Wireless Solutions

- Wireless Introduction & Features
- Industrial Wireless Device Servers
- Wireless AP Introduction & Features
- Industrial Wireless LAN Access Point

Wireless Solutions

Introduction

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. Most industrial plants that deploy wireless are very satisfied with their first applications, and want to add more wireless throughout the plant. Ensuring performance, security, and reliability for many wireless applications can be complex, however. Industrial wireless application networks can provide ready access to reliable information about critical plant operations and physical assets from disparate applications, systems, and devices. Whether you are generating power, refining petroleum, processing chemicals, or manufacturing any other type of product, SUNIX can give you the confidence you need to choose wireless.

Why?

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 markets. 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.

In a factory area, 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 easier and simpler to gain temporary access to plant machinery for diagnostic or programming purposes.

Standards

A wireless local area network (WLAN) is a LAN that does not rely on cables. 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.

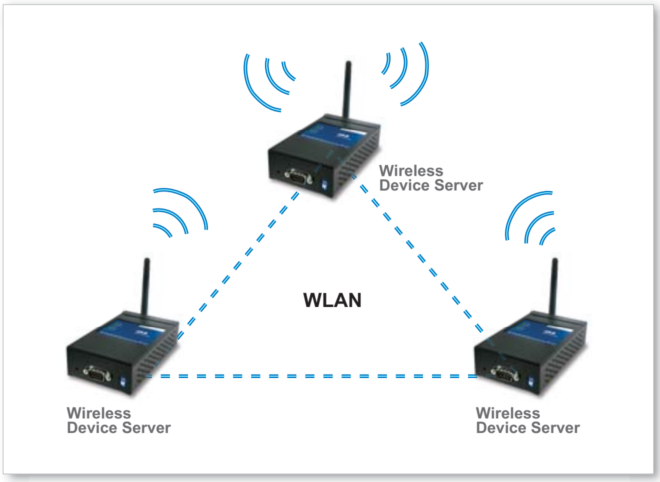
Every application has its own, unique requirements, but certain considerations are common across most wireless applications, like transmission range, data rate, reliability, and security. WLAN technology is ideal for applications where a network infrastructure is already in place, and is typically used when wireless Ethernet/Internet access is required at high data transfer speeds. 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.

	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a
Bandwidth	11Mbps	54Mbps	54Mbps
Frequency	2,4GHz	2.4GHz	5GHz
Distance	300m (outdoor) 45m (indoor)	300m (outdoor) 45m (indoor)	Limited range 20m (indoor)
Spread Spectrum	DSSS	OFDM	OFDM
Deployment	Highest Market Share	Becoming mainstream	Not much deployment

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.

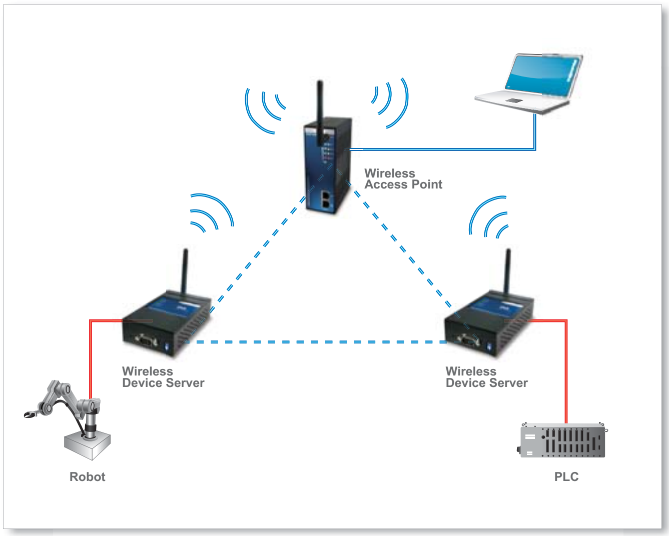
Ad-hoc mode is fast and easy to set up. It is an acceptable method for establishing a temporary, short-range wireless network.



