BLACK BOX
NETWORK SERVICES

Whitepaper Wireless Networking

Wireless Standards, Installations, Security and More!

About Black Box

Black Box (NASDAQ: BBOX) is one of the world's largest technical services company with a focus on design, installation, and maintenance of todays network infrastructure systems. From data communication and telecommunication services to on-site network installations, the company supports more than 175,000 clients in 141 countries with 194 regional offices. With "Free Tech Support" for free and competent technical advice over the phone, free test scenarios, as well as installation and maintenance services, Black Box offers an exceptional service program.

The Black Box Catalog and webstore comprise more than 12,000 products, including wireless routers and access points as well as industrial wireless solutions. The SmartPath System, for example, allows highly scalable, cost-efficient WLANs to be built in accordance with the fast 802.11n standard. Go to http://www.blackbox.eu/SmartPath for additional information.

Black Box also offers WLAN antennas, Ethernet switches, and media converters, as well as cabinets, racks, cables, connectors, and other video, audio, and data infrastructure products. The extensive range of products can be found on our website at www.blackbox.eu

Table of Contents

1.0 Introduction

A rather uncommon technology more than 10 years ago, wireless devices dominate all forms of communication systems today. Progress towards better and faster devices and standards is stunning at times, and it's easy to lose one's overview with the many wireless standards around. Black Box would like to shed light on the various standards and backgrounds here.

2.0 Wireless Standards

Not every wireless standard is indeed a standard. A standard can be recognized by its IEEE ratification. Everything else such as "Turbo" or "Super-G" sound like a standard, but are not and thus sometimes only compatible with themselves.

The IEEE 802.11 wireless Ethernet standards are developed by the Institute of Electrical and Electronics Engineers, Inc. (IEEE). This organization only sets the requirements for the standards, verifying a specific wireless product's compliance with these standards is not its responsibility. IEEE 802.11 standards are true Ethernet standards, they behave like an Ethernet in their application.

Today, WLAN is an everyday name like any other. As such, it nowadays describes the type of application rather than a device or a standard. Users are thus all the more surprised when they realize that all WLAN is not the same. A device for wireless communication compliant with the 802.11 standards can be certified by the Wi-Fi Alliance. This organization sees to the adherence to IEEE wireless standards and the interoperability of WLAN products. All WLAN products conform to IEEE standards, but not all IEEE wireless products are necessarily Wi-Fi certified.

There are a few other wireless standards, such as ZigBee, which are not IEEE Ethernet standards. They are normally used for special applications.

2.1 IEEE Standards

2.1.1 IEEE 802.11 — The First Wireless Ethernet

IEEE 802.11, the predecessor of the 802.11b, was introduced in 1997. It was a beginning, but the standard had serious flaws. 802.11 supports speeds of two Mbps maximum. The standard supports two completely different methods of modulation: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). This lead to confusions and incompatibilities between devices. There were also problems in dealing with collisions and with signals reflected back from surfaces and walls. These flaws were addressed quickly, and the succeeding IEE 802.11b Ethernet Standard was released in 1999.

2.1.2 IEEE 802.11b

The 802.11b extension of the original 802.11 standard increased the WLAN throughput from 2 Mbps to up to 11 Mbps. Under ideal conditions (clear view, no interference or disturbance), 802.11b transmissions can have a range of several hundred meters. That was and is readily advertised, but the presence of obstacles and walls or other wireless devices reduce the range considerably.

The 802.11b upgrade established DSSS as the standard modulation method. DSSS has proven to be more advantageous than FHSS and confining oneself to one modulation technique solved the problem of incompatibility between products. 802.11b devices are compatible with older 802.11 DSSS devices, but not with 802.11 FHSS devices.

In the beginning (around the turn of the millenium), 802.11 FHSS devices were initially approved for use in hospitals. Since laptops with modern wireless network interfaces cannot communicate with them, their incompatibility provides additional security where they are still in use today.

The modulation technique (DSSS/FHSS) determines which sequence the frequencies (channels) of the respective frequency band (802.11 and 802.11b 2.4 GHz) are used for the transmission.

