Industrial Wireless Guidebook

MOXA®

Reliable Networks ▲ Sincere Service

Table of Contents

Wireless Landscape

1-1 Overview

Introduction

Wireless technologies have become increasingly popular in industrial automation as growing numbers of system integrators, government agencies, and industrial operators continue to turn to wireless solutions for their applications. Wireless networks can be quickly deployed to transmit data to areas without existing cable infrastructures. For hard-to-wire locations and worksite landscapes that constantly change, wireless technologies are ideal for providing highly flexible and efficient network connectivity. In addition to mobile versatility, wireless technologies can offer real-time communication for mission-critical applications, high bandwidth for video transmission, and a low total cost of ownership.

However, since wireless communications rely solely on the emission of electromagnetic waves to transmit data, network security is an important factor for administrators to consider. Another major concern is electromagnetic interference (EMI), which can disrupt data transmission, severely reduce data throughput, and compromise network reliability. With over 25 years of industrial automation experience, Moxa offers secure and reliable industrial wireless solutions, such as cellular, and Wi-Fi, for mission-critical applications that demand dependable and uninterrupted system operation.

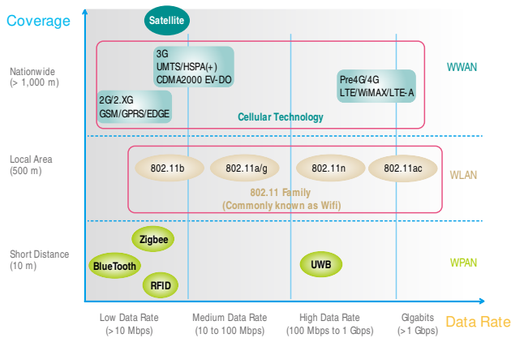
We hope this guidebook will provide you with a more comprehensive understanding of industrial wireless technologies and serve as your most trusted guide to getting un-wired.

It's time to go wireless!

Technology Map

Since the invention of radio transmission, many types of wireless technologies and standards have been developed to meet the requirements of various wireless applications. For the development of every wireless standard, two major variables were considered: coverage area (distance) and data rate (bandwidth).

Wireless technologies can be divided into three categories: WWAN, WLAN, and WPAN.



Technology Selection

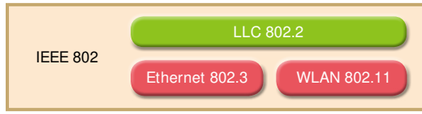
	WWAN (Wireless Wide Area Network)	WLAN (Wireless Local Area Network)	WPAN (Wireless Personal Area Network)
Characteristics	➤ Wide area coverage ➤ Long distance communication ➤ High transmission latency ➤ Medium transmission bandwidth ➤ On-going data transmission cost ➤ Base station restriction	➤ Local area coverage ➤ Long/medium distance communication ➤ Low transmission latency ➤ High transmission bandwidth ➤ Initial AP setup cost	➤ Small area coverage ➤ Short distance communication ➤ Low transmission latency ➤ Low transmission bandwidth ➤ Low power consumption
Applications	➤ Highway signaling control system ➤ Remote monitoring system ➤ Nationwide environmental monitoring	➤ Train to ground communication for mission critical data ➤ High throughput for video to ground transmission ➤ Automated material handling	➤ Street light control ➤ Personnel tracking ➤ Short distance data acquisition

1-2 WLAN Basics

IEEE 802 Standards in the OSI Reference Model

IEEE 802 specifications are only addressed for layer 1 (physical) and layer 2 (data link) of the Open Systems Interconnection (OSI) reference model by the International Organization for Standardization (ISO). The data link layer is composed of 2 sub-layers: Media Access Control (MAC) and Logical Link Control (LLC). The LLC sub-layer manages error/flow control and is essentially the same for all IEEE 802 standards. The MAC sub-layer is for physical addressing and manages media access control. IEEE 802.3 specifications refer to access for Ethernet and IEEE 802.11 specifications refer to access for wireless LANs.

OSI Model	
Layer	Functions
(7) Application	User application interaction Process-to-process communication
(6) Presentation	Data transformation/reformatting Data compression/encryption
(5) Session	Establish communication between end systems Manage user connections
(4) Transport	Error detection/recovery Network connection flow control
(3) Network	Manage network path connections Data routing/relay
(2) Data Link	Access/error/flow control MAC addressing
(1) Physical	Controls raw bit-stream transmission Electrical signaling



History of WLAN Standards

For WLAN applications, the IEEE first published the 802.11 standard in 1997. Three MAC sub-layers and three different physical (PHY) layers are addressed for the 802.11 standard. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are two methods of frequency spreading for the 2.4 GHz ISM band that provide data rates of 1 and 2 Mbps.

IEEE 802.11 was not widely accepted for use until the release of 802.11a/b in 1999. IEEE 802.11a uses the 5 GHz band with orthogonal frequency-division multiplexing (OFDM) modulation to provide data rates of up to 54 Mbps. IEEE 802.11b still uses the 2.4 GHz ISM band to provide data rates of up to 11 Mbps using DSSS modulation, which allows integration of other DSSS-based IEEE 802.11 systems. FHSS-based 802.11 systems, however, cannot be integrated.

The most widely-adopted variation of the IEEE 802.11 protocol suite is IEEE 802.11g, which was an improvement upon the existing IEEE 802.11b standard. Using the same 2.4 GHz band, OFDM modulation allows data rates of up to 54 Mbps.

The IEEE 802.11h standard is an amendment of the IEEE 802.11a standard. Transmission Power Control (TPC) and Dynamic Frequency Selection (DFS) are applied at the PHY layer to meet European regulations and allow compatibility with other standards in the 5 GHz band.

The newest specification to the IEEE 802.11 protocol suite is IEEE 802.11ac, which is backwards-compatible with other 802.11n networks using the 5 GHz range. It provides WLAN throughput of greater than 1 Gbps on the 5 GHz band, offers up to 8 MIMO streams with up to 160 MHz bandwidth each, and uses high-density modulation of up to 256 QAM.

The table below illustrates the development history of 802.11 and the differences between the various versions of 802.11 network standards.

802.11 Standards						
Protocol	Released	Frequency (GHz)	Bandwidth (MHz)	Data Rate (Mbps)	MIMO (max.)	Modulation
802.11	1997	2.4	20	1, 2	1	DSSS, FHSS
802.11b	1999	2.4	20	1, 2, 5.5, 11	1	DSSS
802.11a	1999	5	20	6 to 54	1	OFDM
802.11g	2003	2.4	20	6 to 54	1	DSSS, OFDM
802.11n	2009	2.4 & 5	20 40	6.5 to 28.8 13.5 to 600	4	OFDM
802.11ac	2013	5	20 40 80 160	6.5 to 693.6 13.5 to 1600 29.3 to 3466.4 58.5 to 6933.6	8	OFDM

Wireless Security

802.11 networks use radio signal broadcasts to communicate and anyone with a compatible wireless network interface card can access the WLAN. Security measures to verify WLAN access are critical to prevent unauthorized access to network devices and resources.

Two main types of security measures are available for WLANs:

- Authentication: User/device identity is verified before network access is granted.
- Encryption: Data exchanged between WLAN nodes should be encrypted to make intercepted data unreadable.

Various combinations of authentication and encryption methods are commonly used to provide different levels of WLAN security. In addition to three major types of WLAN security (WEP, WPA, and WPA2), the IEEE 802.1X protocol also provides a robust authentication scheme for every single WLAN connection.

WLAN Security Protocols

Security Protocol	Features
WEP (Wired Equivalent Privacy)	RC4 data encryption No user/password authentication
WPA (Wi-Fi Protected Access)	TKIP + 802.1X + MIC Supports RADIUS authentication Backwards compatible with all systems
WPA2	WPA + AES cipher

WEP

Wired Equivalent Privacy (WEP) is a low-level security measure to provide data confidentiality for wireless communication. Static shared keys (fixed-length alphanumeric strings) are used to encrypt data and are manually distributed to all wireless stations on the wireless network.

In 2001, WEP was found to be highly vulnerable to passive attacks that can compromise the 24-bit RC4 encryption key and is not recommended for high-level security networks. For wireless security that is more robust, Wi-Fi Protected Access (WPA or WPA2) offers improved data encryption and user authentication.

WPA

Wi-Fi Protected Access (WPA) was created in response to the flaws found in WEP. It was designed as a temporary measure until developments in 802.11i security measures were ready. When used with RADIUS and VPN authentication methods, WPA is generally acceptable as an effective method of WLAN security.

WPA2

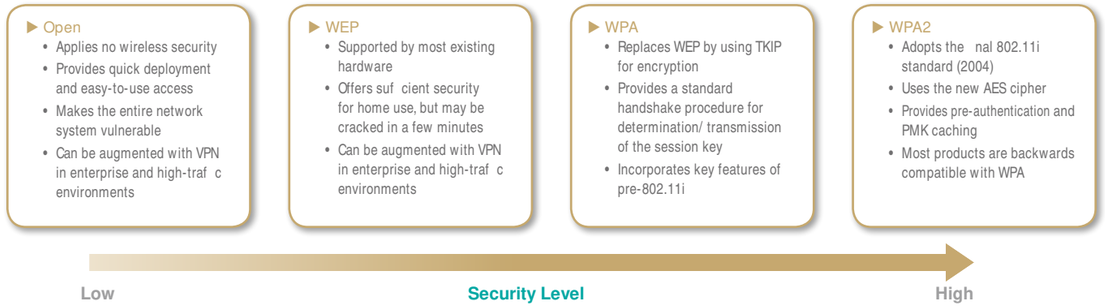
WPA2 is an update to the encryption technology of WPA. WPA uses Temporal Key Integrity Protocol (TKIP) for 128-bit data encryption, while WPA2 uses Advanced Encryption Standard (AES), a substitution-permutation network encryption design that is suitable for WLANs that require highly-secure access control.

802.1X

802.1X is a port-based authentication method that prevents unauthorized access to the network. It is used with WPA to form a complete WLAN security system. On many wireless systems, users can log into individual access points but cannot get further without additional authentication. 802.1X requires users to authenticate with the wireless network itself, not to individual APs or a VPN connection. This provides higher WLAN security, as unauthorized traffic can be denied right at the AP.

Choosing the Right Level of WLAN Security

The right balance between security, transparency, and cost effectiveness is important when determining the type of security to implement on the WLAN. Factors such as the target environment, compatible types of security levels, and the possible impact on network performance when using more sophisticated security methods should all be taken into consideration.



Here are a few key questions for evaluation of WLAN security options:

- Does the environment require high-level security? If the WLAN will transmit information such as medical records, the highest level of security should be applied. However, if the WLAN will only be used to communicate environmental monitoring data, a lower level of security should be applied to optimize WLAN performance.
- What levels of security can the network environment support? WPA and WPA2 encryption technologies provide reliable security, but can the client devices support them? Also, if 802.1X authentication is to be implemented, is a RADIUS server available on the WLAN?
- Will high-level security have an undesirable impact on the performance of the WLAN? How will the performance of wireless devices on the WLAN be affected if encryption is enabled? Encryption/decryption can require significant CPU resources for processing. Can all WLAN devices, including the device servers, handle the additional load for data processing?

The following table summarizes the considerations for implementation and client requirements for WLAN security methods.

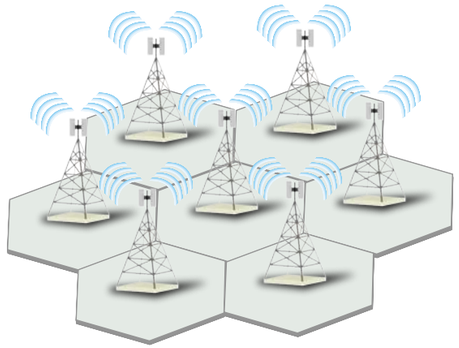
Method	Client Support	Considerations
Open	No special requirement	➤ Can be installed and used quickly ➤ Brings high risk and may damage the network security
WEP	Built-in support for all 802.11a, 802.11b, and 802.11g devices	➤ Provides weak security ➤ Requires manual key management
WPA	Requires WPA-enabled system and network card driver	➤ Provides dynamically generated keys that are periodically refreshed ➤ Provides similar shared key user authentication ➤ Provides robust security for small networks
WPA2	Requires WPA-enabled system and network card driver	➤ Provides robust security for small networks ➤ Requires manual management of pre-shared key ➤ Wireless stations may require hardware upgrade to be WPA2-compliant
802.1X	Requires WPA-enabled system and network card driver	➤ Provides dynamically generated keys that are periodically refreshed ➤ Requires configured RADIUS server ➤ Provides backwards compatibility with the original WPA

1-3 WWAN (Cellular) Basics

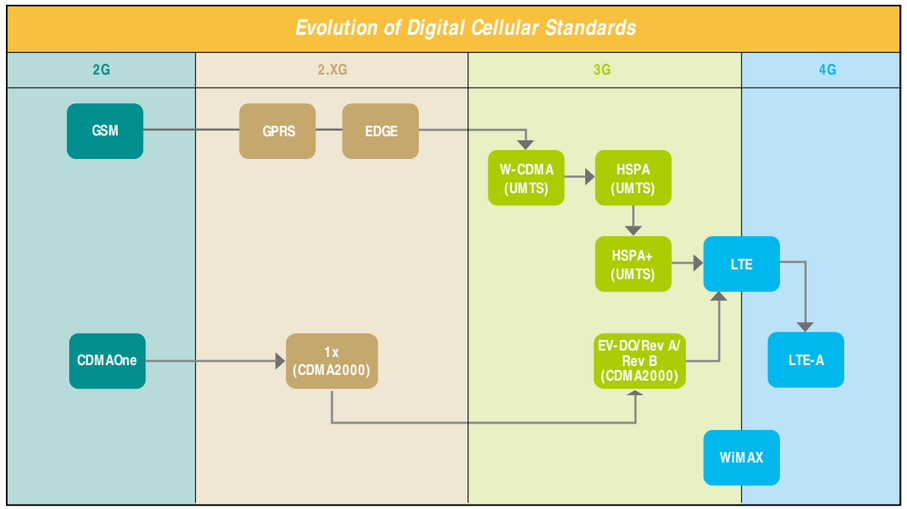
Introduction

A WWAN (wireless wide-area network) can include various types of mobile communication networks, such as traditional microwave transmission, satellite communication, and nowadays cellular network technology. All of these networks offer a wide coverage area and can even be used for global transmission of digital data. In cellular communication, 3G networks served more than 1.5 billion subscribers in 2013 and the number of users is forecasted to increase to 3.5 billion by 2015. However, LTE technology (4G) is showing rapid growth and is expected to replace 3G technology as the leading standard for next generation cellular communication.

Major concerns regarding the use of cellular networks for data exchange include bandwidth, IP management, and high operational cost (such as satellite communication). However, as technologies advance to provide more efficient service, cellular network infrastructures can be deployed at lower costs to potentially replace traditional microwave, RF (radio frequency), and satellite communications.



Evolution of the Cellular Network



2G/2.XG Technology

Circuit-Switched Data for GSM Networks

GSM (Global System for Mobile Communications) is a set of standards for mobile phone communication on 2G digital cellular networks. GSM was developed by the European Telecommunications Standards Institute (ETSI) and became the de facto standard for mobile communication to replace first generation (1G) analog cellular networks. GSM uses circuit-switched data (CSD) for full duplex voice transmission and the technology was expanded over time to introduce data communication— first via circuit-switched transmission, which eventually evolved into packet-switched technologies— and then by GPRS (General Packet Radio Services) and EDGE (Enhanced Data rate for GSM Evolution) for transmitting data via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution).

