BLACK BOX
NETWORK SERVICES

Wireless Mesh

Why intelligent mesh is the best enterprise wireless solution.

SmartPath™ Enterprise
Indoor Wireless Access Point
with Integrated Antennas

SmartPath Enterprise
Wireless Access Point,
Hardened

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

Since its introduction in 1997, wireless Ethernet has rapidly evolved from an exotic, expensive, slow technology to an everyday service available in coffee shops. Enterprise networks have also evolved from strictly cabled networks to integrated networks that include wireless service. Enterprise wireless now fulfills a wide range of functions ranging from secure guest Internet access to videoconferencing.

Since the introduction of wireless Ethernet, the architecture of enterprise wireless networks has progressed from simple access points added to a wired network almost as an afterthought to sophisticated wireless mesh networks, which are now the preferred architecture for enterprise wireless networks.

The progression of wireless networks has evolved through three distinct architectures:

- **Infrastructure mode wireless**, in which access points that act only as simple bridges are connected to a wired network.
- **Controller-based wireless,** which consists of "thin" access points that also act as simple bridges but which are managed and controlled through a central controller.
- **Wireless mesh,** in which intelligent access points act as network switches to route network traffic. These access points are also managed, either through a cloud-based service or through a dedicated appliance, but most of the "brains" and decision making capabilities reside within the access point.

This white paper will examine these three approaches to the enterprise wireless network and explain how intelligent mesh wireless is the preferred solution for most enterprise wireless networks, offering significant advantages in both cost and efficiency. Additionally, we'll examine the best way to approach the installation of a wireless mesh network for maximum coverage. But first, let's take a look at 802.11n—the breakthrough that made advances in wireless architecture possible.

802.11n

Wireless mesh would not be a practical technology without IEEE 802.11n, which carries the actual traffic. This newer standard, which was ratified in 2009, offers far greater speed and range than older wireless standards such as 802.11g. It's not just a step up from older standards, it's so much better in throughput, coverage, and reliability that it can truly be said to be revolutionary. This new wireless standard can theoretically achieve wireless throughput of up to 300 Mbps. As a practical matter, it supports Fast Ethernet throughput of 100 Mbps—enough for high-speed applications such as streaming video, which was marginal at best on 802.11g wireless. Additionally, its effective range is also dramatically larger than earlier 802.11 standards.

802.11n achieves its remarkable performance by operating in both the 2.4- and 5-GHz bands, through the use of channel bonding, and by using multiple wireless signals and antennas instead of one.

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. MIMO uses a transmission technique called spatial multiplexing that sends 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. Because it has multiple signals to choose from, MIMO achieves higher speeds at greater ranges than conventional wireless hardware.

Infrastructure mode wireless

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 travels through the wired network on the way to its destination. Wireless access points do not communicate with each other.

The first enterprise wireless networks were infrastructure mode simply because it was the only option. However, because this wireless topology isn't so much a wireless network as a wireless extension to a wired network, it has some inherent disadvantages that make it difficult to deploy at an enterprise level.

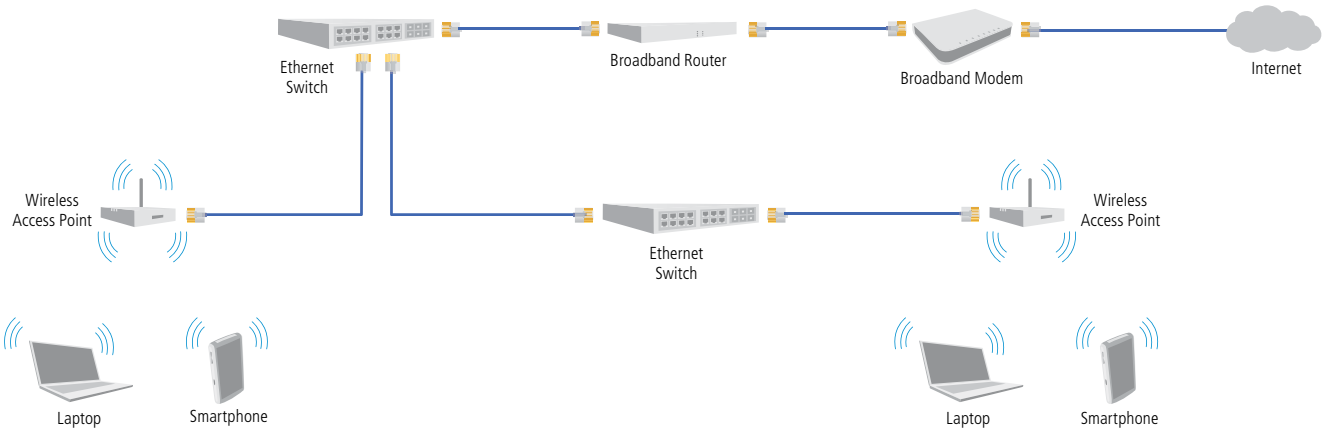
Lack of central management: Because infrastructure mode wireless has limited central management, a network manager has no easy way to determine the status of each access point and to change settings. There's no way of managing a distributed network with multiple SSIDs in multiple locations.

