

## 802.11 Basics

### WIRELESS LAN CONFIGURATIONS

Currently, most wireless networks (WLANs) are based on the IEEE 802.11b, 802.11a or 802.11g standards. These standards define how to wirelessly connect computers or devices to a network. Wireless enabled devices send and receive data indoors and out, anywhere within the range of a wireless access point.

The choice of standard depends on your requirements, including data communications speed and range, the level of security, noise and interference concerns, compatibility issues and cost.

**802.11b** was the first 802.11 standard to be released and have commercial products available. Also called Wireless Fidelity, or Wi-Fi, it has a range suitable for use in big office spaces. Wi-Fi is currently the most popular and least expensive wireless LAN specification. It operates in the unlicensed 2.4 GHz radio spectrum and can transmit data at speeds up to 11 Mbps within a 30m range. It can be affected by interference from mobile phones and Bluetooth devices which can reduce transmission speeds.

**802.11a** has a couple of advantages over Wi-Fi. It operates in a less-populated (but also unlicensed) frequency band (5.15GHz to 5.35GHz) and is therefore less prone to interference. Its bandwidth is much higher than 802.11b, with a theoretical peak of 54 Mbps. However, actual throughput is typically closer to 25 Mbps.

**802.11g** is the latest standard and promises to be the most popular format. It combines the speed the 802.11a and backward compatibility with 802.11b. It operates in the same frequency band as 802.11b but consequently also can be affected by interference.

The following table provides some comparative communications distances at various data communications speeds for each of the 802.11 standards.

**Table 1. 802.11 a, b, g Range Comparison**

Data Rate (Mbps)	802.11a Range (40 mW with 6dBi gain diversity patch antenna)	802.11g Range (30 mW with 2.2 dBi gain diversity dipole antenna)	802.11b Range (100 mW with 2.2 dBi gain diversity dipole antenna)
54	13 m	27 m	-
48	15 m	29 m	-
36	19 m	30 m	-
24	26 m	42 m	-
18	33 m	54 m	-
12	39 m	64 m	-
11	-	48 m	45 m
9	45 m	76 m	-
6	50 m	91 m	-
5.5	-	67 m	67 m
2	-	82 m	82 m
1	-	124 m	124 m

The following table provides information on data rates for each standard. Note that 802.11g systems operate significantly faster when there are no 802.11b clients in the network.

**Table 2. 802.11a, b, g Data Rate Comparison**

	Data Rate (Mbps)	Throughput (Mbps)	Throughput as a % of 802.11b throughput
802.11b	11	6	100%
802.11g (with .11b clients in cell)	54	14	233%
802.11g (no .11b clients in cell)	54	22	367%
802.11a	54	25	417%

## BASIC WIRELESS NETWORK TOPOLOGY

When upgrading to a wireless network the overall layout can be a bit confusing. In the figure below we can see a typical wired client/server network setup including a network hub or (more often in modern networks) switch, a dedicated server, PC and a serial device connected to the network via a serial server. This is referred to as a wired infrastructure configuration.

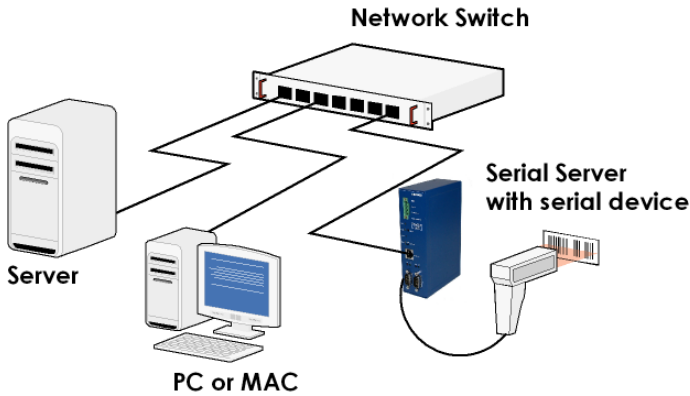


Figure 1. Wired Infrastructure Network Configuration

A simpler wired network configuration (shown below) dispenses with the server and only consists of computers and other networked devices connected via their Ethernet interfaces through the hub or switch. This configuration is called wired peer to peer network.

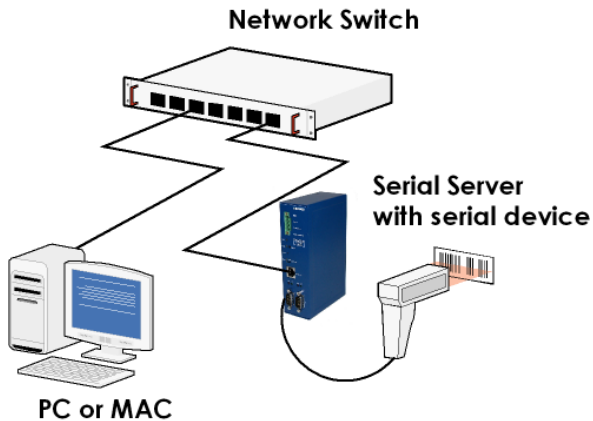


Figure 2. Peer to Peer Configuration

To give either of these existing networks wireless capability, connect a wireless access point (AP) to the network switch as shown in figure below. Laptop or desktop computers equipped with wireless cards, or other wireless devices such as wireless serial servers, communicate with each other and the wired network via the AP. Wireless devices connect to the switch as if they are connected via a normal network cable. A major benefit to adding the wireless segment is that you can avoid running new cables. Another is that you can add up to 32 wireless computer users without having to buy a bigger switch with more ports.