IEEE 802.11b offers up to 11 Mbps and thus net data rates of up to 5 Mbps. It is thus still faster than most Internet connections, but has almost entirely been replaced by newer and faster wireless standards.

2.1.3 IEEE 802.11a

In the beginning, 802.11a was primarily used in the USA, since there it was the 5 GHz and not the 2.4 GHz frequency band that could be used without a license by the general public. 802.11a operates in the 5 GHz band and allows speeds of up to 108 Mbps (65 Mbps net). The 5 GHz frequency band was opened much later in part for Europe per general allocation. The higher frequency allowed higher ranges and faster modulation, but is more sensitive to walls and other "obstacles". The 802.11a standard is still popular today for building-to-building connections of up to 10 kilometers distance.

2.1.4 IEEE 802.11g

802.11g is also an extension of the 802.11b standard and operates in the same 2.4 GHz band as 802.11b. It achieves data rates of up to 54 Mbps using the Orthogonal Frequency-Division Multiplexing (OFDM) technology. Since 802.11g is backward compatible to 802.11b, an 802.11b device can work directly with an 802.11g access point. Unfortunately, most access points cannot perform true dual operation. An 802.11b device will therefore slow down other users (possibly faster 802.11g users) as well.

2.1.5 IEEE 802.11e

This standard defines Quality of Service (QoS) mechanisms for wireless transmissions. QoS makes bandwidth-intensive applications such as voice and video possible.

2.1.6 IEEE 802.11n

802.11n is the latest addition to the standard family, it was only ratified in the year 2009. You can still find a lot of quasi-N or pre-N devices on auction platforms and in classified ads. These operate more or less in accordance with the 802.11n standard, but not exactly. Today, 802.11n operates on the 2.4 and the 5 GHz band. The data throughput has increased to up to 300 Mbps. The net rates differ considerably between 802.11n at 2.4 and 5 GHz. More important, however, are the conditions.

802.11n transmits several data streams simultaneously, several channels are thus used simultaneously as well. For 802.11n at 2.4 GHz the entire frequency band is used. Although the capacity increases, throughput is even faster affected by other users of the frequency band.

2.1.7 IEEE 802.11i

Before standard 802.11i, encryption using WEP was state of the art. Different key lengths safeguarded the transmission. However, they were always statistical algorithms and comparatively easy to crack.

With 802.11i, more dynamic algorithms have entered the scene. This standard defines the encryption technique TKIP (Temporal Key Integrity Protocol) and CCMP (CTR with CBC-MAC Protocol) on the one hand, but also the logic for key exchange and definition, WPA and WPA2.

Today, the techniques in practice are such that a random key (usually a term or the like, then PSK, Pre Shared Key) serves to generate and to negotiate with the counterpart a temporary key at certain intervals with the help of MAC address, date, and time, which is then only valid temporarily for the respective communication.

Not all wireless LAN devices support all techniques, which can lead to incompatibilities. Some terms (PSK) can cause complications, too. And although WEP (apart from an unencrypted WLAN) is the least safe technique, it is the lowest common denominator. Besides, the use of WPA/WPA2 leads to a less favourable net/gross throughput ratio.

2.1.8 IEEE 802.15

This specification describes how information is transferred over short distances in a wireless network (WPAN, Wireless Personal Area Network). This type of network usually consists of a small group network with few members and shorter distances. Bluetooth and infrared, for example, are transmission technologies which are part of the 802.15 standard.

2.1.9 IEEE 802.16

IEEE 802.16 was ratified in January 2001 and is better known as WiMax. It enables a single base station to support many fixed line and mobile users. Also termed the Metropolitan Area Network (MAN) standard, 802.16 aims to make wireless LAN and its bandwidth potential available for mobile devices in city areas. However, since the introduction and implementation of 3G/4G/UMTS, the future of these ideas is doubtful.

2.1.10 IEEE 802.16e

Based on the 802.16a, this standard specifies the mobile wireless interfaces for wireless broadband communication in the licensed frequency bands from 2 to 6 GHz.

2.1.11 IEEE 802.20

A proposed specification for a wireless standard for IP-based services. This standard will probably operate on licensed frequency bands below 3.5 GHz and be used for wireless broadband networks.

