



ARCH ROCK

WHITE PAPER

IP-based Wireless Sensor Networking: Secure, Reliable, Low-Power IP Connectivity for IEEE 802.15.4 Networks

written by
Arch Rock Corporation
www.archrock.com



IP-based Wireless Sensor Networking: Secure, Reliable, Low-Power IP Connectivity for IEEE 802.15.4 Networks

Synopsis

Until recently, the use of the Internet Protocol (IP) on wireless embedded networks was not considered viable, because it was too difficult to scale down IP sufficiently to operate on microcontrollers and low-power links – notably on the IEEE 802.15.4 radio link. The emergence of the IETF 6LoWPAN standard for IP communication over low-power radio has changed all that. This low-power wireless IP option offers a new set of longevity, security and ease-of-integration tradeoffs that make it a superior alternative to existing options.

The need for an IP alternative

Makers of industrial instrumentation have repeatedly grappled with questions of how and when to utilize IP-based interconnects in place of their more traditional, often proprietary, industrial counterparts. In its favor IP offers widespread commercial adoption, rapid development cycles and broad interoperability. Ethernet led the way as an alternative to RS485 and other multi-drop busses; and many industrial standards, including BACNet, LonTalk, CIP and SCADA, introduced an “IP option” using either TCP/IP or UDP/IP over Ethernet.

IP's ease of integration and broad interoperability, however, have raised some fears about vulnerability to attack. Moreover, IP was thought to be unsuited for use in wireless embedded networks, because bulky IP protocols could not be reduced in size to operate on microcontrollers and low-power links such as IEEE 802.15.4 radio. IEEE 802.15.4 packets are quite small, and the entire stack must fit within a very small memory footprint.

Meanwhile, the abundant benefits of operating above IP, rather than directly on the particular link, became apparent as the broad commercialization of Ethernet yielded 10, 100 and 1,000 mbps in short order and at low cost. In addition, WiFi (IEEE 802.11) emerged as the dominant wireless link for computers, laptops and PDAs. Once link-level security was in place with WiFi Protected Access (WPA), this became widespread in industrial environments as well – just another link under IP. Given its high power consumption, WiFi has been most widely adopted on handheld client devices and embedded PCs, which are recharged on a daily basis or mains powered.

The completion in 2007 of the IETF 6LoWPAN (RFC 4944) standard for IPv6 communication over 802.15.4 extends these same communication capabilities beyond handhelds to geographically dispersed low-power devices whose battery power must last for months or even years. To be competitive with more limited link-specific protocols, 6LoWPAN utilizes a pay-only-for-what-you-use header-compression scheme. Its built-in support for AES-128 encryption offers the basis for robust authentication and security, and, through direct integration with IP routers, it can take advantage of advanced network security schemes rather than depending on those provided by ad hoc gateways.

The Internet Engineering Task Force (IETF): the Real OPEN Standards Body

Formed in 1986, the IETF is “a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.” It is an open, standards organization that does not have any formal membership or membership requirements where all its participants and leaders are volunteers. As a result, the standards process and results are unbiased and generally reflect the good of the industry over the ambitions of any one particular organization or company as is the case with other industry standards bodies. More importantly, the results speak for themselves. Today there are more than half a billion IP hosts based on a layered architecture that provides interoperability for diverse applications across broad and ever-evolving communications technology.

The Internet architecture: Standing the Test of Time and Scale

The Internet architecture is defined in layers, with the Internet Protocol (IP) being the middle layer that forms a “narrow waist,” allowing diverse applications above to utilize a variety of communication links below in a common, link-independent fashion. Software is highly leveraged, because it is built on TCP/IP or UDP/IP data transports, regardless of the particular physical devices underneath. IP allows different kinds of links to be connected together as a single network, with routers steering each message to its desired destination, crossing different kinds of links along the way.

