MOXA®

Industrial
WIRELESS
Guidebook




1st Printing November 2007

Preface

The latest development in industrial device networking is the adoption of wireless technology for industrial applications. This is a very exciting development with potentially enormous benefits for system integrators and end users. However, many users may have questions about the different technologies that are available and how best to adapt them to specific applications. Other users may wish to gain a basic understanding of wireless technologies and applications but not know where to begin.

The Industrial Wireless Guidebook was conceived as a helpful introduction to the wireless technologies now being used for industrial applications. Readers can learn basic terminology, the strengths and weaknesses of various wireless technologies, and how to decide on a wireless solution for a specific application. Detailed examples are provided to show how wireless technology is being used in different industries, and can serve as a starting point in developing your own project.

Having been in the business for over twenty years, Moxa has been both a witness and participant to many developments in device networking technology. As new standards, interfaces, and protocols appear, we have kept pace and developed products that help integrate different technologies into one system. We hope you find the Industrial Wireless Guidebook to be a useful resource and look forward to assisting you with any of your device networking needs.

Table Of Contents

About Moxa

Global Market Leader in Industrial Device Networking

Well-known companies that use Moxa products include:

- *Siemens Medical*
- *NCR USA*
- *Toshiba*
- *TSMC**
- *China Telcom*

* Taiwan Semiconductor Manufacturer Corp., the No. 1 silicon wafer manufacturer in the worldwide industrial market.

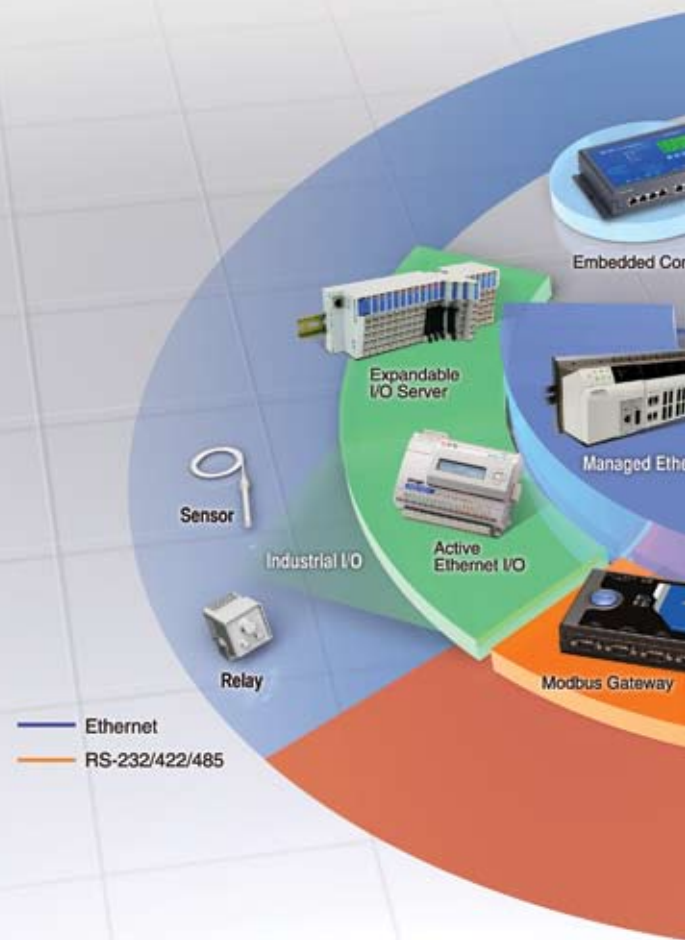
Moxa products have been used globally for more than 20 years to make industrial and commercial networking applications reliable, rugged, and cost effective.

To date, at least 9,000,000 devices have been installed with the aid of Moxa's products.

Product Categories

In addition to providing serial-to-PC and serial-to-Ethernet products, Moxa provides a comprehensive array of solutions that include:

- Industrial Ethernet Switches
- Serial-to-Ethernet Products
- Multiport Serial Boards
- Industrial Video Servers
- Wireless Ethernet Products
- Active Ethernet I/O Servers
- Embedded Computers
- Media Converters
- USB-to-Serial Converters
- Modbus Gateways



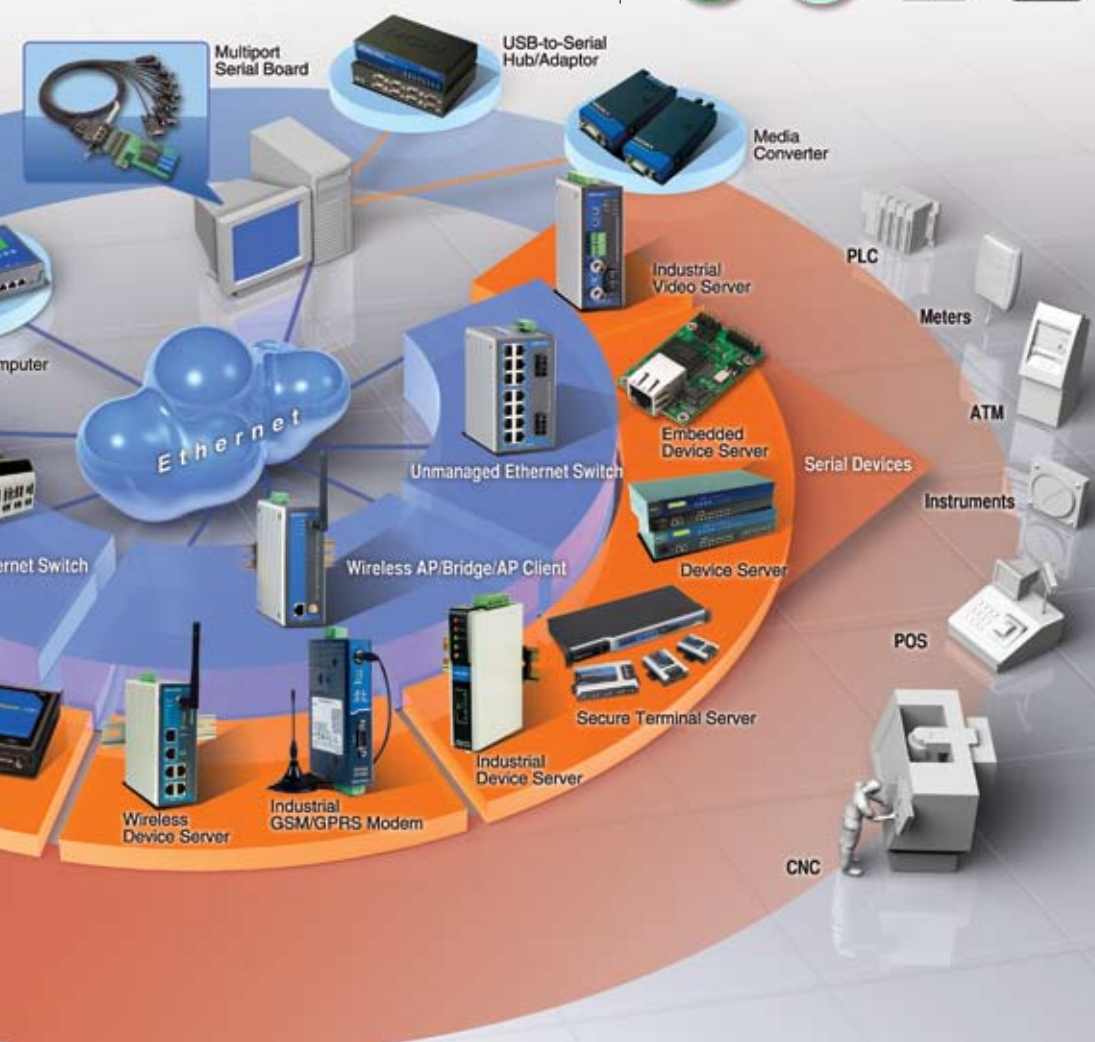
Quality Assurance

- **ISO 9001:2000**
  Research & Development, Manufacturing & Service, Quality Product Design
- **ISO 14001**
  Environmental Management System
- **5-year Product Warranty**
  Most products carry a 5-year warranty; see Moxa's website for full details

Moxa's Green Products

The European Union established the Waste Electrical and Electronic Equipment (WEEE) directive and the Restriction on Hazardous Substances (RoHS) directive.

All of Moxa's new "green products" satisfy the WEEE and RoHS directives.



Overview of the Industrial Wireless Landscape

↘What is Wireless?

Wireless communication involves in the use of some type of electromagnetic radiation, such as infrared or radio waves, to transmit information "over the air". Depending on the application, data may be transmitted just a few meters away (such as when using the remote control for a television set), or many kilometers away (such as when using a cell phone or sending signals to a satellite).

Why Go Wireless?

The convenience of being able to connect devices without the use of wires has led to the unprecedented success of wireless technologies in the consumer goods industry. Based on this success, applications using the same technologies are beginning to appear in various other settings as well, including in industrial environments. Wireless technologies offer a number of key benefits to businesses, including mobility, flexibility, wider coverage, and cost savings.

Mobility and Increased Efficiency

Improved data communication leads to faster and more efficient transfer of information between people in your organization and between you and your customers. Members of your sales team, for example, can remotely check stock levels and prices while on a sales call.

Flexibility and Easy Relocation or Expansion

In a factory setting, stationary systems can be connected over a wireless network to mobile subsystems or robots to achieve a connectivity that would otherwise be impossible. Furthermore, wireless technology can make it much simpler to gain temporary access to plant machinery for diagnostic or programming purposes.

Wider Coverage

Because wireless technology enables you to communicate wherever you are, you can send and receive information at any time without being limited by physical wires.

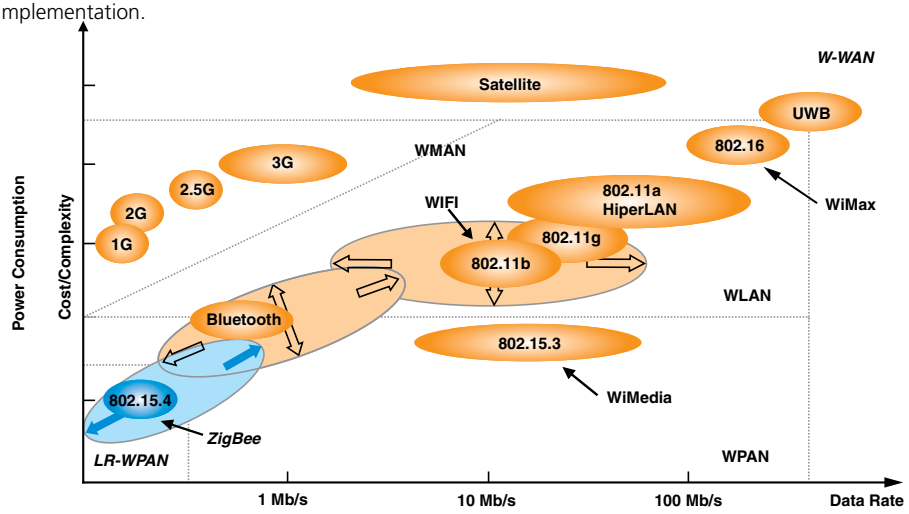
Cost and Time Savings

Wireless networks can be easier and cheaper to install and implement than wired networks. There is no need to purchase meters and meters of wire or to pay additional installation costs to wire your environment. The time required to deploy a wireless solution is also typically significantly shorter than for a wired solution.

The Industrial Wireless Technology Landscape

Different wireless technologies are available to address different application requirements. Some applications require high bandwidth, some require extensive wireless coverage, and some require low power. There are several wireless technologies that are currently being used in different commercial and industrial applications. Some of the more popular options are WLAN, GSM/GPRS, and CDMA.

The following illustration shows how different wireless standards compare in terms of data rate and complexity of implementation.



These technologies can be broadly organized into three major categories:

- WPAN
- WLAN
- WWAN

WPAN

Wireless Personal Area Networks (WPANs) are very small, short-range peer-to-peer or ad hoc networks that typically extend to a maximum of 10 meters. Because of their limited range, WPANs are used mainly as cable replacement solutions for data synchronization and connectivity between devices that are close to each other. In other words, WPANs are primarily used to eliminate cables that connect devices to peripherals.

Bluetooth, the prevalent WPAN technology in use today, allows devices such as phones, mice, headsets, and other peripheral devices to connect wirelessly over a range of 10 meters. Cordless mice and keyboards are typical WPAN applications.

WLAN

A wireless local area network (WLAN) is a LAN without cables. In contrast to WPANs, WLANs provide robust wireless network connectivity for associated clients up to 100 meters away from the access point. Today's WLANs are based on IEEE 802.11 standards and are referred to as Wi-Fi networks.

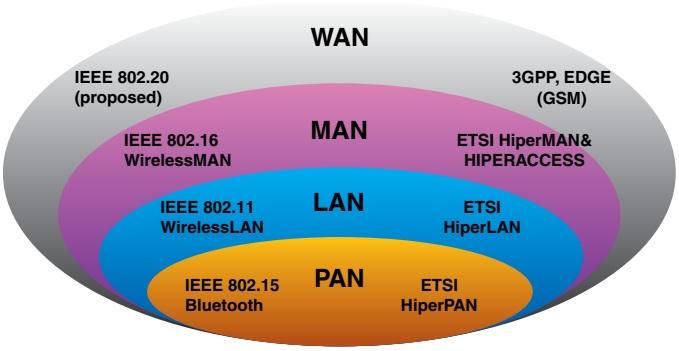
The 802.11b standard, which operates in the 2.4 GHz frequency band at 11 Mbps, was the first commercially successful WLAN technology. As wireless technology matured, a higher transmission rate of 54 Mbps was achieved with 802.11g, which operates in the 2.4 Ghz band, and 802.11a, which operates in the 5 Ghz frequency band. Today, it is common for dual-band Wi-Fi access points and client network adapters to support various combinations of 802.11a, b, and g.

