BLACK BOX®
NETWORK SERVICES

Wireless Networking

Wireless standards, installation, security, and more!

SmartPath™ 802.11n
Wireless Access Point

LongSpan™ Wireless
Ethernet Extender

Wireless Serial Servers,
RS-232/422/485

Table of Contents

1.0 Introduction 3
2.0 Wireless standards 3
2.1 IEEE 802.11—the first wireless Ethernet 3
2.2 IEEE 802.11b 3
2.3 IEEE 802.11a 4
2.4 IEEE 802.11g 4
2.5 IEEE 802.11e 4
2.6 IEEE 802.11n 4
2.7 IEEE 802.11i 4
2.8 IEEE 802.15 5
2.9 IEEE 802.16 5
2.10 IEEE 802.16d 5
2.11 IEEE 802.16e 5
2.12 IEEE 802.20 5
2.13 IEEE 802.11x 5
2.14 IEEE 802.1x 5
2.15 Non IEEE standards 5
2.15.1 Super G 5
2.15.2 XR technology 5
2.15.3 Laser networking 5
2.15.4 ZigBee wireless control 6
2.15.5 Proprietary wireless 6
3.0 Considerations before installing 6
3.1 Security 6
3.2 Speed 6
3.3 Environmental concerns 6
3.3.1 When your building gets in the way 7
3.3.2 Interference from other electronic devices 7
3.4 Ease of installation 8
3.5 Compatibility 8
4.0 Installing a wireless network 8
4.1 Installing an ad-hoc network 8
4.2 installing an infrastructure-mode network 8
5.0 The integrated network solution 9
6.0 Network examples 9
6.1 Ad-hoc wireless network 9
6.2 Infrastructure-mode wireless 10
6.3 Wired network (10BASE-T or 100BASE-TX) 10
6.4 Integrated network 11
7.0 Wireless security 11
7.1 Wireless security standards 11
7.1.1 WEP 11
7.1.2 WPA 12
7.1.3 IEEE 802.11i 12
7.1.4 WPA2 12
7.2 Steps to secure your wireless network 12
7.2.1 Use the security you have 12
7.2.2 Change the default SSID 12
7.2.3 Turn on your encryption and change the factory setting 12
7.2.4 Take advantage of the new security standards 13
7.2.5 Use more than just wireless encryption 13
7.2.6 Turn it off 13
7.2.7 Screen your users 13
7.2.8 Don't let our employees install unauthorized access points 13
7.2.9 Watch out for strange hotspots 13
7.2.10 Hang on to those laptops 13
8.0 Conclusion 14
About Black Box 14

We're here to help! If you have any questions about your application, our products, or this white paper, contact Black Box Tech Support on 0118 965 6000 or go to www.blackbox.co.uk and click on "Live Chat."
You'll be live with one of our technical experts in less than 20 seconds.

1.0 Introduction

In a little more than a decade, wireless has grown from an obscure and expensive curiosity into a practical and affordable networking technology. Today's most common wireless standard is 802.11g Ethernet, also often called Wi-Fi ® (Wireless Fidelity). 802.11g is fast enough to be practical and affordable enough for home networks, and the new 802.11n standard is coming on strong.

The convenience of wireless is appealing—you don't have to deal with running cable, and you can move computers anywhere you want and still be connected to the network. Wireless is especially suited for use with laptop or notebook computers, offering users great freedom of movement.

In this paper we examine current wireless networking technology and explain the basics of how a wireless network is designed and how it can be integrated into a traditional wired network.

2.0 Wireless standards.

Wireless has proliferated into a virtual alphabet soup of standards.

The IEEE 802.11 wireless Ethernet standards are from the Institute of Electrical and Electronics Engineers, Inc. (IEEE). This organisation only sets the specifications for the standards—it doesn't test individual wireless products for compliance to these standards. IEEE 802.11 standards are real Ethernet standards that look like Ethernet to your applications.

You may notice that "Wi-Fi" is sometimes used interchangeably with the 802.11 standards, which is not quite correct. Wi-Fi simply refers to a product that's certified by the Wi-Fi Alliance, an organisation that has a program to guarantee compliance to the IEEE wireless standards and ensure interoperability between Wi-Fi products. All Wi-Fi products meet IEEE standards, but all IEEE wireless products are not necessarily Wi-Fi.

There are a few other wireless standards, such as ZigBee, that are not IEEE Ethernet standards and are generally used in specialty applications.