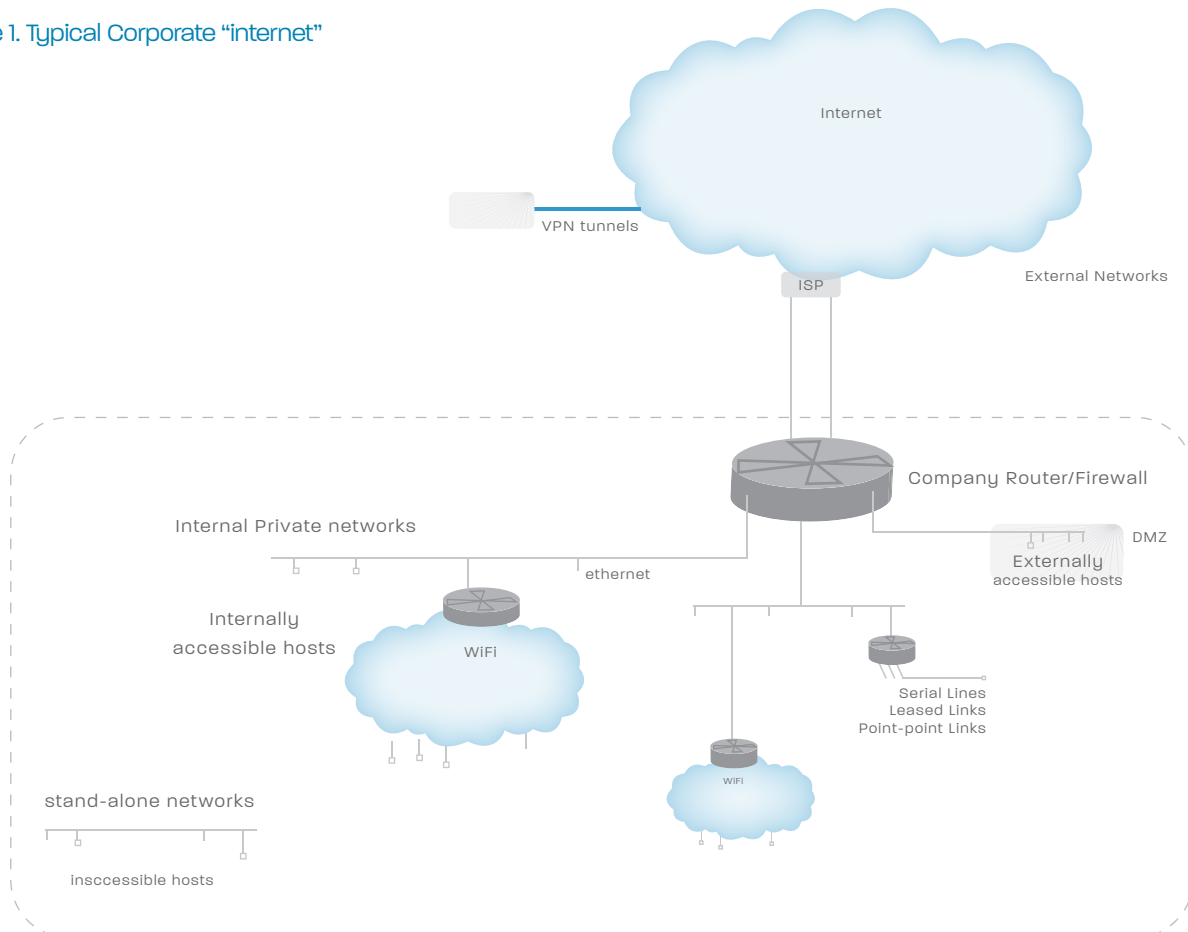
This versatility and independence is one of the primary reasons IP continues to be relevant and pervasive more than 20 years after its initial specification, which has particular significance to someone who is making long-term infrastructure choices. Furthermore, an IP infrastructure is the ONLY network that is proven to scale to networks of a million or more nodes.

The industrial or corporate network is typically a “small internet” composed of Ethernet and WiFi sub-networks. It is connected to the public Internet through specialized firewall routers, which typically allow only certain machines or “hosts” to be accessible from outside while permitting most internal machines to access hosts outside. Each host has an IP address (e.g., 192.168.2.33) and a hostname (e.g., devel.acme.com). The address may be public (accessible externally) or private (accessible only internally). Internet protocols locate and route information to and from accessible hosts, transparently crossing multiple links in order to get there (see Figure 1).

By making details of the underlying physical links available – such as their packet size and how they are interconnected – Internet protocols provide for interoperability, separation, and incorporation of new technology. Applications interact with other applications and with services by transferring application-level information directly, regardless of the physical interconnections. A laptop client machine may access a corporate server, a networked printer and a network control unit in the same fashion, even though one may be wireless, another on the manufacturing floor Ethernet, and a third in the back office. If any of these devices or networks is upgraded, it can still function and interact in the same logical manner.