NOTE: WLAN technologies are discussed in detail in Chapter 2.

WWAN (Cellular)

Wireless Wide Area Networks (WWANs) are digital cellular networks used for mobile phone and data service. They are operated by carriers such as Cingular Wireless, Vodafone, and Verizon Wireless, and provide connectivity over a wide geographical area. Two WWAN technologies—Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA)—dominate WWAN deployments worldwide.

NOTE: The term "cellular" is also used to refer to WWAN technology in general. WWAN technologies are discussed in detail in Chapter 3.



↘WLAN and Cellular: Complementary Technologies

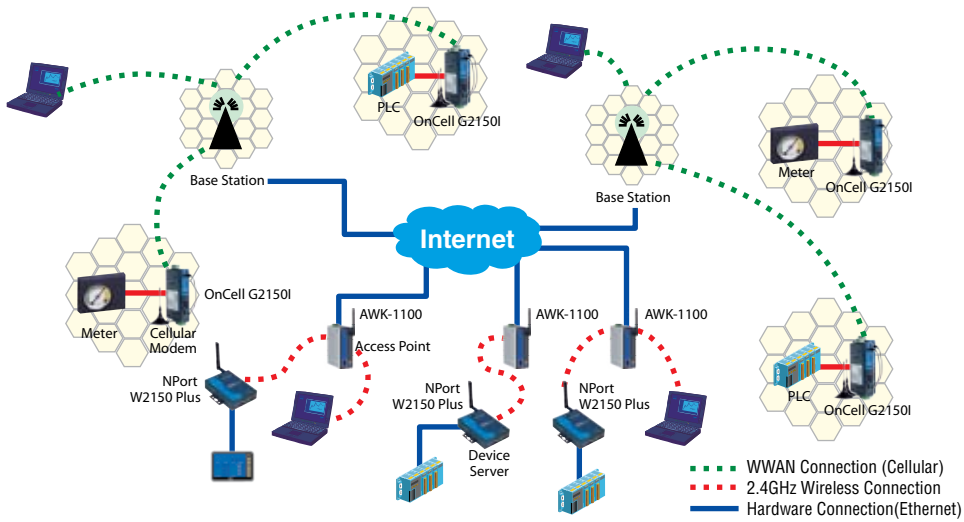
Although wireless LANs and wireless WANs may appear to be competing technologies, they are far more useful when they complement each other. When used together, you get the best of both technologies. WLAN provides high-speed wireless access from within a campus-sized area. Anywhere outside this area, data and applications can still be accessed with WWAN or high-speed cellular coverage.

These complementary technologies can be understood by comparing them to a typical wired scenario. In the office, users plug their laptops into a wired network for high-speed access to email, applications, data, and the Web. When they leave the office and work from home or at a hotel, a dial-up modem is used for remote access to email, applications, and the Web.

In the wireless scenario, the same users have laptops equipped with built-in WLAN adapters. WLAN access is used for high-speed access to applications while in the office. When out of the office, such as when visiting customers, completing a work order in the field, or accessing email from a hotel or airport, access to an 802.11 network may not be readily available. In this case, a WWAN card can be used to connect to a cellular provider's network to obtain secure, remote access to email, applications, and the Web.

Since many computers now come with WLAN connectivity, installing a WWAN card would ensure that when high-speed WLAN access is not available, you are still able to access your data wherever there is cellular network coverage.

WLAN and WWAN Hybrid Model



Getting the Right Wireless Solution

The growing variety of wireless technologies complicates the decision process for organizations and system integrators alike. When choosing a wireless technology for your business needs, there are many aspects to consider. The right wireless technology can provide significant benefits to your organization well beyond savings in wiring costs.

Understanding Your Application

There are many wireless technologies and standards to choose from, such as Bluetooth, Wi-Fi, and GSM/GPRS. How to evaluate between potential industrial wireless solutions? The best starting point is to understand your target application and define the requirements for a successful implementation.

What do you want the application to do? In what type of environment will you be deploying the devices? How many users will the installation support? Will connections be made or maintained over long distances? What are the minimum bandwidth requirements?

Once you understand the needs of your application, you can determine whether an appropriate wireless solution exists for you.

Ranking Your Application Requirements

Every application has its own, unique requirements, but certain considerations are common across most wireless applications, such as transmission range, data rate, reliability, and security. What are the most important considerations for your target application? How would you rank these requirements from the point of view of deploying and managing your application?

Cost and ease of setup and maintenance are also important factors. You must consider your existing network infrastructure and what it is equipped to handle.

	WLAN	Cellular
Range	100 to 300 m	Up to 30 km
Bandwidth	Up to 54 Mbps	Up to 120 Kbps
Security	Essentially open standard with imperfect security measures means special precautions must be taken	Fewer security concerns due to strict licensing and bandwidth allocation for cellular providers
Standards	Open standards that are widely recognized and used	Depends on cellular provider, usually region-based
Setup and Maintenance	Private installations require investment in access points, transmitters, etc.	Cellular provider responsible for infrastructure

Choosing a Wireless Technology

Once you understand your application requirements and priorities, the next step is to decide which wireless technology to use. The nature of your application and target environment will determine whether you employ WLAN, cellular, or both technologies. For some scenarios, you may also need a wired infrastructure to support your wireless implementation.

WLAN technology is ideal for applications where a network infrastructure is already in place, and is typically used when wireless Ethernet/Internet access is required at high data transfer speeds. However, there are well-known security issues with WLAN technology that have not been completely resolved. Also, a new WLAN installation requires careful study and tuning to achieve the desired benefits. In general, use WLAN technology when you need higher bandwidth, you have access to a nearby network infrastructure, and you need a high degree of control and customization.

With cellular communication, bandwidth is typically at 120 Kbps, much lower compared to WLAN. Network availability and reliability is dependent on the specific cellular provider. While the bandwidth is lower, cellular technology offers far superior range to WLAN and provides the highest level of mobility out of all wireless technologies. Worldwide cellular network coverage means that wireless connections can be available in areas that other networking technologies simply cannot reach. In terms of security, cellular signals are considered very secure and not vulnerable to eavesdropping (in the way that WLAN signals are) since cellular providers use heavily restricted and well-defined bands for their networks. For applications that require superior range, security, and simplicity, cellular technology is the most appropriate choice.

Moxa Industrial Wireless Solutions

	802.11 a/b/g	GSM/GPRS
Wireless Embedded Computing	ThinkCore W341  ThinkCore W321  ThinkCore W311 	ThinkCore W345  ThinkCore W325  ThinkCore W315 
Wireless Serial Connectivity	NPort W2150 Plus  NPort W2250 Plus  NPort W2004 	OnCell G2150I  OnCell G2110 
Wireless Ethernet Infrastructure	AWK-1100  AWK-1200 	

Wireless Local Area Networks

↘What is WLAN?

A wireless LAN (WLAN) is simply a local area network that does not rely on wired Ethernet connections. A WLAN can be either an extension to an existing wired network or an alternative to it. With WLAN, there is greater flexibility in networking since users can move around while keeping their computer connected, without having to depend on Ethernet cables.

WLANs generally provide all the features of wired LANs, only without the wires. The only noticeable differences to the end user tend to be in speed and security. Speeds range from 1 to 54 Mbps, with some manufacturers currently offering proprietary 108 Mbps solutions. Since the wireless access point is shared among wireless users in the area, security issues exist with WLANs that do not exist for wired networks.

WLANs can cover areas ranging in size from a small office to a large campus, and many communities have plans for neighborhood and city-wide coverage. Most WLANs use access points that cover areas between 65 and 300 feet in radius.

↘Popular WLAN Standards

One of the most confusing aspects of WLANs is the 802.11 set of standards that are frequently mentioned. 802.11 is the original WLAN specification developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The most widely adopted amendments to this original standard are 802.11a, 802.11b, and 802.11g, although additional amendments continue to be developed.

The Difference Between 802.11a, b, and g

802.11a operates in the 5 GHz to 6 GHz range and supports data rates up to 54 Mbps. To support such high data transfer rates, 802.11a relies on orthogonal frequency division multiplexing (OFDM). OFDM breaks up fast serial information signals into several slower sub signals that are transferred at the same time over different frequencies, providing effective resistance against radio signal interference. Although 802.11a provides high data rates and is the least susceptible to radio interference, its coverage is limited.

802.11b operates in the 2.4 GHz range and supports data rates up to 11 Mbps. Although 802.11b is the oldest and slowest of the main WLAN standards, it is the most widely used. 802.11b provides a greater coverage area than 802.11a, but at significantly lower data rates.

802.11g is the newest standard between the three and combines the best features of 802.11a and 802.11b. It operates in the 2.4 GHz range and supports data rates up to 54 Mbps. It is backwards compatible with 802.11b and provides the same coverage area as well.

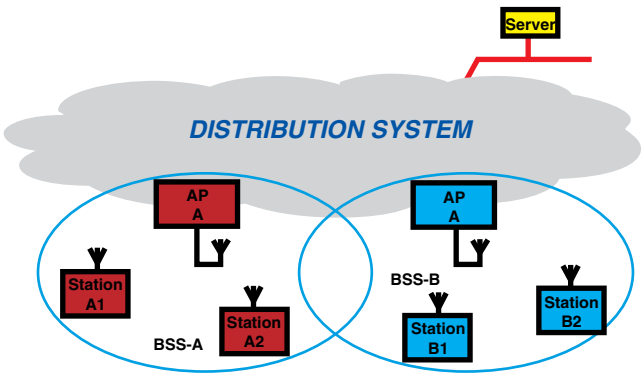
	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a
Popularity	Biggest market share	Mainstream products	Not so popular
Bandwidth	11 Mbps	54 Mbps	54 Mbps
Radio Frequency	2.4 GHz (crowded, may interfere with microwave ovens, cordless phones)	2.4 GHz (crowded, may interfere with microwave ovens, cordless phones)	5 GHz (not crowded)
Distance	300 meters outdoors 45 meters indoors	300 meters outdoors 45 meters indoors	Limited range 20 meters indoors
Spread Spectrum	DSSS (Direct Sequent Spread Spectrum)	OFDM (Orthogonal Frequency Division Multiplexing)	OFDM (Orthogonal Frequency Division Multiplexing)

Choosing Which WLAN Standard to Use

Before deciding which WLAN technology to use, you must consider how well each of these technologies meets your application requirements. For example, 802.11b or 802.11g are suitable choices for providing Internet access. However, if the WLAN is to be used for critical device control, you may wish to avoid radio interference by using 802.11a and the uncrowded 5 Ghz band.

You also need to consider the type of wireless technology that can be supported in your environment. If you already have existing wireless devices on the network, which WLAN standard do they use or support? Do you have a mix of all three types of clients? Note that 802.11b and 802.11g clients can communicate with each other, but not with 802.11a clients. If you are building the wireless network from scratch, you have a lot more flexibility and can generally pick any of the three standards.

Understanding WLAN Terms



- **Station (STA)**
  - Devices with 802.11 ability
- **Basic Service Set (BSS)**
  - A set of stations controlled by a single coordination function
- **Access Point (AP)**
  - Connect one BSS to Wired Network
  - Centralize Coordination for BSS

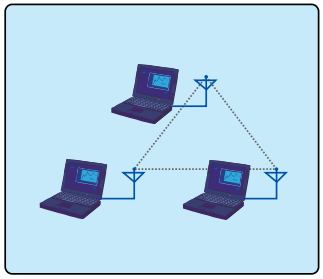
Before proceeding with a WLAN installation, you should be familiar with some common WLAN terminology:

- **Access Point (AP)** – This is a network device that serves as a communications "hub" for wireless stations. The AP typically connects wireless clients to a wired network. An AP establishes one or more Basic Service Sets in its area of radio coverage. WLAN clients that know the name of the BSS (its SSID) can try to authenticate and associate with the AP.
- **BSS (Basic Service Set)** – This is an area of coverage, or "cell", established by an 802.11 wireless access point. Clients in range of the access point can associate with it, provided they know the SSID for the BSS and can authenticate successfully with the access point.
- **ESS (Extended Service Set)** – This is a set of two or more interconnected BSSs that appear as a single BSS, using a common SSID but perhaps different channels.
- **SSID (Service Set Identity)** – Also known as the wireless network name, the SSID is a 32-character, case-sensitive name given to a Basic Service Set established by an access point. An access point can have more than one SSID. The SSID distinguishes one wireless network from another. WLAN clients and other devices looking to join a BSS must first supply the correct SSID. The SSID does not provide any effective security, since it can be sniffed from a wireless network by using a variety of PC-based software programs.
- **Wireless Station (STA)** – This is a device with an 802.11-compliant network adapter that enables it to communicate with other wireless devices, typically through an access point.

↘WLAN Network Modes

There are two modes by which wireless devices on a WLAN can communicate with each other. In ad-hoc mode, devices communicate directly with each other. In infrastructure mode, devices communicate with each other through an access point.

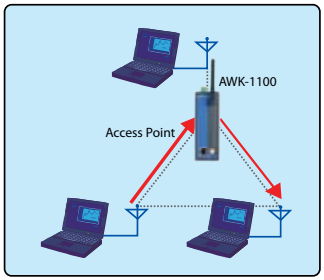
Ad-hoc Mode



Ad-hoc mode is comprised of WLAN-capable devices that are able to automatically locate and communicate with each other. Ad-hoc mode does not require an access point and is therefore the cheapest method of setting up a wireless network.