2.1.12 IEEE 802.11x

This term refers to future wireless 802.11 standards - 802.11f to 802.11m. This term is sometimes also used as a reference to all the existing WLAN standards 802.11a/b/g/n. Attention: 802.11x is not to be confused with the security standard 802.1x.

2.1.13 IEEE 802.1x

With 802.1x, the highest possible (according to many experts) data security in networks can be achieved, irrespective of whether they are wireless or not. Standard 802.1x defines methods regarding authorization and login of a user in a network. The keyword RADIUS is certainly well-known in this context. A RADIUS server is usually a network service (implementable on Windows servers, but also integrated in Smartpath) with a database containing information on which user and with which password is authorized to access which resource, when, from which device, and from which location. This security technique is interesting for companies as fine-tuned security settings can be defined. While WEP and WPA can be implemented fairly easily and fast between the WLAN AP (access point) and the terminal device (PC), 802.1x is more of a concept that may require an entire infrastructure to match.

2.2 Non IEEE-Standards

2.2.1 Super G

Describes a subsection of 802.11g. It is a proprietary extension of the 802.11g standard and doubles the throughput to 108 Mbps. Super G is not an approved IEEE standard. If you want to use it, you should use devices from the same manufacturer to ensure compatibility. Super G is usually downward compatible to 802.11g.

2.2.2 XR-Technologie

Extended Range (XR) Technology is a wireless signal processing technique developed by Atheros Communications for a twofold or even threefold increase (under ideal conditions and especially outdoors with a clear view) of the range of wireless 802.11 networks. In addition, it is to reduce or remove “dead points” in a network.

2.3 Other Transmission Techniques

2.3.1 Laser/FSO

Laser links or FSO (Free Space Optics) offer wireless connections at the same speed as optical fibre cables. Simply put, it's a light transmission as with optical fibre, but without cable and fibre. The wavelength is different from the usual FOC/optical fibre topologies.

Clear view provided, lasers are a good solution for a broadband connection of two buildings or networks. While for WLAN in accordance with 802.11a/b/g/n the net and gross bandwidth diverges, FSO/lasers provide the full bandwidth net.

Lasers devices are available for Ethernet 100 Mbps and Ethernet 1 Gbps. Earlier devices were fully transparent up to 155 Mbps and also permitted ATM or FDDI transits. Compared to early lasers, stability and availability have been improved. Modern lasers impress with features such as heated lenses, autofocus and auto-tracking.

Autofocus in this case is an automatic focus adjustment. Older devices usually had a limited lifespan because the photodiode burned out. The photodiode (the optical receiver) burned out in cases where too much light energy hit it for an extended period of time. This could be caused by direct sunlight (or reflection) on the one hand, or because of a discrepancy between actual and native distance on the other. The latter was the case when, for example, a 500 meter laser was operated over a few meters only.

Auto-tracking allows the entire laser head to move by itself using servo motors. The laser can thus "follow" the light and readjust itself.

Installation and planning decide on the success and the sustainability of a FSO/laser link. Laser devices have to be mounted rock-solid. Avoid east-west links because of the adverse effect of sunlight. Check if there's a clear view between both laser heads at all seasons and situations. Take into consideration that trees grow and that vehicles larger than cars occasionally use roads. Avoid installing laser heads near aircon or heating systems. Anything emitting hot or cold air causes turbulences. Expect soil movement especially in coastal areas. In general, lasers should be readjusted every 12 to 24 months.

2.3.2 60/70 GHz

60 and 70 GHz are new frequencies already in use in some EU countries. Especially 60 GHz has been released by an EU directive for general allocation.

60 and 70 GHz systems allow up to 800 Mbps data throughput while being comparatively immune to weather. Thus these technologies offer an additional, although rather expensive, alternative.

2.3.3 ZigBee Wireless Control

The ZigBee technology was developed for industrial environments that require highly reliable low-speed wireless connections for simple control systems and measurements. Use ZigBee in cost-efficient, fault-tolerant networks with extremely low power consumption. ZigBee is ideal for communication systems between devices such as industrial control systems, fire alarms, and thermostats. A wireless ZigBee device remains in sleep mode most of the time. It only sends a short burst of information either according to a schedule or when set.

