BLACK BOX®
NETWORK SERVICES

Wireless Networking

Wireless standards, architecture, security, and more!

LongSpan™ Wireless Ethernet Extender

Pure Networking™ 802.11n Wireless Access Point

SmartPath™ Enterprise Wireless System

724-746-5500 | blackbox.com/go/Wireless

Table of Contents

We're here to help! If you have any questions about your application, our products, or this white paper, contact Black Box Tech Support at **724-746-5500** or go to **blackbox.com** and click on "Talk to Black Box."
You'll be live with one of our technical experts in less than 30 seconds.

Introduction

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.

Since the mid 1990s, wireless has grown from an obscure and expensive curiosity into a practical technology with range and speed to rival traditional cabled networks.

Wireless is evolving at a breathtaking rate. In this paper we examine current wireless networking technology and explain the basics of how a wireless network is designed and how it works with a traditional wired network. And, although the market offers a wide range of wireless ranging from specialized industrial to laser to 3G/4G cellular, here we discuss only wireless Ethernet—the kind used with computer networks.

IEEE wireless standards.

The IEEE 802.11 wireless Ethernet standards come from the Institute of Electrical and Electronics Engineers, Inc. (IEEE). This organization only sets the specifications for the standards—it doesn't test individual wireless products for compliance to these standards. Because the IEEE 802.11 standards are real Ethernet standards that look like Ethernet to your applications, compatibility with wired Ethernet is seldom an issue.

You may notice that "Wi-Fi" is sometimes used interchangeably with the 802.11 standards, particularly with 802.11g, however, this is not quite correct. Wi-Fi simply refers to a product that's certified by the Wi-Fi Alliance, an organization 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.

IEEE 802.11-1997—the first wireless Ethernet.

IEEE 802.11 was introduced in 1997. It was a beginning, but the standard had serious flaws. 802.11 only supported speeds of 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.

IEEE 802.11-2007.

This 2007 release of 802.11 updated the standard by merging amendments a, b, d, e, g, h, i, and j into the base standard ratified in 1997.

IEEE 802.11b.

Ratified in 1999, 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. 802.11b uses the popular 2.4-GHz band.

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 802.11a.

Also ratified in 1999, 802.11a uses a different band than 802.11b—the 5.8-GHz band called U-NII (Unlicensed National Information Infrastructure) in the United States. 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.

IEEE 802.11g.

802.11g 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.

802.11g wireless Ethernet was the most popular standard for many years and is still in common use, however, the newer 802.11n standard is rapidly taking over as the most popular wireless standard because it offers far greater speed and range.

IEEE 802.11n.

802.11n, which operates in both the 2.4- and 5-GHz bands, is today’s wireless standard. It’s not just a step up from the common 802.11g standard, it’s so much better in throughput, coverage, and reliability that it can be said to be revolutionary.

This new wireless standard can theoretically achieve wireless throughput of up to 300 Mbps. As a practical matter, 802.11n supports Fast Ethernet throughput of 100 Mbps. Additionally, its effective range is also dramatically larger than earlier 802.11 standards.

802.11n achieves this remarkable performance by using multiple wireless signals and antennas instead of one and by using channel bonding.

The technique of using multiple wireless signals and antennas is called Multiple-Input/Multiple-Output (MIMO). Because MIMO transmits multiple data streams simultaneously, it increases 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 uses a transmission technique called spatial multiplexing to send a high-speed data stream across multiple antennas by breaking it into several lower-speed streams and sending the streams 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.

To operate at maximum speed, 802.11n must operate in *channel bonding* mode. Channel bonding combines two adjacent 20-MHz channels into a single 40-MHz channel, effectively doubling bandwidth. Channel bonding increases the chances of difficulties when 802.11n is operated in the same space as older “dumb” wireless networks. Even though 802.11n is backwards compatible, 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 interferes with its operation and forces the 802.11n to slow down to deal with the older standards, resulting in significant network slowdowns.

IEEE 802.11s.

