 TCP/IP 가 설치된 Windows® 시스템에서 사용할 수 있습니다. ARP 를 사용하려면 명령 프롬프트에서 다음 명령을 입력합니다.

```
arp -s ipaddress ethernetaddress
```

```
ping ipaddress
```

여기에서 ethernetaddress 는 인쇄 서버의 MAC 주소 (이더넷 주소) 이고 ipaddress 는 인쇄 서버의 IP 주소입니다. 예 :

■ Windows® 시스템

Windows® 시스템에서는 MAC 주소 (이더넷 주소) 의 각 숫자 사이에 대시 "-" 가 필요합니다.

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

```
ping 192.168.1.2
```

■ UNIX/Linux 시스템

일반적으로 UNIX 및 Linux 시스템에서는 MAC 주소 (이더넷 주소) 의 각 숫자 사이에 콜론 ":" 이 필요합니다.

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

```
ping 192.168.1.2
```

참고

`arp -s` 명령을 사용하려면 동일한 이더넷 세그먼트에 있어야 합니다 (즉 , 인쇄 서버와 운영 체제 사이에 라우터가 있을 수 없습니다).

라우터가 있는 경우 **BOOTP** 또는 이 장에 설명된 다른 방법을 사용하여 **IP** 주소를 입력할 수 있습니다 . 관리자가 **BOOTP**, **DHCP** 또는 **RARP** 를 사용하여 **IP** 주소를 제공하도록 시스템을 구성한 경우 **Brother** 인쇄 서버가 이러한 **IP** 주소 할당 시스템 중 하나로부터 **IP** 주소를 수신할 수 있습니다 . 어느 경우에도 **ARP** 명령을 사용할 필요가 없습니다 . **ARP** 명령은 한 번만 작동합니다 . 보안상의 이유로 **ARP** 명령을 사용하여 **Brother** 인쇄 서버의 **IP** 주소를 성공적으로 구성한 다음에는 **ARP** 명령을 다시 사용하여 주소를 변경할 수 없습니다 . 인쇄 서버는 이러한 모든 시도를 무시합니다 . **IP** 주소를 다시 변경하려면 웹 기반 관리 (웹 브라우저), **TELNET**(**SET IP ADDRESS** 명령 사용) 을 사용하거나 팩토리 리셋으로 인쇄 서버를 재설정하십시오 (그러면 **ARP** 명령을 다시 사용할 수 있습니다).

A

TELNET 콘솔을 사용하여 IP 주소 구성

TELNET 명령을 사용하여 **IP** 주소를 변경할 수도 있습니다 .

TELNET 은 기기의 **IP** 주소를 효과적으로 변경할 수 있는 방법입니다 . 하지만 인쇄 서버에 적합한 **IP** 주소가 미리 프로그래밍되어 있어야 합니다 .

시스템 프롬프트의 명령 프롬프트에 **TELNET** <command line> 을 입력합니다 . 여기서 <command line> 은 인쇄 서버의 **IP** 주소입니다 . 연결되면 **Return** 키 또는 **Enter** 키를 눌러 **"#"** 프롬프트를 표시합니다 . 암호 **"access"**(암호는 화면에 표시되지 않음) 를 입력합니다 . 사용자 이름을 입력하라는 메시지가 표시됩니다 . 이 프롬프트의 질문에 모두 답변합니다 . 그러면 **Local>** 프롬프트가 표시됩니다 . **SET IP ADDRESS ipaddress** 를 입력합니다 . 여기서 **ipaddress** 는 인쇄 서버에 지정하려는 **IP** 주소입니다 (사용할 **IP** 주소는 네트워크 관리자에게 문의하십시오) . 예 :

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

이제 **SET IP SUBNET subnet mask** 를 입력하여 서브넷 마스크를 설정해야 합니다 . 여기서 **subnet mask** 는 인쇄 서버에 지정하려는 서브넷 마스크입니다 (사용할 서브넷 마스크는 네트워크 관리자에게 문의하십시오) . 예 :

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

서브넷이 없는 경우 다음 기본 서브넷 마스크 중 하나를 사용하십시오 .

클래스 **A** 네트워크의 경우 **255.0.0.0**

클래스 B 네트워크의 경우 255.255.0.0

클래스 C 네트워크의 경우 255.255.255.0

IP 주소에서 가장 왼쪽에 있는 숫자로 현재 사용자가 갖고 있는 네트워크 유형을 식별할 수 있습니다. 이 값 그룹의 범위는 클래스 A 네트워크의 경우 1~127(예 : 13.27.7.1), 클래스 B 네트워크의 경우 128~191(예 : 128.10.1.30), 클래스 C 네트워크의 경우 192~255(예 : 192.168.1.4)입니다.

게이트웨이 (라우터) 가 있는 경우 SET IP ROUTER routeraddress 명령을 사용하여 주소를 입력합니다. 여기서 routeraddress 는 인쇄 서버에 지정할 게이트웨이 IP 주소입니다. 예 :

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

SET IP METHOD STATIC 을 입력하여 IP 액세스 구성 방법을 정적으로 설정합니다.

IP 정보를 올바르게 입력했는지 확인하려면 SHOW IP 를 입력합니다.

EXIT 를 입력하거나 Ctrl-D 를 눌러서 (Control 키를 누른 상태로 "D" 를 누름) 원격 콘솔 세션을 종료합니다.

B

색인

A

AES	12
APIPA	3, 25
APOP	21
ARP	3, 25

B

BINARY_P1	22
BOOTP	3, 24
BRNxxxxxxxxxxxx	22
BRNxxxxxxxxxxxx_AT	22

C

CA	19
CA 인증서	19
CIFS	6
CKIP	14
CSR	19
Custom Raw Port	4

D

DHCP	3, 22
DNS 클라이언트	4

E

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

F

FTP	6
-----------	---

H

HTTP	5
HTTPS	20

I

IEEE 802.1x	9
IP 주소	7
IPP	4
IPPS	20
IPv6	6

L

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

M

MAC 주소	16, 22, 23, 24, 25
mDNS	4

N

NetBIOS 이름 확인	4
---------------------	---

P

PCL_P1	22
PEAP	9
POP before SMTP	21
POP over SSL	21
Port 9100	4
POSTSCRIPT_P1	22

R

RARP	3, 23
RFC 1001	22

S

SMTP over SSL	21
SMTP 클라이언트	4
SMTP-AUTH	21
SNMP	5

SNMPv3 20
 SNTP 6
 SSID 11
 SSL/TLS 20

T

TCP/IP 3
 TCP/IP 인쇄 15
 TELNET 5, 26
 TEXT_P1 22
 TKIP 12

W

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

ㄱ

공개 키 암호 체계 19
 공유 키 12
 공유 키 암호 체계 19

ㄴ

네트워크 공유 인쇄 2
 네트워크 인쇄 15
 네트워크 키 13

ㄷ

디지털 서명 19

ㄹ

무선 네트워크 11

ㅁ

보안 용어 19

ㅂ

서브넷 마스크 8

서비스 22
 수직 페어링 15

ㅇ

암호화 12
 오픈 시스템 12
 인증 12
 인증서 19

ㅅ

채널 11

ㅈ

프로토콜 3
 피어 투 피어 1