2.3.4 Proprietary Wireless

Individual providers can use their own proprietary wireless systems for special applications. 900 MHz proprietary wireless is often used in the industrial sector. Microwave radio relays in the range of around 30 GHz are also fairly widespread. Observe the licenses of the respective national regulators.

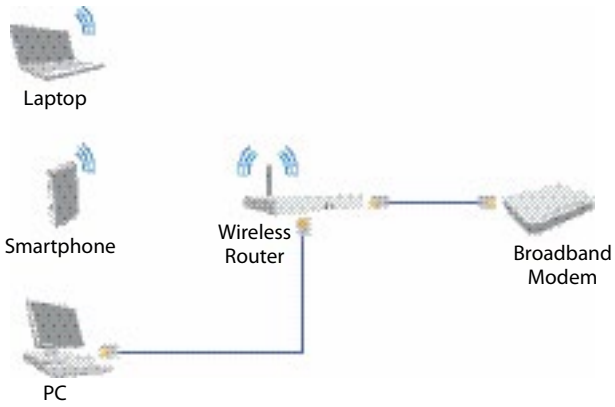
3.0 Wireless in Accordance with 802.11a/b/g/n in Practice

Before planning, installing, and operating a wireless network in practice, you first have to determine the infrastructure type. The type is first and foremost determined by the purpose of the network. If you use your WLAN to provide Internet access for mobile devices, other things need to be considered if you want a wireless connection of two networks.

3.1 Wireless LAN As Infrastructure

Wireless LAN as infrastructure is the attempt to provide network access for mobile devices. It even becomes imperative today, since devices such as the iPad don't even have a normal RJ45 port any more. But WLAN in accordance with 802.11b/g/n is also convenient for notebooks and smartphones.

Wireless network in infrastructure mode: basic service set



The importance of WLAN goes beyond its practical usefulness with the spread of Voice over IP (VoIP) in companies. While WLAN first and foremost serves to provide Internet access for iPads, notebooks, and other mobile devices, it serves as an internal network service for IP telephony (VoIP)..

3.1.1 Planning WLAN As an Infrastructure Service

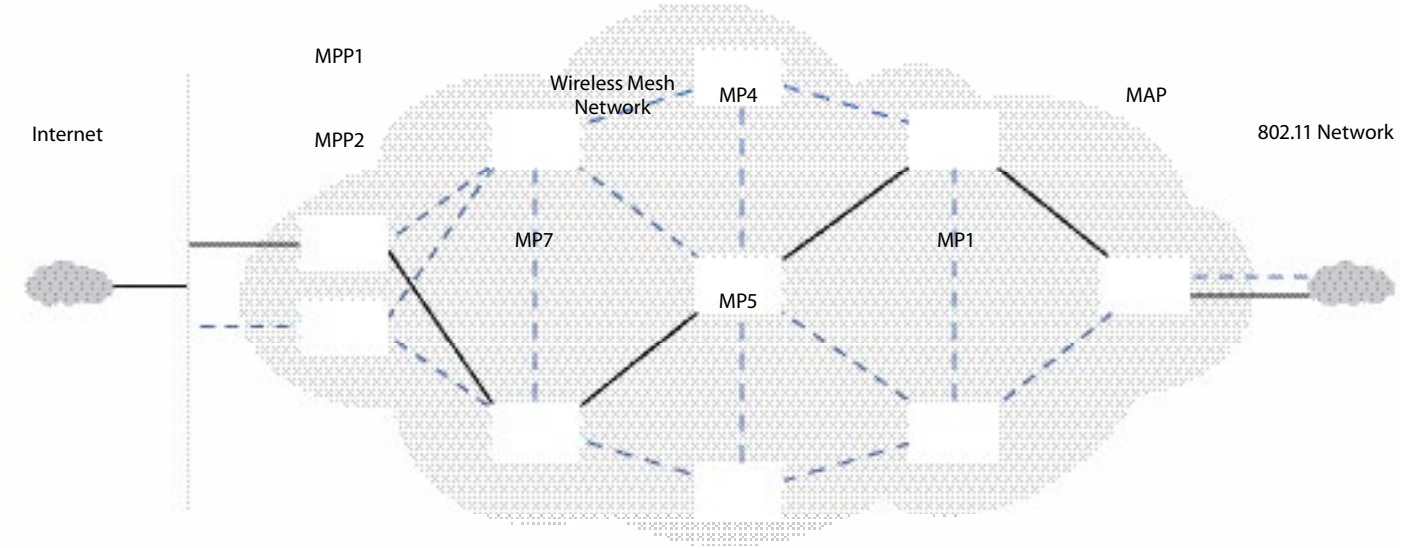
It needs to be ascertained clearly during the planning phase where the priority lies. If the priority lies in the WLAN providing an internal data service for VoIP - latency, bandwidth, and roaming ability are important.