2.1 IEEE 802.11—the first wireless Ethernet.

The precursor to 802.11b, IEEE 802.11, was introduced in 1997. It was a beginning, but the standard had serious flaws. 802.11 supported speeds of only up to 2 Mbps. It supported two entirely different methods of encoding—Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS)—leading to confusion and incompatibility between equipment. It also had problems dealing with collisions and with signals reflected back from surfaces such as walls. These defects were soon addressed, and in 1999, the IEEE 802.11b Ethernet standard arrived.

2.2 IEEE 802.11b.

The 802.11b extension of the original 802.11 standard boosts wireless throughput from 2 Mbps up to 11 Mbps. 802.11b can transmit up to 200 feet (61 m) under good conditions, although this distance may be reduced by the presence of obstacles such as walls.

The 802.11b upgrade dropped FHSS in favor of DSSS. DSSS has proven to be more reliable than FHSS, and settling on one method of encoding eliminates the problem of having a single standard that includes two equipment types that aren't compatible with each other. 802.11b devices are compatible with older 802.11 DSSS devices, but they're not compatible with 802.11 FHSS devices.

IEEE 802.11b was, for some years, the most widely available wireless standard, but it's now largely been replaced by newer and faster wireless standards.

2.3 IEEE 802.11a.

802.11a uses a different band than 802.11b—the 5.8-GHz band called U-NII (Unlicensed National Information Infrastructure) Because the U-NII band has a higher frequency and a larger bandwidth allotment than the 2.4-GHz band, the 802.11a standard achieves speeds of up to 54 Mbps.

2.4 IEEE 802.11g.

802.11g, on the other hand, is an extension of 802.11b and operates in the same 2.4-GHz band as 802.11b. It brings data rates up to 54 Mbps using Orthogonal Frequency-Division Multiplexing (OFDM) technology. Because 802.11g is backward compatible with 802.11b, an 802.11b device can interface directly with an 802.11g access point.

2.5 IEEE 802.11e.

This standard defines Quality of Service (QoS) mechanisms for wireless. QoS makes it feasible to operate bandwidth-sensitive applications such as voice and video.

2.6 IEEE 802.11n.

802.11n is the new kid on the block, just ratified in 2009. This high-speed wireless standard can achieve wireless throughput of up to 300 Mbps by using a technique called Multiple-Input/Multiple-Output (MIMO).

MIMO transmits multiple data streams simultaneously, increasing wireless capacity while also increasing network reliability and coverage.

This wireless transmission method takes advantage of a radio transmission characteristic called multipath, which means that radio waves bouncing off surfaces such as walls and ceilings will arrive at the antenna at fractionally different times. This characteristic has long been considered to be a nuisance that impairs wireless transmission, but MIMO technology actually exploits it to enhance wireless performance.

MIMO sends a high-speed data stream across multiple antennas by breaking it into several lower-speed streams and sending them simultaneously. Each signal travels multiple routes for redundancy.

To pick up these multipath signals, MIMO uses multiple antennas and compares signals many times a second to select the best one. A MIMO receiver makes sense of these signals by using a mathematical algorithm to reconstruct the signals. Because it has multiple signals to choose from, MIMO achieves higher speeds at greater ranges than conventional wireless hardware does.

Although 802.11n supports very high speeds, real-world throughput may not be up to advertised speeds and depends on conditions, distance, and type of encryption used. Even though 802.11n is backwards compatible with 802.11b/g, the one network mistake that most frequently slows 802.11n is to have 802.11n clients share a 802.11n router with 802.11b/g clients. This forces the router to slow down to deal with the older standards, resulting in significant network slowdowns.

2.7 IEEE 802.11i.

IEEE 802.11i addresses many of the security concerns that come with a wireless network by adding Wi-Fi Protected Access (WPA) and Robust Security Network (RSN) to 802.11a and 802.11b standards.

WPA uses Temporal Key Integrity Protocol (TKIP) to improve the security of keys used with Wired Equivalent Privacy (WEP), changing the way keys are derived and adding a message-integrity check function to prevent packet forgeries. RSN adds a layer of dynamic negotiation of authentication and encryption algorithms between access points and mobile devices.

802.11i is backwards compatible with most 802.11x devices, but it loses security if used with non-802.11i devices. For more information about this standard, see Section 7.0 of this white paper.

