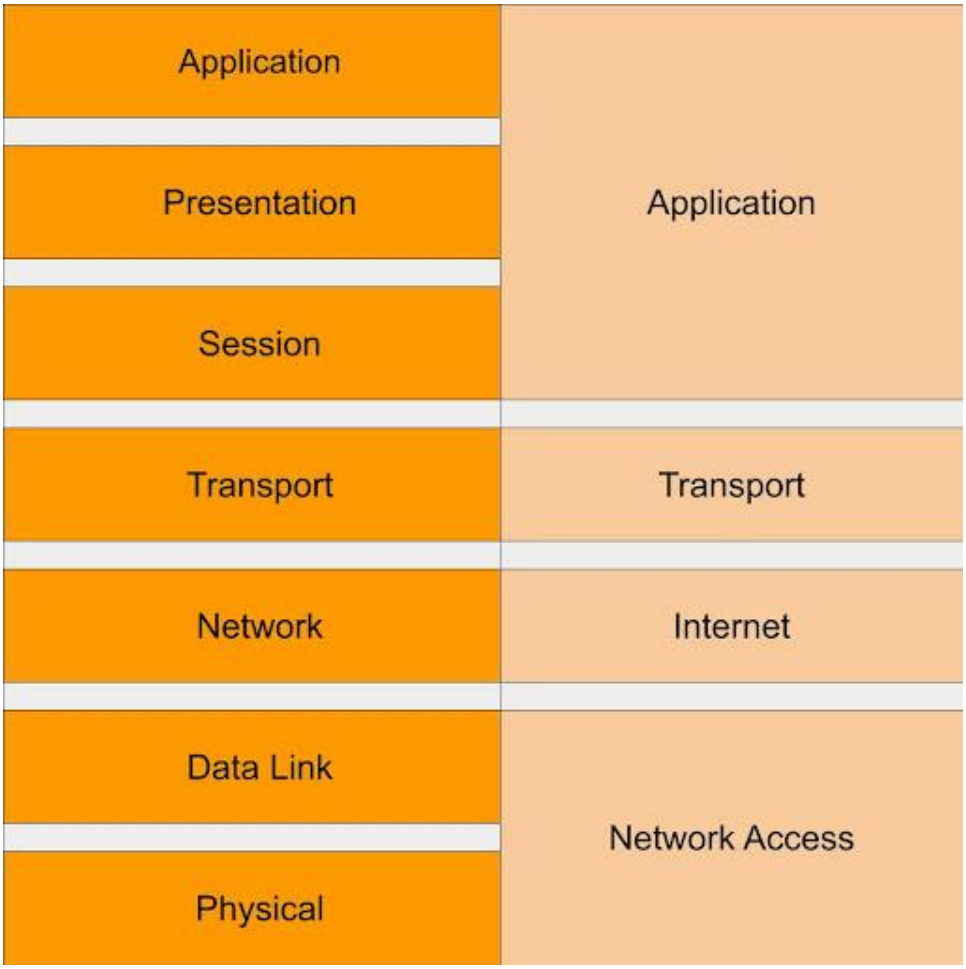
UNIT II

IOT PROTOCOLS - Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Issues with IoT Standardization – Unified Data Standards – Protocols – IEEE802.15.4–BACNet Protocol– Modbus – KNX – Zigbee– Network layer – APS layer Security



IoT Standards and Protocols Explained

For businesses, the transformative power of IoT is increasingly significant with the promise of improving operational efficiency and visibility, while reducing costs.

However, IoT does not come without risks and challenges. While concerns over security and data privacy continue to rise, **the lack of IoT standards** remains one of the biggest hurdles. The increasing number of legacy, single-vendor, and proprietary solutions cause problems with disparate systems, data silos and security gaps. As IoT successes become more dependent on

seamless interoperability and data-sharing among different systems, we want to avoid the scenario of a fragmented market with numerous solutions that simply don't work with each other.

What are Standards?

Before we continue our discussion on standards, let's take a step back and clarify their definition.

According to the European Telecommunications Standards Institute (ETSI), a standard is a "document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at achievement of the optimum degree of order in a given context."

Simply put, a standard is a published document that specifies a product's functionality and verifies its quality. It establishes a transparent, consistent and universal understanding of a technology by eliminating inefficient variety in the marketplace. Standards, therefore, enhance compatibility and interoperability in product development, fuel global adoption, and production, and accelerate time-to-market.

To better illustrate the importance of standards, let's look at light bulbs as a simple example. Nowadays, you can easily go to any store and buy any brand of light bulb, assuming that it is compatible with your lamp as the bulb base and threads have been standardized. This greatly boosts user demand, allowing manufacturers to ramp up their production and reduce costs leveraging economies of scale.

IoT Standards and Wireless Protocols

In the IoT realm, networking standards are hands down the most important. Standard protocols define rules and formats for setting up and managing IoT networks, along with how data are transmitted across these networks. Networking protocols can be categorized into multiple layers accordingly to the communication stack (i.e. OSI or TCP/IP model). In this article, we focus on the physical and network access protocols for data transfer from edge devices.

Even before IoT becomes a worldwide phenomenon, there have been a number of standardized wireless technologies that are widely acknowledged and adopted on a global scale. The most successful examples include Wi-Fi (based on IEEE 802.11a/b/g/n specifications for wireless local area networks), Zigbee (based on IEEE 802.15.4 specification for low-rate wireless personal networks) and GSM/UMTS/LTE (based on 2G/3G/4G mobile broadband standards developed by 3GPP).