Roaming ability is the change from one radio cell to another. This change should be as free from interruption as possible. Especially services such as VoIP or RDP (Terminal Services), for example, are sensitive to short interruptions. The better the radio cells are distributed (channel setup) and the better the access points support roaming (the process of prior authorization at the new AP and subsequent radio cell change), the better roaming works and thus VoIP over your WLAN.

It is also advisable to survey a building that is to be supplied with WLAN beforehand to determine the most suitable positions for access points. Positions of access points need to be such that power and a wired network connection are available there. Special attention should be paid to ensure that WLAN access with adequate cover is possible from anywhere in the building. A thorough site survey by an expert is recommended.

If the priority of a WLAN is to provide Internet access, bandwidth and latency are not that crucial. 802.11b or g are sufficient in that case. Take into consideration that the Internet connection (DSL, cable or the like) limit the possibilities with regards to bandwidth.

Selecting the right encryption method is also important. Not all mobile devices support all encryption techniques. If mobile devices are to access the Internet over your WLAN, it may even make sense to work without encryption. However, in that case you need to consider how to isolate users from each other in your WLAN.



Especially in public networks, the so-called “Hotspots”, this issue is of great importance. All users of a hotspot want to access the Internet, but don’t want to exchange data with each other. Client Isolation, controlled at the access point using the MAC address, ensures the privacy of the hotspot users. These days, special safety measures need to be implemented for Apple users as well. Apple systems bypass many of the safety mechanisms such as “Client Isolation“.

If your WLAN should do both, i.e. provide Internet access and VoIP, access points with VLAN and Multi SSID functions are suitable. That way you generate parallel WLAN networks in one infrastructure. Moreover, you can limit bandwidth, or split the network into an unencrypted segment and one using WPA and/or RADIUS/802.1x

3.1.2 Installing WLAN As an Infrastructure Service

Proper documentation is crucial. Record where the APs are installed, their IP address, and where and how they are connected. There have been various cases where Black Box technicians have spent days searching for APs and other devices due to incomplete or lacking documentation. Avoid such unnecessary downtime and costs by documenting all devices and installation processes, including subsequent changes.

3.1.3 Operating WLAN As an Infrastructure Service

You have to monitor your access points. Once they are in operation, who and how they are online becomes of interest to you. Protective measures need to be taken as well to prevent unauthorized additional access points from being taken brought into operation. Additional APs can pose a security risk. Although Internet access may be possible, hackers could also intercept information there. It also needs to be taken into consideration that with any additional unplanned APs, initial plans with regards to radio coverage may become obsolete.

Network access control functions (NAC), SNMP and other tools can send you mails or alert messages on changes in the infrastructure and prevent unplanned devices or unscheduled users in your WLAN.

3.2 Wireless LAN As a Building-To-Building Connection

When wireless LAN is used as a building-to-building connection, attention shifts to entirely different things. Now radio equipment is used externally, not internally. Natural security barriers don't apply any more. You "broadcast" over external and public ground and all the neighbour has to do now is sit on the balcony to intercept the signals. Thus your priorities in this case are security, sustainability and availability. With regards to security, use the best possible encryption method. Anything less than WPA2 should not be considered.