GPRS

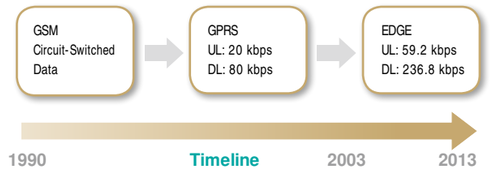
General Packet Radio Service (GPRS) is a packet-switched service for GSM transmission on 2G/2.5G networks to allow simultaneous voice and data transmissions. GPRS can be used for services, including SMS, MMS, email, and internet access. GPRS was first developed by the European Telecommunications Standards Institute, and is now maintained by the 3rd Generation Partnership Project (3GPP).

EDGE

Enhanced Data-rates for GSM Evolution, also known as Enhanced GPRS (EGPRS), IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution, is an extension of GSM. EDGE is a pre-3G digital mobile phone technology that allows higher data rates than GPRS, with transmission rates of up to 384 kbps.

Additional Information

The following figure gives a rough idea of throughput improvement over time with different 2G technologies.



Furthermore, GSM, GPRS, and EDGE operate on four common GSM bands: 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz. However, since different regulations are used in different countries, a common GSM frequency is not used around the world. The accompanying table gives a brief overview of the GSM bands used in a number of countries.

GSM Frequency Band Usage Overview
(Based on major carriers)

Continent	Country	850 MHz	900 MHz	1800 MHz	1900 MHz
America	Brazil	✓	✓	✓	✓
	Canada	✓			✓
	United States	✓			✓
Europe	France		✓	✓	
	Germany		✓	✓	
	United Kingdom		✓	✓	
Africa	South Africa		✓	✓	
Asia	China		✓		
	India		✓	✓	
	Russia		✓	✓	
	Taiwan		✓	✓	
Oceania	Australia		✓	✓	
	New Zealand		✓	✓	

Note 1: For the latest band usage, please contact local carriers.
Note 2: For cellular device compatibility with a particular carrier, please check "Carrier Approval" with your cellular device vendor.

3G Technologies

3GPP— From UMTS to HSPA+

UMTS

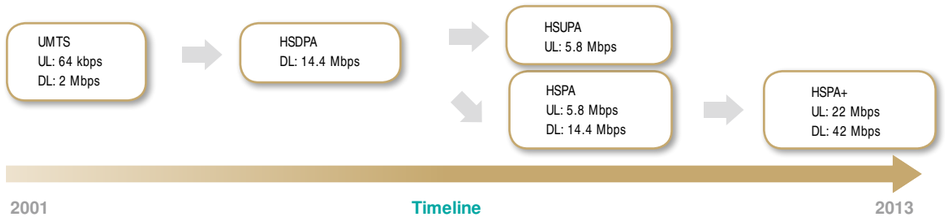
The Universal Mobile Telecommunications System (UMTS) is a GSM-based 3G technology for mobile cellular networks developed by the 3rd Generation Partnership Project (3GPP). UMTS uses Wideband Code Division Multiple Access (W-CDMA) and combines both wireless and satellite cellular technologies to transmit up to 2 Mbps of data to provide greater spectrum efficiency and bandwidth.

HSPA (HSDPA/HSUPA/HSPA+)

High Speed Packet Access (HSPA) is the term for UMTS-based 3G cellular networks that support both HSUPA (High Speed Uplink Packet Access) and HSDPA (High Speed Downlink Packet Access) data to communicate via W-CDMA protocols to provide download rates of up to 14.4 Mbps and upload rates of up to 5.8 Mbps. A newer version, Evolved HSPA (also known as HSPA+), was released in 2008 and is capable of providing data rates of up to 42 Mbps for downloading and 22 Mbps for uploading.

Additional Information

The following figure gives a rough idea of the throughput improvement over time with different 3G-UMTS technologies.



Furthermore, there are 5 commonly used UMTS frequencies: 800, 850, 900, 1900, and 2100. The UMTS frequency usage is different for different operators. The following table gives a rough overview of the UMTS band selection for several major operators around the world.

UMTS Frequency Band Usage Overview (Based on major carriers)

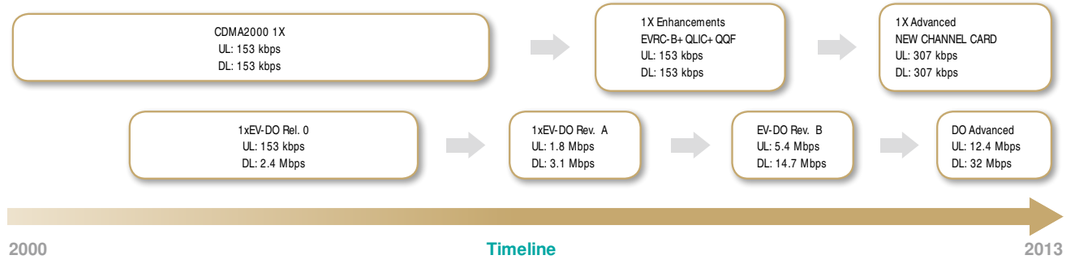
Continent	Country		850 MHz	900 MHz	1700 MHz	1900 MHz	2100 MHz
America	Brazil	TIM BR	✓				✓
		Vivo	✓				✓
	Canada	Bell Mobility	✓			✓	
		Rogers Wireless	✓			✓	
	United States	AT&T Mobility	✓			✓	
		T-Mobile US			✓	✓	
Europe	France	Orange		✓			✓
		SFR		✓			✓
	Germany	O2					✓
		Vodafone					✓
	United Kingdom	T-Mobile					✓
		Vodafone		✓			✓
Africa	South Africa	MTN SA					✓
		Vodacom					✓
Asia	China	China Unicom					✓
	Taiwan	Chunghwa Telecom					✓
Oceania	Australia	Telstra	✓				✓
	New Zealand	Telecom NZ	✓				✓
		Vodafone NZ		✓			✓

Note 1: For the latest band usage, please contact local carriers.
Note 2: For cellular device compatibility with a particular carrier, please check “Carrier Approval” with your cellular device vendor.

3GPP2— From CDMA2000 to EV-DO

CDMA2000, also known as IMT Multi-Carrier (IMT-MC), is an IMT-2000-based standard of Code-Division Multiple Access (CDMA) that was developed by the ITU for sending data between mobile phones and cell towers (or BST, Base Transceiver Station). CDMA2000 and W-CDMA are competing standards in the cellular communication network market.

CDMA2000 actually denotes a family of standards that represent the successive, evolutionary stages of the underlying technology. The different variations are all approved radio interfaces for IMT-2000 and are listed below in chronological order:



4G Technologies

Pre-4G vs. True 4G

Today's operators refer to LTE and WiMAX technologies as fourth generation cellular technologies (4G). However, according to the International Telecommunication Union, “True 4G” technology should provide Gigabit-level data rates when stationary, and a peak rate of 100 Mbps for highly mobile applications and other criteria (details given below). This section gives a brief introduction to pre-4G technology (LTE), and true-4G technology (LTE-A).

Requirements of IMT-Advanced (4G)

- The candidate Radio Interface Technology (RIT) shall be based on an IP-based packet switched network.
- The candidate RIT shall provide a nominal data rate of 100 Mbps when the client is physically moving at high speeds relative to the base transceiver station (BST), and 1 Gbps for low-speed mobility or relatively fixed positions.
- The candidate RIT shall be able to dynamically share and use the network resources to support more simultaneous users per cell.
- The candidate RIT shall be able to use different bandwidth allocations to support a scalable bandwidth of up to (and including) 40 MHz.
- The candidate RIT shall have a minimum downlink peak spectral efficiency of 15 bits/s/Hz, and a minimum uplink peak spectral efficiency of 6.75 bits/s/Hz.
- For indoor environments, the candidate RIT shall have a cell spectral efficiency of up to 3 bits/s/Hz/cell for downlink and 2.25 bits/s/Hz/cell for uplink.
- The candidate RIT shall provide seamless handovers and global roaming across multiple heterogeneous networks.
- The candidate RIT shall offer a high quality of service for next generation multimedia services.

Long Term Evolution (LTE)

The pre-4G 3GPP Long Term Evolution (LTE) technology is often branded "4G-LTE", but the first LTE release does not fully comply with the IMT-Advanced requirements. LTE has a theoretical net bit rate capacity of up to 100 Mbps in the downlink and 50 Mbps in the uplink if a 20 MHz channel is used, and more if multiple-input multiple-output (MIMO), i.e., antenna arrays, are used. The following table gives a theoretical measurement of the LTE data rate.

Long Term Evolution Advanced (LTE-A)

LTE-Advanced (Long Term Evolution Advanced) was formally submitted by the 3GPP organization to ITU-T in fall 2009 as a candidate for the IMT-Advanced standard and is expected to be released in 2013. LTE-Advanced is essentially an enhancement to the existing LTE technology for mobile networks. LTE and LTE-Advanced also make use of additional spectrums and multiplexing to allow higher data speeds. Coordinated Multi-point Transmission will also allow more system capacity to help handle the enhanced data speeds. Release 10 of LTE is expected to achieve the data-speed requirements of IMT-Advanced. Release 8 currently provides up to 300 Mbps of data download, which is still inadequate for IMT-Advanced standards.

LTE Data Speeds

	LTE
Peak Download	100 Mbps
Peak Upload	50 Mbps

LTE Advanced Data Speeds

	LTE Advanced
Peak Download	1 Gbps
Peak Upload	500 Mbps

Additional Information

LTE in 2013 is still a growing technology, and frequency usage or regulation is still evolving over time. The following table gives a snapshot of LTE frequency usage in 2013. For the latest information please contact your local LTE service provider.

LTE Frequency Band Usage Overview
(Based on major carriers)

Continent	Country	700 MHz	800 MHz	850 MHz	900 MHz	1700 MHz	1800 MHz	2100 MHz	2300 MHz	2600 MHz
America	Brazil									✓
	Canada					✓				✓
	United States	✓				✓				
Europe	France		✓							✓
	Germany		✓							✓
	United Kingdom						✓			
Africa	South Africa						✓	✓	✓	
Asia	Japan				✓			✓		
	South Korea			✓				✓		
Oceania	Australia				✓		✓			
	New Zealand						✓			

Note 1: For the latest band usage, please contact local carriers.
Note 2: For cellular device compatibility with a particular carrier, please check "Carrier Approval" with your cellular device vender.

Understanding Wireless Technology

2-1 Radio System Concepts

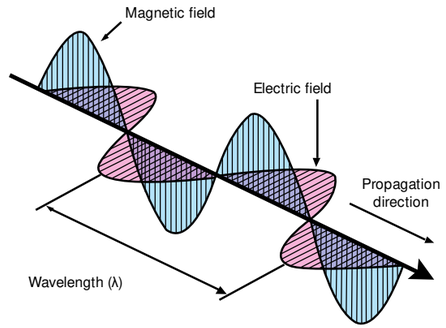
How Radio Works

Electromagnetic Waves

Data is transmitted through the air with Electromagnetic (EM) waves, which are formed by an alternating current that is rapidly changing direction on a conductive material. The rapid oscillation of electric and magnetic fields around the conductor projects electromagnetic waves into the air (see the accompanying figure). In order for current to be radiated into the air in the form of electromagnetic waves, a few factors are critical; namely, the length of the conductor and frequency of the AC current. A higher frequency reduces the requirement for conductor length.

An antenna (also called an aerial) is a conductor device designed to transmit and/or receive electromagnetic waves during wireless communication.

The size (or length) of the antenna is directly proportional to its desired transmission/ reception frequency.

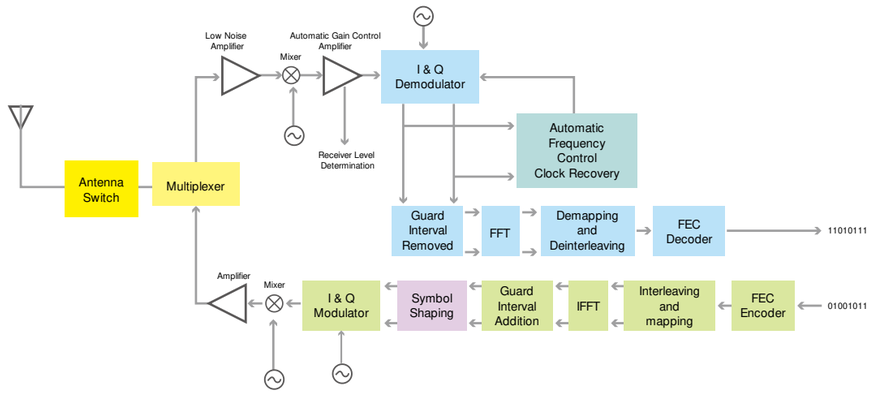


Tx & Rx

Every radio setup includes two major components:

- Transmitter (abbreviated as Tx)
- Receiver (abbreviated as Rx)

Electromagnetic waves are radiated from a transmitter to a receiver. The transmitter encodes voice, video, and data onto a sine wave, and transmits it via radio waves. The receiver receives the radio waves and decodes the waves to retrieve the information. Both the transmitter and receiver use antennas to radiate and capture radio signals. The following figure is an example of the system architecture and block diagram of an IEEE 802.11a radio unit. You can see that the transmitter and receiver are both featured in the same radio unit. The upper path, from the antenna side (left) to a data stream (right), shows how the radio signal is transferred to a data stream via a receiver and several functional blocks while the lower path shows how transmission works. A multiplexer is used to select a path for transmission or reception.



Propagation

As EM waves propagate through the air, they experience the following types of alterations as they encounter different types of obstacles:

Diffraction (Shadow Fading)

Signal strength is reduced after experiencing diffraction. Obstacles causing diffraction usually have sharp edges such as the edges of buildings. When EM waves encounter an obstacle with sharp edges that cannot be penetrated, the EM waves wrap around the obstacle to reach the receiver.

Scattering

When EM waves encounter many small obstacles (smaller than the signal wavelength), the EM waves scatter into many small reflective waves and damage the main signal, causing low quality or even broken links. Such obstacles include rough surfaces, rocks, sand, dust, tree leaves, street lights, etc.

Reflection

When EM waves run into large obstacles such as the ground, walls, or buildings, they reflect and change their direction and phase. If the reflected surface is smooth, the reflected signal will likely represent the initial signal and not be scattered.

All of the above phenomena result in multipath propagation so not all signals will arrive at the receiver antenna at the same time due to obstacles that change the signal paths. Whether you are setting up an outdoor or indoor application, multipath can severely affect received signal quality because the delayed signals are destructive to the main signal. The multipath issue can usually be compensated by antenna diversity at the RF level and/or by OFDM at the baseband level.

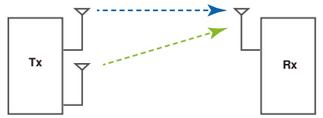
MIMO

MIMO (Multiple Input/Multiple Output, commonly pronounced "my-mo") is a technology that uses multiple transmitters and receivers (with multiple antennas) to improve the performance of wireless communication. The following letters are used to describe such a radio system: M = Multiple; S = Single; I = Input; O = Output. The M, S, I, and O relate to what is done in the air, not the device. For example, regarding a MIMO radio system, MI (multiple inputs) means multiple transmitters send multiple data streams "into" the air. MO (multiple outputs) means multiple receivers acquire multiple data streams "out of" the air. Note that the terms input and output refer to the radio channel carrying the signal, not to the devices with antennas.

The various systems are illustrated below:

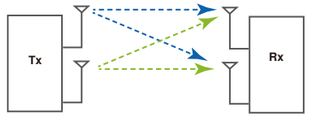
- Single-input single-output (SISO)

- Multiple-input single-output (MISO)



- Single-input multiple-output (SIMO)

- Multiple-input multiple-output (MIMO)



When multiple transmitters and multiple receivers are used, simultaneous data streams can be sent, which increase the data rate. In addition, multiple receivers allow greater coverage and longar distances between devices. The IEEE 802.11n standard uses MIMO to increase speed to 100 Mbps and beyond. MIMO technology is also used in LTE and other wireless standards.