Infrastructure Mode

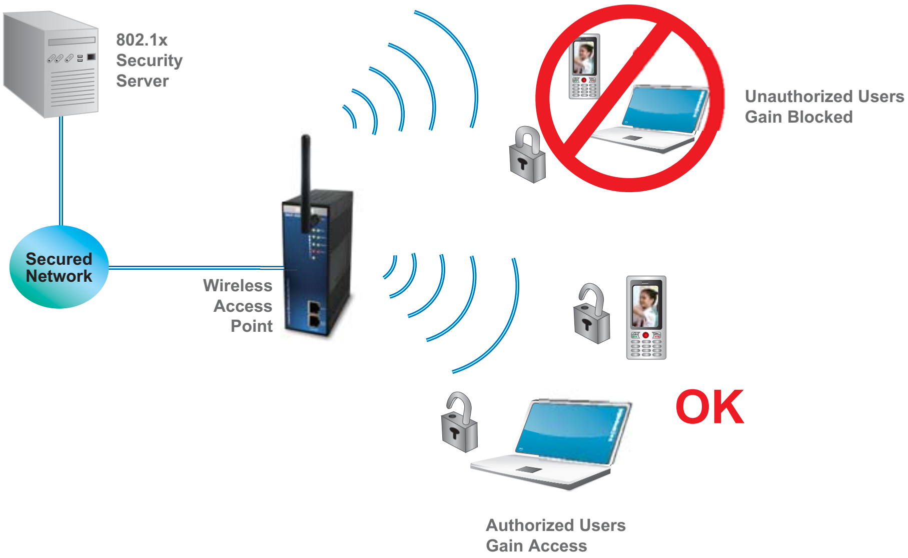
Logically, an infrastructure network is the wireless equivalent of the Ethernet hub. A fundamental aspect of infrastructure mode is that wireless clients cannot talk directly to each other; they must communicate through the network behind the access point.

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.



Security

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.

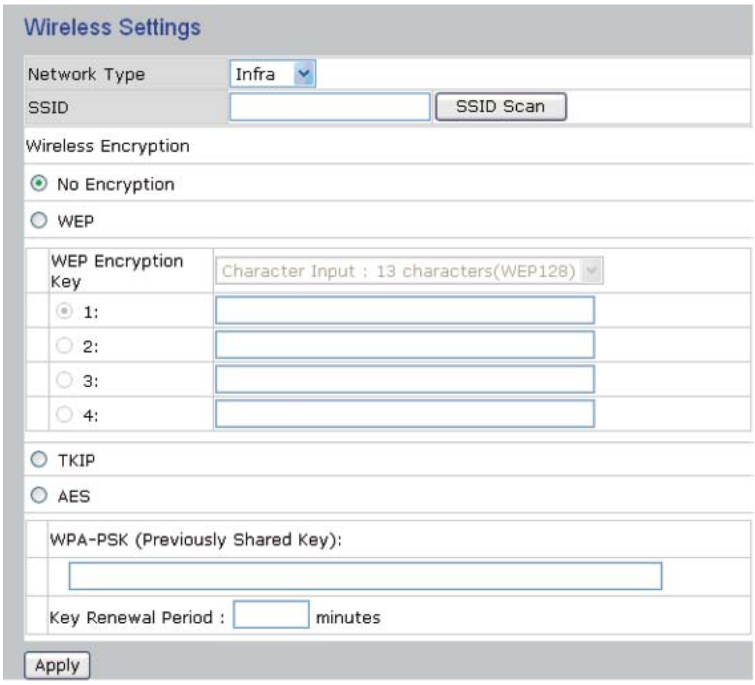


There are two main forms of security that require attention for WLANs:

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.



Wireless Settings

Network Type	Infra
SSID	SSID Scan

Wireless Encryption

● No Encryption

○ WEP

WEP Encryption Key	Character Input : 13 characters(WEP128)
● 1:	
○ 2:	
○ 3:	
○ 4:	

○ TKIP

○ AES

WPA-PSK (Previously Shared Key):

Key Renewal Period : minutes

Apply

The following four methods are currently available for WLAN security: WEP, WPA, WPA2, and 802.1x.

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.