Security is addressed at several levels: physical protection of the wires and devices, encryption of the data that is transferred over wired and wireless links, and control of the ability to name or route messages to hosts and services.

Figure 1. Typical Corporate “internet”



IEEE 802.15.4: a new standard low-power wireless link

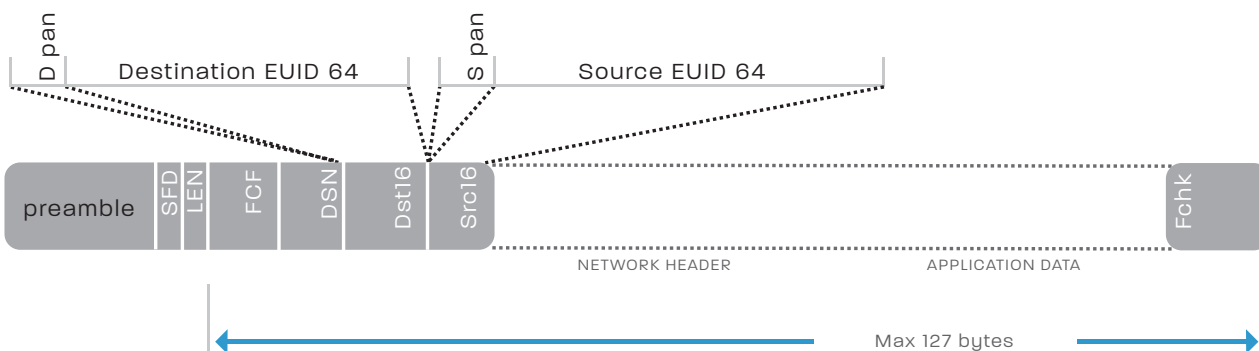
Each communication link conforms to specific lower-level standards, including the coding scheme and the basic structure of a packet, so that the physical devices can talk to each other. IEEE 802.15.4, the latest wireless link standardized by the IEEE (in 2004), is designed to enable the development of compact, low-power, relatively inexpensive embedded devices that can run on batteries for extended periods (1-5 years). It is used in numerous proprietary offerings and industry-specific standardization efforts – including ZigBee, SPI00.11a, and Wireless HART – in home and industrial automation applications. IEEE 802.15.4 carries information on radio transceivers at 2.4 GHz, roughly the same unregulated band as WiFi and Bluetooth. But it transmits at a maximum power of one milliwatt - just one percent of the power of WiFi or cellular phones, with one hundred times the lifetime and at a fraction of the cost. Because this low power limits transmission range, collections of these devices must work together to route information hop-by-hop over longer distances and around obstacles – much the way information is routed in the Internet.

The IEEE 802.15.4 coding scheme spreads information over a spectrum of frequencies with built-in redundancy to make it more robust in harsh environments (e.g., around heavy machinery) than the many prior proprietary low-power radios. Multi-hop routing protocols can further enhance reliability by routing around obstacles, detecting losses and retransmitting packets, and even utilizing multiple next-hop candidates.

Figure 2. illustrates the format of the small IEEE 802.15.4 packets. Each packet begins with several bytes of preamble so the receiver can “lock on” and determine what is coming. The header contains source and destination address fields that specify where it came from and who should receive it. Much like with Ethernet (IEEE 802.3) and WiFi (IEEE 802.11), each device has a unique, relatively large, identifier (EUID 64) associated with it at the time of manufacturing. Because 802.15.4 packets are so small, a 16-bit short address can be assigned dynamically to devices and used instead for communication. Furthermore, collections of devices can be partitioned into distinct logical networks by assigning a 16-bit PAN-ID to each collection, much like the SSID in WiFi networks.

All network protocols built on IEEE 802.15.4 use this same basic frame format and link-level header. The additional information they must exchange for correct operation is placed within the data payload section as a network-level header. For example, when data is communicated over multiple hops, the network header specifies where it starts, where it ends, and how to get from one to the other. Unfortunately, each of the current proprietary protocols and industrial protocols perform this network-level operation differently. Moreover, none of them addresses how such packets are transferred out of or into the 802.15.4 network to and from existing computers, controllers and devices on other networks in the plant, factory or enterprise.