What You Need to Know about a Radio System

Signal Power

Radio signals are transmitted at a certain power level, with power measured in watts. However, power ratings for a WLAN are usually measured in milliwatts (mW). A commercial wireless AP transmits between 30 to 100 mW of power, and about 50 mW for wireless adaptors (clients). Certain applications will require higher transmit power (or Tx power) and may attempt to use power boosters or customized high-power modules to amplify the transmit power. However, such attempts must be performed with caution as power amplification may cause the system to exceed the country's radio emission regulations (i.e., FCC regulations).

Power measured in mW is hard on the math when dealing with extremely small power levels at the receiver end. Therefore, instead of using absolute values (milliwatts) we often convert them into dBm. The unit of dBm is a logarithmic representation of mW. The conversions are as follows:

$$P_{dBm} = 10 \log P_{mW}$$

$$P_{mW} = 10^{\left(\frac{P_{dBm}}{10}\right)}$$

The dBm is an absolute unit which is referenced to the milliwatt. 0 dBm equals 1 milliwatt. The unit dBm is used for a measurement of absolute power. By comparison, the decibel (dB) is a dimensionless unit, used for quantifying the ratio between two values. Roughly speaking, a 3-dB increase represents roughly doubling the power, while a 3-dB decrease means that the power is reduced by about one half. Here is a quick table showing unit conversions:

dBm	mW	dBm	mW	dBm	mW
-3	0.5	9	8	21	126
-2	0.6	10	10	22	158
-1	0.8	11	13	23	200
0	1.0	12	16	24	250
1	1.3	13	20	25	316
2	1.6	14	25	26	398
3	2.0	15	32	27	500
4	2.5	16	40	28	630
5	3.2	17	50	29	800
6	4	18	63	30	1000
7	5	19	79	33	2000
8	6	20	100	36	4000

Transmit Power and Received Sensitivity

When a radio signal is being transmitted through the air, it will experience a great loss in signal strength, known as attenuation, while propagating through free space. Therefore, when evaluating a wireless system, one needs to be aware of the signal power level at the transmitter end and at the receiver end. The signal power received cannot be so weak as to break the communication link, or too strong as to saturate the receiver's amplifiers.

These concerns call for estimating the "power budget" of a wireless system. Power budget estimations will give an idea of how far to extend the wireless link without losing communication. Note that the following calculations are theoretical estimates that are not meant to guarantee communication distance.The formulas come from the Friis Equation and are based on the idea of "Free Space Loss".

The Friis Transmission Formula enables us to calculate the power received (P_r) given that a known power (P_t) is radiated. Friis assumes that both antennas are isotropic, and "Free space" implies that there are no objects present to affect propagation. The theoretical formula may look like this:

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2$$

where G_t and G_r are the gain of the transmitting and receiving antennas, λ is the wavelength, and R is the distance from the radiator.

Since $\lambda = c/F$, where c is the speed of light (3×10^8 m/s) and F is the frequency in Hz, we can simplify the formula and represent the effective transmission distance r (in km) as follows

$$r = \frac{10^{(p_t + g_t + g_r - p_r)/20}}{41.88 \times f}$$

where f is the frequency in MHz, p_t and p_r are in dBm, and g_t and g_r are in dBi.

These parameters are easy to obtain from the design or the product specifications. Plug in the values for these parameters to get the effective distance. In reality, due to system loss or the use of non-isotropic transmitting and receiving antennas, we usually divide the theoretical result by a factor of 4 to obtain a more reasonable distance. In fact, factors of 8 or higher may be used if the system and environmental conditions are not controllable.

The formula also shows that there are many other factors involved that will affect transmission distance. The receiver's sensitivity is the minimum power level that

The formula also shows that there are many other factors involved that will affect transmission distance. The receiver's sensitivity is the minimum power level that is required for the receiver to process received data. The specified sensitivity is not the power detected by the receiving antenna, but the power present at the receiver module. An important point to note from the above equation is that as the frequency increases, the effective distance decreases. Therefore, the 5 GHz band-enabled 802.11a and 802.11n standards will yield a shorter communication distance than 2.4 GHz-enabled 802.11b/g and 802.11n. Users who wish to communicate over long distances should therefore select the 2.4 GHz band and take 802.11b/g/n as their operating standard.

Modulation and Spread Spectrum

Modulation is the process of conveying a message signal by varying one or more properties of a periodic waveform, called the carrier signal, with a modulating signal that encodes the information to be transmitted. The act of extracting the original information-bearing signal from a modulated carrier wave is called demodulation.

There are many RF modulation techniques. The accompanying chart categorizes different digital modulation techniques.

Spread-spectrum techniques are methods for transmitting a radio signal over a bandwidth that is considerably larger than the frequency content of the original information. Spread-spectrum techniques provide the benefits of secure communications, better resistance against interference, noise, and jamming, and limiting the power flux density. To simplify this discussion, only spread-spectrum techniques that pertain to the radio-based physical layers in the 802.11 standard, namely FHSS, DSSS, and OFDM, will be discussed.

Category	Digital Modulation Technology
Phase-shift keying	Binary PSK (BPSK) Binary PSK (BPSK) Quadrature PSK (QPSK) Differential PSK (DPSK) Differential QPSK (DQPSK) Multi-phase shift keying (M-ary PSK or MPSK) π / 4–QPSK
Frequency-shift keying	Audio frequency-shift keying (AFSK) Multi-frequency shift keying (M-ary FSK or MFSK) Dual-tone multi-frequency (DTMF)
Complementary Code Keying	Complementary Code Keying (CCK)
Quadrature amplitude	Multiple Quadrature amplitude modulation (M-ary QAM)
Continuous phase	Minimum-shift keying (MSK) Gaussian minimum-shift keying (GMSK) Continuous-phase frequency-shift keying (CPFSK)
Frequency-division multiplexing	Orthogonal frequency-division multiplexing (OFDM)
Spread-spectrum	Direct-sequence spread spectrum (DSSS) Chirp spread spectrum (CSS) Frequency-hopping spread spectrum (FHSS)

FHSS (Frequency Hopping Spread Spectrum, or FH)

This is one of the modulation techniques used in spread spectrum signal transmission. It is also known as Frequency-Hopping Code Division Multiple Access (FH-CDMA). Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal. The transmitter "spreads" the energy, originally concentrated in a narrow band, across a number of frequency band channels on a wider electromagnetic spectrum. FHSS has the advantages of improved privacy, decreased narrowband interference, and increased signal capacity.

DSSS (Direct Sequence Spread Spectrum, or DS)

DSSS divides a stream of information to be transmitted into small pieces, each of which is allocated to a frequency channel across the spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. Direct sequence spread spectrum is also known as direct sequence code division multiple access (DS-CDMA). This modulation technique is officially accepted and used by the IEEE 802.11b and IEEE 802.11g standards.

OFDM (Orthogonal Frequency Division Multiplexing)

OFDM is a modulation scheme that divides a single digital signal simultaneously across 1,000 or more signal carriers. The signals are sent at right angles (orthogonal) to each other so they do not interfere with each other. OFDM has the ability to overcome multi-path effects by using multiple carriers to transmit the same signal. OFDM is commonly used in the IEEE 802.11a and 802.11g standards. Non/near line-of-sight associations can also be achieved by using the OFDM technique.

The 802.11g (802.11b backwards compatible) standard is used below as an example for how the transmission type of spread spectrum and modulation scheme corresponds to each data rate:

Data Rate (Mbps)	Transmission Type of Spread Spectrum	Modulation Scheme
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK
12	OFDM	QPSK
11	DSSS	CCK
9	OFDM	BPSK
6	OFDM	BPSK
5.5	DSSS	CCK
2	DSSS	QPSK
1	DSSS	BPSK

ISM and Unlicensed Bands

Unlicensed bands are part of the radio spectrum that can be used by anybody without applying for a license. A well-known unlicensed band is the ISM (industrial, scientific, and medical) radio band, which is reserved internationally for the use of radio frequency (RF) energy for industrial, scientific, and medical purposes other than communications. The ISM bands are defined by the ITU-R in 5.138, 5.150, and 5.280 of the radio regulations. Three ISM bands are commonly used:

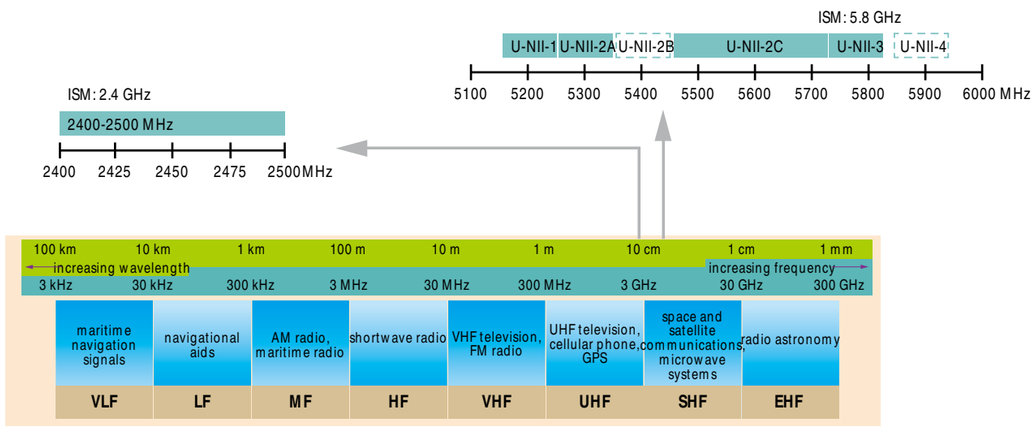
- 2.400 GHz to 2.500 GHz
- 5.725 GHz to 5.875 GHz

Usage of the bands designated in these sections may vary in different countries due to variations in national radio regulations. In the U.S., ISM band usage is governed by FCC (Federal Communications Commission) Part 18, and Part 15 contains regulations for unlicensed communication devices (even those that share ISM frequencies). In European countries, the use of the ISM band is covered by Short Range Device (SRD) regulations issued by the European Commission, based on technical recommendations by CEPT and standards by ETSI.

Regulatory authorities may allocate parts of the radio spectrum for unlicensed communications that may or may not also be allocated as ISM bands. For example, the FCC regulates the usable frequency bands and the maximum allowable power in these frequency bands for the United States. From 1997, it has added additional bands in the 5 GHz range under Part 15.407, known as the Unlicensed National Information Infrastructure (U-NII) bands for WLAN usage.

U-NII band	a.k.a.	Frequency	Bandwidth	Usage	DFS	Power Limitation	Note
U-NII-1	U-NII Low	5.15 to 5.25 GHz	100 MHz	Indoor only	No	50 mW	
U-NII-2A	U-NII Mid, U-NII-2	5.25-5.35 GHz	100 MHz	Indoor & Outdoor	Yes	250 mW	
U-NII-2B	U-NII Upper	5.35 to 5.47 GHz	120 MHz	-	-	-	Not determined yet
U-NII-2C	U-NII Worldwide, U-NII-2e	5.47 to 5.725 GHz	225 MHz	Indoor & Outdoor	Yes	250 mW	Operations on ch 120-128 (5.6 to 5.65 GHz) band is limited because of weather radar
U-NII-3	U-NII Upper	5.725 to 5.825 GHz	100 MHz	Indoor & Outdoor	No	1 W	Overlaps with the ISM band
U-NII-4	U-NII Upper	5.85 to 5.925 GHz	75 MHz	-	-	-	Not determined yet

The following diagram shows the spectrum overview of the ISM and U-NII bands.

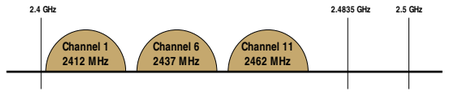


Advantages and Disadvantages of Using Unlicensed Bands

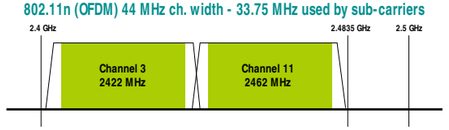
ISM and U-NII are both unlicensed bands, which allow anyone to transmit in these bands without a license from the FCC or related authorities. It is the opening of these unlicensed bands that has allowed the WLAN business to grow in small businesses and homes. However, the freedom of these license-free bands also means a great number of un-licensed users may be sharing the same bandwidth. The powerful emissions of these devices can create electromagnetic interference and disrupt radio communication using the same frequency, so these devices were limited to certain bands of frequencies. In general, communications equipment operating in these unlicensed bands must tolerate any interference generated by other equipment, and it also means that users have no regulatory protection from devices operating on unlicensed bands.

Let's take the 2.4 GHz band as an example. In the following diagram, there are three non-overlapping channels for DSSS operation (IEEE 802.11b). When channel-bonding is applied in IEEE 802.11n, there is only one non-overlapping channel (either ch3 or ch11), which means that the operation of one device can easily interfere with other devices, and vice versa. That is why some vendors do not provide channel-bonding for 2.4 GHz band operation.

802.11b (DSSS) channel width 22 MHz



802.11n (OFDM) 44 MHz ch. width - 33.75 MHz used by sub-carriers



In the following sections, our discussion only includes the 2.4 GHz band and 5 GHz band because they are the most commonly used bands in WLAN applications. In addition to IEEE 802.11 standards, the tradeoffs between these two bands are usually considered with interference (almost entirely in the 2.4 GHz band) and range (bigger power loss shortens the transmission distance in the 5 GHz band).

2.4 GHz Band

802.11b/g are the most commonly used WLAN standards today. The 2.4 GHz ISM band is supported by almost every country worldwide. Not every country supports the same channels in the 2.4 GHz ISM band, so users need to make sure that the wireless AP matches the same standard that is being used in that country. The following chart shows channels that are supported in the 2.4 GHz ISM band for different regulatory domains. Although the ISM band is open between 2.4 to 2.5 GHz, IEEE 802.11b/g standards only use 2.400 to 2.4835 GHz. The minor mismatch is due to channel spacing and provides a buffer to prevent power from leaking into the licensed bands.

Channel Number	Center Frequency (MHz)	Regulatory Domain		
		US	EU	JP
1	2412	Yes	Yes	Yes
2	2417	Yes	Yes	Yes
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes

Channel Number	Center Frequency (MHz)	Regulatory Domain		
		US	EU	JP
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467		Yes	Yes
13	2472		Yes	Yes
14	2484			Yes*

*Ch14 is valid only for DSSS and CCK modes in Japan.

5 GHz Band

802.11a/h/j/n/ac use the 5 GHz band. Compared with the 2.4 GHz band, the 5 GHz band is considered to have more clear options: a full channel width reserved without overlap, and less non-Wi-Fi interference and tighter cell packing for higher capacity. However, every country applies its own radio regulations to allocate the allowable channels and maximum power levels within the 5 GHz band. Network operators should consult local authorities as these regulations are subject to change at any time and may be out of date. See below for channels supported in the 5 GHz band for the three regulatory domains.