Ad-hoc mode is fast and easy to set up. It is an acceptable method for establishing a temporary, short-range wireless network with two to three computers.

Infrastructure Mode



Most WLAN applications use infrastructure mode, where wireless clients only communicate with an access point that is connected to a network backbone. The clients use this access point to gain access to the network behind it.

Conceptually, an infrastructure network is the wireless equivalent of the Ethernet hub. A fundamental aspect of infrastructure mode is that wireless clients cannot talk directly to each other; they must communicate through the network behind the access point.

In general, infrastructure mode is recommended if you need to accomplish any of the following:

- Provide more wireless coverage in your environment
- Support more users at the same time (typically up to 128 simultaneous clients)
- Implement wireless security
- Ensure reliable wireless communication between devices
- Install a more permanent WLAN

Using certain types of access points, infrastructure mode can also provide wireless and security enhancements, including access control, traffic prioritization, and Quality of Service (QoS).

WLAN Security

Unlike wired networks, anyone with a compatible wireless card can receive wireless data transmissions from your WLAN well beyond your walls. Operating an unsecured WLAN network creates an opportunity for outsiders to eavesdrop on your network traffic or to enter your network to access your computers and files. For this reason, security is a critical matter for WLAN installations.

There are two main forms of security that require attention for WLANs:

- Authentication: Wireless stations that attempt to connect to the network should be verified as authorized users before access is granted.
- Encryption: Data exchanged between the access point and wireless station should be encrypted to protect against interception and eavesdropping.

Typically, both authentication and encryption methods are combined in what is commonly called a security profile. The following four methods are currently available for WLAN security: WEP, WPA, WPA2, and 802.1x.

WLAN Security Protocol Briefing

Security Protocols	Features
WEP (Wired Equivalent Privacy)	RC4 data encryption No user/password authentication
TKIP (Temporary Key Integration Protocol)	Extended IV length for enhanced WEP Packet integration check
802.1X	EAP for port-based authentication Supports RADIUS, Kerberos, more
WPA (Wi-Fi Protected Access)	TKIP + 802.1X + MIC Supports RADIUS authentication Backwards compatible with all systems
WPA2 (802.11i)	WPA + AES cipher

WEP

Wired Equivalent Privacy (WEP) provides a basic level of security to prevent unauthorized access to the network and protect wireless data. Static shared keys (fixed length alphanumeric strings) are used to encrypt data and are manually distributed to all wireless stations that want to use the wireless network.

WEP has been found to be seriously flawed and is not recommended for a high level of network security. For more robust wireless security, most access points support Wi-Fi Protected Access (WPA or WPA2) for improved data encryption and user authentication.

WPA

Wi-Fi Protected Access (WPA) is a stronger security method that was created in response to the flaws discovered in WEP. It was intended as an intermediate measure until further 802.11i security measures were developed. When implemented with authentication methods such as RADIUS and VPN, WPA is considered secure enough for all but the most sensitive enterprise applications. For most home and small business use, an effective level of security can be obtained by using WPA with a pre-shared key (PSK) that is shared by all users.

WPA2

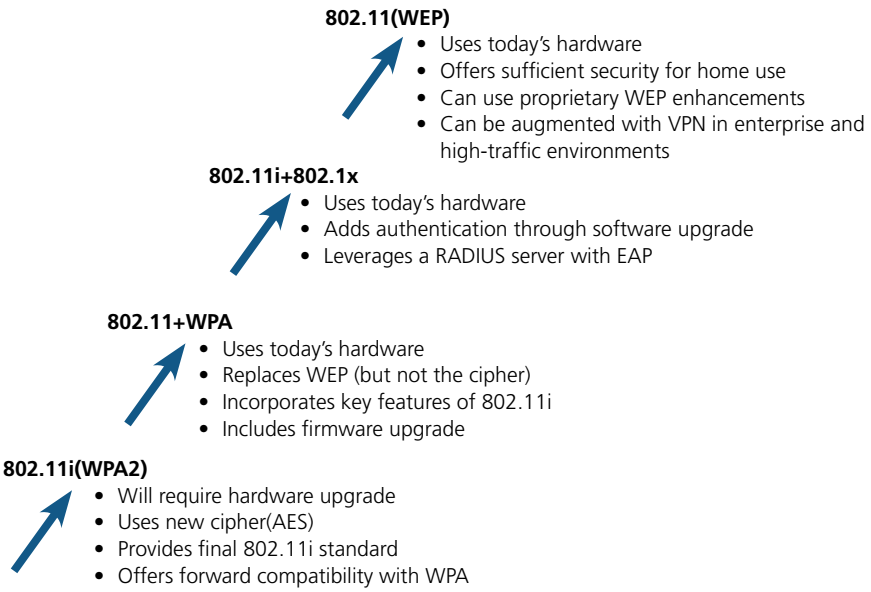
WPA2 is the second generation of WPA. The primary difference between WPA and WPA2 is the technology used for data encryption. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption, while WPA2 uses Advanced Encryption Standard (AES), a stronger encryption technology suitable for industries that require highly secure networks.

802.1X

802.1X is an authentication method that prevents unauthorized users from entering the network. It is used with WPA to form a complete WLAN security system.

On many wireless systems, users either log into individual access points, or can freely enter the wireless network but cannot get further without additional authentication. 802.1X makes users authenticate to the wireless network itself, not to an individual AP, and not to some other level like VPN. This is more secure, as unauthorized traffic can be denied right at the AP.

↘Progression in Wireless Security



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 use for your WLAN. You should take into account your target environment, the security levels that your WLAN can support, and the potential performance hit with stronger security methods.

Here are a few key questions that can help you evaluate your security options:

- Does your environment require a high level of security? If the WLAN will be used to send and receive sensitive information, such as financial data, you would likely want the highest level of security available. On the other hand, if the WLAN will only be used to send and receive raw data from factory equipment, a lower level of security may be preferable in order to optimize wireless performance.
- What level of security can your network environment support? WPA and WPA2 encryption technologies offer reliable security for a range of needs, but can all your clients support it? If you plan to implement 802.1X authentication, do you have a RADIUS server available on the network?
- Will a high level of security cause an unacceptable drop in wireless performance? How will the performance of your wireless devices on the network be affected if you enable encryption? Encryption can be a significant additional processing load, since devices must encrypt outgoing data and decrypt incoming data. Can your devices, including your device servers, handle this additional load?

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

Method	Client Support	Considerations
WEP	Built-in support on 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 backward compatibility with the original WPA

↘WLAN Antennas

Why Antennas are Important

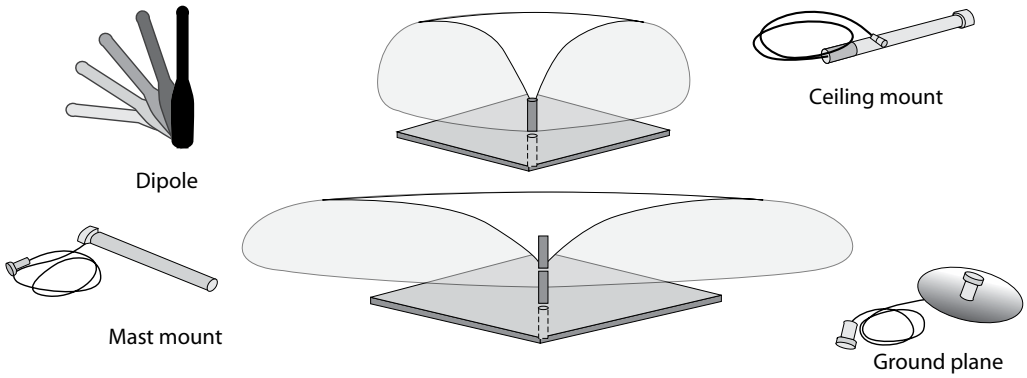
The speed of your wireless connection will vary depending on the strength of the signal you can receive and transmit. Antenna selection can therefore have a significant impact on the speed of your wireless link.

Types of Antennas

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

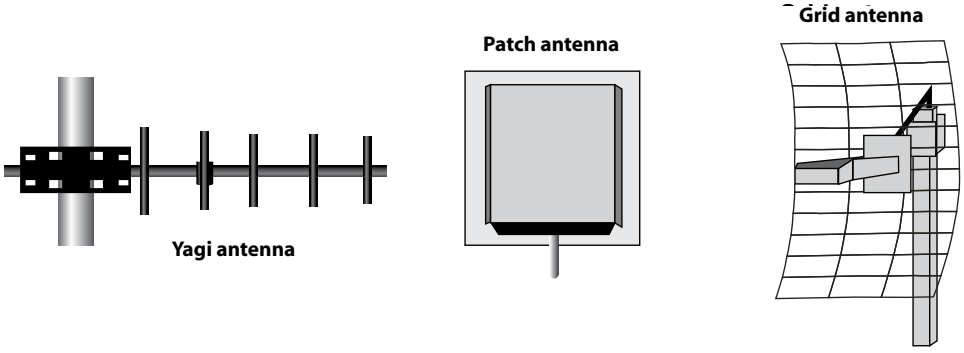
Omni-directional antennas are designed to radiate signals equally in all 360 degrees. Use this type of antenna if you need to transmit from a central node, such as an access point, to users scattered all around the area. In a small office with three or four rooms, an access point with an omni-directional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



Directional

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.

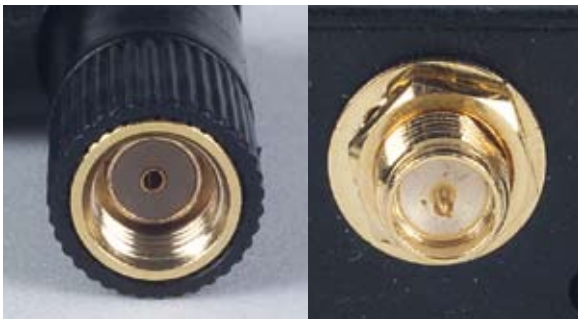
Directional antennas can also be used outdoors to provide short distance point-to-point links or as the customer end of a point-to-multipoint network.



Antenna Connectors

Before you purchase an antenna for your wireless device, you should check the type of antenna connector that your device uses. You will need to buy an antenna with a matching connector.

There are several types of antenna connectors, such as MCX, TNC, and SMA. On WLAN devices, the most commonly used antenna connector is SMA. If you are buying an antenna with an SMA connector, make sure you buy the correct SMA connector type. There are two types of SMA connectors: standard SMA (female) and reverse SMA (male).



Female SMA **Male SMA**

↘WLAN Site Survey

A radio frequency (RF) site survey is a step-by-step process by which you study the environment in which a wireless network will be deployed. It is the first step in the deployment of a wireless network and the most important step to ensure desired operation.

The information obtained in a site survey is used to determine the number and placement of access points that will achieve the desired signal quality and data rate in the desired coverage area. A site survey can also help find sources of interference that could degrade the performance of the WLAN.

Deciding if You Need a Site Survey

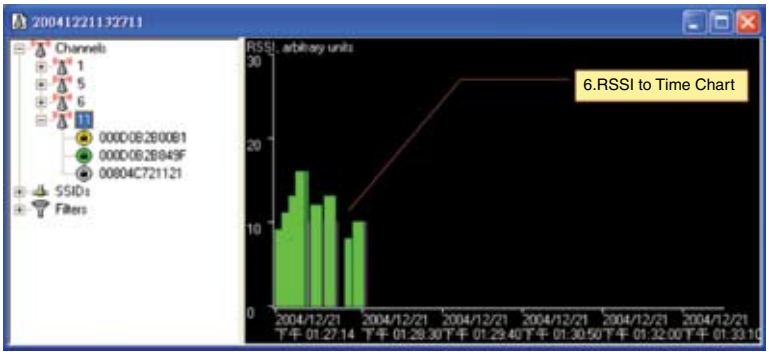
The need for an RF site survey depends on the facility where you are deploying the wireless LAN. For example, a small four-room office may not require a site survey. You can probably install a single access point anywhere within the office and maintain adequate coverage for all wireless stations in all rooms. If this access point encounters RF interference from another nearby wireless LAN, you can configure the access point to use a different wireless channel to solve the problem.

On the other hand, a larger facility, such as an office complex, apartment building, hospital, or warehouse, generally requires an extensive site survey. Without a proper site survey, users may end up with inadequate coverage and poor performance in some areas. In the worst case, you may discover after the fact that the location is unsuitable or that the installation must be redone.

Site Survey Tools

A number of WLAN vendors provide free RF site survey software that can help you determine the effective data rate, signal strength, and signal quality at your site when an access point is installed at a particular location. You can install this software on a laptop and use it to test the effectiveness of potential access point locations.

↘Site Survey Software



You can download this utility from Network Stumbler
www.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe

Performing a Site Survey

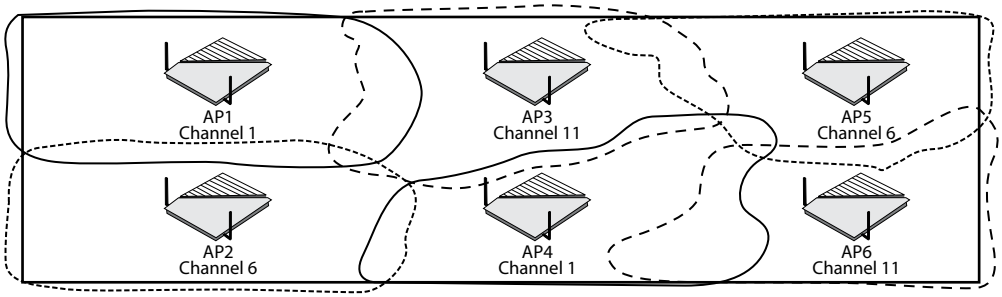
The following general steps should be followed when performing a site survey. Remember, the objective of the survey is to identify potential sources of interference in the target environment and determine the best locations for your access points.