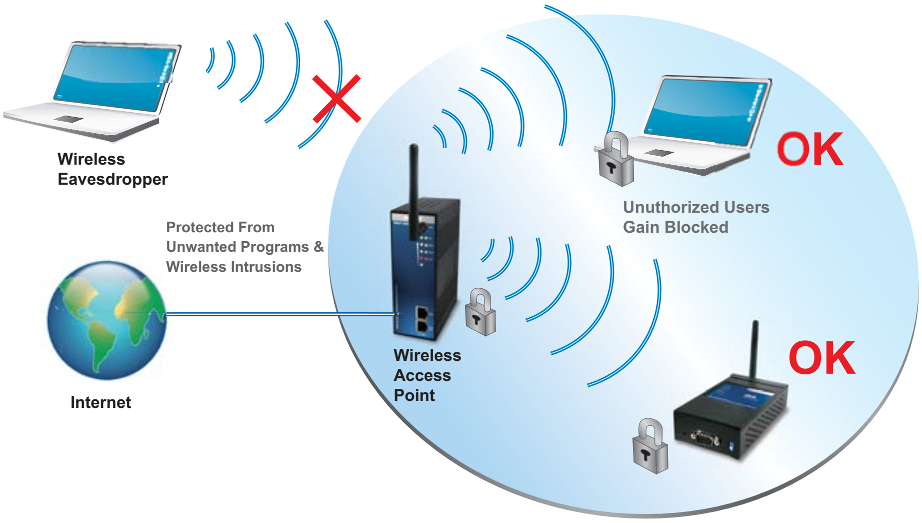
WPA2

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.



Industrial Wireless Device Servers

Model Name		IDS-1011W	IDS-2011W	IDS-3011W
Product				
Description		1-port RS-232 to 802.11 b/g WLAN & 1-port 10/100TX LAN Device Server	1-port RS-422/485 to 802.11 b/g WLAN & 1-port 10/100TX LAN Device Server	1-port RS-232/422/485 to 802.11 b/g WLAN & 1-port 10/100TX LAN Device Server
Serial Communication	Number & Port Types	1 x RS-232	1 x RS-422/485	1 x RS-232/422/485
	Connector	DB9 M	5-pin terminal block	DB9 M
	Speed	110bps ~ 460.8Kbps		
	Serial Parameters	Data Bits: 5,6,7,8 Parity: odd, even, none, mark, space Stop Bits: 1, 1.5, 2		
	Flow Control	XON/XOFF, RTS/CTS, DTR/DSR		
	RS-232 Signals	TxD,RxD,RTS,CTS,DTR, DSR, DCD, RI, GND	—	TxD,RxD,RTS,CTS,DTR, DSR, DCD, RI, GND
	RS-422 Signals	—	TxD+, TxD-, RxD+, RxD-, GND	
	RS-485 (4-wire) Signals	—	TxD+, TxD-, RxD+, RxD-, GND	
	RS-485 (2-wire) Signals	—	Data+, Data-, GND	
	ESD	15KV Protection		
LAN	10/100M Ports	1 x RJ-45 10/100Mbps (auto-negotiation)		
	Protection	1.5KV Magnetic Isolation		1.5KV Magnetic Isolation
Wireless	Modulation	802.11b:CCK,DQPSK, DBPSAK, 801.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM		
	Radio Frequency	DSSS		
	Antenna Connector	Reverse SMA		
	Frequency Band	America/FCC: 2.412~2.462 GHz (11 channels) Europe CE/ETSI: 2.412~2.472 GHz (13 channels)		
	Transmission Rate	802.11b – 11Mbps / 802.11g – 54Mbps		
	Transmission Power	16dBm		
	Receiver Sensitivity	-81dBm @ 11Mbps, PER < 8% -64dBm @ 54Mbps, PER < 10%		
	Wireless Security	SSID Broadcast disable		
	Encryption Security	WEP 64/128 bit; WPA, WPA2, 802.11i (Pre-shared Key (PSK) mode; 802.1X; TKIP		
	Network Mode	Client Mode		
Software	Operation Mode	Virtual COM, TCP Server, TCP Client, UDP, Serial Tunnel		
	Protocols	ICMP, IP, TCP, UDP, DHCP, BootP, ARP / RARP, DNS, SNMP MIB II, HTTPS, SSL, SSH		
	COM Drivers	Windows NT / 2000 / XP / 2003 / Vista TTY Drivers for Linux		
	Configuration	Web Console, Serial Console, IDS Utility for Windows		
	Event Warning	Syslog, E-mail, SNMP trap,Beeper		
Power	Redundancy	Dual Power Inputs (Terminal Block & DC Jack type)		
	Connectors	3-pin Removable Terminal Block + DC Jack		
	Protection	Reverse		
	Consumption	7 Watts maximum		
	Input	12~48 VDC (12VDC)		
	Alarm Contact	—		
Certifications	EMI	FCC Part 15, CISPR (EN55022) Class A		
	EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge) Level 3, EN61000-4-6 (CS) Level 3		
	Shock	IEC60068-2-27		
	Freefall	IEC60068-2-32		
	Vibration	IEC60068-2-6		
Environment	Operating Temperature	-10°C to 55°C		
	Operating Humidity	5% ~ 95%RH		
	Storage Temperature	-20°C ~ 85°C		
Mechanical	Dimensions	72 x 31 x 125 mm (W x D x H) (without connectors)		
	Enclosure	Metal (IP30 protection)		
	Mounting	DIN Rail and Wall Mount		
WARRANTY		5 years		