However, these previously existing standards, are not optimized for a majority of large-scale IoT deployments that require interconnection of huge amounts of battery operated sensors (end nodes). Limited range and coverage, low penetration capability, power-hungry transmissions and high costs are factors that hamper their applicability in many use cases. By exactly filling these gaps, the arising group of low power wide area (LPWA) technologies are now taking over the IoT stage.

The problem is, most existing LPWA networks – typically the ones operating in the license-free spectrum – are proprietary solutions that do not implement a recognized industry-standard protocol. By making their technical specifications publicly available on a royalty-basis, many LPWAN providers are attempting to claim their technologies as "open standards." Nevertheless, this is not really the case.

Strictly speaking, a standard – or let's say an industry standard – must undergo a stringent evaluation process by an established Standards Development Organization (SDO). This guarantees the quality and credibility of the technology. Key global SDO examples include ETSI, IEEE, IETF, 3GPP, etc. So far, technologies that actually implement rigorous LPWA standards published by SDOs have been Narrowband-IoT/LTE-M/EC-GSM (standardized by 3GPP) and mioty (based on Low Throughput Networks – TS 103 357 specifications by ETSI).

Benefits of IoT Standards

So, why should you choose a standard protocol over a proprietary one? From an IoT user's perspective, standardized communication solutions offer significant benefits in terms of:

- **Guaranteed Quality and Credibility –** IoT standards ensure that products and solutions are fit for their intended purposes. In other words, communication technologies that adhere to rigorous standards deliver high Quality-of-Service, robustness against interferences and industry-grade security to ensure reliable and secure transmission of massive IoT sensor data at the edge.
- **Interoperability and Innovation Flexibility –** Standardized communication protocols can be programmed on various commodity, off-the-shelf hardware (i.e. chipsets, gateways) to support multi-vendor solutions and the interconnection of heterogeneous devices. Beside promoting interoperability in the long run, this helps end users avoid commercial risks of vendor lock-in, whereby a single supplier retains total control over functionality design and future product/technology innovation.

- **Global Scalability –** Industrial users with worldwide operations want to adopt IoT connectivity that can be implemented across their global facilities. Standardized solutions function universally and help minimize installation complexity, thereby safeguarding long-term investment.

With a vast assortment of IoT connectivity solutions available on the market, choosing the right technology can determine the success of your digital transformation. By opting for an industry-standard IoT solution, you can secure the longevity and ROI of your IoT architecture by making it quality-assured, vendor-independent and scalable worldwide.

IoT and Other New Technologies

M2M: Machine-to-Machine Communications

One of the new technologies that's part of the Internet of Things is Machine-to-Machine (M2M) communications. M2M, though not well-defined, is a set of methods and protocols to allow devices to communicate and interact over the Internet (or other network) without human intervention. M2M is sometimes considered to be low-overhead short-range wireless communication between machines, utilizing protocols with much less overhead than full-blown TCP/IP. Many M2M applications involve low power wireless devices with limited computing power and narrowly-defined functionality. Low-overhead protocols have been devised for them, including Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and Open Mobile Alliance Light Weight M2M (OMA LWM2M). CoAP is actually a specialized web transfer protocol designed for applications such as smart energy and building automation. There is, of course, no reason why IoT devices cannot use high-powered CPUs and wide bandwidth, and in many applications this is clearly necessary, such as smart cars interacting with external servers. So IoT spans a huge range from very simple low-powered specialized devices and sensors with low bandwidth needs to complex, high-powered devices in large high-bandwidth environments.

WSNs: Wireless Sensor Networks

IoT configurations often involve sensors, which can be connected by wireless networks. Such sensor networks are termed "Wireless Sensor Networks" or WSNs. A WSN comprises spatially distributed autonomous devices equipped with sensors, connected through a wireless network to some type of gateway. The sensors typically monitor physical or environmental conditions. The

gateway communicates with another set of devices that can act on the information from the sensors. Application examples include patient monitoring; environmental monitoring of air, water, and soil; structural monitoring for buildings and bridges; industrial machine monitoring; and process monitoring. The wireless network could be WiFi or Bluetooth, and the protocol one of the three listed above.

The boundaries between these networks are not clearly drawn, and in practice they overlap considerably. Figure 3 shows the relationship schematically:

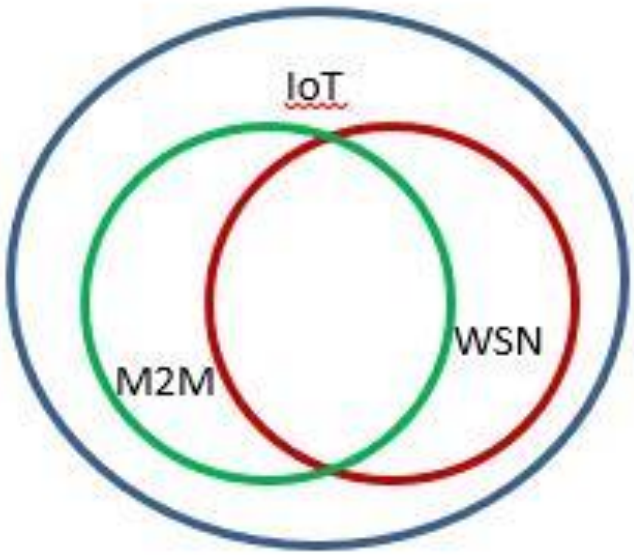


Figure 3. Relationship of IoT, M2M, and WSN

For the purposes of this article, we will regard M2M and WSN as forming part of IoT.