2.8 IEEE 802.15.

This specification covers how information is conveyed over short distances among a Wireless Personal Area Network (WPAN or PAN). This type of network usually consists of a small networked group with little direct connectivity to the outside world. 802.15 is compatible with Bluetooth® 1.1.

2.9 IEEE 802.16.

IEEE 802.16, was ratified in January 2001. It enables a single base station to support many fixed and mobile wireless users. It's also called the Metropolitan Area Network (MAN) standard. 802.16 aims to combine the long ranges of the cellular standards with the high speeds of local wireless networks. Intended as a "last-mile" solution, this standard could someday provide competition for hard-wired broadband services such as DSL and cable modem. 802.16 operates in the 10- to 66-GHz range and has many descendants.

2.10 IEEE 802.16d.

This recent standard, also called IEEE 802.16-2004 or WiMax, can cover distances of up to 30 miles. Theoretically, a single base station can transmit hundreds of Mbps, with each customer being allotted a portion of the bandwidth. 802.16d uses either the licensed 2.6- and 3.5-GHz bands or the unlicensed 2.4- and 5-GHz bands.

2.11 IEEE 802.16e.

This is based on the 802.16a standard and specifies mobile air interfaces for wireless broadband in the licensed bands ranging from 2 to 6 GHz.

2.12 IEEE 802.20.

A proposed specification for a wireless standard for IP-based services. This standard is expected to operate in licensed bands below 3.5 GHz and will be used for mobile broadband wireless networks.

2.13 IEEE 802.11x.

This refers to the general 802.11 wireless standard—b, g, or a. Don't confuse it with 802.1x, a security standard.

2.14 IEEE 802.1x.

802.1x is not part of the 802.11 standard. It's a sub-standard designed to enhance the security of an 802.11 network. It provides an authentication framework that uses a challenge/response method to check if a user is authorised.

2.15 Non IEEE standards.

2.15.1 Super G.

This subset of 802.11g is a proprietary extension of the 802.11g standard that doubles throughput to 108 Mbps. Super G is not an IEEE approved standard. If you use it, you should use devices from one vendor to ensure compatibility. Super G is generally backwards compatible with 802.11g.

2.15.2 XR technology.

Extended Range (XR) technology is a wireless signal processing method developed by Atheros Communications. It's designed to improve the range of 802.11 wireless networks by two to three times, and reduce or eliminate "dead spots" in the network.

2.15.3 Laser networking.

Infrared laser networking offers wireless connections with speed rivaling fibre optic cable. It's ideal for providing emergency backup to fibre.

Laser connections are truly protocol independent, so they're adaptable not only to Ethernet but also to any other network protocol, up to Gigabit Ethernet.

Laser transmission is very reliable. The equipment uses wide beams to compensate for the inevitable movement that occurs in outdoor installations. It also provides better than 99.9% transmission accuracy.

The disadvantages of laser networking are its distance limitations and unsuitability for installation in fog-prone areas.

2.15.4 ZigBee wireless control.

ZigBee technology is designed for industrial environments that require very reliable, low-speed wireless connections for simple controls and sensors. Use ZigBee for economical, fault-tolerant networks with extremely low power consumption. ZigBee is ideal for communicating with devices such as industrial controls, fire alarms, and thermostats. A ZigBee wireless device stays in sleep mode most of the time, sending a short burst of information either on a schedule or when triggered.

2.15.5 Proprietary wireless.

Individual vendors may use their own proprietary wireless schemes for specialised applications. 900-MHz proprietary wireless is a fairly common arrangement in the industrial area, which values reliability over speed, but watch out for proprietary schemes tied to wireless devices that claim to be 802.11x compatible.

3.0 Considerations before installing.

Before deciding to install a wireless network, you should be familiar with wireless and know its strengths and weaknesses.
One big advantage of wireless networking is flexibility. Because there are no wires connecting network components, a wireless network gives you the freedom to move your computer to wherever you want and still be connected to the network.
In addition, a wireless network can be easier to install than a wired network because a properly installed wired network includes running cable, concealing the cable runs, and installing multiple wall outlets.

The disadvantages of wireless are less obvious. Security can be a problem unless appropriate security measures are taken.
Plus wireless can be susceptible to interference from other devices. Knowing about these limitations is important when deciding which network is right for your use and your area.