Lack of redundancy: In infrastructure mode, if a connection to an access point is lost, that access point is lost, creating a dead zone in wireless coverage.

Lack of mobility: Infrastructure-mode wireless networks can't manage a smooth handoff from one access point to the next. A mobile user traveling from one access point to another must log in again and loses their current session.

No provisions for guest access: Infrastructure-mode wireless architectures cannot easily offer different users different levels of network access. For instance, to enable employees to access the corporate network while restricting guest users to Internet access requires a separate network access control system.

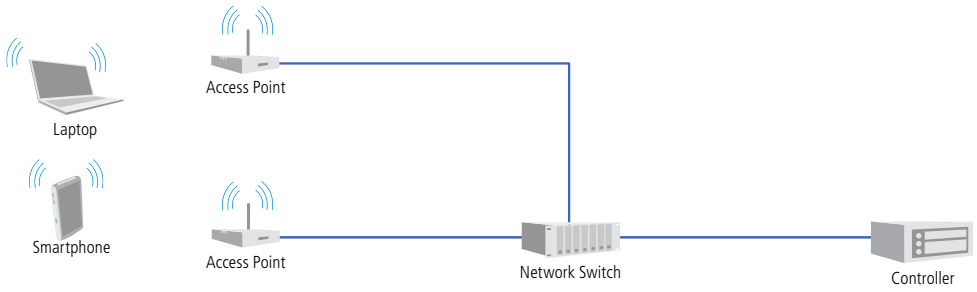
Infrastructure-mode wireless network



Controller-based wireless

A variation on infrastructure-mode wireless, is controller-based wireless, sometimes called split MAC architecture. This architecture was introduced primarily to solve the management and mobility problems of infrastructure mode wireless in enterprise installations. It features "thin" access points under the management of one or more controllers. The access points have little or no intelligence of their own and serve mainly as bridges between the wired and the wireless network, the primary difference from infrastructure-mode wireless being that access points are now under central management.

Controller-based wireless network



Although controller-based architecture does provide central management, policy control, and security functions for large wireless networks and also smooths the mobility issue, this architecture still has some of the same problems as infrastructure-mode wireless, plus it introduces a few issues of its own.

Inefficient traffic flow: Infrastructure-mode architecture adds latency and network bottlenecks because all traffic must travel to the controller and back. This "U turn" architecture makes time-sensitive applications such as voice and video virtually impossible.

Controller expense: The controllers needed for controller-based architecture represent a significant capital expense and often have a separate fee for licensing.

Network reorganization: Network configuration may need to be changed to accommodate a controller.

Reliability issues: The controller represents a single point of failure. Plus, a disconnected access point creates a wireless dead zone.

Difficult to manage: Controller-based wireless often requires a long learning curve for network administrators.

QoS issues: Many systems don't support Quality of Service (QoS). Combined with the latency added by the controller, this issue puts bandwidth- and time-sensitive applications out of reach for most controller-based wireless networks.