Goals of IoT

In the short term, at least, the goals of IoT are straightforward, as illustrated in Figure 4:

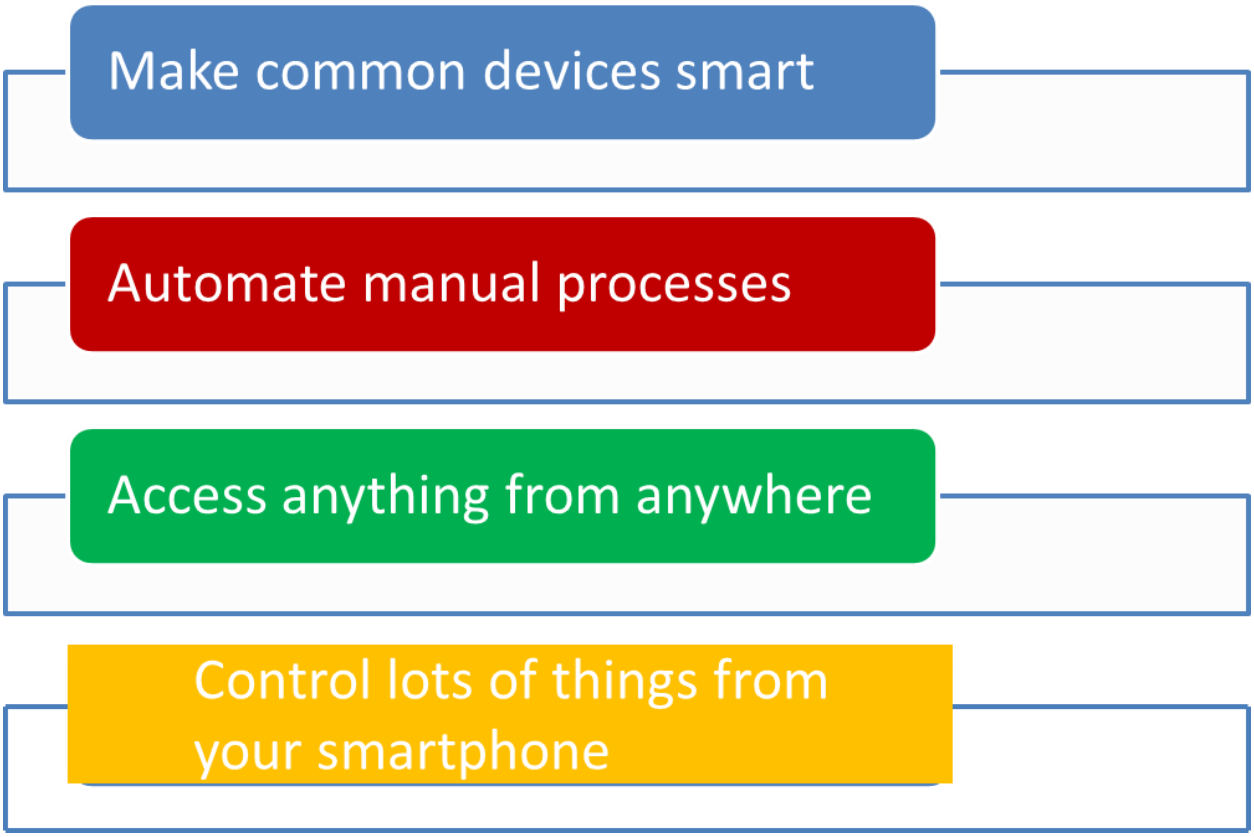


Figure 4. Goals of IoT

The objectives revolve around efforts to reduce costs and save time. But they also promise to make new things possible that are not feasible now, such as devices for improved patient monitoring and improved transportation systems utilizing autonomous vehicles and other modes.

IoT Enabling Technologies

There are many technologies that support IoT and make possible its steady advance. A partial list includes the following:

- Cheap and ubiquitous telecommunications
- Smart software
- Smart devices
- Cheap memory
- Cheap and extremely powerful microprocessors

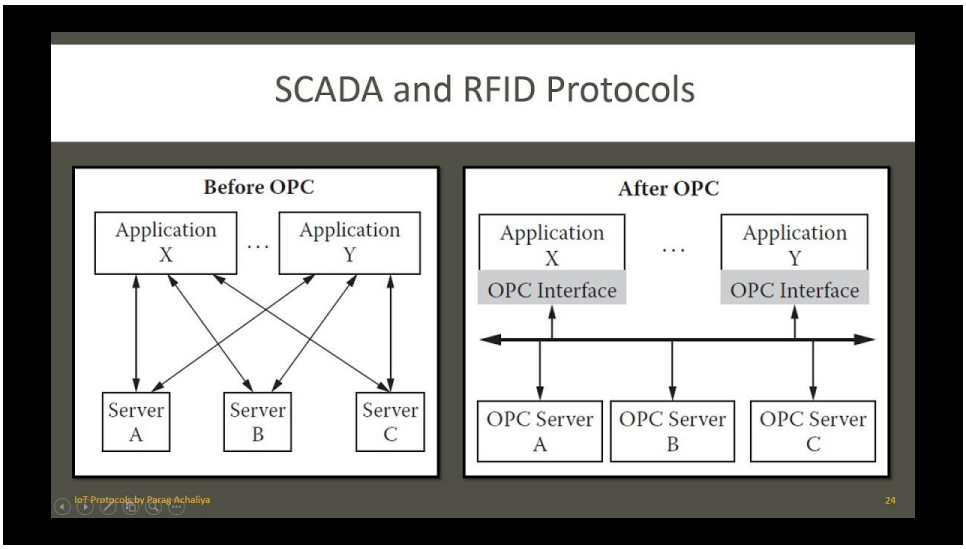
- Cloud Computing
- Big data, event stream processing, real-time analytics
- Machine Learning
- Wireless sensor networks
- Low power short-range and wide area wireless networks
- Embedded systems
- Automation and control Systems
- Existing and emerging telecom technologies: Li-Fi, LPWAN, LTE-Advanced, 5G, WiFi-Direct, BLE, ZigBee, Z-Wave, Thread, HaLow, …