Channel Number	Center Frequency (MHz)	Regulatory Domain		
		US	EU	JP
36	5180	Yes	Yes	Yes
40	5200	Yes	Yes	Yes
44	5220	Yes	Yes	Yes
48	5240	Yes	Yes	Yes
52	5260	Yes**	Yes**	Yes**
56	5280	Yes**	Yes**	Yes**
60	5300	Yes**	Yes**	Yes**
64	5320	Yes**	Yes**	Yes**
100	5500	Yes**	Yes**	Yes**
104	5520	Yes**	Yes**	Yes**
108	5540	Yes**	Yes**	Yes**
112	5560	Yes**	Yes**	Yes**
116	5580	Yes**	Yes**	Yes**

Channel Number	Center Frequency (MHz)	Regulatory Domain		
		US	EU	JP
120	5600	Yes**	Yes**	Yes**
124	5620	Yes**	Yes**	Yes**
128	5640	Yes**	Yes**	Yes**
132	5660	Yes**	Yes**	Yes**
136	5680	Yes**	Yes**	Yes**
140	5700	Yes**	Yes**	Yes**
144	5720	Yes**	Yes**	No
149	5745	Yes	Yes***	No
153	5765	Yes	Yes***	No
157	5785	Yes	Yes***	No
161	5805	Yes	Yes***	No
165	5825	Yes	Yes***	No

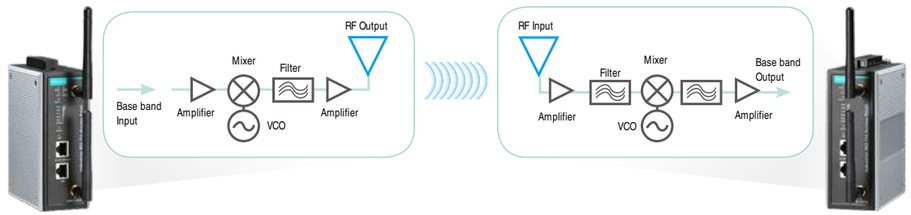
**These channels are dynamic frequency selection (DFS) channels, which will be switched to other channels when a radar signal is detected.
***These channels are only related to the use of Short Range Devices (SRD) with 25 mW power limitation.

2-2 WLAN Antennas

Why Using the Right Antenna is Important

The transmission speed of a wireless connection is significantly related to the radio signal strength of the transmission. Selecting the appropriate antennas for the application environment is the most important step to ensure a strong wireless link.

The figure below is a simple illustration of the wireless signal transmission. After the digital signals get converted into analog form, the signal gets mixed, filtered, amplified, and finally released to the atmosphere. The main function of the antenna is to control how the energy is released and what kind of energy field it is forming. This chapter introduces the key parameters for selecting the right antenna for your application, such as antenna frequency, impedance matching, voltage standing wave ratio (VSWR), gain, and polarization.



Antenna Parameters

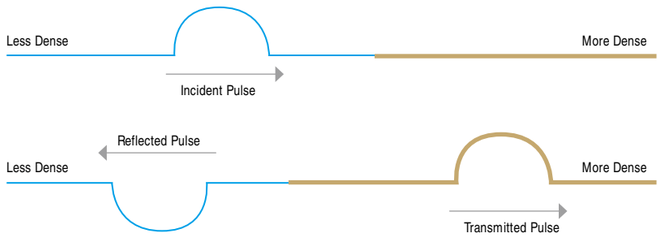
Frequency

An antenna is a transducer that is designed to transmit and/or receive electromagnetic waves. It is like a converter that converts back and forth between electromagnetic waves and electrical currents. Different wireless devices use different antennas to operate in different frequencies and to achieve, for example, a desired range. The most important parameter of an antenna is its working frequency. For example, a 2.4 GHz antenna's wavelength is too short to use with IEEE 802.11a communication and using an antenna with a mismatched frequency will likely cause a very poor performance on both signal radiation and actual data throughput.

Impedance Matching

Maximum power transfer from the transmitter to the antenna requires impedance matching of the antenna system. The figure below demonstrates the reflection effect when the impedance doesn't match between two mediums. Mismatched impedance will cause energy loss and risk circuit damage from the reflected energy pulse.

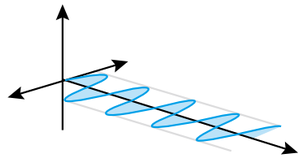
Transmitters generally have an output impedance of 50 ohms and that needs to be matched across the transmission line to the antenna in order to maximize overall efficiency, eliminate line variation with an equal voltage standing wave ratio (VSWR), and reduce transmission line losses.



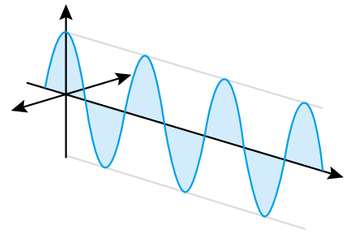
Polarization

Polarization refers to the direction in which the electric field lines point as the signal radiates away from the antenna. The simplest and most common type is linear polarization. An improper antenna installation will decrease signal reception quality. For example, a perfectly aligned horizontal (side to side) antenna will not receive any signals sent from a perfectly aligned vertical (up and down) antenna. An antenna at a 45° alignment (skew polarization) however, can receive signals sent from both horizontal and vertical antennas, but at reduced signal strengths (dB). It is important to know the polarization of the antennas in the WLAN to make sure that signals are being sent and received under optimal conditions. The figures below are the visualization of the horizontal and vertical linear polarizations.

Horizontal Linear Polarization

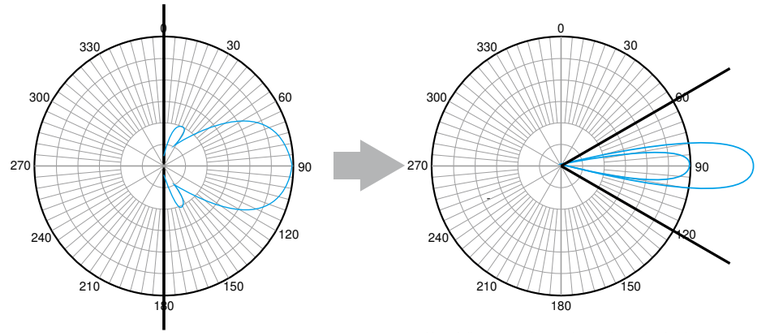


Vertical Linear Polarization



Gain

The gain of each antenna specifies its directivity and electrical efficiency. In general, the lower the gain, the more evenly distributed in all directions the radiation will be. High gain antennas, on the other hand, emit radiation in a more specific direction. The gain defines its power gain or directive gain in terms of the ratio of the intensity, or power per unit surface. In general, when we choose an antenna, the longer the transmission distance, the higher the antenna gain must be. At the same time, we must sacrifice omni-directional coverage.

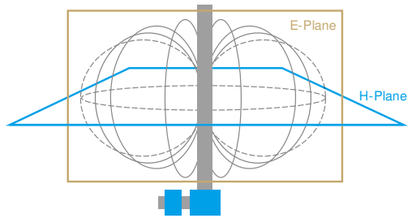


Use of directors makes angle smaller and gain higher

Antenna Radiation Patterns (E-plane and H-plane)

Much about an antenna's performance can be learned from its radiation pattern. The antenna radiation pattern is a three-dimensional illustration of how the antenna emits and receives radio signals (see figure on the right) during communication.

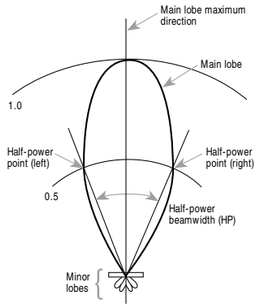
A radiation pattern is essentially the electromagnetic field, which consists of an electric field (E-plane) and a magnetic field (H-plane). The electric field and magnetic field propagate toward the same general direction, but the polarization of their waves are always perpendicular (90° angle) to each other. Radiation patterns are different for various types of antennas. E-plane and H-plane diagrams provide a two-dimensional view of how electric and magnetic fields behave for a particular antenna.



HPBW

Half-power beamwidth, also called the 3-dB beamwidth, is the angular measurement of the main lobe directivity on the antenna radiation pattern where the sensitivity (gain) is one-half (or -3dB) of the maximum value. Sometimes it is also called FWHM (the full width of the beam at half its maximum intensity). The 3-dB beamwidth measurement is commonly used to define the vertical and horizontal angles of a particular antenna.

As a side note, an antenna is a passive component, which means it does not increase the overall input energy in any way. In order to achieve longer distance transmission, it compresses the energy field to make it leaner and longer. Therefore, a higher gain antenna tends to come with a narrower beamwidth.



VSWR

The voltage standing wave ratio (VSWR) is the ratio of the maximum voltage to the minimum voltage on the transmission line (cable) used to measure antenna efficiency. When the transmitter sends signals forward through the transmission line to the antenna, a portion of the signal will bounce back across the transmission line if the antenna is at a different impedance, and mix with oncoming forward signals to create a voltage standing wave pattern.

A 1:1 VSWR (or just 1) indicates that power is being fully absorbed by the antenna (because antenna impedance is also the same as the impedance on the transmission line) and no power is being reflected back to the transmitter, but this is very difficult to achieve. For example, a 50-ohm radio with an antenna impedance of 75 ohms will have a theoretical VSWR of 1.5:1 on the transmission line. For typical antenna systems, a VSWR of 1.2:1 can be considered to be more than acceptable. A VSWR of 2:1, which is common for many antenna systems, means that roughly 10% of the forward signals are being reflected from the antenna. A higher VSWR means lower transmission efficiency and can result in heated transmission lines and damaged transmitters.

VSWR Efficiency Chart		
VSWR	Efficiency	Loss
1	100%	0.00 dB
1.3	98.3%	0.08 dB
1.5	96.0%	0.18 dB
1.8	91.8%	0.36 dB
2	88.9%	0.51 dB
2.5	81.6%	0.86 dB
3	75.0%	1.25 dB
3.5	69.1%	1.61 dB
4	64.0%	1.94 dB
5	55.6%	2.55 dB

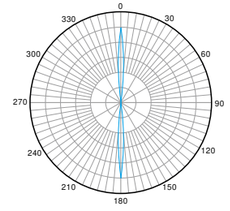
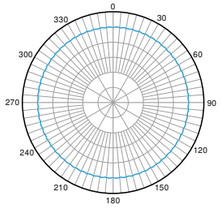
Antenna Types

There are two basic types of antennas for WLAN products, categorized by the direction in which they beam radio signals: omni-directional and directional.

Omni-directional Antennas

Omni-directional antennas are designed to radiate signals equally in all 360 degrees. Use this type of antenna if you need to transmit from a central node, such as an access point, to users scattered all around the area. In a small office with three or four rooms, an access point with an omni-directional antenna should be able to provide sufficient coverage for all wireless stations in all rooms.

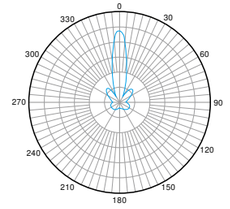
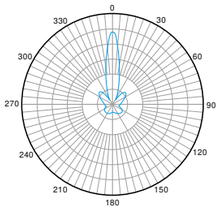
Sample Antenna Spec

Omni-directional Antennas	Antenna Patterns: E-Plane for 2.4 GHz	Antenna Patterns: H-Plane for 2.4 GHz
		

Directional Antennas

Directional or patch antennas provide a more focused signal than omni-directional antennas. Signals are typically transmitted in an oval-shaped pattern with a beam width of approximately 30 degrees. This type of antenna is also ideal for office locations. For example, an access point with a semi-directional antenna can be placed in one corner of a room to provide reliable coverage for its entire length. Directional antennas can also be used outdoors to provide short distance point-to-point links or as the customer end of a point-to-multipoint network.

Sample Antenna Spec

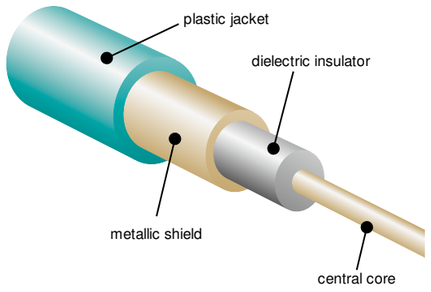
Directional Antennas	Antenna Pattern: E-Plant for 2.4GHz	Antenna Pattern: H-Plant for 2.4GHz
		

2-3 Cables

RF Cables

RF cable, also called coaxial cable, is the most common type of cable used to connect an RF transmitter (or receiver) to the antenna. The core and woven shield are generally made of copper, and the dielectric insulator is commonly made of solid or foamed polyethylene. Some RF cables also include a foil layer between the shield and the dielectric to further reduce loss.

Typically, the metallic shield is at ground potential and the voltage is applied to the main conductor to transmit signals. The main benefit of using an RF cable is that electromagnetic fields are kept within the dielectric insulator with very little radiated loss. In addition, the dielectric insulator protects the transmission line against sources of external interference.



Key Parameters

Impedance Matching

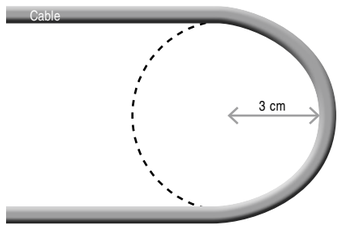
This is the same principle introduced in the antenna section. To have the best transmission efficiency, the connected mediums, such as RF cable, antenna, connector, and source transmitter, must have a matching impedance.

Attenuation

Every RF cable has signal loss, which is referred to as attenuation and is measured in decibels (dB) per 100 feet. Attenuation of RF signals will increase at higher frequencies because RF current travels mostly on the outer surface layer (skin effect) of the core conductor and surface resistance will increase at higher frequencies. Skin effect losses on the core conductor can be reduced by increasing the diameter of the cable. Doubling the cable diameter will reduce the skin effect resistance in half (not including dielectric and shield losses).

Bending Radius

The bending radius is the minimum measure of the inside curvature that a cable can be bent without causing it physical damage, reducing its performance, or shortening its useful life. The figure below illustrates a cable with a bending radius of 3 centimeters.



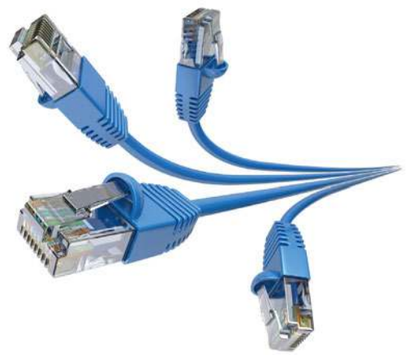
Common Coaxial Cables

Type	Impedance (ohms)	Core	Dielectric Type	Dielectric VF	Dielectric mm	OD mm	Max. Attenuation @ 750 MHz dB/100 ft
LMR-100	50					2.79	20.725
LMR-195	50					4.95	10.125
LMR-200	50	1.12 mm Cu	PF	0.83	2.95	4.95	9.035
HDF-200							
CFD-200							
LMR-400	50	2.74 mm (Cu-clad Al)	PF	0.85	7.24	10.29	3.544
HDF-400							
CFD-400							
LMR-600	50	4.47 mm (Cu-clad Al)	PF	0.87	11.56	14.99	2.264
LMR-900	50	6.65 mm (BC tube)	PF	0.87	17.27	22.1	1.537
LMR-1200	50	8.86 mm (BC tube)	PF	0.88	23.37	30.48	1.143
LMR-1700	50	13.39 mm (BC tube)	PF	0.89	34.29	42.42	0.844

Ethernet Cables

Category 5 (Cat 5) is the fifth-generation standard for twisted-pair Ethernet cables established by the Electronic Industries Association and Telecommunications Industry Association (EIA/TIA). Cat 5 cables contain 4 pairs of wires but use only 2 pairs (rated at 100 MHz) for 10BASE-T and 100BASE-TX (Fast Ethernet) transmission. An enhanced version, CAT 5e, imposes more restricted cross-talk specifications to ensure the stability when using all four pairs for 1000BASE-T (Gigabit Ethernet) communication. Cat 5/5e cables generally have a transmission distance limitation of 100 meters.

Category 6 (Cat) is another commonly used standard for Gigabit Ethernet transmission. It is backwards compatible with Cat 5 and Cat 5e, but at the same time, it allows higher transmission frequency up to 250 MHz. It is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), 1000BASE-T/1000BASE-TX (Gigabit Ethernet), and 10GBASE-T (10-Gigabit Ethernet).