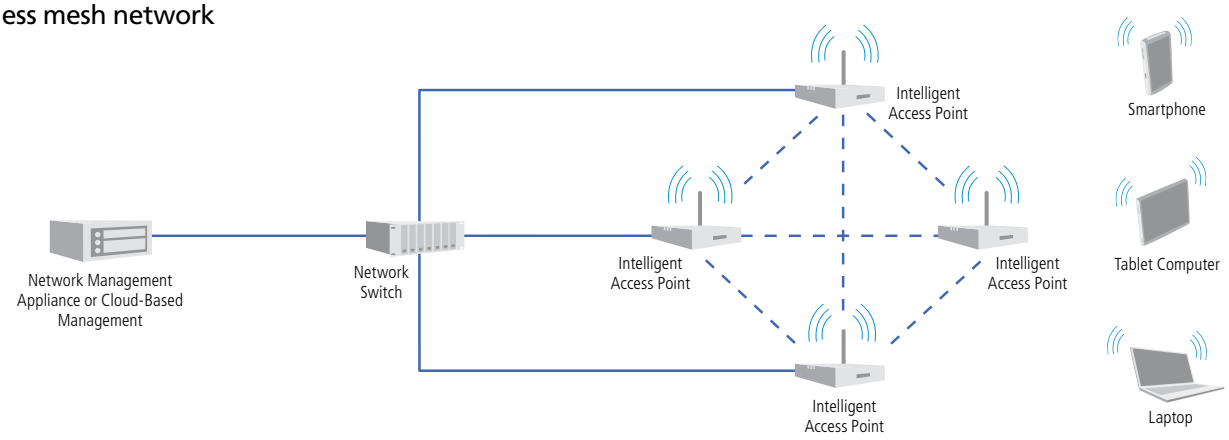
Wireless mesh

Today's low-cost, high-powered processors have made it possible to incorporate the power of a router into an access point, creating an intelligent access point. Intelligent access points create a wireless mesh by independently deciding how to route each packet by the quickest and safest route.

Wireless mesh provides enterprise-level services efficiently because data doesn't have to travel through a controller. Instead, network traffic is securely and efficiently routed to its destination by the most efficient pathway, which may be by way of the wired network or another access point.

Central management in a wireless mesh network is provided by a separate network management appliance or a cloud-based service. This is different from the management of a controller-based network because policy and security are enforced at the access point level rather than at a controller.

Wireless mesh network



Because wireless mesh has many of the capabilities of, and behaves much like, a traditional wired network, it has many advantages over earlier wireless implementations.

Scalability: With wireless mesh, it's easy to start small and add intelligent access points as needed without the up-front expense of a controller.

Redundancy: Wireless mesh is extremely reliable because there is no controller to act as a central point of failure—intelligent access points keep functioning even if management is lost. It's also self-healing, so if an access point fails, other access points take over. If an access point loses its network connection, it can still receive data through other access points.

Ease of use: New intelligent access points automatically join a wireless mesh network and can be centrally managed even in very large distributed networks.

Efficient traffic flow: A wireless mesh network forwards packets directly to where they need to be without requiring them to take a "U-turn" through a controller. This cuts down on latency and network congestion and reduces bottlenecks.

Coverage: Although intelligent access points are most efficient when connected to a wired network, they can also exchange data with another access point. This enables the placement of an intelligent access point in an area that may be difficult or impossible to cable. Combined with the extended range of the 802.11n wireless standard, wireless mesh can dramatically increase a network's reach.

Wireless mesh architecture

Intelligent access points in a wireless mesh network "talk" to each other and work together to find the most efficient pathway to send traffic across the network. This pathway may be through the wired network or through another access point. A wireless mesh network may consist of any number of intelligent access points—even as many as several hundred covering an entire city—most of which are also connected to a wired network. Each intelligent access point implements dynamic routing algorithms and communicates routing information to other access points on the network.

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 one 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.

A wireless mesh network in which each intelligent access point 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 may not always route packets in the most efficient way and provides only very basic security.