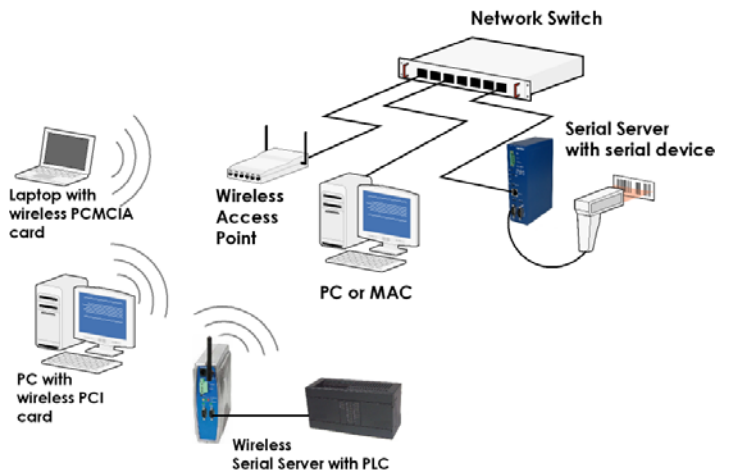


Figure 3. Infrastructure Wireless Network

Wireless devices also can be set up as a peer to peer, or Ad Hoc, network configuration, as shown below.

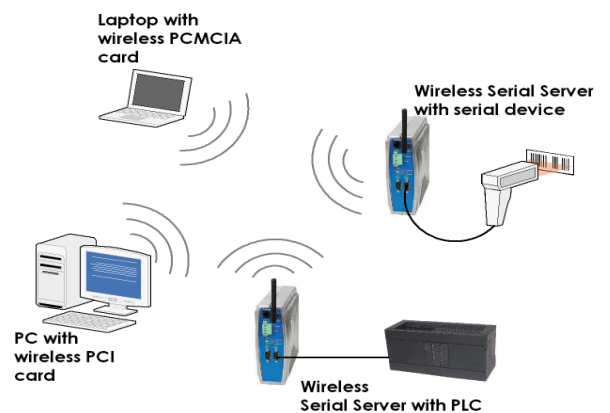


Figure 4. Adhoc Wireless Network

## EXTENDING THE RANGE

WLANs have a flexible architecture. You can easily extend the range and allow seamless roaming between APs. The preferred setup method for roaming within the office environment is to install multiple APs with the same Service Set Identifier (SSID) and security settings, however with each on a unique channel. 802.11 has three truly unique channels: 1, 6 and 11. You can spread out the APs in an overlapping channel layout as shown below:

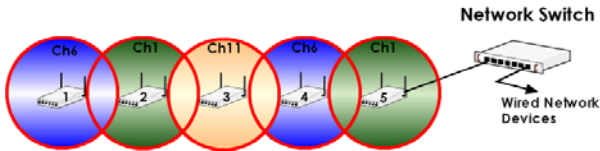


Figure 5. Extending Range

## 802.11 AUTHENTICATION & ENCRYPTION SECURITY BASICS

Like installing locks and keys on a door to control entry, wireless LAN security is designed to control which users can access the wireless LAN. The following table provides a summary of various WLAN security protocols and techniques.

Table 3. Security Types available for 802.11

Data Protection Technology	Description
WEP	<b>Wired Equivalency Privacy</b> , the original security standard for wireless LANs, easily exploited by software that can break the encryption after capturing traffic and recognizing encryption patterns.
802.1X	<b>802.1X</b> is the IEEE standard for wired and wireless LAN access control. It provides a means of authenticating and authorizing devices attached to a LAN. 802.1X defines the <b>Extensible Authentication Protocol (EAP)</b> . EAP uses a central authentication server to authenticate each network user. EAP also has some vulnerabilities.
LEAP	<b>Lightweight Extensible Authentication Protocol (LEAP)</b> , developed by Cisco, is based on the 802.1X authentication framework but addresses several weaknesses using dynamic WEP and sophisticated key management. LEAP also adds MAC address authentication.
PEAP	<b>Protected Extensible Authentication Protocol (PEAP)</b> provides secure transport of authentication data, including passwords and encryption keys. With PEAP, wireless clients can be authenticated without certificates, simplifying the secure wireless LAN architecture.
WPA	<b>Wi-Fi Protected Access (WPA)</b> is a subset of the 802.11i security standard and is expected to replace WEP. WPA combines Temporal Key Integrity Protocol (TKIP) and 802.1X for dynamic key encryption and mutual authentication.
TKIP	<b>Temporal Key Integrity Protocol (TKIP)</b> is part of the IEEE 802.11i encryption standard. TKIP provides per-packet key mixing, a message integrity check, and a re-keying mechanism, fixing the flaws of WEP.
WPA2	<b>WPA2</b> is second generation WPA, providing Wi-Fi users a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