Figure 2. IEEE 802.15.4 Packet Frame Format



IETF 6LoWPAN: Making IP work over a low-power link

The 6LoWPAN working group of the Internet Engineering Task Force (IETF) was chartered to define how to carry IP-based communication over IEEE 802.15.4 links in a manner that conforms to open standards and provides interoperability with other IP links and devices, as well as among 802.15.4 devices.

Not only does such a standard allow many different companies to manufacture LoWPAN devices that can work together in a network, but these devices can work with the many networked computers and devices that already exist. This eliminates the need for an array of complex gateways (i.e., one for each different local 802.15.4 protocol) and the many adapters required for existing applications to communicate through these gateways, as well as the many gateway-specific security and management procedures. Familiar interfaces can be used in existing machines and applications. The vast body of IP-based standards that have been hardened over many years to provide security, authentication, translation, look-up, configuration and management can be adopted directly, rather than reinvented. The existing ecosystem of established IP-based tools, techniques and best practices can be utilized immediately to incorporate and manage these new devices.

Indeed, most industrial communication standards, which were originally developed to provide interoperability over particular industry-specific busses and links, already support an IP option. For example, BACNet evolved from RS232 and RS485, and LONworks from dedicated twisted pairs and power-line, to IP over Ethernet. The Common Industrial Protocol (CIP) evolved from CAN and DeviceNet to EtherNet/IP with the explicit recognition that EtherNet was a placeholder for many additional physical links under IP. WiFi has enjoyed that same path of entry, and even SCADA and Foundation FieldBus have IP options. Although these networks are deployed, utilized, and managed very differently in the industrial setting than in the IT enterprise, the value lies in leveraging broad commercial developments and incorporating new technology without replacing all the old.

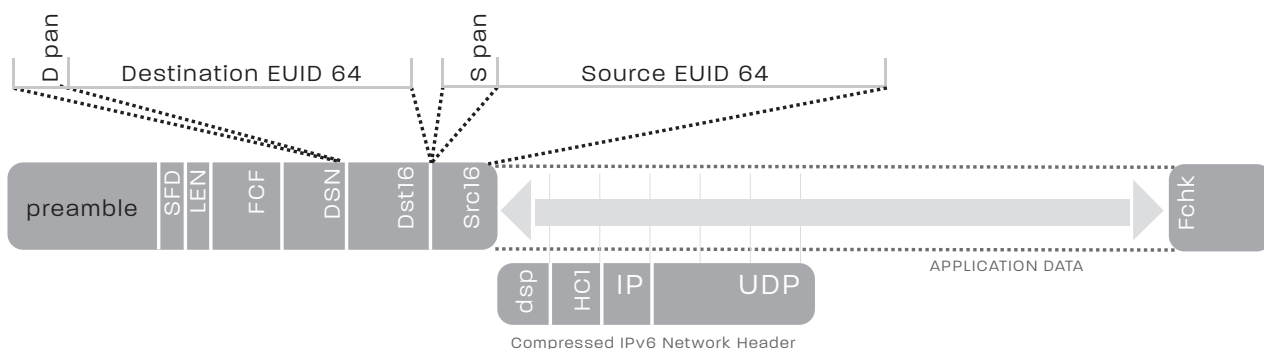
Unfortunately, the utility of IP does not come for free. IP packets contain large addresses and headers, and data payloads may be much too large to fit within the small 127-byte MTU (maximum transmission unit) of 802.15.4. The technical challenge addressed by the 6LoWPAN group was to devise a means of squeezing IP down into small packets that would carry only the bare essentials.

The resulting 6LoWPAN format was conceived as a “pay as you go” plan. The extremely compact basic header expands as broader IP capabilities are utilized. In the example shown in Figure 3, the entire 40-byte IPv6 header plus the 8-byte UDP transport header are compressed down into just 7 bytes, even smaller than a typical ZigBee header.

Starting with the simplest case, when an 802.15.4 device communicates with a nearby 802.15.4 device, the IP addresses of the source and destination can be compressed to almost nothing. A single “header compression” byte is used to say that the IP addresses should be inferred from the link addresses in the basic 802.15.4 packet. When communication occurs with other devices outside the embedded network, the larger IP address is included. When the amount of data exchanged is small enough to fit in a basic packet, it can be included with no overhead; for large transfers, a “fragmentation header” is added to keep track of how the large message is broken into fragments. If a single 802.15.4 can get the packet to its destination, it can be transmitted with no overhead; if multiple hops are required, a mesh routing header is included. Or, IP routing can be used within the embedded network.