3.1 Security.

A primary concern when installing wireless is security. The rapid growth and popularity of wireless networks in both the commercial and residential market led to the use of wireless for many diverse applications, including the transmission of private information. The need for privacy was the impetus to develop new wireless security protocols such as IEEE 802.11i, and it continues to spur efforts to make wireless a more secure technology. For an in-depth look at wireless security, see Section 7.0 of this paper.

3.2 Speed.

802.11g—the most commonly used wireless standard—claims a speed of 54 Mbps. A more realistic estimate of actual throughput is about 25 Mbps, and speed can be even lower if WPA or WEP is turned on (as it should be), if devices are too far from access points, or if there are 802.11b devices on the network. Remember that this is still much faster than typical broadband Internet access. It's fast enough for most small office and home applications but may bog down in a workgroup situation, such as in a design firm where a group of people regularly exchange large files. A wired network or an 802.11n wireless network would be more appropriate for these conditions.

3.3 Environmental concerns.

Environment can affect your wireless network, and your wireless network may affect electronic devices within your environment. Therefore, take a good look at the space where you intend to install your wireless network.

3.3.1 When your building gets in the way.

When you set up your 802.11x network, chances are you won’t get the network to operate effectively at more than a fraction of the promised distance. This is because the distance given as the network range is the maximum distance achieved in open space under ideal conditions. Walls, desks, cubicles, and other large structural features can interfere with wireless transmission. The wireless network will compensate for some of this interference by dropping to a lower speed, but you’re still likely to find that your transmission distance is shorter than anticipated.

Some buildings provide special obstacles to wireless transmission. For example, the solid stone walls, brick, or heavy coats of plaster on lathe in older, historic buildings can interfere with wireless transmission. For this reason, a wireless installation in an old building may require more access points than in a comparable modern building, although wireless can be an ideal way to bring a network to a historical building that can’t be cabled.

3.3.2 Interference from other electronic devices.

The 2.4-GHz frequency used by 802.11b, 802.11g, and 802.11n wireless is appealing for many wireless- and electronic-device manufacturers because the government doesn’t require a license to use it. But no license also means there’s no entity to coordinate use in this frequency. Interference from and with other 2.4-GHz devices can be a problem with wireless networking, especially in dense urban environments and apartment buildings.

Common devices that can interfere with or have interference caused by your wireless network include:

- Baby monitors
- Garage-door openers
- Cordless phones
- Microwave ovens
- A/V senders
- XM radio
- Energy-saving light bulbs
- Other wireless networks
- Many medical devices such as diathermy machines

Many of these devices, because they share the same 2.4-GHz spectrum, can noticeably degrade your wireless network’s performance. A wireless network can also interfere with the performance of other devices operating in the 2.4-GHz spectrum. With devices such as portable phones, this doesn’t matter much, but in the case of critical medical devices, a nearby wireless network can be literally life-threatening.

The problem of interference with nearby devices is extremely variable. One network will experience serious slowdowns in an environment that seems very similar to another wireless network that’s operating perfectly. Most wireless vendors offer a software program that allows you to monitor the signal strength and connection speed. One way to test for interference is to place an access point in your home or business, insert a wireless card in your laptop, and then roam around to evaluate the strength of the signal. This exercise can reveal the areas for placing access points that offer the strongest signal and fastest connection.

Another way to minimise or eliminate interference is to simply remove or reposition the devices that cause it. Keep devices such as microwave ovens at least six feet from access points.

802.11n wireless devices give you the choice of using the 5-GHz spectrum. If you’re having significant interference problems with the 2.4-GHz band, it may be worthwhile to switch to 5-GHz 802.11n.

3.4 Ease of installation.

One of the reasons often given for choosing wireless over a traditional wired network is ease of installation. However, keep in mind that all Ethernet networks can be tricky to install. All networks—wired or wireless—require that you install and configure software and this process can be tricky for the novice user. The only thing that makes wireless networks easier to install than wired ones is that you don't have to run cable.

3.5 Compatibility.

Another consideration is whether a planned wireless installation is compatible with your existing network and with any network you may want to install in the future. 802.11g wireless Ethernet is compatible with wired Ethernet networks, with older 802.11 DSSS equipment, and with the older 802.11b standard. But it is not compatible with older 802.11 FHSS devices and with 802.11a.

802.11n, because it can use either the 2.4- or 5-GHz band or both, is compatible with the 802.11g, 802.11b, and 802.11a wireless standard, although it should be noted that mixing standards results in an impairment of 802.11n speed.