1. Familiarize yourself with the target environment and check for physical barriers that may affect the propagation of wireless signals. A list of materials that can affect or block wireless signals is provided in the next section.
2. Identify user areas, including fixed areas (such as desks) and roaming areas where users may temporarily require wireless connectivity (such as meeting rooms).
3. Based on the information you have obtained on the site's physical barriers and user areas, identify potential locations for access points. Ideally, access points should be centrally located to the wireless clients.
4. Install an access point at each preliminary location and use a site survey tool to check the data rate and signal strength at different points.

   Use a signal strength indicator to determine the outer bounds of coverage for each access point. To ensure good reception throughout the site, access points will need to be spaced close enough to each other so that their outer bounds of coverage overlap. However, you must also make sure that they are spaced far enough from each other so interference is minimized.

   Use the site survey tool to identify sources of interference. You may need to try placing your access points in different locations and re-testing the data rates and signal strength. If you have identified a significant number of sources of interference, you may need to perform a more detailed site survey. If these sources of interference cannot be eliminated, you will likely need to deploy more access points to compensate for the signal loss.
5. Deploy the access points. If you are deploying multiple access points, Moxa recommends configuring each one for a different wireless channel. This will help resolve any interferences issues and improve the wireless signal.

Resolving Interference Issues with Different Channels



Common Obstructions to RF Signals

The strength of the radio signals that between the access points and wireless clients emit may be affected by physical barriers in the area. The following table lists shows common materials that cause signal loss. Signal loss is indicated in dB.

Item	Loss (dBi)	Range Loss
Space	0	100%
Window (without metal)	3	70%
Window (with metal)	5 to 8	50%
Dry wall	5 to 8	50%
Wood wall	10	30%
6" wall	15 to 20	15%
12" wall	20 to 25	10%
Ceiling	15 to 20	15%
Thick ceiling	20 to 25	10%

Be aware of the presence of these materials on your site and use a site survey tool to check if they are causing significant signal loss.

Moxa WLAN Solutions

AWK-1200

Outdoor wireless AP/bridge or AP client

Features

- IP67 protection (IP68 for AP/bridge model)
- Point-to-point, point-to-multipoint wireless connectivity
- WEP, WPA, WPA2, IEEE802.1X authentication
- -20 to 70°C operating temperature range

AWK-1100

Industrial wireless AP/bridge/client

Features

- IEEE802.11g/b compliant
- Redundant 24 VDC power inputs or Power-over-Ethernet
- Powerful security with WPA, 802.1X, and MAC address filtering
- DIN-rail and panel mounting
- Durable metal casing with IP30 rating

NPort W2150 and W2250 Plus

1 and 2-port wireless device servers

Features

- Link any serial device to IEEE 802.11 a/b/g network
- RS-232/422/485 serial interface, up to 921.6K bps
- Web-based configuration using built-in Ethernet or WLAN
- Enhanced remote configuration with HTTPS, SSH
- Secure data access with WEP, WPA, WPA2
- Built-in WLAN site survey tool
- Wireless roaming with user-defined signal strength threshold
- Off-line port buffering and serial data log
- Dual power inputs (1 power jack, 1 terminal block)

ThinkCore W311, W321, and W341

RISC-based wireless embedded computers

Features

- MOXA ART 32-bit ARM9 industrial communication processor
- 32 or 64 MB RAM onboard, 16 MB flash disk
- 802.11 a/b/g wireless LAN
- WEP, WPA and WPA2 encryption
- Infrastructure Mode and Ad-Hoc Mode
- Software-selectable RS-232/422/485 serial
- interface, up to 4 ports
- 10/100 Mbps Ethernet for network redundancy
- 5G vibration and 50G shock resistance
- Linux platform pre-installed
- DIN-rail and wall mounting
- Robust, fanless design

This page intentionally left blank

Industrial Cellular Wireless

↘Cellular Terms

The following are some of the terms that are commonly used in cellular wireless communications:

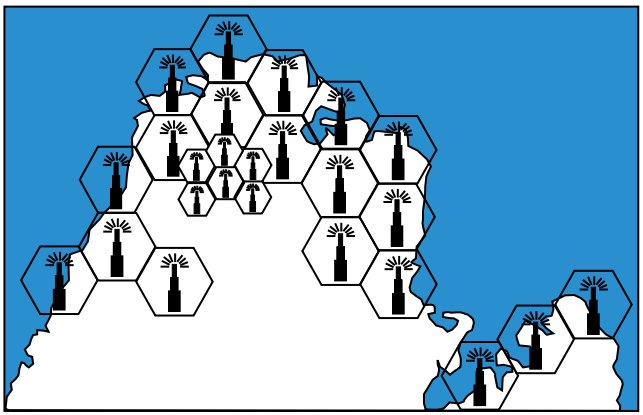
- **Carrier** – This is a telecommunications company that offers itself to the public for hire to provide communications transmission services.
- **Base Station** – This refers to a fixed station in a cellular wireless network, used for communicating with mobile terminals (phones). A base station is what links cellular phones to a wireless carrier's network.
- **Cellular Phone** – As far as subscribers are concerned, the cellular phone (also called mobile phone) is the main piece of equipment that uses cellular networks for communication.
- **Subscriber** – This is a user of a cell phone service and is usually tied to a monthly service plan or contract with a carrier.

↘What is a Cellular Network?

A cellular network is a radio network made up of a number of radio cells that are each served by a fixed transmitter, known as a cell site or base station. The cellular network allows cell phone subscribers to move anywhere within the coverage area and remain connected to the Public Switched Telephone Network (PSTN).

The term "cellular" typically refers to the wireless technology used for mobile phone networks such as GSM, GPRS, CDMA, UMTS, PDC, and others.

↘Cells in a Cellular Network



Overview of Cellular Wireless Technologies

A popular way to describe cellular technology is by generation, with 1G referring to first generation analog cellular technology. The primary difference between these different generations of cellular technologies is the speed at which data is transferred over the network, with 1G referring to first generation analog cellular technology.

1G

1G refers to analog cellular technology that was designed for basic voice calls. The only kind of data transfer supported was analog signal exchange between phones. 1G was widely considered to be wasteful of bandwidth and had extremely limited capabilities for data transmission, security, and location tracking. In most regions worldwide, analog cellular technology has been phased out of commercial use.

2G

The real starting point for comparing cellular technologies for data communication is with 2G, which is used by the majority of today's cell phones. 2G refers to digital cellular technology, where voice calls are converted into binary and transmitted in digital form. With sophisticated data compression and manipulation, several calls can occupy the same bandwidth of a single analog call. 2G is designed for voice calling and simple SMS (Short Message System) text messaging between phones.

Global System for Mobile (GSM) communications is the most popular 2G standard and cellular technology for mobile phones around the world. GSM operates in the 850 MHz and 1900 MHz bands in the USA and in the 900 MHz and 1800 MHz bands everywhere else. Data transfer speeds are typically low, around 9.6 Kbps.

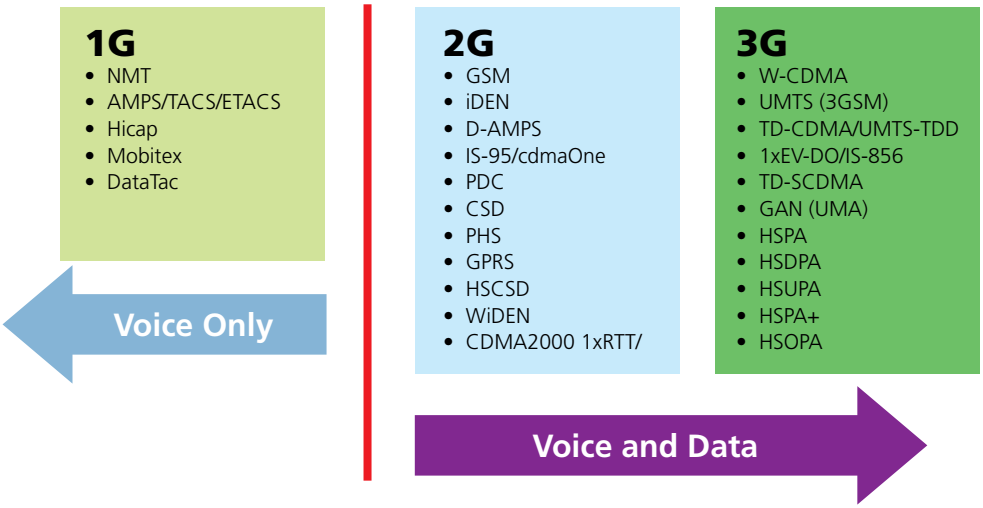
2.5G

Because of the limited data transfer speeds available with 2G technologies, many carriers found ways to enhance data transfer speeds enough to support services such as browsing the Internet or sharing multimedia files. Enhancements were made to work over existing cellular networks and are often described as 2.5G technology. On GSM networks, for example, carriers can offer General Packet Radio Service (GPRS) for 115 Kbps data transfer speeds.

3G

Cellular technology that is described as 3G is intended to provide broadband speeds for high-speed Web navigation, videoconferencing, TV streaming, and similar applications. 3G technology is designed for "always on" Internet (TCP/IP) access and achieves speeds between 100 and 300 Kbps.

↘Three Generations of Cellular Technologies



↘Data Bandwidth Comparison

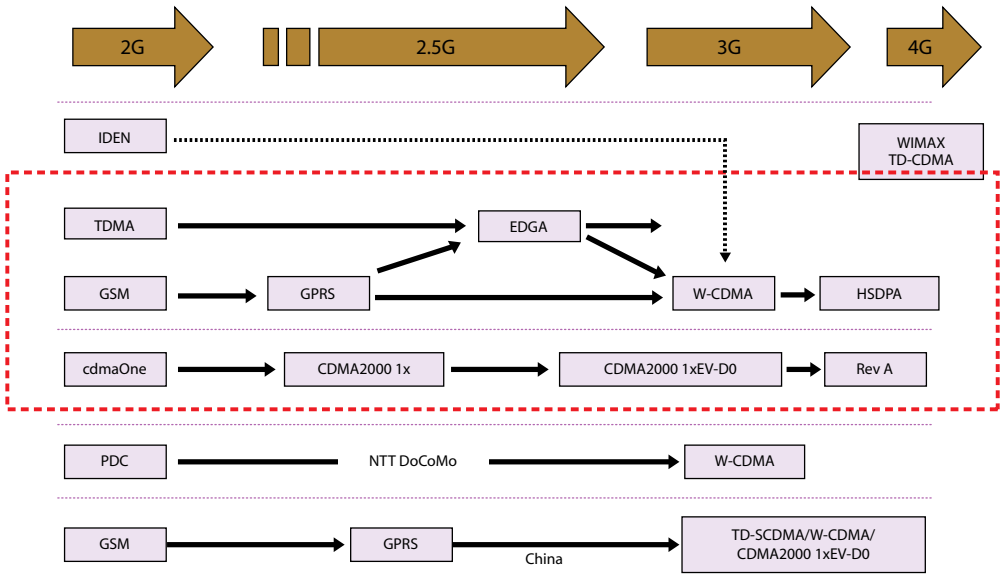
The primary difference between the three generations of cellular technology is maximum bandwidth supported, with newer technologies supporting higher bandwidths. The following table lists the theoretical maximum bandwidth for each cellular technology and the data throughput that is typically achieved.

Technology	Generation	Connection Type	Theoretical Max (kbps)	Carrier Max (kbps)	Typical Throughput (kbps)
GSM	2G	Circuit	------	9.6	------
GSM GPRS Class 10	2.5G	Packet	86.2	54.2	20 to 40
GSM Edge Class 10	2.75G	Packet	237	237	80 to 160
HSDPA	3.5G	Packet	>1800	>1800	>700
UMTS(W-CDMA)	3G	Packet	384	384	200
IS-95 (cdmaOne)	2G	Packet	------	14.4	------
CDMA 1 x RTT	2.75G	Packet	307	153	60 to 80
1 x EVDO (CDMA2000)	3G	Packet	>2000	>2000	300 to 500

Cellular Standards

A survey of cellular technology will uncover acronyms such as CDMA, GSM, and GPRS. These refer to cellular communication standards that have been adopted by different carriers around the world. Although there are many proprietary and regional differences, two competing sets of standards dominate the worldwide market: GSM/GPRS and CDMA.

Evolution of Cellular Technologies



GSM/GPRS

GSM standards are based around GSM (Global System for Mobile Communication), the most widely used 2G cellular technology worldwide. With GSM, all subscriber and wireless provider information is stored on interchangeable modules known as SIM (Subscriber Identification Module) cards. By swapping out the SIM card, users can painlessly switch phones or providers. For this and other reasons, GSM is enormously popular and well-supported throughout the world, making it particular suited for international roaming. However, the 850 MHz and 1900 MHz bands are used in North America, while the 900-MHz and 1800-MHz bands are used everywhere else.