SCADA and RFID Protocols

SCADA (Supervisory Control and Data Acquisition) and RFID (Radio Frequency Identification) protocols are two critical technologies that have transformed various industries. SCADA systems allow for remote monitoring and control of industrial processes in the oil and gas, energy, and manufacturing industries. These systems collect data from sensors and deliver it in real-time to human operators, allowing them to monitor and adjust the process as needed.

On the other hand, RFID is a wireless technology that communicates with tags attached to objects via radio waves. These tags contain one-of-a-kind identification codes that allow the system to track the object's location, movements, and other data. RFID has a wide range of applications, including supply chain management, inventory control, and security and access control.

SCADA and RFID technologies have significantly improved industrial processes, making them more efficient, safe, and secure. We can expect even more advancements and opportunities in the future as these technologies continue to evolve.



Understanding SCADA Protocols: Communication and Control Systems

SCADA (Supervisory Control and Data Acquisition) protocols are used in industrial processes to enable communication and control. Sensors, controllers, and communication devices are among the components of a SCADA system. The SCADA protocols used to control and communicate with these components are critical for ensuring that industrial processes run efficiently and safely.

SCADA communication protocols are used to transfer data between SCADA system components. Modbus, DNP3 (Distributed Network Protocol), and IEC 60870-5 are the most common communication protocols used in SCADA systems. These protocols define the structure of the data being transmitted, the type of data, and the method of data transfer.

Control protocols are used to manage the various components of a SCADA system. OPC (OLE for Process Control), BACnet (Building Automation and Control Networks), and SNMP are the most common control protocols used in SCADA systems (Simple Network Management Protocol). These protocols are used to configure devices, set and adjust system parameters, and manage alarms and events.

SCADA systems allow for remote monitoring and control of industrial processes while providing real-time data to human operators. These systems are used in various industries, including energy and water treatment, manufacturing, and transportation. SCADA protocols allow these systems to operate seamlessly, ensuring the process's efficiency and safety.

Understanding SCADA protocols is critical for ensuring that industrial processes run efficiently and safely. Properly selecting and implementing communication and control protocols are critical

for a SCADA system's integrity. SCADA systems are poised to continue revolutionizing industries and providing critical support for industrial processes as new protocols, and technological advancements emerge.

RFID Protocols: Types and Standards for Identification and Tracking

RFID (Radio Frequency Identification) protocols identify and track objects using radio waves. RFID protocols of various types and standards are used in various industries for various applications.

The most common RFID protocols are low-frequency (LF), high-frequency (HF), and ultra-high-frequency (UHF). LF RFID operates at a frequency of 125-134 kHz and is used for short-range communication, typically up to 10 cm. HF RFID operates at a frequency of 13.56 MHz and is used for short- to medium-range communication (up to 1 meter). UHF RFID operates at a frequency range of 860-960 MHz and is used for long-range communication up to several meters.

Aside from these, several RFID standards are used for identification and tracking. The most widely used standards for HF RFID are ISO 14443 and ISO 15693, and ISO 18000-6c for UHF RFID. These standards specify the RFID system's frequency, data rate, and encoding. They also define the RFID tag's data structure, including the identification number, manufacturer code, and other pertinent information.

RFID protocol and standard implementation vary depending on the application. For example, LF RFID is commonly used in animal identification, whereas HF RFID is used in access control, payment systems, and inventory management. UHF RFID is used in supply chain management, asset tracking, and other applications that require long-range communication.

RFID protocols and standards are critical in identifying and tracking objects across industries. The appropriate protocol and standard are chosen based on the specific application requirements. RFID is poised to continue revolutionizing industries and enabling a new level of visibility and control as technology advances, and new standards emerge.

Why is lack / Issues of standardization a problem with IoT

The lack of standardization is a problem for the Internet of Things (IoT) because it makes it difficult for different devices and systems to communicate and work together seamlessly. IoT devices are made by many different manufacturers and can use a wide variety of communication

protocols and data formats, making it challenging to develop a unified standard that works across all devices.

Lack of standardization

The lack of standardization creates interoperability issues, which can lead to compatibility problems and limited functionality.

For example, if two IoT devices cannot communicate with each other because they use different protocols or data formats, they cannot work together to achieve a common goal.

The absence of standardization can also cause security risks, as it can be easier for hackers to exploit vulnerabilities in systems that are not using standard security protocols.

In addition, it can hinder the development of new applications and services that could bring value to businesses and consumers.

Overall, the lack of standardization in the IoT industry can lead to reduced efficiency, increased costs, and a slower rate of innovation. Therefore, there is a need for standardized communication protocols, data formats, and security measures to ensure that the IoT can reach its full potential.