Something else to watch out for when considering compatibility is that some vendors—even though they are subject to 802.11x compatibility tests—will decide they have a better solution for speed or security and will build proprietary solutions into their wireless equipment. This means that although in theory all 802.11x devices work together—in actual practice they sometimes don't.

4.0 Installing a wireless network.

A wireless network can operate in two modes: ad-hoc and infrastructure. In ad-hoc mode, your computers talk directly to each other and do not need an access point. In infrastructure mode, network traffic passes through a wireless access point. An infrastructure-mode wireless Ethernet segment can be easily added to a traditional wired network to make an integrated wired and wireless network.

4.1 Installing an ad-hoc network.

Installing a simple ad-hoc network in a limited area (such as in a small office or home) requires placing wireless network interface cards (NICs) in PCs that don't have built-in wireless. They install just like any other NIC, but usually sport antennas that stick out of the computer's case like little ears. PC-card versions are available for laptop and notebook computers.

4.2 Installing an infrastructure-mode network.

To install a larger network in infrastructure mode, both NICs and access points must be installed and configured. Placing access points to ensure proper coverage and performance can be tricky. For a smaller installation, simple trial and error will often find the best locations for access points. However, a large wireless network needs some organisation. The best way to decide where to place access points is by performing a site survey. This is done by placing access points in various locations around the intended coverage area and recording signal strength and quality. Network and power connections must also be considered. Often the best place for access points is on the ceiling. Although an access point can easily be mounted on the ceiling, most buildings do not have Ethernet and power connections on the ceiling. A partial solution to this problem is to run just an Ethernet connection to the access point and use an access point that can be powered through the Ethernet cable. These access points get power from a PoE power source in the wiring closet that provides DC power over the unused wire pairs in the UTP Ethernet cable. This feature eliminates the need to run an AC power cable to the access point, making installation easier.

Access points and NICs must be configured after they're installed. Most vendors supply configuration tools with their wireless products, and some even provide for bulk configuration of access points on the same network. Access points can be config - ured via Telnet, Web-based browsers, or SNMP; from a wireless station; or by using a serial console port built into the access point itself.

5.0 The integrated network solution.

Wired and wireless networks each have different strengths—wired networks are faster and more secure; wireless is versatile and doesn't require cable runs. However, the ideal network might include both wireless and wired network segments combined into a single, integrated network. An integrated network enables you to take advantage of the flexibility of a wireless network while still retaining the higher security of a wired network for confidential data.

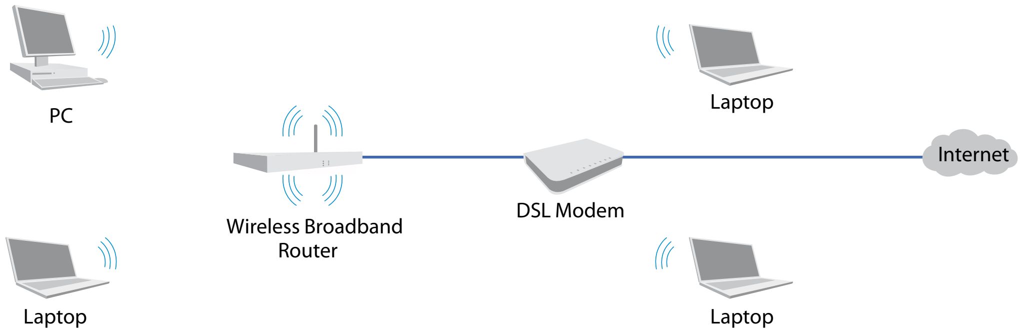
An Ethernet switch makes this possible by keeping general network traffic off the wireless segment. An Ethernet switch is a bridging device that connects multiple network segments to create one homogeneous network but still keep one segment (or subnetwork) isolated from another. This division makes the network more efficient because each network segment keeps its traffic to itself. It also makes sure your wireless access points transmit only data intended for wireless computers—data traveling on the wired network segment is not transmitted over the wireless network segment.

6.0 Network examples.

6.1 Ad-hoc wireless network.

Ad-hoc wireless networks are an inexpensive and flexible option. An 802.11x network in ad-hoc mode is entirely wireless. Each workstation relates on a peer-to-peer basis with other workstations. You can add a wireless broadband router to an ad-hoc network to provide Internet access to computers on the network. An ad-hoc network is most suitable for casual small networks where security is not a major concern.