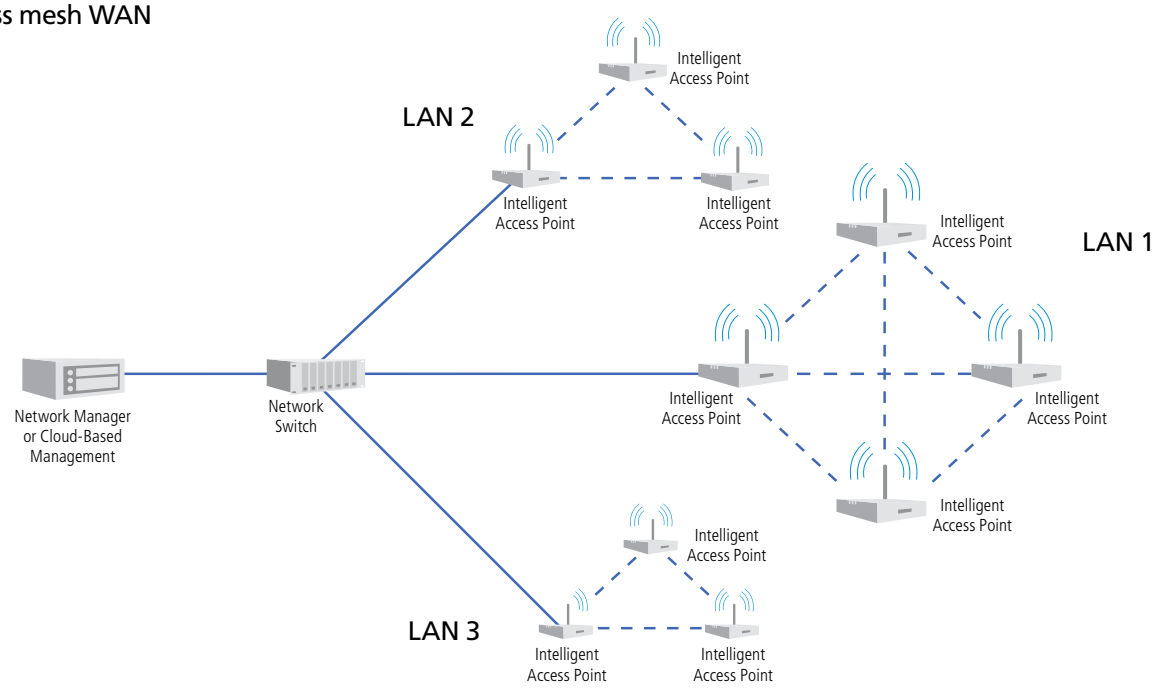
To reap the full benefit of a mesh network, you must have central management to optimize routing, establish policies, create a guest network, and provide a convenient way to keep a large number of access points up to date with the latest firmware.

Although a wireless mesh network may be managed through a management appliance, cloud-based management is catching on because it avoids the up-front cost of a management appliance, because it scales well to different sized networks, and because it can easily manage a wireless mesh that's spread across widely separated locations.

A wireless mesh network that covers a very large territory or that covers two or more widely separated areas, is usually divided into clusters, each cluster being a wireless mesh local area network (LAN). Together multiple LANs form a wireless mesh wide area network (WAN). The wireless LAN acts as a peer network, with each intelligent access point efficiently passing along packets to their destinations on the LAN, while also enforcing policies. Access points within the same LAN also sense the strength of radio signals coming from other access points and adjust their own signals to achieve maximum coverage with minimum overlap.

Wireless mesh products available today are proprietary and may operate at OSI Layer 2 (Data Link Layer) and Layer 3 (the Network Layer), routing data both by MAC addresses and by IP addresses. Although still in the preliminary development phase, an official mesh wireless standard is in development: IEEE 802.11s is a proposed amendment to the 802.11 standard that defines wireless mesh both in static topologies and in ad-hoc networks. This standard is expected to operate at Layer 2 only.

Wireless mesh WAN



Wireless mesh deployment

Good planning ensures smooth wireless mesh deployment. To get started, examine the basic requirements of your installation. First, consider who your users are and take the time to fully understand their access requirements. Talk to department managers within your organization and make sure everyone has documented how they use the network. Ask if guest access is required.

Next, make a complete list of applications your wireless mesh network will need to support. Begin with mission-critical applications, paying special attention to high-bandwidth and time-sensitive applications. Identify applications with minimum service levels.

Voice applications—for instance, the integration of mobile phones and IP-PBX for Voice over WLAN (VoWLAN)—require a careful evaluation of network requirements to ensure that the network contains enough access points for reliable service. Voice traffic is very sensitive to network jitter and latency, so an inadequate number of intelligent access points can degrade call quality and cause clipped conversations or dropped calls.

Other applications that require special attention are those that generate a large data stream, for instance, video, network backups, and large file transfers. The wireless network needs to be designed to compensate for these bandwidth-intensive activities so they don't interfere with others trying to use the wireless network.

Upgrading an existing wireless network

If you're upgrading from an existing WLAN with traditional 802.11g access points, you already have a head start on wireless mesh. Start with a site survey with the existing access points in place. If their coverage is adequate, the simplest approach is to just replace the existing 802.11g access points with 802.11n intelligent access points. Because these access points offer greater coverage and capacity than older access points and because they can exchange data with each other without going back to the wired network, this one simple step increases wireless performance dramatically without changes to network topography. This approach also maintains existing VLANs and security policies.

