

Wireless Networking

Terminology you should know

SSID (Service Set Identifier, Network Name)

An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other.

SSIDs are case sensitive text strings. The SSID is a sequence of alphanumeric characters (letters or numbers). SSIDs have a maximum length of 32 characters.

The SSID on wireless clients can be set either manually, by entering the SSID into the client network settings, or automatically, by leaving the SSID unspecified or blank.

Most Wi-Fi Hot Spots use a public SSID that is set on the access point to broadcast to all wireless devices in range. Many private wireless access points have the automatic SSID broadcast feature disabled in an attempt to improve network security.

passphrase

In computer networking, a passphrase is one or a few small words for use as a security setting. Some WiFi home networking equipment utilize passphrases to generate static WEP keys rather than create the long hexadecimal numbers WEP requires. That setup software then automatically sets the appropriate WEP key based on the passphrase provided.

However, not all WiFi gear supports passphrases. In addition, passphrases normally cannot be used on a network when mixing equipment from different manufacturers, as each manufacturer generally employs different algorithms for generating keys.

WEP (Wired Equivalent Privacy)

WEP is a protocol that adds security to wireless local area networks (WLANs) based on the 802.11 Wi-Fi standard. WEP was designed to give wireless networks the equivalent level of privacy protection as a comparable wired network.

WEP is based on a security scheme that utilizes a combination of secret user keys and system-generated values. Wireless devices use the WEP keys to encrypt the data stream when communicating over the wire.

The keys themselves are not sent over the network but rather are generally stored on the wireless adapter or in the Windows Registry.

WPA (Wi-Fi Protected Access)

WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). It was developed by the networking industry in response to the shortcomings of WEP.

One of the key technologies behind WPA is the Temporal Key Integrity Protocol (TKIP), which addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not offer. With this feature, WPA provides security comparable to VPN tunneling with WEP.

WPA-PSK (WPA Pre Shared Key)

WPA Pre Shared Key (WPA-PSK) is a simplified but still powerful form of WPA suitable for home Wi-Fi networking. To use WPA-PSK, a person sets a static key or "passphrase" as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them.

Infrastructure mode

Infrastructure wireless mode connects a wireless network to a wired Ethernet network. Infrastructure mode wireless also supports central connection points for WLAN clients.

A wireless access point (AP) is required for infrastructure mode wireless networking. To join the WLAN, the AP and all wireless clients must be configured to use the same SSID. The AP is then cabled to the wired network to allow wireless clients access to the Internet, shared files or printers. Additional APs can be added to the WLAN to increase the reach of the infrastructure and support any number of wireless clients.

Compared to ad-hoc wireless networks, infrastructure mode networks offer the advantage of scalability, centralized security management and improved reach.

ad-hoc mode

On wireless computer networks, ad-hoc mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in a peer-to-peer fashion.

To set up an ad-hoc wireless network, each wireless adapter must be configured for ad-hoc mode versus the alternative infrastructure mode. In addition, all wireless adapters on the ad-hoc network must use the same SSID and the same channel number. An ad-hoc network tends to feature a small group of devices all in very close proximity to each other.