	2G	2.5G	3G
GSM standards	GSM	GRPS GPRS/EDGE	UMTS (3GSM)

GPRS (General Packet Radio Service) is the 2.5G extension for GSM networks. GPRS was further developed for even better performance with Enhanced Data rates for GSM Evolution (EDGE), also known as Enhanced GPRS (EGPRS) protocol.

3G service is implemented using a standard called Universal Mobile Telecommunications System (UMTS), also known as 3GSM. Although this technology is not directly compatible with GSM, the standard is implemented so that devices support both standards, switching seamlessly between them as needed. As with GSM, the United States implements UMTS on different frequencies from the rest of the world, making transparent global roaming difficult. One potentially confusing aspect of UMTS is that it is based on an underlying standard called W-CDMA, which is not related to the CDMA set of standards.

CDMA

The term "CDMA" (Code Division Multiple Access) refers to both a spread spectrum technique and a cellular standard popular in North America. (The standard is more clearly referred to as cdmaOne or IS-95.) CDMA networks boast greater range and clarity than GSM. However, it was originally far more difficult for users to switch phones and carriers, since subscriber information was programmed directly into the phone rather than on a SIM card. International roaming on CDMA was also previously impossible since CDMA was only implemented in a few countries. A user identification module (UIM) has recently been introduced to offer CDMA subscribers the same conveniences as GSM subscribers. International roaming contracts between carriers have also been improved and expanded so CDMA subscribers can roam to more areas outside their home networks.

	2G	2.5G	3G
CDMA standards	CDMA (cdmaOne or IS-95)	CDMA2000 1x (1xRTT)	CDMA2000 1xEV-DO (EVDO)

CDMA2000 1x (or 1xRTT) is the 2.5G extension for CDMA networks, and CDMA2000 1xEV-DO (EVDO) is the 3G extension. Both 1xRTT and EVDO are popular with carriers wishing to offer 2.5G or 3G service. In some cases, carriers that use GSM for 2G services have decided to use EVDO for 3G service.

Other Standards

In certain regions, other proprietary standards are also widely supported, such as iDEN in North America, and PDC or FOMA in Japan. China has introduced its own official 3G standard called TD-SCDMA (Time Division-Synchronous Code Division Multiple Access).

	2G	3G
Other standards	iDEN (USA and Canada) PDC (Japan)	FOMA (Japan) TD-SCDMA (China)

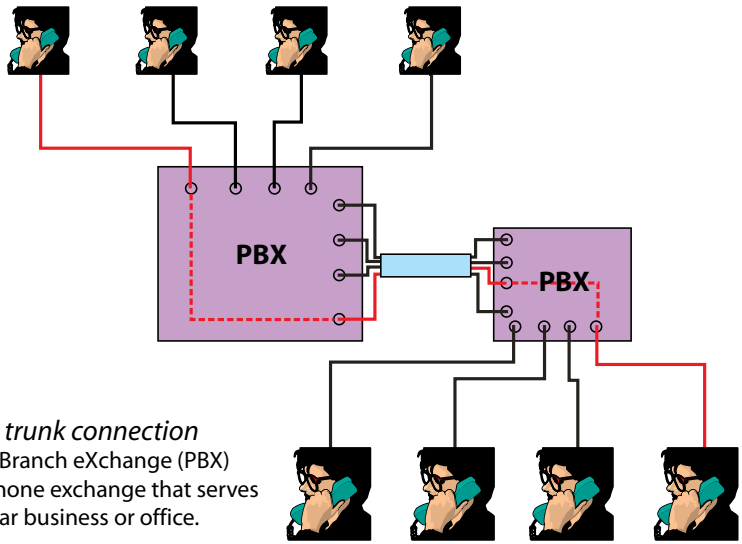
↘Cellular Communication Modes

There are three methods that can be used to establish cellular connections and transfer data over the network – circuit switched data, packet switched data, and short messaging service.

Circuit Switched Data

Circuit Switched Data (CSD) is the traditional technology used for the exchange of data. With CSD, a circuit connection is made and is exclusively reserved (dedicated) for its users. Users are charged based on the duration of the connection. This can be inefficient and costly for certain data applications. With Internet connections, for example, more time is spent reading the information than is spent exchanging data, but you are still billed for the time spent reading. This is partially addressed by many corporate email services, where the user works offline and only connects to the server to download and receive emails.

How Circuit Switching Works

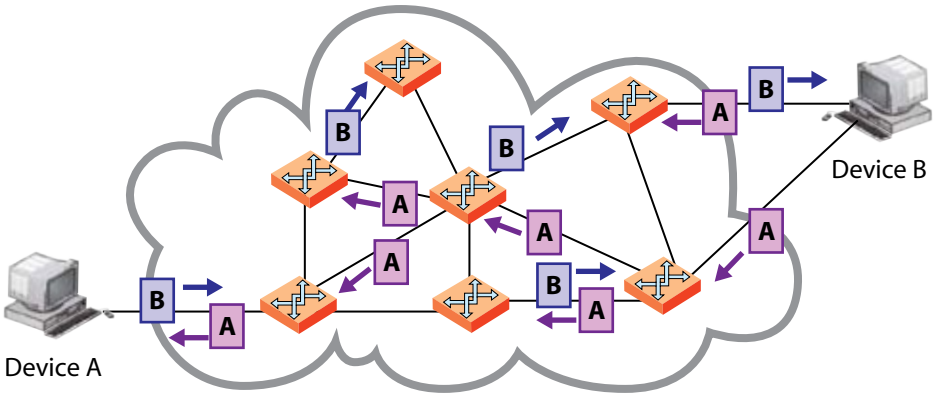


Tandem trunk connection
A Private Branch eXchange (PBX) is a telephone exchange that serves a particular business or office.

Packet Switched Data

Packet Switched Data (PSD) is a technology where the communication "pipe" is efficiently shared by multiple users. Data is sent to a specific address after a short delay. This delay depends on the number of users as well as the level of priority requested for the information. Billing is based on the volume of data rather than the duration of the connection. PSD is the same method used for Internet communication. Since it maximizes the use of the network, it will eventually be used for even voice communication, with high priority assigned to that form of traffic.

How Packet Switching Works



Short Messaging Service

Short Messaging Service (SMS) or "text messaging" is a mechanism that allows brief text messages (up to 160 characters) to be sent to a cellular phone. Several of the major phone standards support it.

Considerations When Choosing A Communication Mode

When choosing the appropriate communication mode for your application, take note of the following:

- In North America, CSD will be completely phased out by end of 2007. "Device server-like cellular modems" will take the place of CSD-based modems. All major manufacturers are in the process of the developing or have already developed alternative products. Moxa, for example, will be releasing an Ethernet modem soon.
- In addition to GPRS, there are several alternative high-speed PSD technologies available in North America, such as GPRS EDGE, CDMA, and HSDPA.
- A number of PLC manufacturers have adapted SMS as an optional communication method for their PLCs.

↘Choosing the Right Cellular Wireless Technology

The use of cellular technology for industrial applications is on the rise, but it can be difficult to differentiate between all of the options, standards, and carriers. Choosing the right cellular technology depends on your application. With a basic understanding of the different cellular technologies, you can evaluate your application requirements and target environment to determine the appropriate cellular solution. A good way to begin is by answering the following question about your application:

- What kind of data needs to be exchanged, and at what speeds? For frequent data transfer at broadband speeds, you would look for a 3G cellular solution. This would be indicated by support for UMTS, EVDO, FOMA, or TD-SCMA, depending on the carriers in your area.
- Will the application require TCP/IP or web access? Remember, TCP/IP access is only available with 2.5G devices and higher. Depending on your bandwidth requirements, a device that supports GPRS may be ideal. GPRS provides reasonable data transfer speeds for many applications. Since GPRS was built on top of GSM networks, a device that supports GPRS also enjoys the roaming benefits of worldwide GSM networks.
- Will the application require sending or receiving text messages? For certain applications, only simple data exchange is needed, and it may even be useful to use a cell phone to provide or receive data. Expensive 3G devices may be overkill when a device that can send and receive SMS text messages will suffice. For example, text messaging has proven useful as a simple tool for remote device management.
- ·What kind of devices will be communicating over the cellular network? Is a PC in a control center connecting to a remote PLC? Is a traffic light timer reporting status to an engineer's cell phone? Depending on the application, you may be looking for a cellular router, a cellular modem, or an embedded computer with cellular functions.
- What are your roaming requirements? If your application and device will require international travel, GSM is ideal. If 3G performance is needed, a dual UMTS/GSM device may be a good compromise.
- Which GSM bands are supported? Since GSM can be implemented in four different bands, you will need to make sure your device supports the appropriate bands for your needs. Quad-band devices are the only solution that will support GSM networks in any country.
- What is the desired coverage area and what are the available options for this area? This means finding out which cellular networks will best support that coverage area, the cellular standard that is used, and the frequency band for that region. It's also important to ask which carriers will provide the most effective and reliable

service, and how subscriber information and roaming is handled. Be sure to select a carrier that provides the service most tailored to your needs.

Cellular Antennas

As with other wireless technologies, antennas are used in cellular communication to send and receive radio signals. The strength of the radio signal that a device can send and receive is determined by the type and specifications of its antenna.

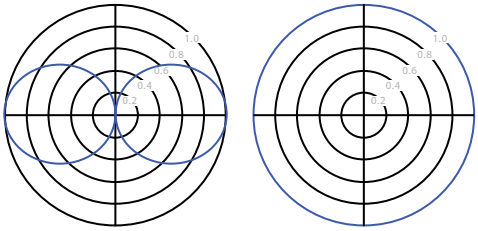
Antenna Types

Omni-directional antennas and directional antennas are the two most common antenna types used for wireless equipment, including cellular wireless.

Omni-directional

An omni-directional antenna transmits signals equally in a 360-degree pattern. This type of antenna is used when coverage in all directions is required, such as for a device in motion.

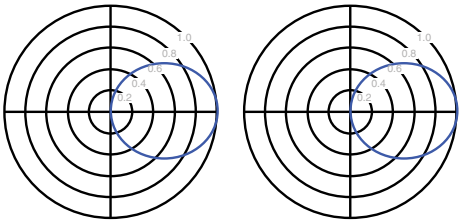
Types of Omni-directional Antennas

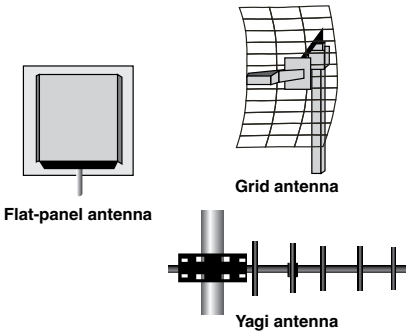


Directional

A directional antenna offers stronger signals in a particular direction for increased transmission distance, but at a narrower coverage angle.

Types of Directional Antennas





Selecting the Right Antenna Type

In order to select the right type of antenna for your application, you will need to consider the site location.

Deployment Environment

The target environment for your application dictates the type of antenna that you should use. If you are deploying your application in an urban area where building density is high, the recommended antenna type for both stations and clients is omni-directional. If you are deploying in an open space environment, a directional antenna may be more suitable since it can be pointed towards the station for better signal reception.

Will the application involve only outdoor connections or both outdoor and indoor connections? If both outdoor and indoor reception is required, the recommended antenna type is omni-directional. If it is a strictly outdoor application (e.g., located on a mountain, offshore, or on a building rooftop), a directional antenna would be a better choice.

Antenna Specifications

Once the choice of omni-directional or directional antenna has been made, you will need to decide on three important specifications for your antenna: gain, VSWR, and impedance.

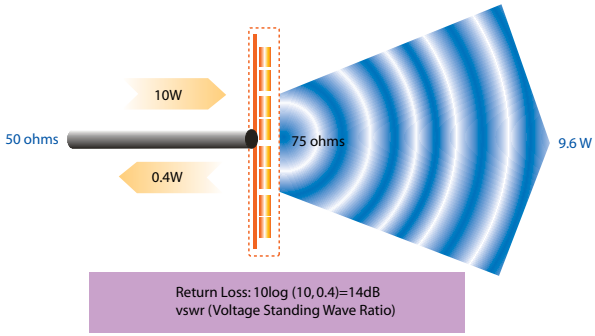
Gain

Antenna gain indicates how well the antenna focuses RF energy in a particular direction. Antenna gain is expressed in dBi (the ratio of the power radiated by the antenna in a specific direction to the power radiated in that direction by an isotropic antenna fed by the same transmitter). Manufacturers will typically specify the gain for each antenna that is produced.

The appropriate antenna gain depends on the strength of the cellular signal in your target environment. Signal strength is typically measured in RSSI (Received Signal Strength Indication), which ranges from 0 to 100. An RSSI of 0 or 1 is not strong enough to support GSM or GPRS. You may need to inquire with your carrier about the possibility of obtaining higher RSSI in the desired area. For RSSI values up to 12, a 10 dBi antenna is ideal. For RSSI values up to 20, you will want a 3 to 5 dBi antenna. For RSSI values greater than 20, you will want a 0 to 3 dBi antenna.

Voltage Standing Wave Ratio

Voltage Standing Wave Ratio (VSWR) compares the maximum amount of voltage or current that can be delivered by the radio to the minimum voltage or current that is actually emitted through the transmission line and antenna. In perfect conditions, where no energy is lost between the radio-end connector to the base of the antenna and the antenna is perfectly tuned to the testing frequency, VSWR will be 1:1. This means that no power is wasted or lost from the radio to the antenna. A good antenna should have a VSWR of 1:1 to 1:25.