To upgrade from controller-based wireless networks, you need to replace the "thin" access points with intelligent access points. However, unlike when you upgrade from traditional access points, you may also need to add a local VLAN for access or use tunnels to replicate the controller-based wireless network's overlay network.

Planning a new wireless mesh network

If you're building a wireless network from scratch and don't have an existing wireless network to model your network on, you must plan ahead to determine network requirements. Factors to consider when planning a new wireless mesh network are:

- Determine how much wireless service you need: How many users will need wireless service and what applications will they use? Will only certain groups within the organization need wireless access, or will it be rolled out across the enterprise? Will you provide guest access to visitors? Do you need support for voice services? Will you be adding voice services in the future?
- Think about wireless devices other than computers: Will most of your users be on computers? Today's wireless users are increasingly not on desktop, or even laptop computers, but are using handheld mobile devices such as smartphones and PDAs. Also consider devices such as bar-code readers, environmental sensors, VoIP phones, and medical monitors.
- Look for sources of interference: Are microwave ovens in use? Are wireless telephones or video surveillance systems operating in the 2.4-GHz spectrum? Is there a nearby radar installation? Use a spectrum analyzer to help pinpoint sources of radio interference that may harm wireless transmission.
- Check the blueprints: With blueprints, you can see the location of elevators, load-bearing walls, and other building characteristics that may impact signal quality. Different materials, such as concrete walls, brick walls, cubicle walls, glass, and elevator shafts all affect signal quality differently.

Site surveys

A site survey is often recommended before installing a wireless network. This consists primarily of walking around with a site survey tool to measure the radio frequency (RF) coverage of a test access point or an existing wireless network. Whether or not you decide to do a site survey before installing a new wireless mesh network will probably depend on the cost of the survey and the complexity of the environment. You may not need a site survey at all—a wireless mesh network is more forgiving than a traditional wireless network because intelligent access points automatically adjust their channels and radio power levels to compensate for coverage gaps and interference. Additionally, because access points don't need to be connected to a wired network, you can quickly add one now to increase coverage and connect it to the wired network later if it seems to work in that location.

- Predeployment Survey: A site survey before deployment can find the best locations for the intelligent access points. Typically, access points are placed in different locations for testing and adjusted as necessary. After they're are permanently installed, another survey is performed to confirm that wireless performance is adequate. Although this is the most reliable way to deploy a wireless network, it can be expensive, time consuming, and impractical across many sites.
- Deploy and Check: An alternative to the predeployment survey is to make an educated guess about the best locations for access points, install them, then do a site survey to verify coverage and check for interference. This saves the cost of one survey and is a quicker way to get a network up and running.
- Deploy without Survey: For simple sites, especially if the installation is small, wireless coverage is fairly predictable. It can be perfectly feasible to install access points and never do a site survey. If you have many locations with the same approximate structure, you can use the same installation plan for every site based on a site survey done on the first site. In remote locations, it may be more cost effective to install more intelligent access points rather than send someone to do a site survey.

Budgeting a wireless network

The hardware cost of a wireless mesh network is driven by the number of access points needed. Although a site survey is the most accurate way to estimate this, there also simple guidelines that can help you estimate how many access points you'll need.

- Access points per square foot: The usual way of budgeting access points is per square foot, based on the square footage of a building. One access point for every 4000 to 5000 square feet is standard for office space with cubicles. If your network is expected to support voice as well as data, increase this to one access point per 3000 or even 2000 square feet. In very lightweight networks, you can get away with as little as one access point per 10,000 to 15,000 square feet, provided the network supports low client densities and you're willing to put up with a few dead spots.
- Number of clients per access point: Another way to determine the number of access points needed by the number of wireless clients supported by the network. Even though the makers of access points often claim they support up to 120 clients, typical deployments support from 5 to 15 clients per access point. Remember that clients include not just computers, but also mobile devices and VoIP phones.
- Distance between access point: 30 to 100 feet between access points is standard, depending on whether the area covered has many walls or includes open space.

A wireless mesh network is more than just the access points. Remember to account for the cost of CAT5 cable and power provisioning. If the access points are powered by power over Ethernet (PoE), you will require PoE switches. Labor costs can also be significant, especially if you're paying for a site survey or for installation in non-standard environments such as factory floors. Plus, all but the simplest wireless mesh networks benefit from central management, so you should include the price of a management appliance or cloud-based management.