Compatibility Issues

Compatibility problems can be a common issue with IoT (Internet of Things) devices. There are several reasons why compatibility issues can arise in IoT, including:

- Protocol incompatibility: IoT devices use different communication protocols, which can lead to incompatibility issues between devices from different manufacturers.

- Security protocols: IoT devices have different security protocols, which can also lead to incompatibility issues. For example, if one device uses a more secure encryption protocol than another, they may not be able to communicate with each other.

- Firmware updates: IoT devices often receive firmware updates, which can sometimes cause compatibility issues if one device's firmware is updated while the other remains on an older version.

- Power requirements: IoT devices have different power requirements, which can lead to compatibility issues. For example, if one device requires more power than another, they may not be able to communicate with each other.

Introduction to Unified Data

Unified data is when a company merges its many fragmented data sources into one, single central view. Unified data provides a more complete and accurate picture of a company's data, but unifying the data is far from simple. To tie data sources together, companies need a system to unite them, such as an analytics platform.

Why is unified data so great?

Companies strive to unify their data because, by default, most data is inaccessible. It's often scattered throughout the company and divided into information silos among business units and teams. Without a central way to manage data, businesses can't make informed decisions. Marketing teams can't accurately measure demand for their product. Product teams can't fully understand their customer journey, and analytics teams, which are often tasked with breaking down information silos, can't provide accurate business intelligence to leadership. When companies are able to unify their data, they make all of their business units more productive. But unifying data can pose a tremendous organizational challenge, as well as an engineering one.

The challenge of creating unified data

The technologies that businesses use to store data are highly fragmented. There are tens of thousands of hardware and software providers that each have their own vernacular, programming languages, syntaxes, and practices. On-premise storage servers may not be able to speak to cloud-hosted business intelligence tools which can't access virtualized servers. Conventions like application programming interfaces (APIs) can connect systems, but don't always offer enough functionality. Additionally, not all data is the same. There's big data, thick data, and structured, unstructured, and multi-structured data. Some systems can only process certain types of data, and each dataset can vary wildly. It is little wonder that 85 percent of companies strive to be data-driven yet only 37 percent claim to be successful at using their data. Most data ecosystems rival the United Nations in complexity. Every application speaks slightly different dialects and they require translators to communicate. Businesses that succeed at unifying their data, are better able to plan, budget, forecast, and build products. For unification, many businesses turn to analytics platforms.

How can analytics platforms help with unified data?

Analytics platforms are purpose-built to capture, store, and analyze data from a variety of sources. They are, by definition, tools for unifying data. Most offer pre-built integrations to common systems and universal APIs for less common ones. They allow enterprises to tie their ERP, CRM, web applications, marketing systems, customer applications, and data partners together to view the data from one interface. The best analytics platforms have highly intuitive interfaces that are designed to mask the complexity of the underlying data architecture. They use dashboards to help users visualize their data. Some platforms offer machine learning algorithms to simplify and automate the process of analysis. Brands can use an analytics platform to knit data from across silos, business units, and teams together and provide everyone access. The more individuals within a business that are data-informed, the better. At e-signature provider DocuSign, the product team gave over 100 individuals across the business access to its Mixpanel instance so that the data science team wouldn't serve as an insight bottleneck.

How to create a unified data ecosystem

Analytics platforms each have their own quirks. Some are designed to be highly accessible but lack advanced features for manipulating data. Others are designed to handle massively complex datasets but suffer from what's known as featuritis–a confusing interface with too many features. Some platforms strike a balance of high functionality and high usability. When teams evaluate analytics platforms, they should find the one that best fits their current and future needs. **Teams can examine analytics platforms based on these factors:**

- **Integrations**: Can the platform integrate with most data sources?
- **Performance**: Does the platform have a high storage capacity?
- **Reliability**: Does the platform guarantee access?
- **Availability**: Does the platform guarantee uptime?
- **Latency**: Can users access data in near real-time?
- **Concurrency**: Can the platform use faster, non-relational query techniques?
- **Compliance**: Is the platform data center compliant?
- **Innovation**: Is the company constantly improving its product?

In addition to features, it's important for teams to consider process issues like internal data governance and quality. Pieces of legislation like the European Union's GDPR are forcing many companies into an era greater data transparency. Customers increasingly demand to know what data businesses collect on them, and what they use it for. Businesses need to ensure that they are being transparent with user data. At the same time, data breaches are increasingly common. Any teams seeking to unify their data must also consider the potential danger of making it easier for hackers to access. To keep themselves safe, teams can publish internal data governance guidelines and make sure their partners are compliant and can customer data secure.