Impedance

Impedance represents the relationship between voltage and current that a device is capable of accepting or delivering. The most common impedance values are 50

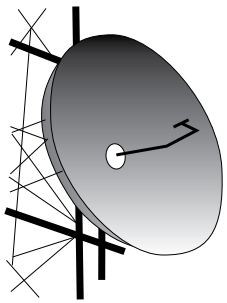
ohm, 75 ohm, and 300 ohm. Cellular antennas have an impedance of 50 ohm. A mismatch of impedance between the device and the antenna will cause lower signal efficiency and increased signal reflections.

Tips for Cellular Antennas

- Look for an antenna with a VSWR of less than 2.5 and impedance of 50 ohm. This combination ensures the best antenna performance.
- Make sure the connector type matches the connector on your cellular equipment.
- Make sure that the antenna's wireless band is allowed in your country and compatible with your wireless equipment.
- Ilf you are using a directional antenna, try rotating the antenna to determine the position where it generates and receives the strongest signal.
- If you are using an omni-directional antenna, there is no need to adjust the antenna direction.
- Check the RSSI before and after installing the antenna. The ideal RSSI is 21. If RSSI is less than or equal to 12, use a 10 dBi antenna. If RSSI is more than 20 but less than 12, use a 3 to 5 dBi antenna. If RSSI is more than 21, use a 0 to 3 dBi antenna. If you are using a 0 dBi antenna, your RSSI should be 12 or higher.

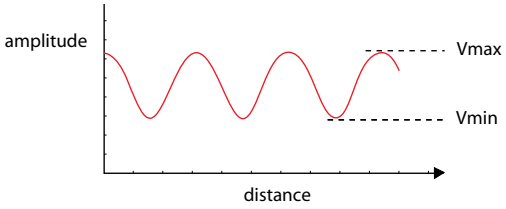
High Gain Antennas

When trying to boost the signal strength for a device, most people assume that a high gain antenna will resolve the problem. This is only partially true. While high gain antennas will improve the device's sensitivity to incoming signals, the increased gain will not strengthen the signal coming from the device. High gain antennas are of no use if the original signal is not strong enough.



There are better and more efficient ways to improve the signal than using a high gain antenna.

- Use the same gain but adjust the VSWR or impedance to improve the signal. Gain affects efficiency, as well as impedance and VSWR.
- Check the area for materials that may cause poor reception or transmission. If there are concrete walls in the area, for example, you may try placing the antenna in a better location.



Cellular Wireless Certifications

One of the challenges that organizations typically face when first attempting a cellular installation is compliance. Compared to other commercial and industrial products, the compliance requirements for wireless devices is much stricter with regard to import regulations, local regulatory laws, and safety standards. The number of certifications required depends on the country where the device is to be imported and operated.

Before purchasing any wireless device, be sure to check your country's certification requirements. Verify that your device is in full compliance and can be obtained in your country.

Certification Organizations

The following are some of the organizations that provide certifications for wireless devices:

- Radio Equipment and Telecommunications Terminal Equipment (R&TTE): This organization covers all radio equipment and any equipment intended to be connected to public telecommunications networks.
- European Telecommunications Standards Institute (ETSI): This organization develops harmonized standards that allow manufacturers to declare compliance.
- PCS Type Approval Certification Review Board (PTCRB): This organization provides the framework within which GSM Mobile Equipment (ME) Type Certification can take place for members of the PTCRB.
- Global Certification Forum (GCF): This organization provides a unique service that assures mobile wireless terminal interoperability for operators and vendors.

G2150i Certification: An Example

To show a real-world example of the number of certifications required for importing and operating single wireless equipment, we can take a look at Moxa's OnCell G2150I. The G2150I is a quad-band GSM/GPRS modem that transmits data and short messages (SMS) over GSM/GPRS mobile networks.

↘OnCell G2150I Certificate with List of Standards Required for Compliance

QTK

CERTIFICATE

Issued Date: March. 09, 2007
Report No.: 072L058-ITCEP07V03

This is to certify that the following designated product

Product : Industrial Cellular Modem
Trade name : Moxa
Model Number : OnCell G2150I
Company Name : Moxa Technologies Co., Ltd

This product, which has been issued the test report listed as above in QuieTek Laboratory, is based on a single evaluation of one sample and confirmed to comply with the requirements of the following EMC standard.

EN 55022: 1998+A1: 2000+A2: 2003
EN 61000-3-2: 2000
EN 61000-3-3: 1995 + A1: 2001
EN 55024: 1998+A1: 2001+A2: 2003
IEC 61000-4-2 Edition 1.2: 2001-04
IEC 61000-4-3: 2002+A1: 2002
IEC 61000-4-4: 2004
IEC 61000-4-5 Edition 1.1: 2001-04
IEC 61000-4-6 Edition 2.1: 2004-11
IEC 61000-4-8 Edition 1.1: 2001-03
IEC 61000-4-11 Second Edition: 2004-03

TEST LABORATORY

George Chen

George Chen / President

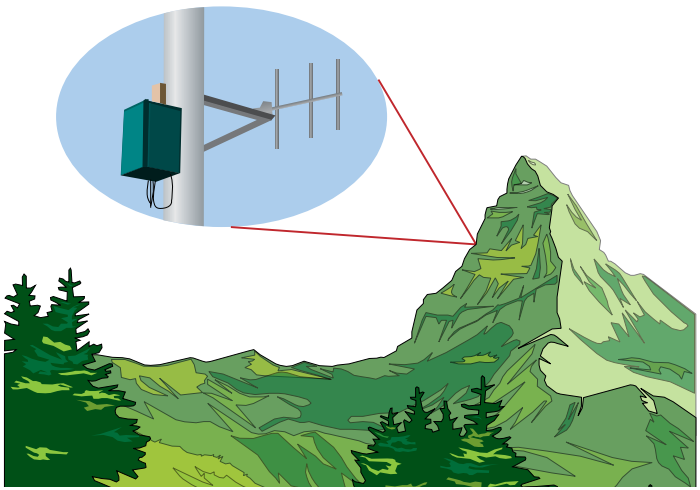
QuieTek

The following table shows the certifications required by different regions to import and operate a GSM/GPRS modem:

Item	Title	Region
CE for EMC	CE EMC Certification	Europe
	CE EMC Report	Europe
R&TTE EN301511	R&TTE EN301 511 Certification	Europe
R&TTE EN301489-1,-7	R&TTE EN301 511 Report	Europe
	R&TTE EN301 489-1-7 Certification	Europe
	R&TTE EN301 489-1-7 Report	Europe
R&TTE EN60950-1	R&TTE EN60950-1 LVD Certification	Europe
	R&TTE EN60950-1 LVD Report	Europe
GCF-CC	Global Certification Forum Certification Criteria Report (GCF-CC)	Europe
FCC for EMC	FCC part15 EMC Certification	USA
	FCC part15 EMC Report	USA
FCC Part 22/24	FCC part 22H/24E Certification	USA
PLMN01	PLMN01 & CNS13438 Certification	Taiwan
PTCRB	PCS Type Approval Certification Review Board	America

Evaluating Total Cost of Ownership

The best way to demonstrate the advantages of industrial cellular solutions is to do a side-by-side comparison of both wired and wireless implementation costs for a given application. For example, suppose your project is to automate data collection from a feeder terminal unit (FTU) located on a mountain one kilometer away. Communication to the FTU can be established with one of the following three technologies: ADSL PSTN, fiber Ethernet, and wireless. You could do a side-by-side comparison between the three technologies to determine the most cost-effective solution.



One of your initial tasks would be to determine the costs of setting up the infrastructure required for communication. The following table shows an estimate of the initial infrastructure costs for the three possible solutions.

Initial Costs

	Infrastructure Costs	Monthly Fees	Maximum Bandwidth
ADSL PSTN	ADSL operator	$50.00 USD / month $30.00 USD / month	8 Mbps (download) 56 Kbps (upload)
Fiber Ethernet	1 km fiber cable Construction costs Licensing costs	None	100/1000 Mbps
Cellular	Cellular carrier	Charged by packet sent, usually with basic monthly payment	GSM: 9.6 Kbps GPRS: 20 to 40 Kbps EDGE: 80 to160 Kbps HSPA: 2 Mbps

The following table breaks down the communication costs over five years for both wired and wireless communication. Note that the licensing cost for the wired solution is not yet included.

Comparing Cellular and Fiber Optic Approaches

	Cellular Solution		Fiber Optic Solution	
Initial Costs	None		1 km fiber patch cords Construction licensing	$2,000.00 $5,000.00
Communication Costs	Monthly	$44.99 x 12 months x 5 years	None	
Total		$2,699.00		$7,000.00

Based on these figures, an industrial cellular installation would achieve a lower total cost of ownership and would be the most cost-effective solution.

Moxa Cellular Solutions

OnCell G2100 Series

Isolated quad-band industrial GSM/GPRS modem

Features

- Quad-band 900/1800, 850/1900 MHz GSM/GPRS
- GPRS Class 10
- Circuit-Switched Data mode up to 14,400 bps
- Seperate RS-232 and RS-422/485 serial interfaces
- 2.5 KV RMS isolation for 1 minute for all serial signals
- 15 KV ESD surge protection
- LED indicators for status, signal level
- DIN-rail, wall mounting
- SMS Tunnel Mode

ThinkCore W315, W325, W345

RISC-based wireless embedded computers with GSM/GPRS

Features

- MOXA ART 32-bit ARM9 industrial communication processor
- 32 or 64 MB RAM onboard, 16 MB flash
- disk
- Built-in quad band GSM/GPRS 850/900/1800/1900 MHz
- Supports GPRS Class 10, Coding Scheme from CS1 to CS4
- Software-selectable RS-232/422/485 serial
- interface, up to 4 ports
- 10/100 Mbps Ethernet for network redundancy
- Pre-installed Linux platform
- DIN-rail or wall mounting
- Robust, fanless design

NPort 6650 and NM-GPRS/GSM

8, 16, and 32-port rackmount terminal servers

Features

- Up to 2 ports for high density environments
- SSL support for secure communication
- Secure remote management and configuration with SSH or SSL
- Powerful DES, DES, and AES hardware encryption engine
- Any baudrate supported
- 10/100BaseTx Ethernet port supporting 802.af Power Over Ethernet (POE)
- Port buffers to hold serial data if Ethernet fails
- SD slot for optional expansion of port buffers
- Slot for network expansion module
- Quad-band 900/1800, 850/1900 MHz GSM/GPRS
- LED indicators for status, signal strength
- GPRS Class 10
- CSD data connection
- Circuit-Switched Data mode up to 14,400 bps
- Short message alert
- Real COM Mode

NPort 6450 and NM-GPRS/GSM

4-port secure terminal server

Features

- LCD control panel for IP address configuration
- Versatile socket operating modes, including TCP Server, TCP Client, UDP, Pair Connection, Real COM driver, and RFC2217
- Secure modes for TCP Server, TCP Client, Pair Connection, and Real COM
- Any baudrate supported with high precision
- 10/100BaseTx Ethernet port supporting 802.af Power Over Ethernet (POE)
- Port buffers to hold serial data when Ethernet is off-line
- SD slot for optional expansion of port buffers
- Slot for network expansion module
- Quad-band 900/1800, 850/1900 MHz GSM/GPRS
- LED indicators for status, signal strength
- GPRS Class 10
- CSD data connection
- Circuit-Switched Data mode up to 14,400 bps
- Short message alert
- Real COM Mode

Real-World Industrial Wireless Applications

↘Wireless Applications

A number of challenges in industrial environments could be easily resolved by integrating a wireless solution. WLAN or GSM/GPRS technology could be used, depending on the target environment (indoor or outdoor) or whether the target application is fixed or mobile.

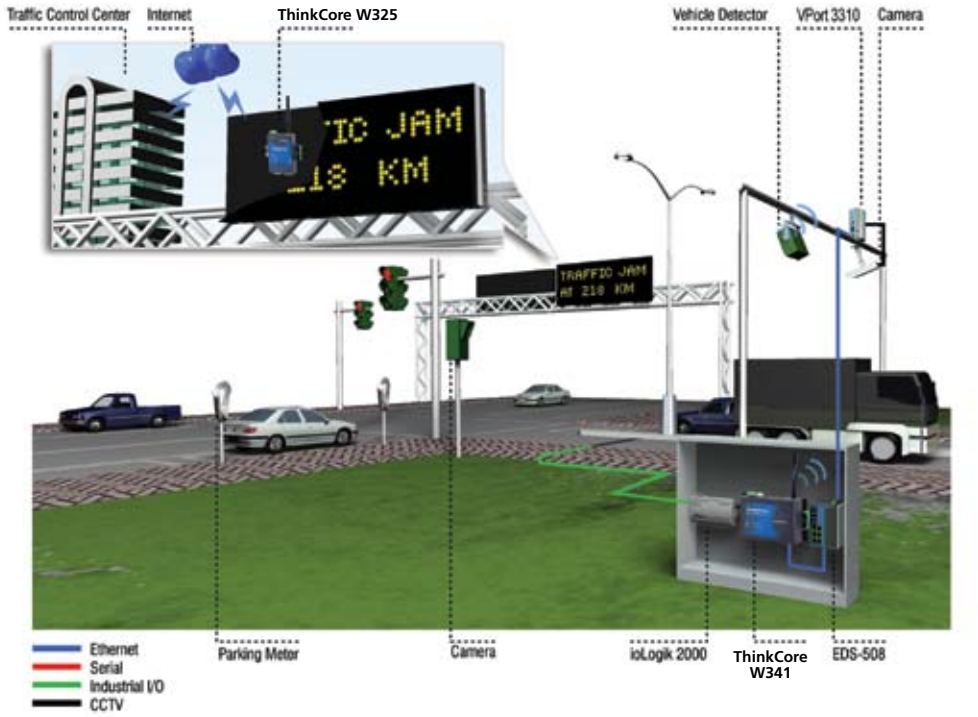
This chapter provides examples of real-world industrial challenges that could be solved by implementing a WLAN or cellular solution, or by a combination of both.

