# Wireless Glossary



# Ad-hoc Mode:

Ad-hoc mode is a wireless network framework that does not have a central access point. Each wireless client communicates directly with each other. When the Brother wireless machine is part of ad-hoc mode network, it receives all print jobs directly from the computer sending the print data.



# Infrastructure Mode:

Infrastructure mode is a wireless network framework that has a central access point at the heart of the network. In infrastructure mode, wireless devices communicate with each other through an access point. When the Brother wireless machine is part of infrastructure mode network, it receives all print jobs via an access point.

The access point can also act as a bridge or a gateway to a wired network, and wireless devices can communicate not only with each other but also with a wired network.



# **Network Card**

A piece of hardware used to connect a computer, printer or other device to a network. Most modern wireless devices have a network card built in.

# Wireless Network (WLAN) settings

Settings such as SSID, authentication and encryption of your wireless network environment allow users to connect to the wireless network. If you do not know them, contact your network administrator or the manufacture of your access point/router for assistance.

#### **Access Point**

A hardware device that acts as a communication hub for users of a wireless device to connect to a wired LAN.

#### DHCP

Short for Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

#### **One-push Setup/Secure Easy Setup**

This feature automatically detects which mode your access point uses for one-push configuration (SecureEasySetup<sup>™</sup>, Wi-Fi Protected Setup<sup>™</sup> or AOSS<sup>™</sup>). By pushing a button on the wireless access point/router and the machine, you can setup the wireless network and security settings.

### Router

A router is a device that receives and sends packets of data from one device to another on a network or to another network. The router also tracks and manages traffic on the network.

# SECURITY

#### SSID

SSID is short for Service Set Identifier, a unique identifier to avoid interference on a wireless network, and it is also referred to as ESSID (Extended Service Set Identifier). The SSID is a 32byte or less value. This value or name is assigned to the access point.

The wireless network devices you want to associate to the wireless network should match the access point. The access point and wireless network devices regularly send wireless packets (referred to as a beacon), which has the SSID information. When your wireless network device receives a beacon, you can identify the wireless network that is close enough for the radio waves to reach your device.

#### WPA/TKIP/AES

WPA, short for a Wi-Fi® Protected Access, is a data encryption specification for a wireless LAN. It improves upon the security feature of WEP by using Extensible Authentication Protocol (EAP) to secure network access and an encryption method to secure data transmissions.

WPA is designed for use with an 802.1X authentication server that distributes different keys to each user. However it can also be used in a less secure "Pre-Shared Key (PSK)" mode. PSK is designed for home and small office networks where every user has the same passphrase. WPA-PSK is also called WPA-Personal. WPA-PSK enables the Brother wireless machine to associate with access points using TKIP or AES encryption method. WPA2-PSK enables the Brother wireless machine to associate with access points using AES encryption method.

TKIP (short for Temporal Key Integrity Protocol) is an encryption method. TKIP provides per-packet key, mixing a message integrity and re-keying mechanism.

AES (short for Advanced Encryption Standard) is the Wi-Fi® authorized strong encryption standard.

WPA-PSK/ WPA2-PSK and TKIP or AES use a Pre-Shared Key (PSK) that is 8 or more characters in length, up to a maximum of 63 characters.

# WEP

WEP is short for Wired Equivalent Privacy, a security protocol for a wireless local area network (WLAN) defined in the IEEE 802.11b standard. WEP is designed to provide a wireless LAN with a level of security comparable to that of a wired LAN.

WEP was the standard set in 1999 and since then hackers have devised ways to exploit WEP security flaws. The most widely recommended solution to WEP security problems is to switch to WPA or WPA2. Either is much more secure than WEP.