## DEFAULT SECURITY SETTINGS

To provide basic authentication, most APs support simple MAC address filtering. Default security values are built-in and, in most cases, the AP implements these values on power up. However, you may want to make changes. Typically the following three parameters are configurable:

**SSID** – The Service Set Identifier will normally default to the manufacturer's name. You can set it to any word or phrase you like.

**Channel** – Normally the channel setting will default to channel 6. However, if a nearby neighbor is also using an access point and it is set to channel 6, there can be interference. Choose any other channel between 1 and 11. An easy way to see if your neighbors have access points is to use the search feature that comes with your wireless card.

**WEP Key** – WEP is disabled by default. To turn it on you must enter a WEP key and turn on 128-bit encryption.

## WIRED EQUIVALENT PRIVACY (WEP)

WEP is the original security protocol for WLANs, defined in the 802.11 standard. WEP was the only encryption available on early 802.11 devices and is not an industrial security algorithm.

Although simple to implement, WEP is easily hacked. Significant security improvements can be made simply by implementing two options built in to the Access Point: MAC address filtering and hiding the SSID. These measures will stop unwanted traffic from accidental intrusion and casual hackers, but are not sufficient for sensitive data or mission-critical networks.

## LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL (LEAP)

LEAP is a proprietary authentication solution that is based on 802.1X but adds proprietary elements of security. The standard was developed by Cisco and, although implementation is simple, it shares some weaknesses with WEP and should not be used if high security is required for your configuration. LEAP helps eliminate security vulnerabilities through the use of the following techniques

**Mutual Authentication** – The client must authenticate the network and the network needs to authenticate the client.

**User-Based Authentication** – LEAP eliminates the possibility of an unauthorized user access the network through a preauthorized piece of equipment by the use of usernames and passwords.

**Dynamic WEP Keys** – LEAP uses 802.1X to continually generate unique WEP keys for each user.

**PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL (PEAP)**

PEAP is a flexible security scheme that creates an encrypted SSL/TLS (Secure Sockets Layer / Transport Layer Security) channel between the client and the authentication server, and the channel then protects the subsequent user authentication exchange. To create the secure channel between client and authentication server, the PEAP client first authenticates the PEAP authentication server using digital certificate authentication. When the secure TLS channel has been established, you can select any standard EAP-based user authentication scheme for use within the channel.

After the user is successfully authenticated, dynamically generated keying material is supplied by the authentication server to the wireless AP. From this keying material, the AP creates new encryption keys for data protection.

**TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)**

TKIP is part of the IEEE 802.11i encryption standard for WLANs and is the next generation of WEP. It enhances WEP by adding a per-packet key mixing function, a message integrity check and a re-keying mechanism. TKIP encryption replaces WEP's small (40-bit) static encryption key, manually entered on wireless APs and client devices, with a 128 bit per-packet key. TKIP significantly mitigates WEP's vulnerabilities but does not provide complete resolution for its weaknesses.

**Wi-Fi PROTECTED ACCESS (WPA)**

WPA was introduced as a subset of the 802.11i security standard based on TKIP. WPA addresses the weaknesses of WEP with the dynamic encryption scheme provided by TKIP. WPA dynamically generates keys and removes the predictability that intruders rely on to exploit the WEP key. WPA also includes a Message Integrity Check (MIC), designed to prevent an attacker from capturing, altering and resending data packets.

**Wi-Fi PROTECTED ACCESS 2 (WPA2)**

Launched in September 2004 by the Wi-Fi Alliance, WPA2 is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. The authentication method used depends on whether Personal Mode or Enterprise Mode is being implemented. Encryption is the same in both modes. The encryption mechanism is the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES). AES satisfies U.S. government security requirements.

When a user associates with an access point, WPA2 mutual authentication process is initiated. The AP blocks access to the network until the user provides the appropriate credentials. The mutual authentication process ensures that only authorized users can gain access to the network. It also ensures that the client is connecting to an authorized server. If the user's credentials are accepted by the authentication server, the client is admitted to the WLAN.

Table 4. WPA and WPA2 Mode Types

	WPA		WPA2	
	Authentication	Encryption	Authentication	Encryption
<b>Enterprise Mode (Business and Government)</b>	IEEE 802.1X/EAP	TKIP/MIC	IEEE 802.1X/EAP	AES-CCMP
<b>Personal Mode (SOHO/personal)</b>	PSK	TKIP/MIC	PSK	AES-CCMP