Thus, the simplest, most frequent case is handled very efficiently, with additional information included in the header as the task becomes more complex. As a result, 6LoWPAN is just as efficient as current link-level protocols for the limited cases they address, but, unlike those protocols, it extends gracefully to much broader usage.

Figure 3. IETF 6LoWPAN packing IP into a small IEEE 802.15.4 packet



Security and wireless instrumentation

Once various devices and networks can be connected together, it is critical to assess the security implications of such connections. For one thing, wireless communication raises the possibility of devices “overhearing” each other; physical security alone cannot be relied on to protect the information transfer. Encryption provides a basic level of protection. IEEE 802.15.4 specifies a very strong form of encryption, AES-128, and essentially all 802.15.4 chips perform the encryption in hardware. Each device contains a protected key, typically established during commissioning, which is used to encrypt packets as they are transferred to the radio and decrypt packets as they are received. The key is also used to authenticate the device to the infrastructure, so that rogue devices cannot pretend to provide useful information.

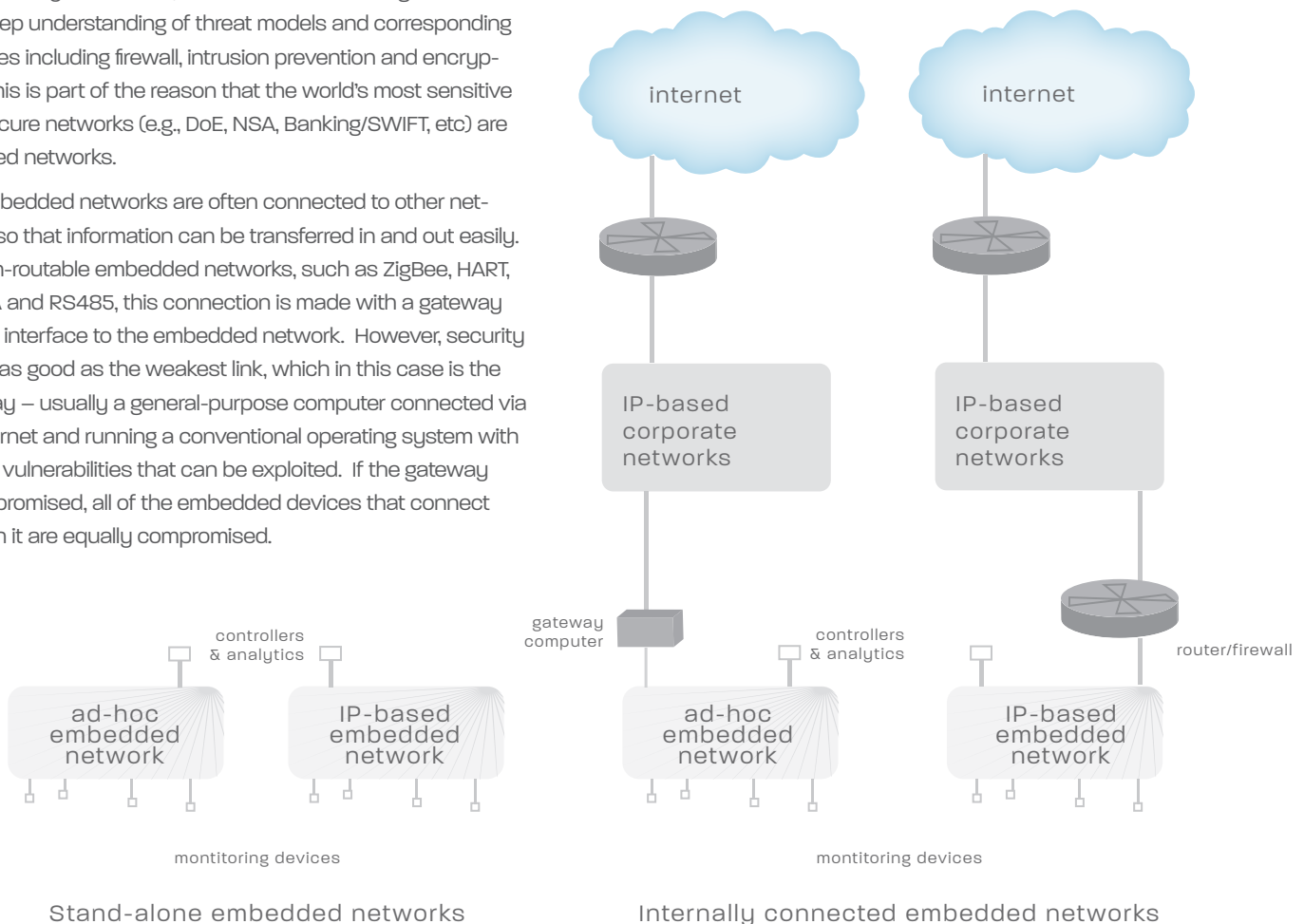
Additional security measures, illustrated in Figure 4, focus on how the embedded wireless network is connected to other networks. Of course the most secure network is stand-alone, disconnected from all other computing devices. The level of protection here is the same whether the network is IP-based or a proprietary non-routable protocol, because there is no physical way to route into or out of the network. Access can be obtained only from within, but IP has the advantage of a broad and deep understanding of threat models and corresponding remedies including firewall, intrusion prevention and encryption. This is part of the reason that the world’s most sensitive and secure networks (e.g., DoE, NSA, Banking/SWIFT, etc) are IP-based networks.