This proposed amendment to the 802.11 standard defines how wireless devices negotiate a mesh network both in static topologies and in an ad-hoc network. IEEE 802.11s operates at Layer 2—the Data Link Layer—relying on MAC addresses for its operation. It relies on 802.11a, 802.11b, 802.11g, or 802.11n to carry the actual traffic, with the newer 802.11n in most common use.

IEEE 802.11u.

This amendment, ratified in 2011, simplifies the process of adding mobile users to the wireless network, enabling devices such as laptop computers and smartphones to quickly select an appropriate network by viewing information about available networks. Devices that are not previously authorized to join a network can become authorized based on rules set by the network administrator. These rules may be quite sophisticated and may require new devices to complete an on-line enrollment. This standard has not yet been widely adopted but promises to simplify wireless network connections in congested areas where a wireless device may have access to dozens of competing wireless networks.

IEEE 802.11i.

IEEE 802.11i, also called WPA2, 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. It 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.

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.

IEEE 802.21

This 2008 standard manages the handoff when mobile devices travel between networks of the same type or between networks of different types. This results in a seamless user experience when, for instance, a smartphone moves out of the range of an 802.11n network and switches to a 3G cellular network.

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.

IEEE 802.16.

IEEE 802.16, was ratified in January 2001 and 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.

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.

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.

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.

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.

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 authorized.

Considerations before installing wireless.

Before deciding to install a wireless network, you should be familiar with wireless and know its strengths and weaknesses. One major 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 installing a 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 installation.

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 **pp. 13–15** of this paper.

Speed.

802.11g—still a commonly used wireless standard, although 802.11n is rapidly gaining ground—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.

With an actual throughput of about 100 Mbps and an extended range, 802.11n provide far more flexibility than 802.11g, making it the first wireless standard that can truly be considered to be a replacement for wired networks. It can be used in situations where large files are exchanged, for instance in a design firm, and it’s ideal for archival backups.

Environmental concerns.

Environment can affect your wireless network, and your wireless network may affect electronic devices within your environment. Take a good look at the space where you intend to install your wireless network and remember that 802.11n only operates at optimal speed in a “clean” environment with no interference from older 802.11b/g devices.

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.

Newer wireless technology can help bring wireless to difficult structures. 802.11n offers a far better range than older standards, although it can still be stopped dead by the wrong architecture. Wireless mesh networks can also help work around difficult buildings by passing data from wireless router to wireless router until it reaches its destination.

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 minimize 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.

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.

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 802.11g, 802.11b, and 802.11a wireless, although it should be noted that mixing standards slows 802.11n significantly.

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.

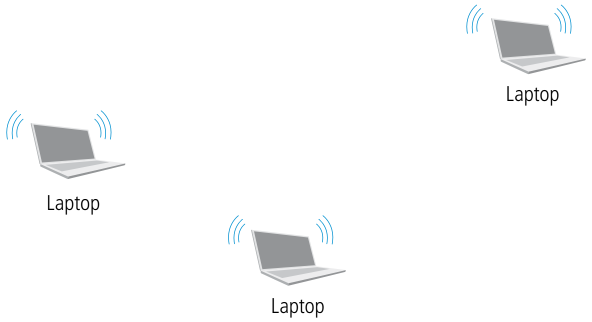
Wireless network architecture.

A wireless network can have one of three basic architectures: ad-hoc, infrastructure, or mesh.

The ad-hoc wireless network.

A ad-hoc network, also called a peer-to-peer network, is a casual network in which wireless devices talk directly to each other without the use of an access point. An ad-hoc network can spring up, for instance, between two laptop computers in a coffee shop. All that is required for an ad-hoc network is two or more compatible wireless devices.

Ad-hoc wireless network



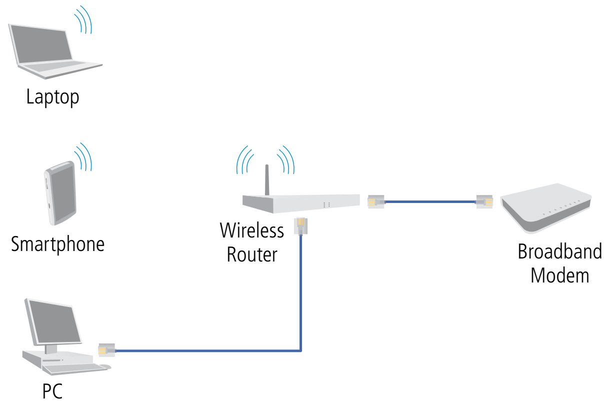
The infrastructure-mode network.