Key Parameters

Bending Radius

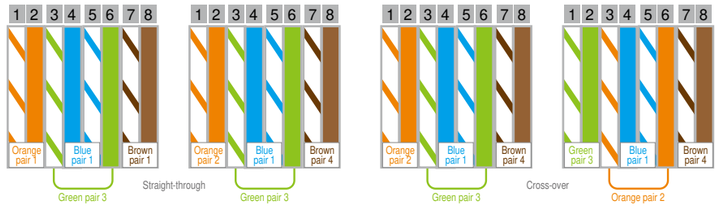
Most Category 5 cables can be bent at any radius exceeding approximately four times the diameter of the cable.

Maximum Cable Segment Length

The recommended length for a CAT 5 cable segment is 100 meters (TIA/EIA 568-5-A). Repeaters and switches can be used to extend the transmission distance. Media converters, such as Ethernet-to-fiber converters, can be used to significantly extend transmission distance.

Straight-through vs. Cross-over

Twisted pairs of Ethernet cables can be rearranged to provide connectivity between different types of devices. A typical straight-through cable, also called a patch cable, has identical twisted-pair arrangements on both ends (RJ45 connector) and is used to connect a computer to a switch or router. A cross-over cable has the orange twisted pair crossed over with the green twisted pair, and is used to connect two computers directly to allow communication. However, newer network interfaces with auto-MDIX ports are capable of detecting the type of connection to automatically choose MDI or MDIX configuration, which eliminates the need for cross-over cables.



10BASE-T and 100BASE-TX vs. 1000BASE-T

10BASE-T and 100BASE-TX Ethernet connections require two cable pairs. 1000BASE-T Ethernet connections require four cable pairs (8 pins). Listed below are the pin assignments for these three standards (10BASE-T, 100BASE-TX, 1000BASE-T) on both MDI (Media Dependant Interface) and MDI-X (Media Dependant Interface cross-over).

10/100BASE-TX MDI and MDI-X PORT PINOUTS		
Pin	MDI Signal Name	MDI-X Signal Name
1	Transmit Data plus (TD+)	Receive Data plus (RD+)
2	Transmit Data minus (TD-)	Receive Data minus (RD-)
3	Receive Data plus (RD+)	Transmit Data plus (TD+)
6	Receive Data minus (RD-)	Transmit Data minus (TD-)
4, 5, 7, 8	Not used	Not used

1000BASE-T MDI and MDI-X PORT PINOUTS		
Pin	MDI Signal Name	MDI-X Signal Name
1	Bi-directional Pair A Plus (BI_DA+)	Bi-directional Pair B Plus (BI_DB+)
2	Bi-directional Pair A Minus (BI_DA-)	Bi-directional Pair B Minus (BI_DB-)
3	Bi-directional Pair B Plus (BI_DB+)	Bi-directional Pair A Plus (BI_DA+)
4	Bi-directional Pair C Plus (BI_DC+)	Bi-directional Pair D Plus (BI_DD+)
5	Bi-directional Pair C Minus (BI_DC-)	Bi-directional Pair D Minus (BI_DD-)
6	Bi-directional Pair B Minus (BI_DB-)	Bi-directional Pair A Minus (BI_DA-)
7	Bi-directional Pair D Plus (BI_DD+)	Bi-directional Pair C Plus (BI_DC+)
8	Bi-directional Pair D Minus (BI_DD-)	Bi-directional Pair C Minus (BI_DC-)

2-4 Connectors

Before placing an order for antennas and cables for your wireless device(s), the connector types must first be determined. In general, terms such as plug, pin, and prong refer to male connectors, and terms such as receptacle, socket, and slot refer to female connectors. For electrical connectors, connector gender (male and female) is not enough to identify the right connector. This chapter provides several commonly used connectors and their pictures as a reference to your selection.

Antenna Connectors

There are various types of coaxial RF antenna connectors designed for different applications. This section introduces several commonly-used antenna connector types as a guideline for identifying and selecting the appropriate connector.

Connector	Frequency Range	Male Connector	Female Connector
SMA (Sub-Miniature version A)	DC to 18 GHz		
RP-SMA (Reverse Polarity SMA)	DC to 18 GHz		
QMA (Quick SMA)	DC to 18 GHz		
N-type (named after Paul Neill)	DC to 11 GHz		
TNC	DC to 11 GHz		

Ethernet Connectors

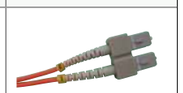
Copper Cable Connectors

The chart below shows information for RJ45 and M12 connector types, which are two of the most popular types of Ethernet connectors. RJ45 connectors are very common for typical indoor applications, while M12 connectors are used mostly for outdoor environments or for applications that encounter frequent shock/vibration.

Connector	Data Rate	Male Jack
RJ45 (Registered Jack 45)	10/100 Mbps (4 pins) 1000 Mbps (8 pins)	
M12	10/100 Mbps (4 pins) 1000 Mbps (8 pins)	

Optical Fiber Connectors

Optical fiber connectors are used to quickly connect/disconnect an optical fiber connection. Optical fiber connectors are usually spring loaded to ensure that optical fiber cross-sections are firmly pressed together to eliminate air gaps, which can cause signal loss. The accompanying table shows commonly-used optical fiber connectors

Connector	Ferrule Diameter	Standard	Male Jack
LC (Lucent Connector)	1.25 mm	IEC 61754-20	
SC (Subscriber Connector)	2.5 mm	IEC 61754-4	

Ethernet Pluggable Modules

SFP and SFP+ Ethernet modules are types of interface converters (or transceivers) that can be interchanged on a variety of network device ports to provide a gigabit interface. These compact transceivers are an improvement to the bulky GBIC (gigabit interface converter) transceivers. Pluggable modules are available for copper cable connections but are generally used for fiber connections.

Connector	Data Rate	Distance	Transceiver
SFP (Small Form-factor Pluggable)	155 Mbps to 4.25 Gbps	< 140 km	
SFP+ (Small Form-factor Pluggable Plus)	6 G to 10 G	< 80 km	

Industrial Wireless

3-1 Industrial Design Concepts

Introduction

Wireless failures at home or in the office will be an inconvenience until a replacement device is installed. Wireless network failures in industrial applications, however, can jeopardize the safety of onsite personnel, damage expensive machinery/equipment, and possibly translate into thousands of dollars per minute in production losses.

In addition to network redundancy, industrial operators must also assess the application environment for elements that can impact network performance, compromise device reliability, and lead to unplanned system downtime.

Industrial Hazards

Many industrial wireless applications, such as those for mining, railway, and oil & gas, are deployed in harsh environments and require the use of industrial-grade devices. While some environmental factors are obvious, such as extreme temperatures and moisture, there are other elements that are not so apparent but can also quickly disable an unprotected device. This chapter introduces several examples of interferences and environmental difficulties that are commonly seen in industrial applications.

Electrical Interference

Description

There are many different kinds of electrical interference in an industrial environment: electrostatic discharge accumulated on a human body, surge caused by indirect lightning strikes, and bursts generated by factory generators. Failing to properly design your system to protect against such interference can result in unstable communications, or sometimes your device could be permanently damaged, causing a complete shutdown of your system.

Industrial Solution

Industrial-grade devices are designed to protect internal components, and circuits are specially designed to be able to withstand different types of interference. In addition, the manufacturer will test the products to make sure they can operate reliably in harsh conditions so end-users can rest assured that the products will be more stable, more reliable, and have a longer life than non-industrial products.

Radiated Electromagnetic Interference

Description

Radiated electromagnetic interference is most obvious near an electrical substation. The high voltage and strong current flow cause a coupling effect with nearby electrical devices. If the devices are not properly protected, the internal circuits of the devices can wear out more quickly or be permanently damaged. The same effect can also be seen near factory generators and large transformers.

Industrial Solution

For industrial-grade devices, a metal casing and properly designed isolation can overcome such interference.

Flammable Gases

Description

In certain industries, the working environment could be permeated with flammable gas or dust, and to prevent electrical equipment from causing a fire or explosion, strict regulations are in place to define what kind of devices can be used in these extreme hazardous locations.

Industrial Solution

Different levels of anti-explosive design are stipulated. For example, an encapsulation design refers to a device that is airtight, or equivalent methods that prevent sparks from coming into contact with the surrounding flammable gases. An intrinsically safe design refers to a device that will not ignite flammable gases under any circumstances, even if there is direct contact between the device and gas.

Extreme Temperatures

Description

Under a hot summer sun, devices locked inside an outdoor cabinet can easily reach a temperature of 70°C (158°F), whereas a similar cabinet located at a high altitude could experience a temperature of -30°C (-22°F) on a cold winter night. Without a proper design, electronic devices inside the cabinet could either over-heat, or be unable to boot up if the temperature is too low.

Industrial Solution

Two major design focuses for industrial-grade products are heat-dissipation and low-temperature operation. By selecting the right components and mechanical design, engineers can ensure that devices will be able to operate reliably in both extremely hot and extremely low temperatures.

Shock and Vibration

Description

Wireless technology is widely used in mobile communications. However, for devices installed in vehicles with RJ45 connectors and/or standard power jacks, the continuous vibration of the vehicle can cause the connections to wiggle loose.

Industrial Solution

In order to provide a more reliable connection, industrial products designed for mobile communications often come with M12 connectors for data communication and terminal blocks for power and DI/DO connections.

3-2 Robust Wireless Concepts

Introduction

Ensuring the stability and reliability of wireless devices is critical for industrial deployments. With an industrial-grade hardware design, wireless devices can withstand higher levels of disturbance in harsh industrial environments. However, to further enhance the reliability of wireless network communication for mission-critical applications, an industrial-grade software design is also required. In this chapter, we discuss several major industrial concerns for wireless technology, and introduce the corresponding software solutions designed to answer those concerns.

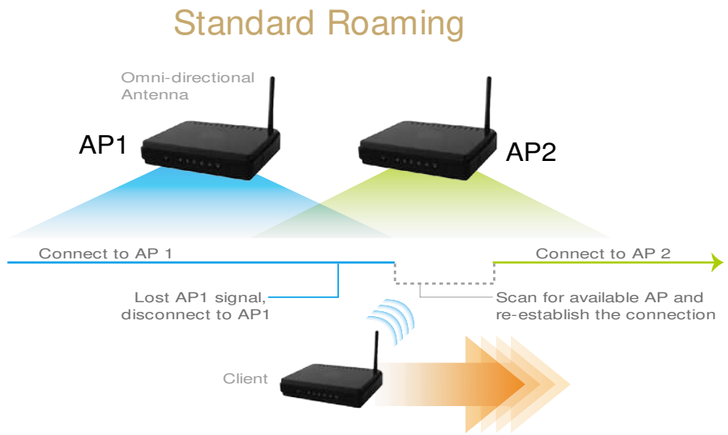
Concerns for Wireless Local Area Networks

Wi-Fi Mobile Communication: Roaming Break/Recovery Time

Recent advances in wireless technology have made it possible to use wireless for mission-critical mobile applications, such as railway (Train-to-Ground), buses (wayside AP communication), and factory AGV (Automated Guided Vehicle). The most crucial aspect of these mission-critical wireless applications is ensuring uninterrupted communication between wireless clients and access points (AP), even when the wireless client is roaming at considerable speeds between different APs. In this section, we introduce the differences between standard roaming, client-based roaming, and controller-based roaming.

Standard Roaming

The following figure illustrates the standard roaming mechanism for most commercial-grade wireless devices. The moving client device will stay connected with the current AP until signals get too weak to maintain further communication. It then disconnects from the current AP and starts scanning for a new AP with which to establish a connection. The standard roaming process can take 3 to 5 seconds, or more, to complete.

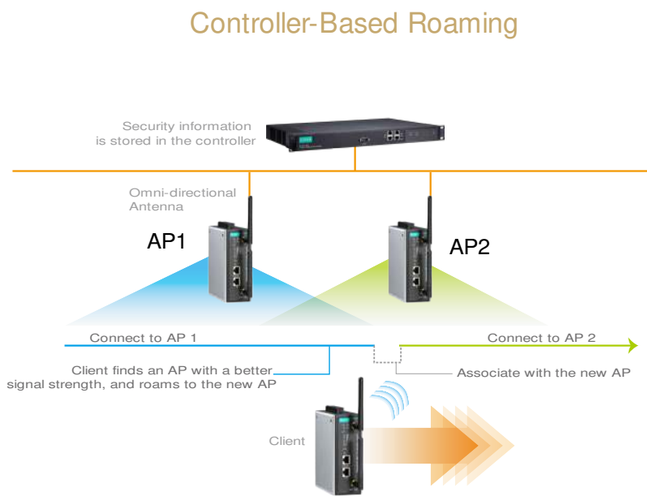


Client-Based Roaming

The following figure illustrates Moxa's proprietary client-based Turbo Roaming mechanism. The major difference from standard roaming, which takes at least 2 seconds to roam and connect to a different AP, is that the Moxa wireless client actively searches for APs with a stronger signal to connect to, without waiting for a complete disconnection. This preemptive type of roaming mechanism allows the client to successfully roam and connect to a different AP in a matter of milliseconds, which is several orders of magnitude faster than standard roaming.

Controller-Based Roaming

Moxa's preliminary Controller-Based Turbo Roaming is specifically designed for mission-critical applications that require highly-available wireless network communication. With the Wireless Access Controller, the mobile client can seamlessly roam between APs even when the highest security settings are applied. Furthermore, with advanced controller-based roaming, wireless client devices can roam between different network subnets, as well as provide IP mobility (Mobile IP).



Anti-Interference Techniques for Wireless Signals

The rapid advancement of wireless technology has lead to an increase in wireless deployments around the world, and in order to prevent Wi-Fi equipment from interfering with each other, many standards and mechanisms have been set up, including Collision Avoidance (CDMA-CA), Communication Control (RTS/CTS), and Inter Frame Spacing (IFS). However, even when these mechanisms are working perfectly, instability in wireless connections caused by a lack of 802.11 radio signals, or co-channel or adjacent-channel interferences can occur. Many approaches are available to overcome these problems.

Auto Channel Assessment and Adjustment

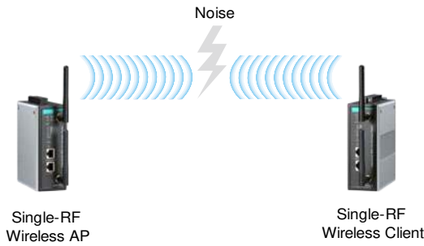
One commonly known approach is auto channel assessment and adjustment. This approach examines the current channel to determine its quality. When the current connection fails the examination, the device will automatically switch to a cleaner channel. However, channel adjustment and renegotiation can still result in packet loss and is unacceptable for latency-intolerant applications.

Dual Channel Wireless Redundancy

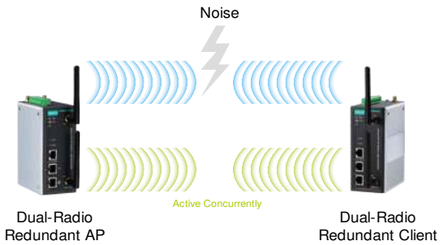
For mission-critical applications, higher reliability and stability is required. Zero-packet-loss wireless communication can be achieved, using concurrent dual-radio transmission, to provide highly reliable wireless connectivity for safety-critical applications, with benefits such as optimized data throughput, interference immunity, and latency-free transmissions.

The figures below illustrate the differences between standard radio communication and dual radio redundancy.

Traditional Single-RF Wireless Network



Concurrent Dual-Radio Technology



Redundant Wireless Bridges

Moxa's AeroLink Protection provides a reliable wireless bridge between two networks. With AeroLink Protection, a network has two or more wireless client nodes— with AeroLink Protection enabled— connected to a single access point. One serves as the active node, while the others are passive, backup nodes. If the active node stops sending or receiving data for any reason, AeroLink Protection completely restores the communication link within 300 ms, including the time required for network convergence and Address Resolution Protocol (ARP) updating.