It can be assumed that the connection should be sustainable and functional in almost any situation. A long-term test is thus necessary to check whether this can be achieved over the planned link. For this purpose, the frequencies 5 GHz and 60 and 70 GHz offer alternatives. They are less prone to interference than 2.4 GHz in this case. Besides WLAN, DECT and Bluetooth also operate at 2.4 GHz. The less disturbance you have while transmitting on the planned frequencies, the better your chances of a sustainable radio link.

You should aim for a clear view between radio transmitters and receivers. Although 5 GHz signals can travel through trees and bushes, each obstacle in the path will weaken your signal further. Check what is in between the two radio transmitters, whether it can grow or be modified.

Not only the direct line of sight needs to be kept clear, but also the so-called Fresnel zone. Depending on range and frequency, this zone extends a few meters above and below, to the left and the right of the direct line of sight. Radio waves don't travel in an entirely straight line. Anything inside the Fresnel zone will weaken your radio signal further.

Usually, a 5GHz system in accordance with 802.11a or 802.11n is chosen for building-to-building links. If that's the case, check the distance to the nearest military installation or airport. Radar systems use the same or neighboring frequencies. According to EU legislation, WLAN systems have to shut down once a radar facility is detected. It is also important to know that 5 GHz systems are subject to a forced disconnect every 24 hours induced by the system and frequency selection. Depending on your system, this can be set at a time of your choice. This is usually done at night, your server backups or SQL transactions should not be scheduled during that time, though.

WLAN building-to-building links are also suitable as backup connections for FSO/laser links. Preceded by the corresponding RSTP (Rapid Spanning Tree Protocol) switch, it's an ideal combination to improve the sustainability of the FSO/laser link.

Users can get the idea of switching several radio links in parallel to increase bandwidth. Suffice it to mention that depending on frequency and environment, this would only work to a limited extent or not at all (see point 7.5).

Naturally, such radio links should be in accordance with the national regulations of the respective regulator.

Wireless network in infrastructure mode: basic service set

Building mit Outdoor
Mesh Access Point
(MAP)

Building mit Outdoor
Mesh Access Point
(MAP)

4.0 Power Supply

WLAN access points are available with their power supplied via small plug-in units or PoE. For PoE (Power over Ethernet), the network cable provides both Ethernet connectivity and power for the AP.

WLAN devices with PoE are usually the more professional devices. The difficulty of how to change a power supply or perform a reset at a later date need to be taken into consideration if the AP is built into the suspended ceiling. In this case, PoE is the ideal option as it allows your network switch to monitor everything fast and easily.

5.0 Consumer Device, Industrial Device, or Outdoor Device

You should firmly distinguish between a consumer device, an industrial device, and an outdoor device. Although consumer devices are cheap, they are not suitable for all environmental conditions. Industrial devices can tolerate higher temperatures, but are not suitable for outdoor use without weatherproof housing. In contrast, outdoor devices are suitable for the environmental conditions and weather conditions in outdoor use.

6.0 Antennas and Antenna Cables

FFor the performance of your wireless network, antennas and antenna cables are among the most crucial components. You should certainly not cut costs here. Besides, antenna cables shouldn't be too long. The signal attenuation in the antenna cable minimizes your range. You shouldn't use antenna cables longer than eight meters if at all avoidable.

Antennas are generally divided into omnidirectional and directional antennas. Additional (technical) terms are in circulation for both categories, however, the two terms mentioned here already describe their function best. Use directional antennas for building-to-building connections, and omnidirectional antennas preferably for infrastructure services.

It is a popular misconception that directional antennas that transmit into different directions can be connected to a single access point with two or three antenna connections (Diversity, MIMO).

7.0 Other Technical Terms and Issues of Importance

7.1 Diversity

Radio waves are reflected by the walls in closed rooms. Radio waves emitted by the transmitter thus reach the receiver on different paths. Diversity is used to determine the best direct path or reflected path based on the two antennas.

7.2 Country Settings

When installing an access point, the respective country where the device is to be operated is set first. Receivers (notebooks, etc) should be set accordingly.