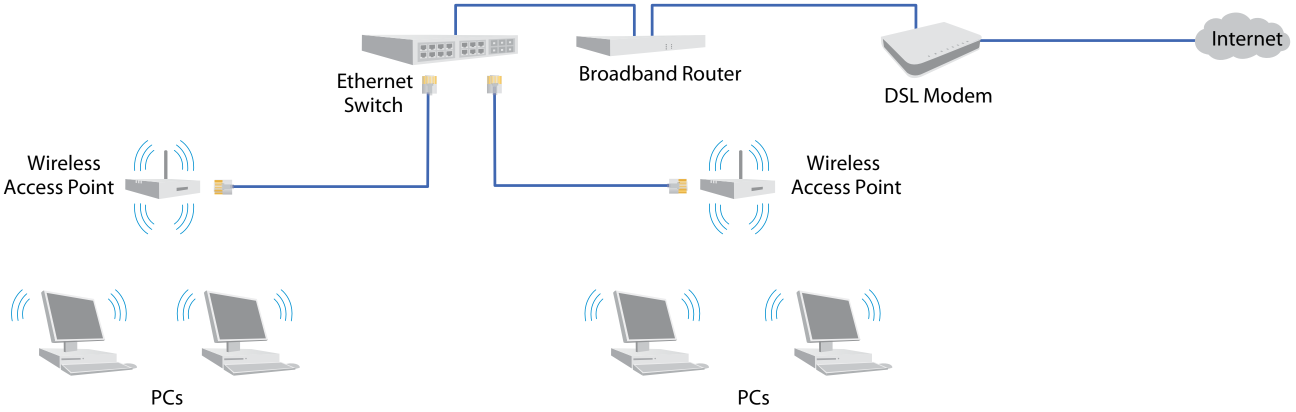
Ad-hoc wireless network



6.2 Infrastructure-mode wireless.

For installations larger than small workgroups, choose an infrastructure-mode wireless network. An 802.11x network in infrastructure mode depends on access points connected together. Each workstation communicates with an access point rather than directly with another workstation. Infrastructure mode is suitable for small-to-medium-sized wireless networks, but it may not offer enough bandwidth for networks with heavy traffic.

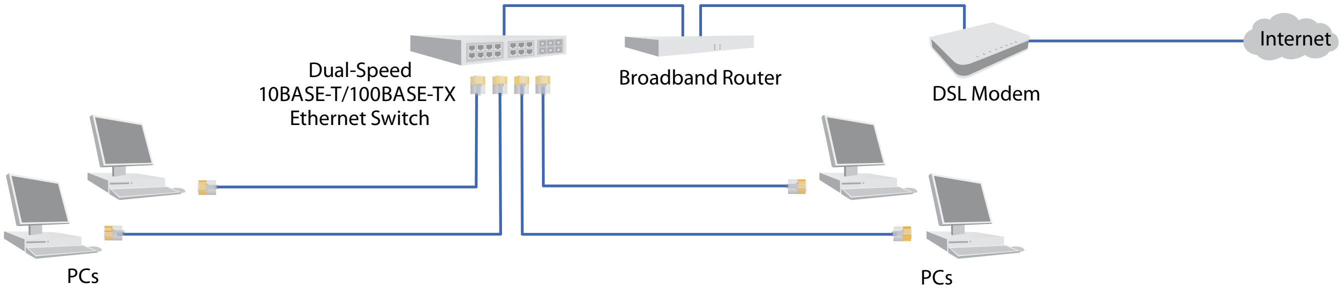
Infrastructure-mode wireless network



6.3 Wired network (10BASE-T, 100BASE-TX, or 1000BASE-T).

A wired network such as this 100BASE-TX network offers both high speed and security. It's easier to support large networks with many users on a wired network. However, a wired network lacks the flexibility of a wireless network—users must stay near a network connection and can't move their computers at will.