IEEE 802.15.4 Protocol

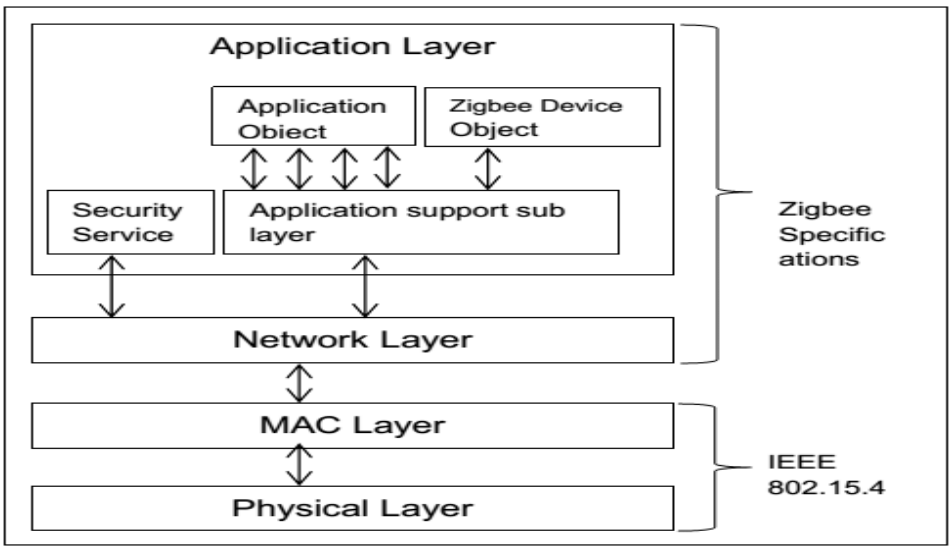
IEEE 802.15.4 is a member of the IEEE 802.15 standards for Wireless Personal Area Networks, which includes protocols such as IEEE 802.15.1 (Bluetooth), and IEEE 802.15.3 (UWB Wireless). IEEE 802.15.4 specifies the MAC and PHY Layers for Low-Rate Wireless Personal Area Networks (LR-WPAN).

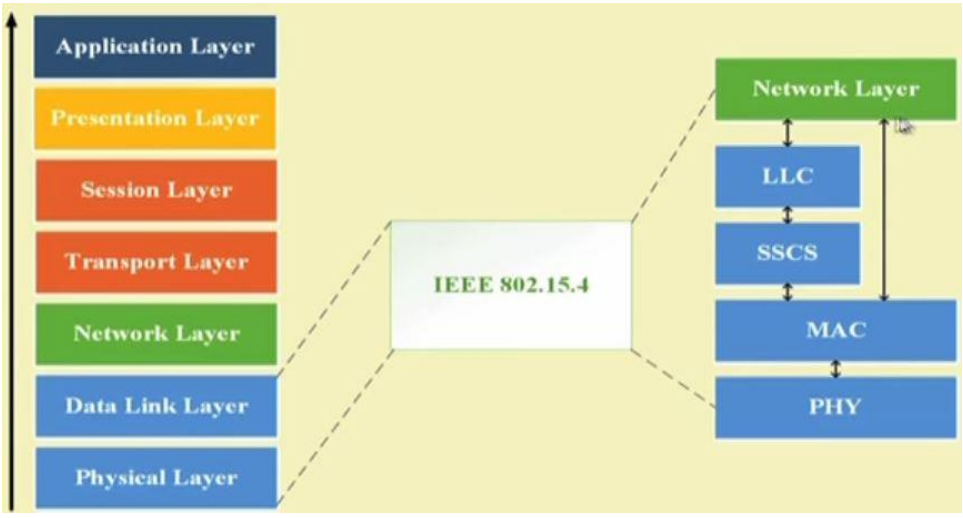
IEEE 802.15.4 is currently used as a medium for a wide variety of network protocols, including ZigBee, 6lowPAN and TinyOS.

History

IEEE 802.15.4 was published by task group 4 (TG4) in 2003, and following the formation of IEEE 802.15 TG4b, has since gone into hibernation. TG4b was formed to revise and improve upon the original IEEE 802.15.4 specification, their enhancements were approved and published in June 2006 as IEEE 802.15.4-2006.

In March 2005, an extension to the IEEE 802.15.4 specification, IEEE 802.15.4a was released, specifying two additional optional PHYs with improved precision in ranging and locating.





BACnet Protocol : Architecture, Working, Types, Objects & Its Applications

BACnet protocol was developed by a committee named ASHRAE or the American Society of Heating, Refrigerating & Air-Conditioning Engineers in 1987. The main motto of this committee is to make a protocol that would provide systems from various manufacturers to communicate together in a pleasant way. So this protocol is a registered brand of ASHRAE. Since the time protocol was developed it is undergoing continuous changes with an open agreement procedure. So that all interested parties are welcome to participate with no fees. So this article discusses an overview of **Bacnet Protocol** basics – working with applications.

What is BACnet Protocol?

A data communication protocol that is used to build an automated control network, is known as BACnet or Building Automation Control Network. This data communication protocol is both an ISO & ANSI standard used for interoperability between cooperating building automation devices. Bacnet Protocol includes a set of rules for governing the data exchange on a computer network that simply covers all from what type of cable to utilize, to form a particular command or request in a normal way.

To attain interoperability across a broad spectrum of equipment, the BACnet specification includes three major parts. Primary, Secondary, and tertiary. So the primary part defines a technique to represent any kind of building automation apparatus in a normal way.

The secondary part describes messages that can be transmitted across a network of computers to check and manage such equipment. The final part describes a set of suitable LANs which are used for conveying BACnet communications.

Why is Bacnet Protocol required?

The **BACnet protocol's importance** is to define typical techniques that manufacturers can execute to build components as well as systems that are interoperable through other components & systems of BACnet.