↘Transportation

Traffic Control

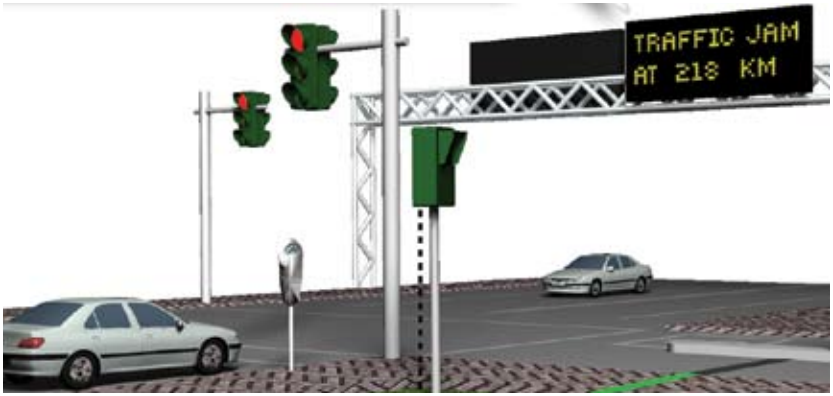
In dense urban areas with a strong network infrastructure, traffic control equipment can be connected to a central control center using industrial-grade Ethernet or serial cables. However, there are many suburban, rural, and industrial areas where roadside cabinets have no convenient access to a network line. Installing additional lines involves far too much effort and expense to be feasible, especially for a large number of cabinets distributed over entire regions.

With cellular technology, these traffic control devices can be connected to the main control center with almost no additional investment in infrastructure or equipment. Since these devices need to be managed by PCs that are designed for TCP/IP, a 2.5G or 3G cellular solution would be required. A device server with cellular functions, such as a GPRS module, would be an excellent solution to support the multiple devices in the cabinet. With proper configuration, the main control center would have access to every traffic control device as if they were physically connected by land lines.



Public Information Display

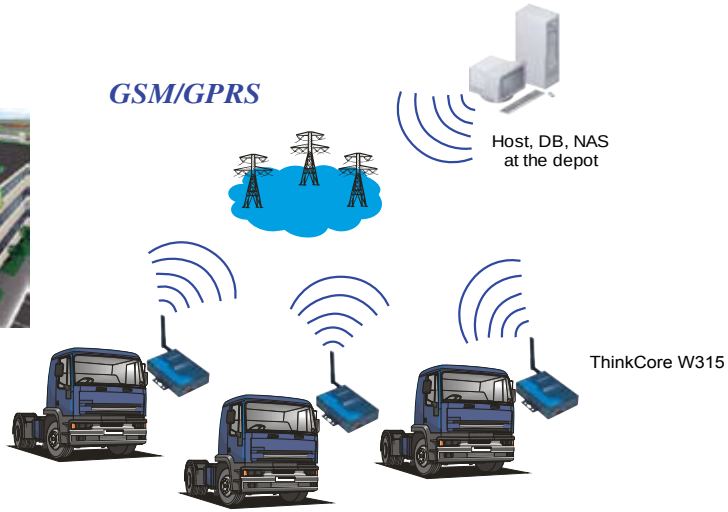
Industries such as transportation or finance often use public message boards to present information, such as traffic congestion information or real-time stock quotes. Cellular technology can allow such messaging and communication for previously untapped, hard-to-wire locations, such as on highways and on buildings. Message display can be controlled in real-time from a remote monitoring location. A GSM/GPRS modem can be used for simple setups that do not require advanced computing functions. For more complex setups, an embedded computer with GSM/GPRS capabilities can be used.



Fleet Management

The introduction of wireless technologies in industrial applications has revolutionized even fleet management. Various fleet management tasks can now be performed remotely, regardless of the vehicle's location. Depending on the management tasks required, you have two options for integrating wireless technology into your fleet operations.

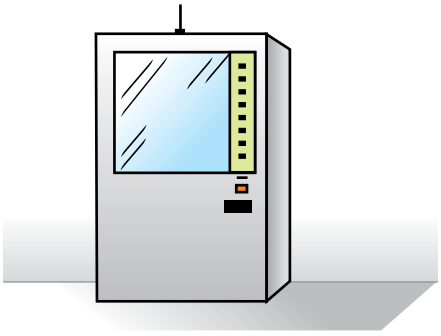
- If you need to monitor the status of cargo onboard a vehicle, such as perishable goods, or if you need to track vehicle location in real-time, the long distance coverage of cellular technology is required. You can install a wireless embedded computer that supports GSM/GPRS communication on the vehicle. With this setup, vehicle dispatching becomes even more efficient. Instead of paper-based work orders, you can send wireless work instructions, reminders, or other text messages to drivers.
- If you only want to monitor vehicle utilization or performance such as vehicle speed, fuel consumption, or braking patterns, you can connect a WLAN-enabled embedded computer to the vehicle's monitoring instruments. Whenever the vehicle returns to the depot, its Information can be downloaded wirelessly to a central monitoring server.



↘Retail

Outdoor Vending Machines

Vending machines are a great example of an application uniquely suited for a cellular solution. Typically, vending machines are scattered throughout a wide area and managed by a third party. While they may be installed at offices and other locations with a modern IT infrastructure, they do not have any access to that infrastructure. Supplies are traditionally monitored through periodic in-person visits.



Vending Machine with GPRS Module

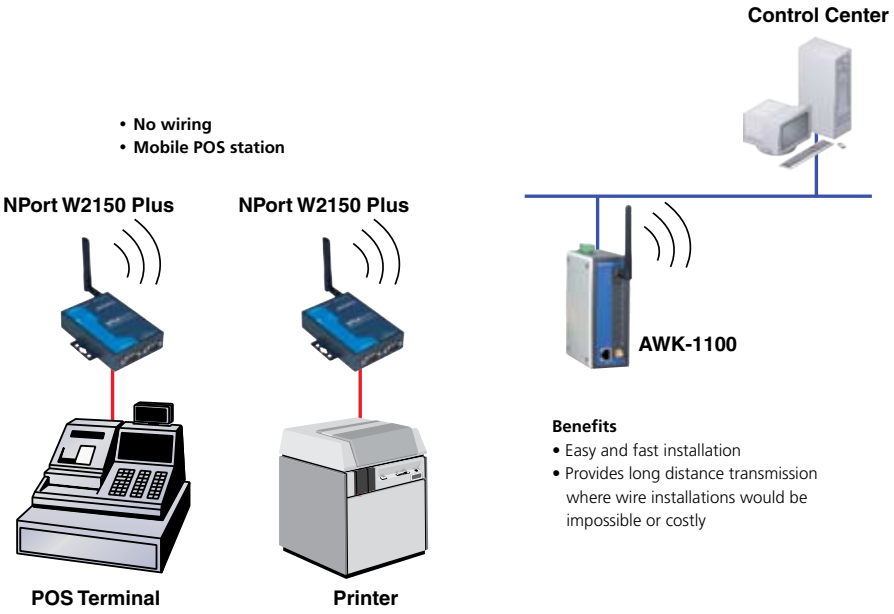
A cellular solution could allow remote monitoring of an entire region of vending machines. Vending machine control boards have serial and other connectors that are used to report supply, income, and status information. With an industrial cellular modem installed, this information could be reported to a cell phone by text message. Instead of visiting each vending machine location regularly, suppliers could visit only those locations reporting low supplies. Since this application requires only text messaging, a 2G cellular solution supporting GSM or CDMA would be suitable, with the actual choice depending on the available regional carriers.

Some vending machines accept credit cards for payment and must be able to send credit authorization requests to the credit card companies. It may be expensive or difficult to wiring the machines to a phone line. Instead, a GPRS module could be installed on the machine and wired to the credit card device. Credit authorization requests could then be sent wirelessly via the cellular network.

Inventory Management

Traditionally, retail devices such as point-of-sale terminals, receipt printers, and barcode scanners are connected to a back-end server through a wired connection. However, wires protruding from walls and floors can be unsightly, inconvenient, and even dangerous to employees, especially in an environment where goods are frequently moved.

Your retail facility or warehouse can benefit from safer, more accurate, and more efficient operations by integrating WLAN into your environment. Set up a WLAN environment and connect a wireless device server to each device that needs to communicate with the back-end server or other network devices.



Benefits

- Easy and fast installation
- Provides long distance transmission where wire installations would be impossible or costly

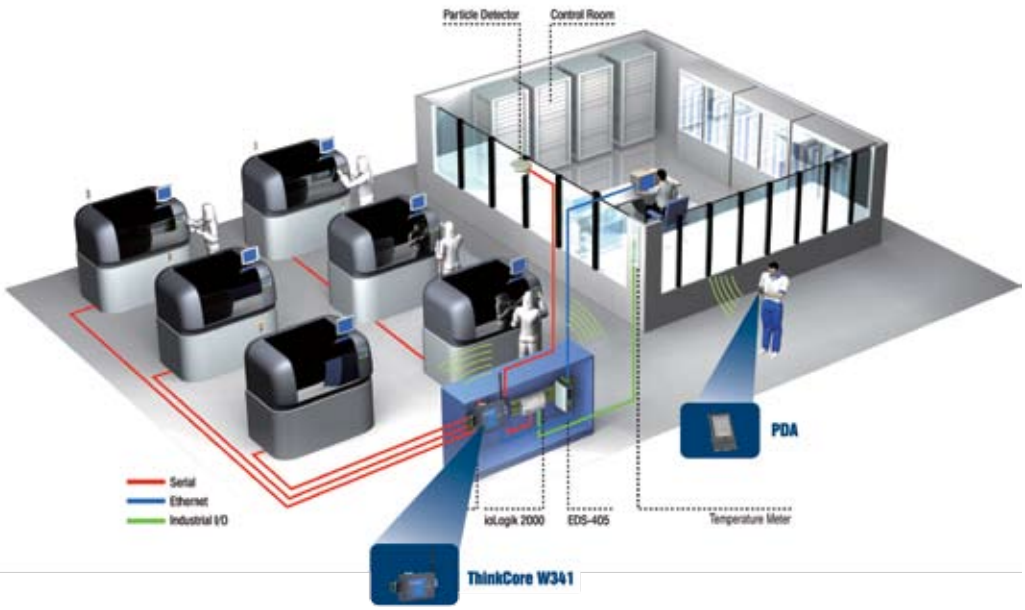
↘Manufacturing

Manufacturing Automation

In the past, management of semi-conductor plants was made difficult due the use of different protocols by different machines, such as SECS/GEM or SECS/HSMS. The use of different protocols makes it hard to establish a coordinated system that can collect, analyze, and process data from every station in the plant. Data must both be processed and sent back to a back-end server for storage.

An embedded computer supporting WLAN can be installed to manage data collection and protocol conversion. The embedded computer can collect data from different interfaces, and provides a programming platform that can be used with custom protocol conversion software. It can also perform preliminary processing before data is sent back to the back-end server, or store the data for backup purposes. With WLAN capability, data can be sent back to the server wirelessly.

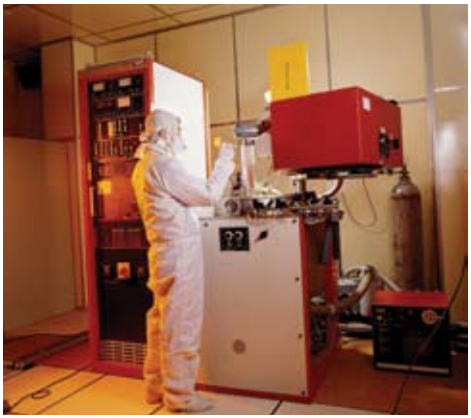
Wireless operation is also an advantage for particle detection in the cleanrooms used in semi-conductor plants. Cleanrooms are areas that must maintain a very low level of environment pollutants, such as dust, airborne microbes, and aerosol particles. Particle detectors typically must be connected to a computer, but the computer itself can be source of unwanted particles. Instead, a lightweight wireless serial device server can be used to transmit information from the particle detector to a monitoring station in another room. If protocol conversion is desired, a wireless embedded computer may be employed instead.



Production Environment Maintenance

The machines used in production areas typically require two connections: one for power and one for the network. However, protruding wires contribute to a disorderly production environment and can be the cause of workplace accidents.

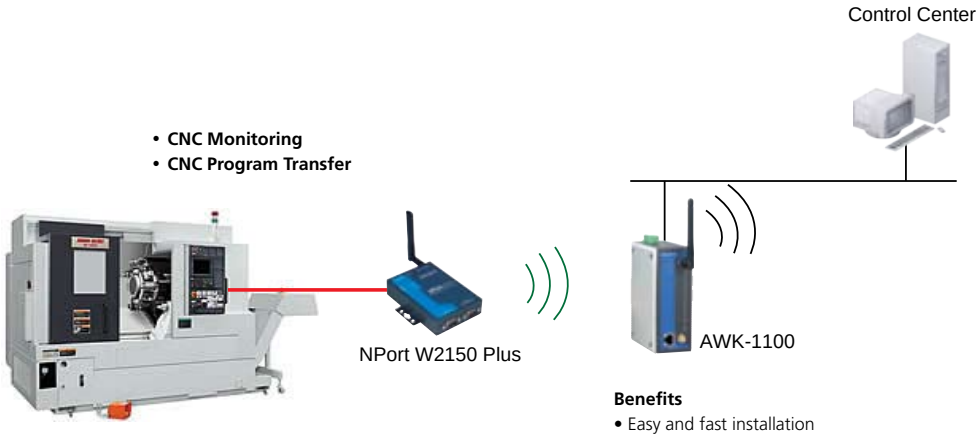
In many situations, the wired network can be replaced with WLAN, which can eliminate up to half the cables that are used in your environment. Fewer cables can also mean a cleaner, safer work area for your employees. With fewer cable connections, machines would also be easier and faster to relocate.