Note : All models are supplied without power adaptor

Industrial Wireless Device Servers

Model Name		DS-2042W-I	DS-3042W
Product			
Description		4-port RS-422/485 with 2KV Isolation to 802.11 b/g WLAN & 2-port 10/100TX LAN Device Server	4-port RS-232/422/485 to 802.11 b/g WLAN & 2-port 10/100TX LAN Device Server
Serial Communication	Number & Port Types	4 x RS-422/485	4 x RS-232/422/485
	Connector	5-pin terminal block	DB9 M
	Speed	110bps ~ 460.8Kbps	—
	Serial Parameters	Data Bits: 5,6,7,8 Parity: odd, even, none, mark, space Stop Bits: 1, 1.5, 2	
	Flow Control	XON/XOFF, RTS/CTS, DTR/DSR	
	RS-422 Signals	TxD+, TxD-, RxD+, RxD-, GN	
	RS-485 (4-wire) Signals	TxD+, TxD-, RxD+, RxD-, GN	
	RS-485 (2-wire) Signals	Data+, Data-, GND	
	ESD	15KV Protection	
	Isolation	2.5KV (optional)	
LAN	10/100M Ports	2 x RJ-45 10/100Mbps (auto-negotiation)	
	Redundancy	10ms (Redundant Dual LAN Ports)	
	Protection	802.11b:CCK,DQPSK, DBPSAK, 801.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM	
Wireless	Modulation	DSSS	
	Radio Frequency	Reverse SMA	
	Antenna Connector	America/FCC: 2.412~2.462 GHz (11 channels)	
	Frequency Band	Europe CE/ETSI: 2.412~2.472 GHz (13 channels)	
	Transmission Rate	802.11b – 11Mbps / 802.11g – 54Mbps	
	Transmission Power	16dBm	
	Receiver Sensitivity	-81dBm @ 11Mbps, PER < 8% -64dBm @ 54Mbps, PER < 10%	
	Wireless Security	SSID Broadcast disable	
	Encryption Security	WEP 64/128 bit; WPA, WPA2, 802.11i (Pre-shared Key (PSK) mode; 802.1X; TKIP	
	Network Mode	Client Mode	
Software	Operation Mode	Virtual COM, TCP Server, TCP Client, UDP, Serial Tunnel	
	Protocols	ICMP, IP, TCP, UDP, DHCP, BootP, ARP / RARP, DNS, SNMP MIB II, HTTPS, SSL, SSH	
	COM Drivers	Windows NT / 2000 / XP / 2003 / Vista TTY Drivers for Linux	
	Configuration	Web Console, Serial Console, IDS Utility for Windows	
	Event Warning	Syslog, E-mail, SNMP trap, Relay, Beeper	
Power	Redundancy	Dual Power Inputs (Terminal Block & DC Jack type)	
	Connectors	6-pin Removable Terminal Block	
	Protection	Reverse	
	Consumption	7 Watts maximum	
	Input	12~48 VDC (12VDC)	
	Alarm Contact	1 x Configurable Relay Output	
Certifications	EMI	FCC Part 15, CISPR (EN55022) Class A	
	EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge) Level 3, EN61000-4-6 (CS) Level 3	
	Shock	IEC60068-2-27	
	Freefall	IEC60068-2-32	
	Vibration	IEC60068-2-6	
Environment	Operating Temperature	-10°C to 55°C	
	Operating Humidity	5% ~ 95%RH	
	Storage Temperature	-20°C ~ 85°C	
Mechanical	Dimensions	52 x 106 x 144 mm (Wx DxH) (without connectors)	
	Enclosure	Metal (IP30 protection)	
	Mounting	DIN Rail and Wall Mount	
WARRANTY		5 years	

Note : All models are supplied without power adaptor

Wireless AP

Introduction

SUNIX Wireless Access Point is a reliable IEEE802.11b/g WLAN with 2-port LAN Access Point. It can be configured to operate in AP/Bridge/Repeater mode. Users are able to configure Wireless Access Point by Windows Utility or WEB interface via LAN port or WLAN interface. The wireless LAN solution with up to 54Mbps data transfer rate gives an easy way to connect hard-to-wire serial devices.