Wireless mesh bandwidth

Although you often hear about how much coverage an access point provides, capacity rather than coverage is the limiting factor in an enterprise environment. The real challenge is not how far the signal reaches, but how to deliver enough bandwidth to meet user demands. It's important to document the applications that use the wireless network so that you know how much bandwidth is needed.

To increase capacity for more bandwidth, add more access points and either turn down their radio power to avoid interference or rely on the inherent intelligence of intelligent access points to compensate for other access points. If you plan for sufficient capacity, complete coverage will follow automatically.

Standard wireless densities for office deployment

Requirements	Expected data rate with 802.11g clients	Expected data rate with 802.11n clients 20 MHz	40 MHz	Access point (AP) density
Light coverage	12 to 24 Mbps	39 Mbps	81 Mbps	(1) AP per 8000 square feet
Standard office deployment	36 Mbps	104 Mbps	216 Mbps	(1) AP per 5000 square feet
Standard office deployment with voice	54 Mbps	130 to 144 Mbps	270 to 300 Mbps	(1) AP per 2000–3000 square feet

Operating and managing a wireless mesh network

A successful wireless mesh network involves more than just installing intelligent access points. After the network is deployed, you also need to optimize, troubleshoot, and manage it.

The network's environment can change when your building's structure changes, when users change how they use the network, or when other wireless networks are installed nearby and cause interference. Because things change, you need to periodically look over the network to see how it's performing. Do a periodic walkthrough to check signal strength and find dead spots. Check to see if access points are overloaded or underused. Most wireless mesh management systems include event-monitoring and debugging tools, including tools that enable you to see how individual access points are being used.

Wireless mesh networks that span large organizations across many sites can be a challenge to manage successfully. Fortunately, there are management systems that enable you to configure and manage all the access points in a system, even if you have thousands distributed across many sites. A good management system enables you to configure, manage, and set global security policies from one central site. It alerts you to faults and alarms, so they can promptly dealt and it has a logging function so you can view the network's history.

A very large wireless mesh network with complex security policies may seam daunting but is easily managed given the right tools and a little organization.

Conclusion

802.11n wireless in a mesh architecture offers a wide range of advantages including:

- **True wireless:** Intelligent access points, although they're more efficient on a wired network, don't require a wired connection, making it easy to quickly place access points where they're needed.
- **Scalable:** Access points are quick to install and automatically join the network. Cloud-based management grows with the wireless mesh network.
- **Efficient:** Traffic in a wireless mesh network is sent directly to its destination by the fastest and most reliable route. Local traffic moves faster because it doesn't need to travel to a central controller.
- **Reliable:** Wireless mesh is self healing—If an intelligent access point goes out, other access points take over. If an access point's signal is temporarily blocked by a large object—for instance, by a forklift—the network compensates. If wireless mesh loses its connection to its management system, it continues to operate.
- **Self configuring:** Wireless mesh automatically incorporates new nodes into the network without help from an administrator.
- **Manageable:** Most wireless mesh systems can be centrally managed, even if the network consists of wireless mesh clusters spanning the globe.
- **Easy roaming:** For devices such as smartphones, which may travel through the range of several access points, mesh provides smooth handoffs from access point to access point for a seamless user experience.
- **Cost effective:** The availability of cloud-based management enables wireless mesh networks to add access points as needed without the expense of a central controller.

Today's wireless mesh, which combines the speed and range of 802.11n wireless transmission with an intelligent mesh architecture, is not only efficient enough to act as a replacement for traditional wired networks, it's also a far more cost-effective than controller-based wireless solutions. This is the future of wireless networking, available for your network today.

About Black Box

Black Box is a leading technology product solutions provider that helps customers build, manage, optimize, and secure their networks. The company is a single source for cabling, cabinets and racks, data comm, digital signage, infrastructure, KVM switching, networking, security, wireless, and more. The Black Box catalog and Web site offer an extensive range of products including SmartPath™ Enterprise Wireless. More information is available at http://www.blackbox.com/go/SmartPath.

Black Box is ISO 9001 certified and has received numerous industry recognitions, including the following awards: Info Security Products Global Excellence, CRN Tech Innovator, TMC Communications Solutions Product of the Year, Network Products Guide Reader Trust, Network Products Guide Product Innovation, Five Star ratings from SC Magazine, and a Cabling Business Magazine Award of Excellence. Black Box provides its customers with free, 24/7 pre- and post-sales technical support.