Furthermore, the passive node can be connected to a different access point on a different frequency, providing frequency-level redundancy. If there is interference on the active channel, the backup path will transmit the data via a backup device and backup frequency. The technology uses the wireless radio's standard wireless protocol to detect that the link has been disconnected. As soon as a serious interruption is detected, Aerolink Protection takes action. The switchover to the passive node, and full network recovery, takes less than 300 ms.

AeroLink Protection not only guards against both device and wireless link failure, but also offers the ability to scale up your redundancy paths by adding additional hardware— providing even stronger protection for your wireless bridge network when needed. If you need extra-robust resistance to radio frequency interference, three or more different backup frequencies can be used when the 5 GHz range is available.

AeroLink Protection is a client radio feature that negotiates with every other AeroLink Protection-enabled client in range to set up the active node and passive nodes. Because AeroLink Protection works at a low level, layer 2, it is effectively invisible to higher network protocol levels, so it is easy to add an AeroLink Protection bridge to an existing network. The fast recovery time and simple setup allow users to form a reliable wireless bridge that will ensure their daily operations are uninterrupted, no matter what kind of failures occur.

Concerns for Wireless Wide Area Networks

Reliable and Consistent Cellular Connectivity

Cellular technology is commonly deployed in applications that involve long distance communication or device monitoring over a large area. Onsite troubleshooting and diagnosis can be a real problem due to the widely spread geographic distribution. Therefore, having a stable and reliable connection is a key concern for industrial operators. There are many different approaches to overcoming this problem, but some result in a high data transmission cost. Moxa's Guaranlink provides a 3-tiered checking mechanism that allows users to maintain a reliable connection but at the same time keep the data transmission cost to a minimum.

Standards

4-1 IEEE 802 Standards

IEEE 802.1
Bridging (networking) and Network Management

IEEE 802.3
Ethernet

IEEE 802.11
The WLAN standard was originally 1 Mbps and 2 Mbps, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.

IEEE 802.15
Wireless PAN

IEEE 802.16
Broadband Wireless Access (WiMAX certification)

IEEE 802.17
Resilient packet ring

IEEE 802.18
Radio Regulatory TAG

IEEE 802.19
Coexistence TAG

IEEE 802.20
Mobile Broadband Wireless Access

IEEE 802.21
Media Independent Handoff

IEEE 802.22
Wireless Regional Area Network

IEEE 802.23
Emergency Services Working Group

IEEE 802.24
Smart Grid TAG (November, 2012)

IEEE 802.3 Ethernet

IEEE 802.3a
10BASE2 10 Mbps (1.25 Mbytes/s) over thin Coax (a.k.a. thinnet or cheapernet)

IEEE 802.3b
10BROAD36

IEEE 802.3c
10 Mbps (1.25 Mbyte/s) repeater specs

IEEE 802.3d
Fiber-optic inter-repeater link

IEEE 802.3e
1BASE5 or StarLAN

IEEE 802.3i
10BASE-T 10 Mbps (1.25 Mbyte/s) over twisted pair

IEEE 802.3j
10BASE-F 10 Mbps (1.25 Mbyte/s) over optical fiber

IEEE 802.3u
100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbps (12.5 Mbyte/s) with auto-negotiation

IEEE 802.3x
Full Duplex and flow control; also incorporates DIX framing, so there's no longer a DIX/802.3 split

IEEE 802.3y
100BASE-T2 100 Mbps (12.5 Mbyte/s) over low quality twisted pair

IEEE 802.3z
1000BASE-X Gbps Ethernet over optical fiber at 1 Gbps (125 Mbyte/s)

IEEE 802.3ab
1000BASE-T Gbps Ethernet over twisted pair at 1 Gbps (125 Mbyte/s)

IEEE 802.3ac
Max frame size extended to 1522 bytes (to allow "Q-tag"). The Q-tag includes 802.1Q VLAN information and 802.1p priority information.

IEEE 802.3ad
Link aggregation for parallel links; since moved to IEEE 802.1AX.

IEEE 802.3ae
10 Gbps (1,250 Mbyte/s) Ethernet over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW

IEEE 802.3af
Power over Ethernet (12.95 W)

IEEE 802.3ah
Ethernet in the First Mile

IEEE 802.3ak
10GBASE-CX4 10 Gbps (1,250 Mbyte/s) Ethernet over twin-axial cable

IEEE 802.3an
10GBASE-T 10 Gbps (1,250 Mbyte/s) Ethernet over unshielded twisted pair (UTP

IEEE 802.3ap
Backplane Ethernet (1 and 10 Gbps (125 and 1,250 Mbyte/s) over printed circuit boards)

IEEE 802.3aq
10GBASE-LRM 10 Gbps (1,250 Mbyte/s) Ethernet over multimode fiber

IEEE 802.3as
Frame expansion

IEEE 802.3at
Power over Ethernet enhancements (25.5 W)

IEEE 802.3au
Isolation requirements for Power over Ethernet (802.3-2005/Cor 1)

IEEE 802.3av
10 Gbps EPON

IEEE 802.3aw
Fixed an error in an equation in the publication of 10GBASE-T (released as 802.3-2005/Cor 2)

IEEE 802.3az
Energy Efficient Ethernet

IEEE 802.3ba
40 Gbps and 100 Gbps Ethernet. 40 Gbps over 1 m backplane, 10 m Cu cable assembly (4x25 Gbit or 10x10 Gbit lanes) and 100 m of MMF and 100 Gbps up to 10 m of Cu cable assembly, 100 m of MMF or 40 km of SMF respectively

IEEE 802.3bc
Move and update Ethernet related TLVs (type, length, values), previously specified in Annex F of IEEE 802.1AB (LLDP) to 802.3.

IEEE 802.3bd
Priority-based Flow Control. An amendment by the IEEE 802.1 Data Center Bridging Task Group (802.1Qbb) to develop an amendment to IEEE Std 802.3 to add a MAC Control Frame to support IEEE 802.1Qbb Priority-based Flow Control.

IEEE 802.3.1
MIB definitions for Ethernet. It consolidates the Ethernet related MIBs present in Annex 30A&B, various IETF RFCs, and 802.1AB annex F into one master document with a machine readable extract (workgroup name was P802.3be).

IEEE 802.3bf
Provide an accurate indication of the transmission and reception initiation times of certain packets as required to support IEEE P802.1AS.

IEEE 802.3bg
Provide a 40 Gbps PMD which is optically compatible with existing carrier SMF 40 Gbps client interfaces (OTU3/STM-256/OC-768/40G POS).

IEEE 802.3bj
Define a 4-lane 100 Gbit/s backplane PHY for operation over links consistent with copper traces on "improved FR-4" (as defined by IEEE PIEEE 802.3ap or better materials to be defined by the Task Force) with lengths up to at least 1 m and a 4-lane 100 Gbit/s PHY for operation over links consistent with copper twinaxial cables with lengths up to at least 5 m.

IEEE 802.3bk
This amendment to IEEE Std IEEE 802.3 defines the physical layer specifications and management parameters for EPON operation on point-to-multipoint passive optical networks supporting extended power budget classes of PX30, PX40, PRX40, and PR40 PMDs.

IEEE 802.3bm
100G/40G Ethernet for optical fiber

IEEE 802.3bn
10G-EPON and 10GPASS-XR, passive optical networks over coax

IEEE 802.3bp
1000BASE-T1 – Gigabit Ethernet over a single twisted pair, automotive & industrial environments

IEEE 802.3bq
25G/40GBASE-T for 4-pair balanced twisted-pair cabling with 2 connectors over 30 m distances

IEEE 802.3br
Specification and Management Parameters for Interspersing Express Traffic

IEEE 802.3bs
200GbE (200 Gbit/s) over single-mode fiber and 400GbE (400 Gbit/s) over optical physical media

IEEE 802.3bt
Power over Ethernet enhancements up to 100 W using all 4 pairs balanced twisted-pair cabling, lower standby power and specific enhancements to support IoT applications (e.g. lighting, sensors, building automation).

IEEE 802.3bu
Power over Data Lines (PoDL) for single twisted-pair Ethernet (100BASE-T1)

IEEE 802.3bv
Gigabit Ethernet over plastic optical fiber (POF)

IEEE 802.3bw
100BASE-T1 – 100 Mbit/s Ethernet over a single twisted pair for automotive applications

IEEE 802.3by
Optical fiber, twinax and backplane 25 Gigabit Ethernet

IEEE 802.3bz
2.5GBASE-T and 5GBASE-T – 2.5 Gigabit and 5 Gigabit Ethernet over Cat-5/Cat-6 twisted pair

IEEE 802.3ca
100G-EPON – 25, 50, and 100 Gbit/s over Ethernet Passive Optical Networks

IEEE 802.3cb
2.5 Gbit/s and 5 Gbit/s Operation over Backplane

IEEE 802.3cc
25 Gbit/s over Single Mode Fiber

IEEE 802.3cd
Media Access Control Parameters for 50 Gbit/s and Physical Layers and Management Parameters for 50, 100, and 200 Gbit/s Operation

IEEE 802.3ce
Multilane Timestamping

IEEE 802.3c
YANG Data Model Definitions

IEEE 802.3cg
10 Mbit/s Single Twisted Pair Ethernet

IEEE 802.3ch
Multi-Gig Automotive Ethernet (2.5, 5, 10 Gbit/s) over 15 m with optional PoDL

IEEE 802.3ck
100, 200, and 400 Gbit/s Ethernet using 100 Gbit/s lanes

IEEE 802.3cm
400 Gbit/s over multimode fiber

IEEE 802.11 Wireless Local Area Network

IEEE 802.11a
54 Mbps, 5 GHz standard (1999, shipping products in 2001)

IEEE 802.11b
Enhancements to 802.11 to support 5.5 and 11 Mbps (1999)

IEEE 802.11c
Bridge operation procedures; included in the IEEE 802.1D standard (2001)

IEEE 802.11d
International (country-to-country) roaming extensions (2001)

IEEE 802.11e
Enhancements: QoS, including packet bursting (2005)

IEEE 802.11F
Inter-Access Point Protocol (2003) Withdrawn February 2006

IEEE 802.11g
54 Mbps, 2.4 GHz standard (backwards compatible with b) (2003)

IEEE 802.11h
Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)

IEEE 802.11i
Enhanced security (2004)

IEEE 802.11j
Extensions for Japan (2004)

IEEE 802.11k
Radio resource measurement enhancements (2008)

IEEE 802.11n
Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)

IEEE 802.11p
WAVE— Wireless Access for the Vehicular Environments (such as ambulances and passenger cars) (July 2010)

IEEE 802.11r
Fast BSS transition (FT) (2008)

IEEE 802.11s
Mesh Networking, Extended Service Set (ESS) (July 2011)

IEEE 802.11T
Wireless Performance Prediction (WPP)— test methods and metrics recommendation cancelled

IEEE 802.11u
Improvements related to HotSpots and 3rd party authorization of clients, e.g, cellular network offload (February 2011)

IEEE 802.11v
Wireless network management (February 2011)

IEEE 802.11w
Protected Management Frames (September 2009)

IEEE 802.11y
3650 to 3700 MHz Operation in the U.S. (2008)

IEEE 802.11z
Extensions to Direct Link Setup (DLS) (September 2010)

IEEE 802.11aa
Robust streaming of Audio Video Transport Streams (June 2012)

IEEE 802.11ac
Very High Throughput 5 GHz (2013)

IEEE 802.11ad
Very High Throughput 60 GHz (December 2012)

IEEE 802.11ae
Prioritization of Management Frames (March 2012

IEEE 802.11af
TV Whitespace (February 2014)

IEEE 802.11ah
Sub-1 GHz license exempt operation (December 2016)

IEEE 802.11ai
Fast Initial Link Setup (December 2016)

IEEE 802.11aj
China Millimeter Wave (February 2018)

IEEE 802.11ak
General Links (June 2018)

IEEE 802.11aq
Pre-association Discovery (July 2018)

4-2 Safety and Certifications

ATEX Directive
There are two ATEX directives: the ATEX 95 equipment directive 94/9/EC is for the manufacturer, and the ATEX 137 workplace directive 99/92/EC is for the user of the equipment. Areas classified into zones (0, 1, 2 for gas-vapor-mist and 20, 21, 22 for dust) must be protected.

EN 300 220
Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD) for the radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW.

EN 300 328
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems for the data transmission equipment operating in the 2.4 GHz ISM band and using wide band modulation techniques. (Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive.)

EN 300 440
Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range.

EN 301 489
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services.

EN 301 489-1
Part 1: Common technical requirements

EN 301 489-3
Part 3: Specific conditions for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 40 GHz.

EN 301 489-7
Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS.)

EN 301 489-9
Part 9: Specific conditions for wireless microphones, similar Radio Frequency (RF) audio link equipment, cordless audio and in-ear monitoring devices.

EN 301 489-17
Part 17: Specific conditions for Broadband Data Transmission Systems (2.4 GHz and 5 HGz).

EN 301 489-24
Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA and E-UTRA) for Mobile and portable (UE) radio and ancillary equipment.

EN 301 511
Global System for Mobile communications (GSM); Harmonized EN for mobile stations in the GSM 900 and GSM 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC).

EN 301 893
Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN. (Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive.)

EN 50371
Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz) — General Public.

EN 50385
Product Standard to Demonstrate the Compliance of Radio Base Stations and Fixed Terminal Stations for Wireless Telecommunication Systems with the Basic Restrictions or the Reference Levels Related to Human Exposure to Radio-Frequency Electromagnetic Fields (110 MHz to 40 GHz) — General Public.

EN 50155
Railway applications— Electronic equipment used on rolling stock.

EN 50121
Railway applications— Electromagnetic compatibility.

EN 50121-1
Part 1: General

EN 50121-2
Part 2: Emission of the Whole Railway System to the Outside World

EN 50121-3-1
Part 3-1: Rolling Stock— Train and Complete Vehicle

EN 50121-3-2
Part 3-2: Rolling Stock— Apparatus

EN 50121-4
Part 4: Emission and Immunity of the Signalling and Telecommunic-ations Apparatus

EN 55032 / 55035
Information technology equipment; Radio disturbance characteristics; Limits and methods of measurement.

EN 62368-1
Information technology equipment— Safety, Part 1: General requirements.

IEC 61000-4
Part 4: Electromagnetic Compatibility; Testing and Measurement Techniques Package.

IEC 61000-4-2
Part 4-2: Electrostatic discharge immunity test (ESD)

IEC 61000-4-3
Part 4-3: Radiated, radio-frequency, electromagnetic field immunity test (RS).

IEC 61000-4-4
Part 4-4: Electrical fast transient/burst immunity test (EFT).

IEC 61000-4-5
Part 4-5: Surge immunity test (Surge).

IEC 61000-4-6
Part 4-6: Immunity to conducted disturbances, induced by radio-frequency fields (CS).

IEC 61000-4-8
Part 4-8: Power frequency magnetic field immunity test (PFMF).

IEC 61000-4-12
Part 4-12: Oscillatory waves immunity test (Ring-Wave).

EN 61000-6
Part 6: Electromagnetic Compatibility— Generic standards.

EN 61000-6-1
Part 6-1: Generic standards— Immunity for residential, commercial and light-industrial environments.

EN 61000-6-2
Part 6-2: Generic standards— Immunity for industrial environments.

EN 61000-6-3
Part 6-3: Generic standards— Emission standard for residential, commercial, and light-industrial environments.

EN 61000-6-4
Part 6-4: Generic standards— Emission standard for industrial environments.

IEC 62479
Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz). Its superseded standard is EN 50371.

IEC 62443
Part 4-1: Security for industrial automation and control systems. Secure product development lifecycle requirements

Part 4-2: Technical security requirements for IACS components

FCC Part 15
FCC Part 15 regulates unlicensed radio-frequency transmissions. The related radio frequency devices include receivers, computers, and other commercially assembled products that can emit RF. They can be intentional, unintentional, or incidental radiators.

FCC Part 15 Subpart A
Subpart A contains a general provision that devices may not cause interference and must accept interference from other sources.