In an infrastructure-mode wireless network, access points connected to the wired network act as a bridge to wireless clients. All wireless access points are connected to the wired network and all wireless traffic—even that going from one wireless client device to another—travels to the wired network on the way to its destination. Infrastructure mode is the most common network architecture in use today, although wireless mesh networks are making inroads.

Infrastructure-mode wireless combines the strengths of both wired and wireless networks—wired networks are faster and more secure; wireless is versatile and doesn't require cable runs. Plus, it enables wireless users to reach devices such as printers that are normally connected to a wired network.

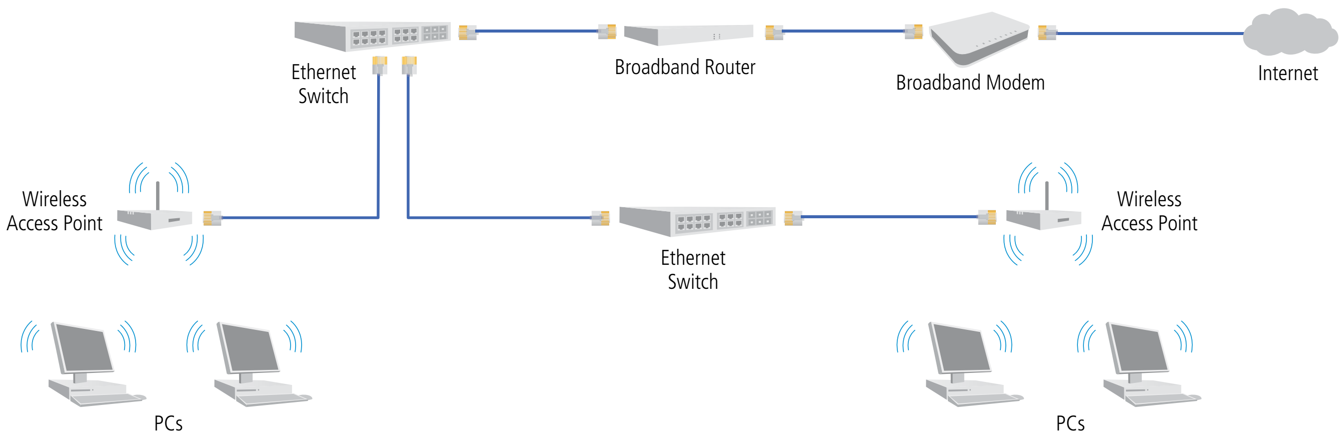
The simplest form of the infrastructure-mode network is the common home wireless network, which has a wireless router (an access point, switch, and router in one box, connected to a broadband modem. This kind of a simple wireless network is called a Basic Service Set (BSS).

Infrastructure-mode wireless network: Basic Service Set



When the network expands to include more than one BSS, it becomes an Extended Service Set (ESS) consisting of multiple access points on one logical network. This is the wireless model used by most larger buildings such as businesses, schools, and hotels.

Infrastructure-mode wireless network: Extended Service Set



An ESS infrastructure-mode wireless network supports roaming so that a mobile device—for instance, a smartphone or laptop computer—automatically and seamlessly moves from one access point to the next.

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 organization. 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.

The wireless mesh network.