SUNIX Wireless Access Point also provides dual Ethernet ports in switch mode, so that users can use Daisy Chain to reduce the usage of Ethernet switch ports. In addition, SUNIX Wireless Access Point offers PoE (PD) feature on ETH2 which is fully compliant with IEEE802.3af specifications. Therefore, SUNIX Wireless Access Point is the best communication solution for outdoor wireless applications.

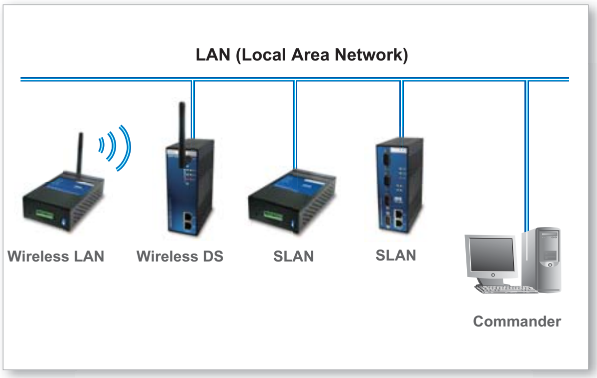
Features

- **WLAN interface support up to 54Mbps link speed**
- **Support WEP / WPA / WPA2 / 802.1X / Radius / TKIP high security capability**
- **Support AP / Bridge / Repeater mode**
- **Daisy Chain support to reduce usage of switch ports**
- **Support Redundant Power Inputs**
- **Fully Compliant with IEEE802.3af**
- **Secured Management by HTTPS and SSH**
- **Event Warning by Syslog, Email, SNMP Trap, Relay and Beeper**

Getting Wired Less

Though wireless is not for every thing, but if your application uses mobile equipment that is controlled over a network, or cabling installation is impossible for one or other reason, then wireless local area network (WLAN) is the right option. The IEEE802.11 standard paved the way to use radio frequency (RF) technology to send Ethernet packets on air. WLAN applications work as the same way as wired LAN over TCP/IP protocol.

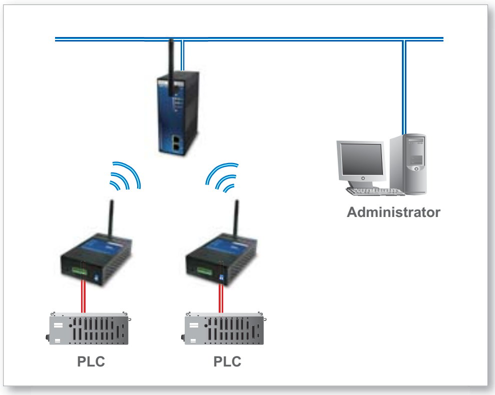
Wireless is easy to deploy, highly flexible, and cost-effective technique, which makes it ideal for many networking requirements.

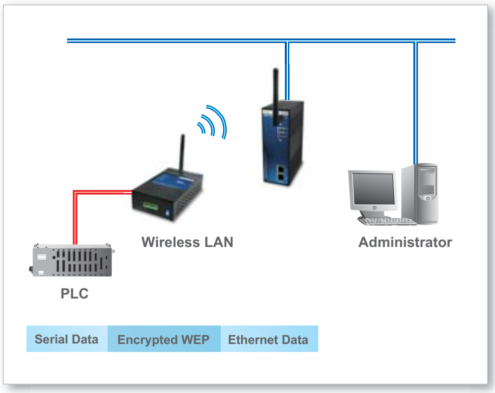


Wireless Networking Modes

There are two major methods to configure a wireless LAN; Ad-hoc mode and Infrastructure mode. In Ad-hoc mode, stations use peer-to-peer transmission to transfer data from station to station. There is no requirement of AP (Access Point) to a wired network. It is the most convenient and cost-effective setup.

Infrastructure mode requires an AP, which can be use by itself to set up a WLAN, or connect WLAN to a wired LAN, so all communication goes through the Wireless AP.