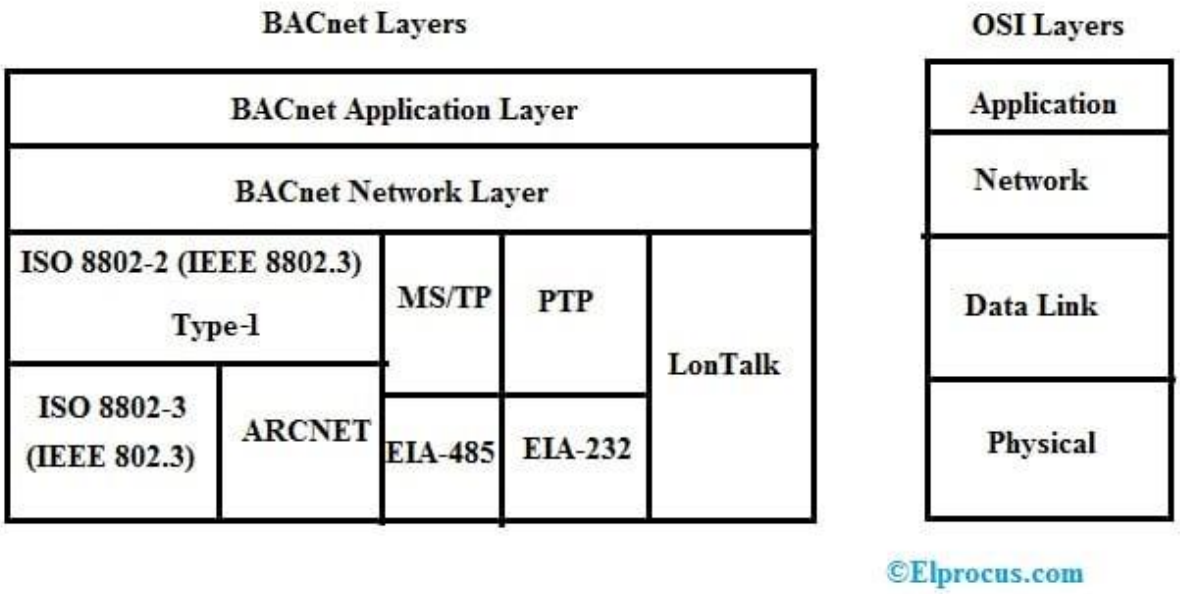
It also specifies how data is signified on the network as well as the services that are utilized to transmit data from one node of BACnet to another node. It also has messages that recognize network & data nodes.

BACnet is used as a tool by owners of buildings & system specifiers for the specification of the interoperable system. This protocol does not change the need for indicating what a consumer needs. So, it provides simply some consistent tools to assist the creation & specification of systems that can interoperate.

BACnet protocol is used in all types of automated building systems. So, there are interoperable products available within different categories like security, fire, lighting, elevators, HVAC, etc. This protocol simply addresses the interoperability goal through simply defining a general working model of automation devices, a technique used for defining the data that they include, & also a technique used for explaining protocols that a single device can utilize to inquire one more device to execute some preferred action.

Bacnet Protocol Architecture

The BACnet protocol architecture is predominately restricted to lighting controls, HVAC & gateways. This protocol highlights lightweight and efficient communication which is optimized for short messages, small networks, and inter-networks.



Bacnet Protocol Architecture

BACnet protocol architecture is a collapsed architecture that matches to 4-layers of the OSI model. The four layers in the BACnet architecture mainly include Application, Network, Data Link & Physical. Even though, just the Network layer & Application layer are simply BACnet.

The above architecture is the BACnet protocol stack which includes different layers as shown in the diagram. This protocol is a collapsed version of the OSI stack. The transport and session layers are not used. The application layer takes on the functions of these two layers.

BACnet Physical Layer

The upper layers of BACnet do not depend on the physical layer. So the Physical layer of BACnet makes it feasible for BACnet to be executed on different networks. The physical layers of BACnet have been specified with ARCNET, Ethernet, IP tunnels, BACnet/IP, RS-232, RS485, and Lonworks/LonTalk. RS232 is for point-to-point communication. RS485 supports up to 32 nodes with a distance of 1200 m at 76Kbps.

BACnet Protocol Link Layer

BACnet protocol is implemented directly with LonTalk or IEEE802.2 link layers. So it specifies Point to Point (PTP) data link layer for RS232 connections. It specifies MS/TP data link layer intended for RS-485 connections. The standard simply specifies BVLL (BACnet Virtual Link Layer) which states all the services required through the BACnet device at this link layer.

IP BACnet Virtual Link Layer encapsulates required control data in a header of BACnet virtual link control information. Because of IP, BVLL, and BACnet protocol devices can directly communicate over IP networks without the requirement of any router device.

BACnet protocol utilizes BBMD (BACnet broadcast management device) concept which executes the required broadcast for the preferred link layer. So, the BACnet broadcast message is changed into IP-based broadcast or multicast messages.

BACnet Network Layer

This layer simply specifies the required addresses of the network for routing. BACnet network includes a minimum of one or above segments that are connected with bridges once they utilize similar LAN technologies. If they utilize various LAN protocols then they are connected through routers.

Application Layer

BACnet does not separate presentation as well as application layers. So it takes care of reliability & sequencing or segmentation mechanisms generally connected with both the session & transport layers. BACnet includes devices like objects to exchange service primitives which are described with ASN.1 syntax & serialized with ASN.1 BER.

BACnet Security Layer

The concept of BACnet security can be understood easily with an example say when BACnet device-A requests a session key from the key server for establishing secure communication through device-B, then this key is transmitted to both the device-A & device-B through the key server which is known as 'SKab'. BACnet protocol uses 56-bit DES encryption.

How Does Bacnet Protocol Work?

BACnet is a typical electronic communication protocol that works by allowing different kinds of manufacturers' building automation as well as monitoring systems like fire alarms, HVAC, and perimeter security for communicating with each other. This protocol can work with nearly any normal data protocol including TCP/IP.