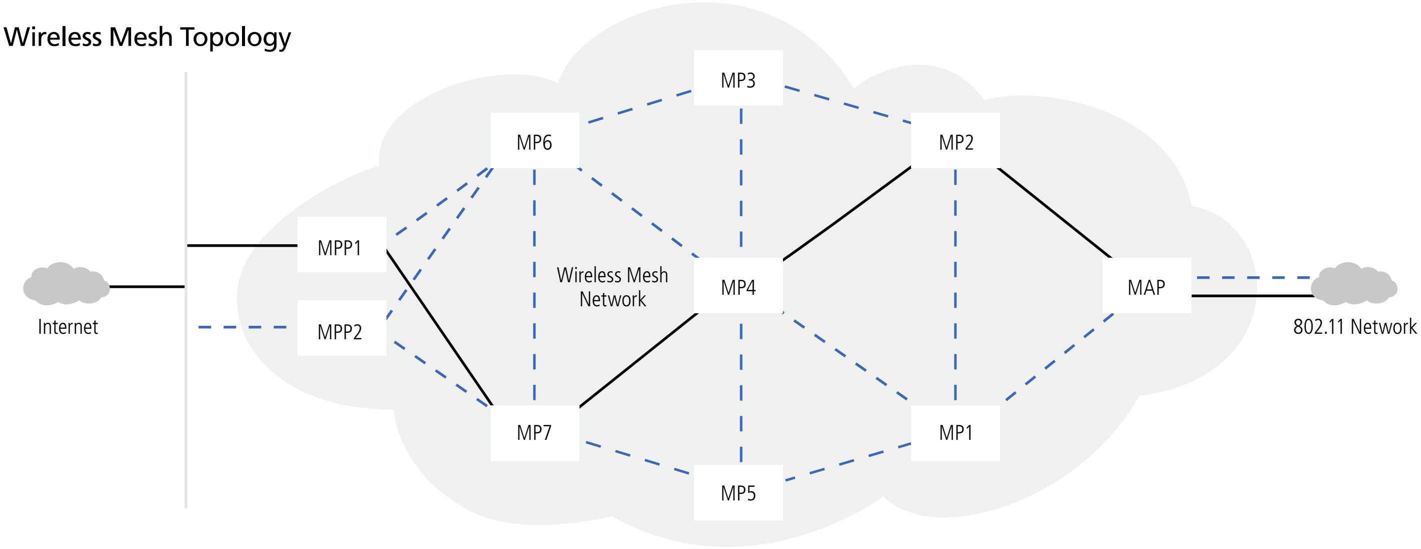
Until recently, the standard way to construct a wireless network was to build an infrastructure-mode network, which is essentially treated as an accessory to a wired network with access points doing little except providing a bridge between the wired and the wireless network.

Today's faster processors, however, have made it possible to create "smart" access points, which act as routers to direct traffic, not just between wireless clients and the wired network, but also to other access points. This kind of topology in which access points have evolved into routers that actively work to find the best way to direct traffic and can direct traffic to other access point, is called a wireless mesh network.

In a wireless mesh network (WMN), access points—now usually wireless routers—communicate with each other and may actively route traffic across the network using both the wired and wireless network. The proposed 802.11s standard defines three kinds of wireless mesh devices:

- Mesh Point (MP): A wireless station with routing capability and no connection to a wired network.
- Mesh Point Portal (MPP): A mesh point that serves as a gateway and traffic aggregator to another network.
- Mesh Access Point (MAP): An access point with routing capability.

Wireless Mesh Topology



Wireless mesh devices work with each other to find the most efficient pathway to send traffic across the network. This pathway may be through the wired network or through one or more wireless routers. A wireless mesh network may consist of any number of wireless routers—even as many as several hundred covering an entire city. The routers "talk" to each other to establish the most efficient way to send packets across the network. Each router implements dynamic routing algorithms and communicates routing information to other routers on the network. This enables data to hop across the network from one device to another until it reaches its destination.

Data travels across a wireless mesh network in much the same way that data travels on a wired network—packets travel across the network by hopping from node to the next, with each node automatically choosing the quickest, safest pathway for them until they reach their destination. Because mesh networks are largely self-organized and self-configured, they require minimal configuration.

Even in a network that consists primarily of wireless mesh, information needs to get back to an access point on a wired network and ultimately the Internet. This communication to the wired network is called the backhaul. Very large wireless mesh networks can impose a significant delay on the backhaul and need to be specially configured with dedicated backhaul nodes that other nodes send outgoing data directly to. Backhaul nodes are usually MPPs, which send the data directly to the wired network and the Internet.