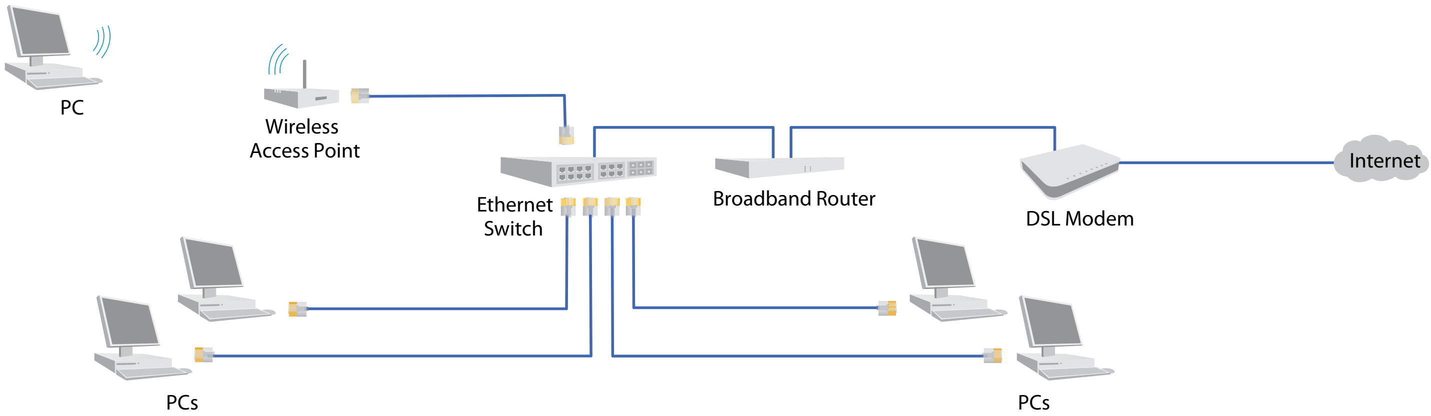
Wired network



6.4 Integrated network.

By combining wired and wireless networks, you can build an integrated network that offers the freedom of wireless to some users, while maintaining the security of a wired network for others.

Integrated network



7.0 Wireless security.

Wireless has long been regarded as quite vulnerable to hacking, and it is still true that wireless can never be 100% secure. However, advances in wireless security have progressed to the point where you can, with reasonable precautions, trust all but the most sensitive data to your wireless network. 802.11i wireless is even good enough for government work—many 802.11i devices meet the Federal Information Processing Standard (FIPS) 140-2 requirements for securing sensitive-but-unclassified communications with the Advanced Encryption Standard.

7.1 Wireless security standards.

7.1.1 WEP.

The 802.11b Ethernet standard includes a security protocol called Wired Equivalent Privacy (WEP), which encrypts data packets well enough to keep out most eavesdroppers. WEP encrypts each 802.11 packet separately with an RSA RC4 cipher stream generated by a 64-bit or 128-bit RCA key. But several cryptoanalysts have identified weaknesses in the RC4's key scheduling algorithm that make the network vulnerable to hackers. Software tools such as AirSnort have long been widely available on the Internet to enable hackers to crack WEP and gain access to wireless networks.

Although it's clear that the underlying cryptography of WEP, RC4 algorithm, is insufficient, the larger problem is that wireless users often either do not activate WEP at all or fail to change the default passwords. When you fail to take these basic precautions, you leave your wireless network vulnerable to casual hacking.

7.1.2 WPA.

Wi-Fi Protected Access (WPA) is a wireless security standard created by the Wi-Fi Alliance to address the weaknesses in WEP. WPA was intended as an intermediate measure to increase network security until the 802.11i standard was ready. WPA is forward compatible with 802.11i.

WPA uses dynamic session keys called Temporal Key Integrity Protocol (TKIP) to address the problem of users who don't enable WEP or who don't change the default key. TKIP automatically derives its encryption keys from a master key using a mathematical algorithm and changes the keys at regular intervals. This eliminates the problem of people who forget to change keys.

There are two types of WPA—WPA Enterprise and WPA Personal—each has its own authentication mode. WPA Enterprise features a central authentication server such as a RADIUS server to authenticate users. WPA Personal uses a simplified authentication method that depends on a pre-shared key or password entered into each wireless device. Once the password is entered, the TKIP mechanism takes over and changes keys automatically.

WPA depends on the 802.1x protocol, which incorporates the Extensible Authentication Protocol (EAP). EAP enables authentication between a client device and the authentication server. Like WEP, WPA uses the RC4 stream cipher.

7.1.3 IEEE 802.11i.

This is the official IEEE standard that specifies security mechanisms for 802.11 networks. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, an improvement over the RC4 stream cipher used by WEP and WPA. AES is secure enough to meet the FIPS 140-2 specification.

Like WPA 802.11i uses 802.1x with EAP to authenticate users and includes a mechanism for creating fresh keys at the start of each session.