But embedded networks are often connected to other networks so that information can be transferred in and out easily. For non-routable embedded networks, such as ZigBee, HART, SCADA and RS485, this connection is made with a gateway and an interface to the embedded network. However, security is only as good as the weakest link, which in this case is the gateway – usually a general-purpose computer connected via IP/Ethernet and running a conventional operating system with known vulnerabilities that can be exploited. If the gateway is compromised, all of the embedded devices that connect through it are equally compromised.

To reduce its vulnerability, the gateway is typically put behind a firewall that limits the scope of the networks with which it can communicate.

When the embedded network is itself IP-based – when sensor nodes natively support IP, as the advent of 6LoWPAN permits – the gateway is reduced to a simple router between the conventional network and the embedded network. This is a specialized device that need not run a general-purpose operating system or applications. It can be configured and managed like the other routers and firewalls that protect the conventional network. In fact, it can provide an additional level of firewall, access control, and authentication for the embedded network. It can provide basic translation services, such as the network address translation and firewall rules typically used in home and commercial networks, and expose embedded devices to the internal corporate network selectively, much like the DMZ hosts on a conventional network.

Figure 4. Security of Wireless Embedded Networks



As instruments and sensors become connected with low-power wireless links, they essentially become wireless servers of physical information (in contrast to the cell phone and PDA, which are wireless clients). In enabling an extremely efficient implementation of IP over 802.15.4 radios, an organization can protect such monitoring points in much the same way that it protects critical servers containing sensitive information or hosting critical business processes.

Summary

Instruments, meters and gauges were once sparsely connected, often with humans serving as the only means of transporting the information they gathered. With the dramatic advance of highly integrated microcontrollers, sensors and now low-power, cost-effective, high-quality CMOS radios, these instru-

ments can be treated as networked devices serving physical information for purposes of monitoring, analysis and control.

Internet protocols provide a set of widely-used, long-standing, open standards that deal with diverse and evolving suites of devices and networks with well-established mechanisms for protecting critical network resources. But only with the advent of 6LoWPAN have these protocols been scaled down sufficiently to be useful in wireless embedded networks. The 6LoWPAN breakthrough is to leverage the shared context that is typical of the use cases for this technology to obtain a very compact and efficient implementation of IP, removing the factors that have given rise to a plethora of ad hoc standards and proprietary protocols. Now low-power wireless devices on IEEE 802.15.4 can simply join WiFi devices, Ethernet devices, and a host of others that make up the IP family.

About Arch Rock

Arch Rock is a pioneer in open-standards-based wireless sensor network technology. The company's products, which gather data from the physical world and integrate it into the enterprise IT infrastructure using IP networking and web services, are used in environmental monitoring, tracking and logistics, industrial automation and control. Arch Rock's founders, while at the University of California-Berkeley and Intel Research, did seminal research and development work on WSNs, creating three generations of wireless sensor nodes, mesh networking protocols, and the leading operating system for sensor networks. For more information, visit <http://www.archrock.com>.

©Arch Rock Corporation. All Rights Reserved.