A wireless mesh network in which each mesh router is on its own to connect to other nodes and decide where to send data is called a fully distributed network. This model is inexpensive to set up, but isn't centrally managed and provides only basic security. Fully distributed wireless mesh is an ideal way to bring wireless Internet service to sites such as shopping malls or motels where the cost of running cable to access points in an infrastructure-mode network may be prohibitive and where, because the network is public, there are no expectations of high security.

Larger, enterprise-class networks require some kind of central management to optimize routing and enforce security, as well as to provide a convenient way to keep a large number of wireless mesh routers up to date with the latest firmware.

A centrally managed WMN is usually under the control of one or more controllers, however, cloud-based, fee-for-service management is now also available and is a good option for a wireless mesh network large enough or sensitive enough to require management but not large enough to justify the cost of a controller.

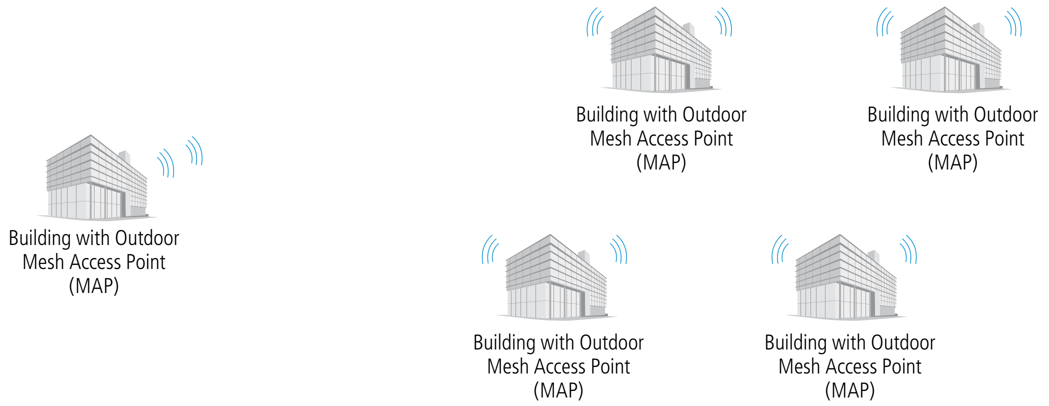
Partial mesh refers to wireless in which access points communicate with each other but do so in very limited ways. Common applications are point-to-point wireless connections that act as a simple bridge between buildings or between a wired network and a full wireless mesh network.

Partial Mesh: Point-to-point wireless

Building with Outdoor Mesh Access Point (MAP)
Building with Outdoor Mesh Access Point (MAP)

Another common application for partial mesh is point-to-multipoint wireless for last mile connections by Internet service providers.

Partial Mesh: Point-to-multipoint wireless


Building with Outdoor Mesh Access Point (MAP)
Building with Outdoor Mesh Access Point (MAP)
Building with Outdoor Mesh Access Point (MAP)
Building with Outdoor Mesh Access Point (MAP)
Building with Outdoor Mesh Access Point (MAP)

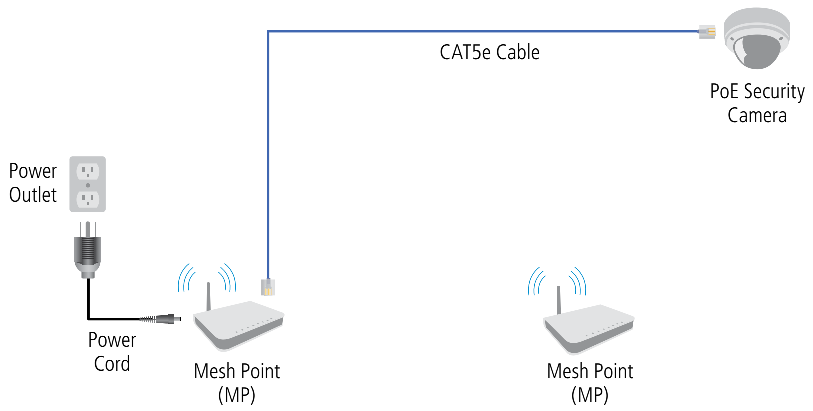
Power over Ethernet (PoE)

No discussion of wireless would be complete without a mention of Power over Ethernet.