FCC Part 15 Subpart B
US limits and methods of measurement of radio disturbance, measuring radio waves accidentally emitted from devices not specifically designed to emit radio waves (unintentional), both directly (radiated) and indirectly (conducted).

FCC Part 15 Subpart C to H
These subparts handle unlicensed devices specifically designed to emit radio waves (so-called “intentional”), such as wireless LAN, cordless telephones, low-power broadcasting, walkie-talkies, etc.

FCC Part 22
FCC Part 22 regulates public mobile services, such as air-ground radiotelephone, commercial aviation air ground service, cellular, offshore radiotelephone service, rural radiotelephone service, and commercial paging.

FCC Part 24
FCC Part 24 regulates Personal Communications Services, PCS (Narrowband PCS 901-902, 930-931, 940-941 MHz; Broadband PCS 1850-1990 MHz).

UL 62368-1
General Requirements for Information Technology Equipment (ITE). This standard is applicable to mains-powered or battery-powered information technology equipment.

UL Class 1, Division 2
According to ANSI/NFPA areas description, Class I, Div. 2 means the area where ignitable concentrations of flammable gases, vapors, or liquids are present within the atmosphere under abnormal operating conditions. UL has a series of certification documents for such a hazardous location.

Industrial Wireless AP/Bridge/Client




		Single-Radio Wireless AP/Bridge/Client		Single-Radio Wireless AP/Client	Single-Radio Wireless Client
		AWK-4131A	AWK-3131A	AWK-1131A	AWK-1137C
WLAN	Operation Mode	AP, Client, Master, Slave, Client Router, Sniffer	AP, Client, Master, Slave, Client Router, Sniffer	AP, Client, Sniffer	Client, Slave Client Router, Sniffer
	IEEE 802.11 Standards	a/b/g/n	a/b/g/n	a/b/g/n	a/b/g/n
	Number of RF modules	1	1	1	1
Interfaces	Number of Antenna Connectors	2 (2x2 MIMO)	2 (2x2 MIMO)	2 (2x2 MIMO)	2 (2x2 MIMO)
	Antenna Connector Type	N-type (female)	RP-SMA (female)	RP-SMA (female)	RP-SMA (female)
	Total Number of LAN Ports	1	1	1	2
	LAN Port Type	Waterproof RJ45	RJ45	RJ45	RJ45
	LAN Port Speed	10/100/1000BaseT(X)	10/100/1000BaseT(X)	10/100/1000BaseT(X)	10/100 BaseT(X)
	RS-232 Console Port	1, Waterproof RJ45	1, RJ45	1, RJ45	–
	DB9 RS-232/422/485 Serial Port	–	–	–	1
	DI/DO	✓	✓	–	–
	DI/DO Connector Type	M12 (female 8-pin A-coded)	10-pin terminal block	–	–
Housing Protection	IP-rating	IP68	IP30	IP30	IP30
Standards and Certifications	Hazardous Location	–	UL/cULCI D2, ATEX Zone2, IECEx	–	–
	EMC	EN 61000-6-2/6-4	EN 61000-6-2/6-4	EN 55032/24	EN 55032/55024 EN 61000-6-2/6-4

Cellular IP Gateways and Cellular Routers






		Cellular IP Gateways				Cellular Routers	
		OnCell G3151 OnCell G3251	OnCell G3150-HSPA	OnCell G3111-HSPA OnCell G3151-HSPA	OnCell G3150A-LTE	OnCell G3470A-LTE	OnCell 5104-HSPA
Cellular Interface	Standards	GSM/GPRS	GSM/GPRS/EDGE/UMTS/HSPA	GSM/GPRS/EDGE/UMTS/HSPA	GSM/GPRS/EDGE/UMTS/ HSPA/LTE	GSM/GPRS/EDGE/UMTS/ HSPA/LTE	GSM/GPRS/EDGE/UMTS/HSPA
	4G Band Options	–	–	–	EU model: 800/900/1800/2100/2600 MHz (B1/B3/B7/B8/B20) US Model: 700/850/ AWS/1900/2100/2600 MHz (B2/B4/B5/B13/B17/B25)	EU model: 2100/1800/ 2600/900/800 MHz (B1/B3/B7/B8/B20) US model: 1900/AWS/ 850/700 MHz (B2/B4/B5/B13/ B17/B25)	–
	LTE Data Rate	–	–	–	20 MHz bandwidth: 100 Mbps DL, 50 Mbps UL 10 MHz bandwidth: 50 Mbps DL, 25 Mbps UL	20 MHz bandwidth: 100 Mbps DL, 50Mbps UL 10 MHz bandwidth: 50 Mbps DL, 25Mbps UL	–
	3G Band Options	–	800/850/AWS/1900/2100 MHz	800/850/900/1900/2100 MHz	EU model: 2100/1900/850/800/900 MHz US Model: 2100/1900/ AWS/850/900 MHz	EU model: 800/850/900/ 1900/2100 MHz US model: 850/900/AWS/ 1900/2100 MHz	800/850/AWS/1900/2100 MHz
	HSPA Data Rate	–	14.4 Mbps DL, 5.76 Mbps UL	14.4 Mbps DL, 5.76 Mbps UL	42 Mbps DL, 5.76 Mbps UL	42 Mbps DL, 5.76 Mbps UL	14.4 Mbps DL, 5.76 Mbps UL
	2G Band Options	850/900/1800/1900 MHz	850/900/1800/1900 MHz	850/900/1800/1900 MHz	850/900/1800/1900 MHz	850/900/1800/1900 MHz	850/900/1800/1900 MHz
Ethernet Interface	Number of Ports	1 (10/100M, RJ45)	1 (10/100M, RJ45)	1 (10/100M, RJ45)	1 (10/100M, RJ45)	–	1 (10/100M, RJ45)
SIM Interface	Number of SIMs	1	1	1	2	2	2
Serial Interface	Number of Ports	OnCell G3151: 1 OnCell G3251: 2	1	1	1	–	–
	Serial Standards	OnCell G3151/G3251: RS-232/422/485	OnCell G3150-HSPA: RS-232/422/485	OnCell G3111-HSPA: RS-232 OnCell G3151-HSPA: RS-232/422/485	RS-232/422/485	–	–

Wireless Device Servers

		NPort W2150A NPort W2150A-T	NPort W2250A NPort W2250A-T
Wireless Interface	RF Standard	802.11a/b/g/n	
	Frequency Band	2.4 GHz or 5 GHz	
	Max. Transmission Rate	150 Mbps	
	Encryption	128-bit TKIP/AES-CCMP EAP-TLS/TTLS, PEAP, LEAP, etc.	
	Network Topology	AP-Client	
	Transmission Distance	100 m	
LAN Interface	Ethernet Port	1 x 10/100 Mbps (RJ45)	
Serial Interface	Number of Ports	1	2
	Serial Standards	1	
	Connector		
	Serial Communication Parameters	Data Bits: 5, 6, 7, 8; Stop Bits: 1, 1.5, 2; Parity: None, Even, Odd, Space, Mark	
	Flow Control	RTS/CTS, XON/XOFF	
	Baudrate	50 bps to 921.6 kbps	

Wireless Embedded Computers

		UC-2100	UC-3100	UC-5100	UC-8100-ME-T	UC-8540/8580
Physical Characteristics	Installation	DIN-rail, wall mounting	DIN-rail, wall mounting	DIN-rail, wall mounting	DIN-rail, wall mounting	Wall mounting
	Dimensions	57 x 80 x 30.8 mm	UC-3101: 128.5 x 89.1 x 26 mm UC-3111, UC-3121: 128.5 x 89.1 x 41 mm	57 x 136 x 100 mm	141 x 125.6 x 54.8 mm	UC-8540: 190 x 120 x 125 mm UC-8580: 270 x 134 x 88 mm
	Operating Temperature	-10 to 70°C	-30 to 70°C	Standard models: -10 to 60°C Wide-temperature models: • With LTE accessory: -40 to 70°C • With Wi-Fi accessory: -10 to 70°C	-40~70°C	Standard models: -25 to 55°C Wide-temperature models: • With LTE accessory: -40 to 70°C • With Wi-Fi accessory: -10 to 70°C
Computer	CPU	TI AM335x Cortex-A8 600 MHz	TI AM335x Cortex-A8 1 GHz	TI AM335x Cortex-A8 1 GHz	TI AM335x Cortex-A8 1 GHz	NXP LS1021A Cortex-A7 dual core 1GHz
	RAM	256 MB	512 MB	512 MB	512 MB/1 GB	1 GB
	eMMC	8 GB	4 GB	8 GB	8 GB	4GB / 8GB
Wireless Interface	Cellular Standard	LTE CAT.1	LTE CAT.1	LTE CAT.1	LTE CAT 3	LTE CAT.4/CAT.6
	SIM Slot	2	2	2	1	2 for each module Up to 8
	Wi-Fi Standard	802.11 a/b/g/n/ac	802.11 a/b/g/n	802.11 a/b/g/n/ac	–	802.11 a/b/g/n/ac
	GPS	–	–	–	v	v
Interface	Serial Ports	–	Up to 2 (supports 1 additional CAN port)	4 (supports 2 additional CAN ports)	2	1
	LAN Ports	1	2	2	2	2
	DI	–	–	4	–	UC-8580: 3
	DO	–	–	4	–	UC-8580: 3
	USB	–	1	1	1	1
Storage	MicroSD Slot	1	–	–	–	–
	SD Slot	–	Up to 1	1	1	–
	mSATA	–	–	–	–	1
Security	TPM	Optional	Optional	Optional	Optional	–

Smart Remote I/O




		ioLogik 2512-WL1	ioLogik 2542-WL1	ioLogik 2512-HSPA	ioLogik 2542-HSPA
Input/Output	Digital Input Channels	8	–	8	–
	Configurable DIO Channels	8	12	8	12
	Analog Input Channels	–	4	–	4
Cellular	GSM/GPRS/EDGE	–	–	✓	✓
	UMTS/HSPA	–	–	✓	✓
Ethernet	Port (Connector)	4 (RJ45)	4 (RJ45)	4 (RJ45)	4 (RJ45)
	Speed	10/100 Mbps	10/100 Mbps	10/100 Mbps	10/100 Mbps
	Industrial Protocols	CGI commands, Modbus TCP Client (Master), Modbus TCP Server (Slave), Moxa AOPC (Active Tag), MXIO Library, RESTful API, SNMPv1/v2c Trap, SNMPv1/v2c/v3			
	Management	BootP, IPv4, SMTP, TCP/IP	BootP, IPv4, SMTP, TCP/IP	BootP, IPv4, SMTP, TCP/IP, DHCP	BootP, IPv4, SMTP, TCP/IP, DHCP
Serial	Port (Connector)	2 (RJ45)	2 (RJ45)	2 (RJ45)	2 (RJ45)
	Interface	RS-232/422/485	RS-232/422/485	RS-232/422/485	RS-232/422/485
	Industrial Protocols	Modbus/RTU (master/gateway), serial tunnel mode (client/server)			
Environmental Limits	Standard Operating Temperature	-10 to 60°C	-10 to 60°C	-10 to 60°C	-10 to 60°C
	Wide Operating Temperature	-30 to 70°C	-30 to 70°C	-30 to 70°C	-30 to 70°C
	Storage Temperature	-40 to 85°C	-40 to 85°C	-40 to 85°C	-40 to 85°C
	Ambient Relative Humidity	5 to 95% (non-condensing)	5 to 95% (non-condensing)	5 to 95% (non-condensing)	5 to 95% (non-condensing)
Software	Programmability	Click&Go Plus	Click&Go Plus	Click&Go Plus	Click&Go Plus
	Active OPC Server	✓	✓	✓	✓
	MXIO	✓	✓	✓	✓
	Configuration Utility	✓	✓	✓	✓
Standards and Certifications	Safety	UL 508	UL 508	UL 508	UL 508
	EMI	CISPR 22, FCC Part 15B Class A	CISPR 22, FCC Part 15B Class A	CISPR 22, FCC Part 15B Class A	CISPR 22, FCC Part 15B Class A
	EMS	IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8			
	Shock	IEC 60068-2-27	IEC 60068-2-27	IEC 60068-2-27	IEC 60068-2-27
	Vibration	IEC 60068-2-6	IEC 60068-2-6	IEC 60068-2-6	IEC 60068-2-6
	Hazardous Location	Class I Division 2; ATEX Zone 2	Class I Division 2; ATEX Zone 2	Class I Division 2; ATEX Zone 2	Class I Division 2; ATEX Zone 2

Glossary

2G
2G: GSM, 2.5G: GPRS, 2.75G: EDGE

3G
3G: UMTS/CDMA2000, 3.5G: HSPA/EV-DO, 3.75G: HSPA+

4G
Pre-4G: LTE/WiMax, 4G: LTE-A/WirelessMAN-Advanced

Ad hoc network (wireless)
An ad hoc network is characterized by temporary, short-lived relationships between nodes. Ad hoc wireless networks do not rely on preexisting infrastructures and are used for applications such as wireless bridging for data forwarding.

AES
Advanced Encryption Standard— AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AP
Access Point— An AP is an 802.11 device that is wired to the backbone network to provide wireless access to other 802.11 devices.

APN
Access Point Name— APN is generally the name of a gateway between a GPRS (or 3G) mobile network and Packet Data Network, usually the public Internet.

ATO
Automatic Train Operation— ATO is a safety system used for the operation of train and subway systems.

BER
Bit Error Rate or Bit Error Ratio— BER is the percentage of bits that have errors relative to the total number of bits received in a transmission, usually expressed as ten to a negative power. For example, a transmission might have a BER of 10, meaning that of 1,000,000 bits transmitted, one bit was in error.

BPSK
Binary Phase Shift Keying— BPSK is the simplest form of PSK and uses a type of phase modulation with 2 distinct carrier phases separated by 180° to signal ones and zeros to encode bits of data.

BSS
Basic Service Set— A BSS is a building block of 802.11 networks. A BSS is a set of stations that are logically associated with each other.

BSSID
Basic Service Set Identifier— A BSSID is a 48-bit identifier in the frame header used by all stations in a BSS for identification.

CBTC
Communication-based Train Control

CCK
Complementary Code Keying— CCK is an 802.11b modulation scheme adopted in 1999 to gain higher data rates (> 2 Mbps) at the expense of shorter transmission distance.

CRC
Cyclic Redundancy Check— A CRC is a mathematical checksum that can be used to detect data corruption in transmitted frames. The CRC is a linear hash function, and should not be used for data security assurance.

CDMA2000 Code Division Multiple Access 2000— CDMA2000 (also known as IMT Multi-Carrier) is a family of 3G mobile technology standards, which use CDMA channel access to send voice, data, and signaling data between mobile phones and cell sites.

CMS
Changeable Message Signs— CMS are digital message displays placed at roadside or on overhead gantries to inform drivers of road conditions and/or emergencies.

CSD
Circuit Switched Data— CSD is the original form of data transmission developed for the time division multiple access (TDMA)-based mobile phone systems like Global System for Mobile Communications (GSM). CSD uses a single radio time slot to deliver 9.6 kbps data transmission to the GSM Network and Switching Subsystem where it could be connected through the equivalent of a normal modem to the Public Switched Telephone Network (PSTN) allowing direct calls to any dial-up service.

CSMA/CA
Carrier Sense Multiple Access with Collision Avoidance— CSMA/CA is a CSMA method that tries to avoid simultaneous access (collsions) by deferring access to the medium. 802.11 and AppleTalk's LocalTalk are two protocols that use CSMA/CA.

CTS
Clear to Send— CTS is the frame type used to acknowledge receipt of a Request to Send and the second component used in the RTS-CTS clearing exchange used to prevent interference from hidden nodes.

DDNS
Dynamic DNS— DDNS is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DNS configuration of its configured hostnames, addresses, or other information.