CNC Management System

CNC machines are traditionally programmed directly by operators that physically visit each machine. For hundreds or even thousands of CNC machines that need programming, it is a task that can be extremely time-consuming.

A WLAN installation is one way to control and send instructions to multiple CNC machines remotely and simultaneously. Depending on complexity of data processing required, each CNC machine could be connected to a wireless device server or wireless embedded computer. WLAN operation eliminates the cost of running cables to each machine and makes it easy to move machines anywhere in your production environment.



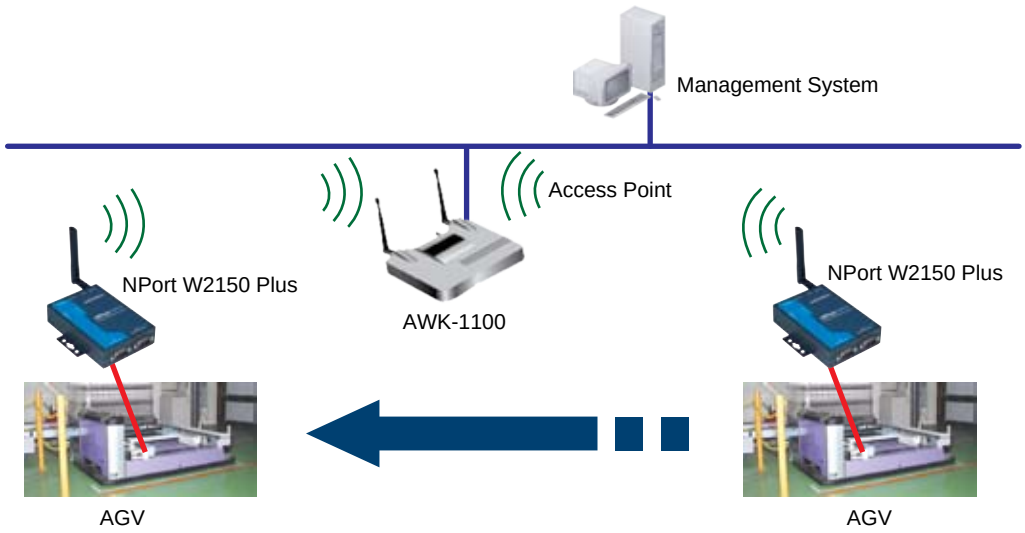
Benefits

- Easy and fast installation
- Provides long distance transmission where wire installations would be

Automated Guided Vehicles

For real-time control of untethered devices such as Automatic Guided Vehicles (AGVs), wireless is a necessity. AGVs require mobility, and wiring them to the network is simply impractical, if not impossible.

Depending on the level of control that you want to achieve, you could outfit each AGV with a wireless device server or a wireless embedded computer. If you simply need to monitor the location of the vehicle or control its movements, a wireless device server would be sufficient. A wireless embedded computer would be more fitting if additional data conversion or other computing tasks were required, such as a backup operating plan in case the AGV loses connection with the back-end server.

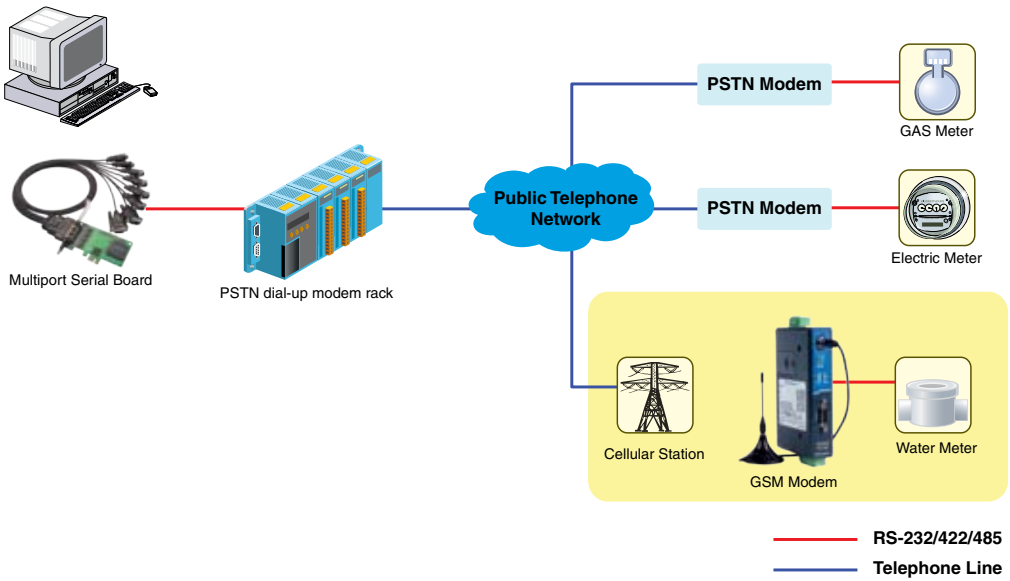


Automated Meter Reading

Dial-up and PSTN Network

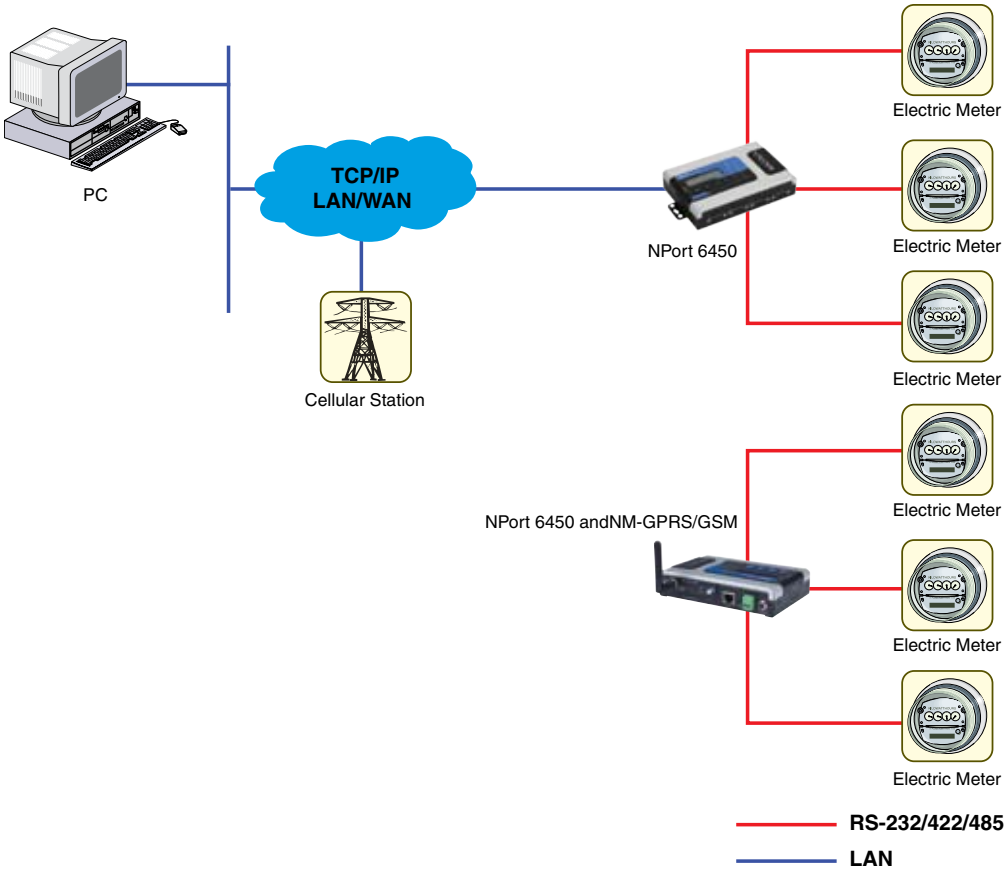
The traditional setup for automated meter reading (AMR) typically involves one PSTN modem for each meter that needs to be monitored. Meter data is sent back to a back-end server over the traditional wired public telephone network. However, implementing AMR with the wired telephone network can be very expensive, especially in very remote areas.

Integrators can save wiring costs or reach very remote areas by switching to wireless AMR. It is an easy and cost-effective way to perform automated reading. You only need to replace the PSTN modems with a GSM modem. No other changes to the network or network devices are required. Meter data can be sent back to the back-end server using the cellular network. If additional front-end computing is required, a cellular embedded computer can be used instead of the GSM modem.



IP-Enabled Meters

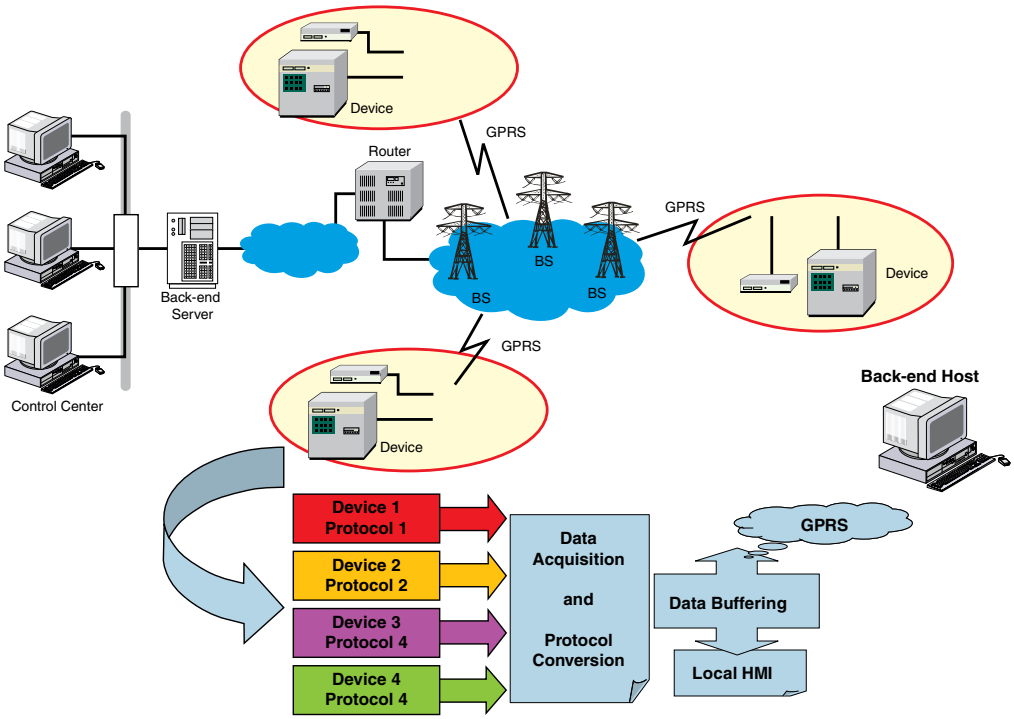
If you are using a multi-port device server to connect multiple meters to your TCP/IP network, you can quickly and easily switch to wireless. Instead of using a network cable to connect the device server to the TCP/IP network, simply attach an industrial cellular modem to the device server. This eliminates the need for a wired connection to the TCP/IP network. Meter data can then be sent to the back-end server using the cellular connection.



Environment Monitoring

Unmanned weather stations play an important role in analyzing and predicting weather patterns. These unmanned stations need to collect and store large amounts of weather data. This data must be periodically uploaded to a back-end server for analysis and long-term storage. Monitoring equipment is located outdoors and sometimes in very remote areas. It can be difficult and expensive to connect this equipment to a monitoring station with cables.

Instead, monitoring equipment can obtain cellular capability with the installation of a wireless embedded computer that supports GPRS. Protocol conversion, data acquisition, and storage can all be performed locally by the embedded computer. The data can then be sent wirelessly to the monitoring station by GPRS. For simpler setups where only data collection is required, a GSM/GPRS modem can be connected to the equipment for an instant cellular connection.



MOXA®

USA
Moxa Technologies, Inc.
Toll-free: 1-888-MOXA-USA (1-888-669-2872)
Tel: +1-714-528-6777
Fax: +1-714-528-6778
www.Moxausa.com
USA@moxa.com

Europe
Moxa Europe GmbH
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99
www.moxa.com
Europe@moxa.com

Taiwan
Moxa Technologies Co., Ltd.
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231
www.moxa.com.tw
Taiwan@moxa.com

China
Moxa Technologies Shanghai, Inc.
Tel: +86-21-5298-8618
Fax: +86-21-5298-8643
www.moxa.com.cn
China@moxa.com

Moxa Technologies Beijing, Inc.
Tel: +86-10-6872-3959/60/61
Fax: +86-10-6872-3958
www.moxa.com.cn
China@moxa.com

Moxa Technologies Shenzhen, Inc.
Tel: +86-755-8368-4084/94
Fax: +86-755-8368-4148
www.moxa.com.cn
China@moxa.com

20th MOXA Since 1987
20 Years of Excellence

PN: 1900000009896