Depending on the country, different frequencies and channels with varying radiated power outputs are approved. For 802.11b/g, only channels 1 to 11 are (officially) approved in the USA for example, in Europe, however, it's channels 1 to 13 (Switzerland excluded).

Differences in the 5 GHz spectrum vary even more from country to country. Operating your radio devices against country regulations can potentially cause you slight to major difficulties!

7.3 MAC Filters

Every network device can be uniquely identified by its so-called MAC address. Although there are ways and means to bypass this uniqueness with methods of a hacker, "MAC Filters" add additional security to your WLAN in general.

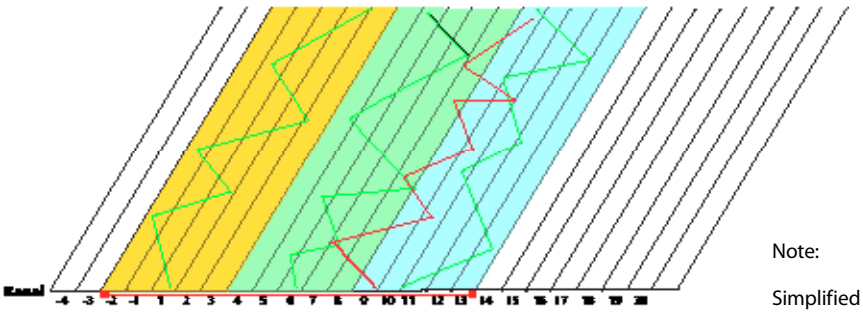
7.4 Shared Medium

Wireless LAN is a shared medium. Radio waves are available only once (limited to one radio cell or channel) and are used simultaneously or in parallel by the participants. That means that if your wireless LAN offers a bandwidth x and y participants use it, each participant will only have x/y of this bandwidth available.

7.5 Channels

For 802.11b/g, 11 channels are available in Europe. Based on frequency modulation, they cannot be used in parallel without overlap. The actual transmission in a WLAN set to channel 6 is between channels 4 to 8. Another WLAN set to channel 7 will operate between channels 5 to 9. Channels 5 to 8 will thus be used by both WLANs so that the APs' potential cannot be fully utilized. The net bandwidth of either WLAN is thus lower than possible. Only channels 1, 6 and 11 don't overlap and thus offer the best performance.

802.11b/g frequency modulation in the 2.46 GHz band



WLAN 1 (Green)

WLAN 2 (Green)

WLAN 3 (Green)

WLAN 4 (Red) overlapping frequency band

Note:

Simplified example illustration. Channel hopping not according to the actual algorithm.

8.0 Conclusion

Planning your wireless network in advance can save problems later on. Black Box recommends that you start with listing and evaluating all your requirements for the WLAN. According to that list you then decide on the corresponding network type:

List the following criteria:

• What are the security requirements?

• What are the bandwidth requirements?

• Are there any environmental conditions that may affect the radio transmission?

• How can the installation be carried out most conveniently?

• How many network user are there?

• How many laptops and similar devices require wireless access?

• How many smartphones require access?

Wireless technology has already come a long way since its inception and is still developing further. It is common practice today to equip networks with a considerable number of wireless devices. Through progress in wireless technology, wireless connections are indeed able to compete with cable-based transmissions with regards to performance and security.

Whether you want to build or extend a large or a small network, or consider a cable-based, wireless, or integrated network, Black Box has a solution for you! We provide the right products and offer technical service for planning, design, installation, and maintenance of the network, all tailored to your requirements today and tomorrow.

BLACK BOX
NETWORK SERVICES

Data

Conception, Installation, Products & Maintenance for Cable, Wireless, and Hybrid Systems

Voice

Conception, Installation, Products & Maintenance for IP Telephone and Private Branch Exchanges

Technology Product Solutions

Direct sales of more than 12,000 IT Product Solutions with Free Telephone Support

October 2011

Why Black Box

» **Comprehensive service and product portfolio**

12,000 product solutions and expert service provider with global e

» **FREE TECH SUPPORT**

Free technical advice without phone queues or contract

» **Test scenarios**

Free testing of our catalog products in your application