DSSS
Direct-Sequence Spread Spectrum— DSSS is a transmission technique that spreads a signal over a wide frequency band for transmission. At the receiver, the widespread signal is correlated into a stronger signal; in addition, any narrowband noise is spread widely. Most of the 802.11-installed bases at 2 Mbps and 11 Mbps are composed of direct-sequence interfaces.

DTIM
Delivery Traffic Indication Message— A DTIM is a type of traffic indication message (TIM), which indicates the presence of data buffered on the access point. DTIMs are sent by beacon frames periodically by an access point to synchronize a wireless network and are used to indicate that broadcast and multicast frames buffered by the access point will be delivered shortly.

2G
2G: GSM, 2.5G: GPRS, 2.75G: EDGE

3G
3G: UMTS/CDMA2000, 3.5G: HSPA/EV-DO, 3.75G: HSPA+

4G
Pre-4G: LTE/WiMax, 4G: LTE-A/WirelessMAN-Advanced

Ad hoc network (wireless)
An ad hoc network is characterized by temporary, short-lived relationships between nodes. Ad hoc wireless networks do not rely on preexisting infrastructures and are used for applications such as wireless bridging for data forwarding.

AES
Advanced Encryption Standard— AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AP
Access Point— An AP is an 802.11 device that is wired to the backbone network to provide wireless access to other 802.11 devices.

APN
Access Point Name— APN is generally the name of a gateway between a GPRS (or 3G) mobile network and Packet Data Network, usually the public Internet.

ATO
Automatic Train Operation— ATO is a safety system used for the operation of train and subway systems.

BER
Bit Error Rate or Bit Error Ratio— BER is the percentage of bits that have errors relative to the total number of bits received in a transmission, usually expressed as ten to a negative power. For example, a transmission might have a BER of 10, meaning that of 1,000,000 bits transmitted, one bit was in error.

BPSK
Binary Phase Shift Keying— BPSK is the simplest form of PSK and uses a type of phase modulation with 2 distinct carrier phases separated by 180° to signal ones and zeros to encode bits of data.

BSS
Basic Service Set— A BSS is a building block of 802.11 networks. A BSS is a set of stations that are logically associated with each other.

BSSID
Basic Service Set Identifier— A BSSID is a 48-bit identifier in the frame header used by all stations in a BSS for identification.

CBTC
Communication-based Train Control

CCK
Complementary Code Keying— CCK is an 802.11b modulation scheme adopted in 1999 to gain higher data rates (> 2 Mbps) at the expense of shorter transmission distance.

CRC
Cyclic Redundancy Check— A CRC is a mathematical checksum that can be used to detect data corruption in transmitted frames. The CRC is a linear hash function, and should not be used for data security assurance.

CDMA2000 Code Division Multiple Access 2000— CDMA2000 (also known as IMT Multi-Carrier) is a family of 3G mobile technology standards, which use CDMA channel access to send voice, data, and signaling data between mobile phones and cell sites.

CMS
Changeable Message Signs— CMS are digital message displays placed at roadside or on overhead gantries to inform drivers of road conditions and/or emergencies.

CSD
Circuit Switched Data— CSD is the original form of data transmission developed for the time division multiple access (TDMA)-based mobile phone systems like Global System for Mobile Communications (GSM). CSD uses a single radio time slot to deliver 9.6 kbps data transmission to the GSM Network and Switching Subsystem where it could be connected through the equivalent of a normal modem to the Public Switched Telephone Network (PSTN) allowing direct calls to any dial-up service.

CSMA/CA
Carrier Sense Multiple Access with Collision Avoidance— CSMA/CA is a CSMA method that tries to avoid simultaneous access (collsions) by deferring access to the medium. 802.11 and AppleTalk's LocalTalk are two protocols that use CSMA/CA.

CTS
Clear to Send— CTS is the frame type used to acknowledge receipt of a Request to Send and the second component used in the RTS-CTS clearing exchange used to prevent interference from hidden nodes.

DDNS
Dynamic DNS— DDNS is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DNS configuration of its configured hostnames, addresses, or other information.

DSSS
Direct-Sequence Spread Spectrum— DSSS is a transmission technique that spreads a signal over a wide frequency band for transmission. At the receiver, the widespread signal is correlated into a stronger signal; in addition, any narrowband noise is spread widely. Most of the 802.11-installed bases at 2 Mbps and 11 Mbps are composed of direct-sequence interfaces.

DTIM
Delivery Traffic Indication Message— A DTIM is a type of traffic indication message (TIM), which indicates the presence of data buffered on the access point. DTIMs are sent by beacon frames periodically by an access point to synchronize a wireless network and are used to indicate that broadcast and multicast frames buffered by the access point will be delivered shortly.

EAP
Extensible Authentication Protocol— The EAP is a framework authentication protocol used by 802.1X to provide network authentication. Authentication itself is delegated to sub-protocols called methods.

EDGE
Enhanced Data-rates for GSM Evolution— EDGE, also known as Enhanced GPRS (EGPRS), IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution, is a digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM.

EFT
Electrical Fast Transient— An EFT is a short-lived burst of energy in a system caused by a sudden change of state. The European standard for EFT testing is EN-61000-4-4. The U.S. equivalent is IEEE C37.90.

EIRP
Effective Isotropic Radiated Power— An antenna system will have a footprint over which the radio waves are distributed. The power inside the footprint is called the effective isotropic radiated power.

EMC
Electromagnetic compatibility— EMC is the branch of electrical sciences that studies the unintentional generation, propagation, and reception of electromagnetic energy with reference to unwanted effects (Electromagnetic interference, or EMI) that such energy may induce.

EMI
Electromagnetic Interference— EMI, also called radio-frequency interference (RFI) when in high frequency or radio frequency, is the level of emmitted electromagnatic interference to the surrounding environment.

EMS
Electromagnetic Susceptibility— EMS is the inability of a device, circuit, or system to perform without degradation in the presence of an electromagnetic disturbance.

ESS
Extended Service Set— ESS is a set of two or more interconncted BSSs that appear as a single BSS, using a common SSID but perhaps different channels.

ETSI
European Telecommunications Standards Institute— ETSI is a multinational standardization body with regulatory and standardization authority over much of Europe.

EV-DO
Enhanced Voice-Data Optimized or Enhanced Voice-Data Only— EVDO, EV, or Ev-DO is a telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access.

FCC
Federal Communications Commission— The FCC Rules in Title 47 of the Code of Federal Regulations govern telecommunications in the United States. Wireless LANs must comply with Part 15 of the FCC rules, which are written specifically for RF devices.

FER
Frame Error Rate— FER is similar to bit error rate (BER), but is measured as a fraction of packets with errors.

FHSS
Frequency Hopping Spread Spectrum— FHSS is a technique that uses a method of transmitting radio signals by rapidly switching a carrier among many frequency channels to reduce interference.

GPRS
General Packet Radio Service— GPRS is a packet-oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications (GSM).

GSM
Global System for Mobile Communications, originally Groupe Spécial Mobile— GSM is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones.

GTK
Group Transient Key— GTK is derived from the group master key by combining with the group random number; the GTK is used to derive the group key hierarchy, which includes keys used to protect broadcast and multicast data.

GuaranLink
GuaranLink is Moxa's proprietary technology to ensure a more reliable and consistent cellular connectivity.

HSDPA
High Speed Downlink Packet Access— Downlink speed: 14.4 Mbps

HSPA
High Speed Packet Access— HSPA is a combination of two mobile telephony protocols, High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA), that improves the performance of existing 3rd generation mobile telecommunication networks utilizing the W-CDMA protocols. Uplink speed: 5.76 Mbps / Downlink speed: 14.4 Mbps

HSUPA
High Speed Uplink Packet Access— HSUPA is a 3G mobile teoephony protocol in the HSPA family with uplink speeds of up to 5.76 Mbps; HSUPA is also known as Enhanced Uplink (EUL).

IBSS
Independent Basic Service Set— An IBSS is an 802.11 network without a controlling access point.

IEEE
Institute of Electrical and Electronics Engineers— IEEE is a professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence. It has more than 400,000 members in more than 160 countries, about 51.4% of whom reside in the United States.

HSPA
High Speed Packet Access— HSPA is a combination of two mobile telephony protocols, High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA), that improves the performance of existing 3rd generation mobile telecommunication networks utilizing the W-CDMA protocols. Uplink speed: 5.76 Mbps / Downlink speed: 14.4 Mbps

HSUPA
High Speed Uplink Packet Access— HSUPA is a 3G mobile teoephony protocol in the HSPA family with uplink speeds of up to 5.76 Mbps; HSUPA is also known as Enhanced Uplink (EUL).

IBSS
Independent Basic Service Set— An IBSS is an 802.11 network without a controlling access point.

IEEE
Institute of Electrical and Electronics Engineers— IEEE is a professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence. It has more than 400,000 members in more than 160 countries, about 51.4% of whom reside in the United States.

IPsec
Internet Protocol Security— IPsec is a technology protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

Isolation transformers
Isolation transformers are generally composed of two separate windings with a magnetic shield between these windings to offer noise control. The main benefit offered by isolation transformers is the input-to-output isolation, where the output circuit can be re-grounded and isolated from input or other ground noise sources. This isolation can also be useful where Ground Potential Rise protection cannot be afforded by normal bonding procedures.

ITS
Intelligent Transportation Systems

ITU
International Telecommunication Union

LLC
Logical Link Control— LLC is an IEEE specification that allows further protocol multiplexing over Ethernet. 802.11 frames carry LLC-encapsulated data units.

LTE
Long Term Evolution— LTE is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using a different radio interface together with core network improvements.

M2M
Machine to machine— M2M refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. M2M uses a device (such as a sensor or meter) to capture an event (temperature, inventory level, etc.), which is relayed through a network (wireless, wired, or hybrid) to an application (software program), that translates the captured event into meaningful information (for example, items need to be restocked).

MAC (MAC address)
Media Access Control— MAC addresses are unique identifiers assigned to network interfaces for communications on the physical network segment, and are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

MIB
Management Information Base— A MIB is a virtual database used for managing the entities in a communications network. Most often associated with the Simple Network Management Protocol (SNMP), the term is also used more generically in contexts such as in the OSI/ISO network management model. While intended to refer to the complete collection of management information available on an entity, it is often used to refer to a particular subset, more correctly referred to as a MIB-module.

MIMO
Multiple-Input/Multiple-Output— MIMO is the use of multiple antennas at both the transmitter and receiver to improve communication performance. It is one of several forms of smart antenna technology. Note that the terms input and output refer to the radio channel carrying the signal, not to the devices having antennas.

OCM
OnCell Central Manager— OCM is Moxa's proprietary technology that allows devices attached to private cellular networks to be accessed over the web.

OFDM
Orthogonal Frequency Division Multiplexing— OFDM is a technique that splits a wide frequency band into a number of narrow frequency bands and inverse multiplexes data across the subchannels. 802.11a and 802.11g are based on OFDM. 802.11n and 802.11ac use MIMO to transmit multiple OFDM data streams.

OSI layers (OSI model)
Open Systems Interconnection— The OSI model (ISO/IEC 7498-1) is maintained by the International Organization for Standardization. It is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it.

PER
Packet Error Rate— PER is similar to bit error rate (BER), but is measured as a fraction of packets with errors.

PHY
PHY is the common IEEE abbreviation for the physical layer of the OSI model.

RADIUS
Remote Authenticated Dial-In User Service— RADIUS is a protocol used to authenticate dial-in users. It has become more widely used because of 802.1X authentication, and is the most common type of authentication server used in 802.1X systems.

RIP
Routing Information Protocol— RIP is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15.

RSSI
Received Signal Strength Indicator— RSSI is a measurement of the power present in a received radio signal.

RF
Radio frequency

Surge
Also referred to as "spikes," electrical surges are sudden, brief rises in voltage and/or current to a connected load. Standard electrical equipment operating at 120 volts can be damaged by surges of 500 volts or greater.

SSID
Service Set Identity— An SSID is a string used to identify an extended service set. Typically, the SSID is a recognizable character string for the benefit of users.

TD-LTE
Time-Division Long-Term Evolution— TD-LTE, also referred to as Long-Term Evolution Time-Division Duplex (LTE-TDD), is a 4-G mobile-telecommunications technology/standard co-developed by several major Chinese telecommunication companies.

TIM
Traffic Indication Map— A TIM is a bitmap element to indicate to any sleeping listening stations if the Access Point (AP) has any buffered frames present for it. Because stations should listen to at least one beacon before the listen interval, the AP periodically sends this bitmap on its beacons as an information element.

TKIP
Temporal Key Integrity Protocol— TKIP is one of the improved encryption protocols in 802.11i. TKIP uses the fundamental operations of WEP with new keying and integrity check mechanisms to offer additional security.

Turbo Roaming
Turbo Roaming is Moxa's proprietary technology that is capable of providing seamless millisecond-level handoffs for 802.11 roaming.

UMTS
Universal Mobile Telecommunications System— UMTS is a third generation mobile cellular system for networks based on the GSM standard, which standard. It is developed and maintained by the 3GPP (3rd Generation Partnership Project).

VPN
Virtual Private Network— A VPN enables a host computer to send and receive data across public networks, such as the Internet, with all the functionality, security, and management policies of the private network.

VRRP
Virtual Router Redundancy Protocol— VRRP is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

W-CDMA
Wideband Code Division Multiple Access— W-CDMA, UMTS-FDD, UTRA-FDD, or IMT-2000 CDMA Direct Spread is an air interface standard found in 3G mobile telecommunications networks.

WLAN
Wireless Local Area Network

WMAN
Wireless Metropolitan Area Networks (also known as WiMAX)

WPA / WPA2
Wi-Fi Protected Access— WPA and WPA2 are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

WPAN
Wireless Personal Area Network— A WPAN is a PAN carried over wireless network technologies such as IrDA, Wireless USB, Bluetooth, Z-Wave, ZigBee, or even Body Area Network. The reach of a WPAN varies from a few centimeters to a few meters.

WWAN
Wireless Wide Area Network— A WWAN differs from a wireless local area network (WLAN) by using mobile telecommunication cellular network technologies such as LTE, WiMAX (often called a wireless metropolitan area network or WMAN), UMTS, CDMA2000, GSM, cellular digital packet data (CDPD), and Mobitex to transfer data. It can also use Local Multipoint Distribution Service (LMDS) or Wi-Fi to provide Internet access.

Your Trusted Partner in Automation

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures.

The Americas

Moxa Americas
Toll Free: 1-888-MOXA-USA
Tel: +1-714-528-6777
Fax: +1-714-528-6778
usa@moxa.com

Moxa Brazil
Tel: +55-11-95261-6545
brazil@moxa.com

Europe

Moxa Germany
Tel: +49-89-37003-99-0
Fax: +49-89-37003-99-99
europe@moxa.com

Moxa France
Tel: +33-1-30-85-41-80
Fax: +33-1-30-47-35-91
france@moxa.com

Moxa UK
Tel: +44-1844-355-601
Fax: +44-1844-353-553
uk@moxa.com

Asia-Pacific

Moxa Asia-Pacific and Taiwan
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231
asia@moxa.com
japan@moxa.com
taiwan@moxa.com

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045
india@moxa.com

Moxa Russia
Tel: +7-495-287-0929
Fax: +7-495-269-0929
russia@moxa.com

Moxa Korea
Tel: +82-2-6268-4048
Fax: +82-2-6268-4044
korea@moxa.com

China

Moxa Shanghai
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505
china@moxa.com

Moxa Beijing
Tel: +86-10-5976-6123/24/25/26
Fax: +86-10-5976-6122
china@moxa.com

Moxa Shenzhen
Tel: +86-755-8368-4084/94
Fax: +86-755-8368-4148
china@moxa.com

MOXA®
Reliable Networks ▲ Sincere Service