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.

Some wireless mesh routers can even function as Power over Ethernet (PoE) power source equipment (PSE). They require a power outlet, but can provide power to a connected device such as an IP camera.

Power over Ethernet: Mesh access point providing power to a PoE-enabled IP security camera.



Wireless security.

Wireless has long been regarded as quite vulnerable to hacking, and although it is still true that wireless can never be 100% secure, there is a lot you can do to make it secure enough for all but the most sensitive applications.

In addition to securing your wireless through the various encryption and authentication standards available for wireless networks, there are other security precautions you can take. Some of them are as simple as making sure that company laptop computers are secured.

Wireless security standards.

802.11x wireless Ethernet supports several security standards. Advances in these wireless security standards 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.

The 802.11 Ethernet standard includes a security protocol called Wired Equivalent Privacy (WEP). Although WEP has largely been supplanted by newer security protocols, it's still supported by all 802.11x protocols and can encrypt 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.

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.

IEEE 802.11i, also called WPA2, is the current IEEE standard for encryption in 802.11 networks. For more information about this standard, see **page 5**.

IEEE 802.11u, provides access control for mobile devices joining the wireless network. For more information about this standard, see **page 5**.

To take advantage of these wireless security standards, it's important to turn them on in the first place. A surprising number of wireless networks aren't secured at al,l and most intrusions into wireless networks are from casual users taking advantage of unsecured networks. Even if you have a small home network, you can prevent casual access to your network simply by turning on basic security measures.

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

Take advantage of the new security standards.

You may have to invest in new hardware to enjoy the high security provided by IEEE 802.11i, IEEE 802.11u, 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.

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.

Install NAC

Controlling which devices have access to your wireless network is more of an issue than ever in this day of handheld mobile devices. This is why network access control (NAC) is important. The 802.11u standard provides some access control for mobile devices but is not yet widely adopted. To gain complete control over which devices join a network, you may require a separate NAC application to protect the network, both wired and wireless.

Although NAC may be software only, it's usually a dedicated appliance that ensures that only known devices are allowed to connect to your network and that they meet your network's requirements before they are granted access. NAC keeps untrusted and unauthorized devices off the network protecting against everything from wireless Internet moochers to hackers stealing sensitive information through an unprotected network port.

Keeping untrusted devices off the network is pure NAC—NAC at its most basic level. But many vendors have expanded the functionality of their NAC products to include other services. It may also be able to dictate already trusted users' level of access and manage users' access once they're on the network.

Because NAC operates across the entire network, not just the wireless portion, it also addresses the problem of employees that install unauthorized access points. This can be a real security concern—just one unsecured access point can be a vulnerable entry point for an entire network.

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. Wireless hotspots in coffee shops and hotels can provide a quick back door to a corporate network.

Another 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.

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.

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.

Other steps to secure your wireless network.

- Use more than just wireless encryption. Encryption is a good start, but wireless computers on your network need the same virus protection, spyware protection, and firewall protection as any other computer on your network.
- 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.
- Even if you can't install NAC, you can still 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.

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
- Number of smartphones

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.

About Black Box

Black Box Network Services is a leading networking provider, serving 175,000 clients in 141 countries with 196 offices throughout the world. The Black Box catalog and Web site offer an extensive range of products including wireless routers and access points as well as industrial wireless solutions. Its LongSpan™ Wireless Ethernet Extender provides a cost-effective way to extend an Ethernet network up to 40 miles. More information is available at http://www.blackbox.com/go/LongSpan. The SmartPath enterprise-class wireless enables smart mesh wireless networks without the need for a central controller. Learn more about SmartPath at http://www.blackbox.com/go/SmartPath.

Black Box also offers wireless antennas, Ethernet switches, and media converters, as well as cabinets, racks, cables, connectors, and other video, audio, and data infrastructure products. To view Black Box's comprehensive offering, see our Web site at blackbox.com.

Black Box is also known as a leading communications system integrator, dedicated to designing, sourcing, implementing, and maintaining today's complete communications systems.