7.1.4 WPA2.

WPA2 is an implemenation of IEEE 802.11i that has been approved by the Wi-Fi Alliance.

7.2 Steps to secure your wireless network.

7.2.1 Use the security you have.

A surprising number of wireless networks aren't secured at all and most intrusions into wireless networks are from casual users taking advantage of unsecured networks. Even if you have a small home network that doesn't support the newer security standards, you can prevent casual access to your network simply by turning on very basic security measures.

7.2.2 Change the default SSID.

The Service Set Identifier (SSID) is a unique identification number attached to wireless packets. The SSID is essentially the password a mobile device needs to connect to an access point. The SSID doesn't really act to secure your wireless network because it can easily be found in packets simply by using a packet sniffer. However, changing the SSID from the factory default can go a long way to deter very casual users who aren't going to go to the trouble of using a packet sniffer.

7.2.3 Turn on your encryption and change the factory setting.

Wireless devices often come with their security features turned off. Make sure you turn on encyrption and that you use the highest level of encryption available with your device. In other words, choose WPA or WPA2 over WEP. Change the factory default password to something longer than the usual 6- to 8-character password and do not include English words within the password.

7.2.4 Take advantage of the new security standards.

You do have to invest in new hardware to enjoy the high security provided by IEEE 802.11i or WPA2 AES encryption. However, if you have anything you MUST keep secure, the additional cost is well worth the expense. For the highest level of encryption generally available, look for FIPS 140-2 certified devices. Remember that all your wireless devices—computers, routers, and access points—must use the same encryption.

7.2.5 Use more than just wireless encryption.

Wireless computers on your network need the same virus protection, spyware protection, and firewall protection as any other computer on your network.

7.2.6 Turn it off.

Small office and home wireless networks should be turned off at night and on weekends when they're not being used. Hackers can't access what isn't turned on.

7.2.7 Screen your users.

Wireless routers can usually be set to allow only specific MAC addresses to access your wireless network. Hackers can mimic MAC addresses, so this is not a complete security measure, but it will go a long way to discourage the casual freeloader.

7.2.8 Don't let your employees install unauthorised access points.

Unauthorised access points can range from a nuisance to a real security threat in a large network. Because it's so easy for users to plug in an access point, you have to constantly guard against it. Just one unsecured access point can be a vulnerable entry point for an entire network.

7.2.9 Watch out for strange hotspots.

Usually, when you think about wireless security, you think about outsiders hacking into your network through your wireless access points. Keep in mind, though, that your network's most vulnerable point may be where you link to your home network through someone else's wireless network.

When you use a wireless hotspot in a coffee shop or hotel, this unsecured connection can provide a quick back door to your home network.

A type of attack that can happen is the rogue wireless access point. A hacker sets up an access point with a stronger signal than that of the hotspot, then, when you turn on your computer, this rogue access point offers to connect you to what seems like the correct network. You wind up entering your username and password for the hacker to access. Fortunately, this type of rogue access point attack is quite rare.

To help keep traveling laptops from being a security weak spot, install a good software firewall. Look for a hotspot that uses WPA or WPA2, which provide protection against this type of attack. Also consider using a Virtual Private Network (VPN) to encrypt data so that prying eyes can't see what's going to and from your home network. Just to be safe, it's always a good idea not to send or receive sensitive information at an unfamiliar hotspot.

7.2.10 Hang onto those laptops.

Theft of laptop and notebook computers is sadly a common occurrence. A stolen computer can provide express entry into your network. Use physical locks and lock access to the computer itself with password security or even with a fingerprint scanner. If a computer is stolen, change network passwords immediately.

8.0 Conclusion.

Planning your wireless network up front can save a lot of expense and inconvenience later. Black Box recommends that you assess and list your network requirements before you decide what kind of network to use. Consider factors such as:

- Security requirements
- Bandwidth requirements
- Environmental factors that may interfere with wireless transmission
- Ease of installation
- Total number of network users
- Number of laptop users who will want wireless connections

Wireless is a maturing technology that has come a long way since its inception. It's now standard, rather than exceptional, to build new networks with significant wireless components. And with new advances in wireless technology, your wireless links will rival your wired links for performance and security.

Whether you're interested in commercial or residential applications, and whether you're considering a wired, a wireless, or an integrated network, Black Box has your solution! We'll supply the products and technical service required to plan, design, install, and maintain the network that's best for you.