Wireless & Safety

Data safety is the biggest concerns critics have for the wireless LAN since the data is transmitted by radio waves. SUNIX provides the best security features like WPA and WEP to guarantee the confidentiality of data. SUNIX wireless products offer complete suit of WPA (WPA-PSK, TKIP and IEEE802.1X) encryption for secured WLAN.

Redundancy

Communication redundancy is provided by offering two Ethernet ports, which means communication without any lost of data bit. In case of failure, the backup path will be activated in less than 10ms to keep the communication continuous.

Dual DC power inputs with AC power adaptor option means avoiding any failure due the power outage. SUNIX products mean the quality and features that keeps your mission critical industrial networks running without any failure.

POE SUPPORT

WAP-5000 series supports PD at ETH2 and converts the electrical power up to 8 Watts. This feature is fully compliant with IEEE802.3af specification and provides 1KV isolating protection. This PD feature enables AP to speed up the installation of equipment and extend the range of layout to a maximum of 100 meters without additional power source. Therefore, WAP-5000 series is the best WLAN AP solution for PoE (PD) applications such as IP cameras and/or VOIP.

Industrial Wireless LAN Access Point

Model		WAP-5002	WAP-5002P
Product			
Description		Industrial 802.11b/g Wireless LAN Access Point with 2-port RJ45 LAN	Industrial 802.11b/g Wireless LAN Access Point with 2-port RJ45 LAN (1-port PoE PD)
Wireless	Modulation	802.11b:CCK,DQPSK, DBPSAK 801.11g: OFDM with BPSK, QPSK, 16QAM, 64QAM	
	Radio Frequency	DSSS	
	Antenna Connector	Reverse SMA	
	Frequency Band	America/FCC: 2.412~2.462 GHz (11 channels) Europe CE/ETSI: 2.412~2.472 GHz (13 channels)	
	Transmission Rate	802.11b – 11Mbps / 802.11g – 54Mbps	
	Transmission Power	16dBm	
	Receiver Sensitivity	-81dBm @ 11Mbps, PER < 8% -64dBm @ 54Mbps, PER < 10%	
	Wireless Security	SSID Broadcast disable	
	Encryption Security	WEP 64/128 bit; WPA, WPA2, 802.11i (Pre-shared Key (PSK) mode; 802.1X; TKIP	
	Network Mode	AP, Bridge, Repeater	
LAN	10/100M Ports	2 x RJ45 10/100Mbps (Switch Mode)	2 x RJ45 10/100Mbps (1-port PoE)
	Protection	1.5KV Magnetic Isolation	
Power Over Ethernet	PoE Port	—	ETH 2
	Standard	—	IEEE802.3af compliant PD
	Power Consumption	—	8 Watts maximum
	Protection	—	Overload & Short Circuit
	Isolation Voltage	—	1000 VDC min
	Isolation Resistance	—	100000000 ohms min
Software	Protocols	ICMP, IP, TCP, UDP, DHCP, BootP, ARP / RARP, DNS, SNMP MIB II, HTTPS, SSL, SSH	
	Configuration	Web Console, SSH Console, Utility for Windows	
	Status Monitoring	Associated wireless clients (AP mode), Current DHCP mappings, System event log (local log, remote syslog, SNMP trap), Wireless link status monitor (AP Client mode)	
	Port Security	MAC based access control, IP filtering, DHCP server disable, static DHCP mapping	
	DHCP	DHCP Client / DHCP Server	
	Alarm Notification	Link down/Power down alarm by Relay, Output/SNMP Trap/System Log	
Power	Redundancy	Dual Power Inputs (Terminal Block)	
	Connectors	6-pin Removable Terminal Block	
	Protection	Reverse	
	Consumption	6 Watts maximum	
	Input	12~48 VDC (12VDC)	
	Alarm Contact	1 x Configurable Relay Output	
Certifications	EMI	FCC Part 15, CISPR (EN55022) Class A	
	EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge) Level 3, EN61000-4-6 (CS) Level 3	
	Shock	IEC60068-2-27	
	Freefall	IEC60068-2-32	
	Vibration	IEC60068-2-6	
Environment	Operating Temperature	-10°C to 55°C	
	Operating Humidity	5% ~ 95%RH	
	Storage Temperature	-20°C ~ 85°C	
Mechanical	Dimensions	52 x 106 x 144 mm (Wx DxH) (without connectors)	
	Enclosure	Metal (IP30 protection)	
	Mounting	DIN Rail and Wall Mount	
WARRANTY		5 years	

Note : All models are supplied without power adaptor