BACnet protocol enables the comprehensive BMSs (building management systems) development that allows operators to construct, observe & control different building systems within a single application.
This protocol is also used to expand the flexibility & scope of the automation that can

be executed. For instance, an automation system could be setup such that once the fire protection system notices a fire, then the system sends commands to the following.

- To the control system of the elevator to send all elevators to the ground floor immediately.
- To the paging system of the building to transmit an audible voice signal to inform occupants of the building wherever the blaze was detected & how to go out from the building.
- From the audio or visual systems of the building to flash messages on TV displays within the conference rooms.
- To an interface of phone system for sending alerts through text message to the facilities & engineering teams of the building.

With BACnet protocol, all the data is signified in terms of an object. So each object signifies data regarding a device or component. Signifying information like an object simply provides the benefit that the latest objects can be formed otherwise existing objects can be modified based on the requirements of the user.

An object signifies physical information (physical inputs, outputs) & nonphysical information (software/calculations). It is very significant to note that every object may signify a single portion of information otherwise a group of information which executes the same and exact function.

BACnet Object

BACnet object is a concept that allows the communication as well as a group of data related to i/ps, o/ps, software & calculations to be executed. The BACnet Object can visible itself in different ways like Single Points, Logical Groups, Program Logic, Schedules & Historical Data.

The BACnet objects are both physical & non-physical. For instance, a thermostat is considered a physical concept & the HVAC system is considered the output device. The best example of a non-physical concept is the maintenance schedule of an HVAC in the software form.

All BACnet objects include different properties of information exchange & commands. These properties represented in a tabular format with two columns. The first column includes the name of the property & the second column provides the value of the property. In the second column, the Information can exist in a write-enable/read-only format.

The BACnet object example for a binary input of a sensor within a building is shown below.

Object Name	Space Temp
Type of Object	Binary Input
Present Value	11001
Status Flags	Normal, InService
High Limit	11110
Low Limit	11011

In the above table, the first four properties are necessary by the BACnet standard whereas the last two properties are simply considered optional. So, these optional objects are frequently necessary by a developer, however, those objects should match the standard of BACnet. The example will show simply a few of the properties of an object. In real life, particularly in a building automation setting, different properties would be there within the object. Most experts & sources specify there are 23 standard BACnet objects utilized in building automation systems. So, standard objects operate in the BACnet standard.

The 23 standard BACnet objects are Binary i/p, Binary o/p, Binary value, Analog i/p, Analog o/p, Analog value, Averaging, LifeSafety Zone, LifeSafety Point, Multi-State i/p, Multi-State o/p, Multi-State value, Loop, Calendar, Notification Class, Command, File, Program, Schedule, Trend Log, Group, Event Enrollment & Device.

Once a set of objects executes a specific function then it is known as a BACnet device. All these objects should include an identifier, data type & additional information like read-only, modified through other devices, and many more.

Different Types

The different **types of BACnet protocols** are discussed below.

BACnet/IP

This is normally used with existing VLAN & WAN networks. So the devices can connect directly to hubs or Ethernet switches. This LAN is a high-performance & fast

type, but very costly. BACnet/IP utilizes UDP/IP for compatibility through existing IP infrastructure. Once BACnet/IP is utilized with several IP subnets, then extra device functionality known as BBMDs (BACnet Broadcast Management Devices) is necessary to handle broadcast messages of inter-subnet BACnet.

BACnet MS/TP

This kind of LAN uses EIA-485 twisted pair for signaling up to 4k feet. So it is a very famous type of BACnet LAN which is used for unitary as well as application-specific controllers. This BACnet MS/TP is not expensive.

BACnet ISO 8802-3 (Ethernet)

BACnet is directly used with Ethernet 8802-3 networks which are similar to BACnet/IP in terms of speed & cost, although restricted to a single physical infrastructure that does not utilize IP routers.

BACnet over ARCNET

This BACnet is MAC type which includes two forms like 2.5Mbs coax & 156Kbs above EIA-485. This BACnet is supported by a limited number of vendors with ARCNET.

BACnet Point-to-Point

This BACnet Point-to-Point is simply used over the networks of dial-up telephones. Generally, thus direct EIA-232 connection is no longer used for a direct Ethernet connection.

BACnet over LonTalk Foreign Frames

This BACnet simply allows LonTalk's transport component for carrying BACnet messages. But, the two protocols are not interoperable.

BACnet over ZigBee

Generally, this MAC is a wireless mesh network used with less costly devices. So it is normally used as a gateway to ZigBee devices & not like a native BACnet transport.

Bacnet to Modbus Converter

Protocon-P3 Gateway is a BACnet to Modbus converter which is used in designing automation systems in different applications like HVAC, access control, lighting control & fire detection systems, and their related equipment. The Protocon-P3 Gateway combines such BACnet systems & devices with Modbusbased management systems over Modbus RTU protocol & Modbus TCP/IP.

Bacnet to Modbus Converter

The main features of Bacnet to Modbus Converter include the following.

- It includes a front panel that has LED for indication of quick diagnostic
- Windows-based configuration utility.
- It supports up to 100 BACnet devices interface to TCP Master/Slave or Modbus RTU.
- It has the capacity for interfacing up to 5K mapping points.
- It supports the COV bit packing feature.

Bacnet Protocol Vs Modbus

The difference between Bacnet Protocol and Modbus include the following.

BACnet Protocol	Modbus
It was developed by ASHRAE.	It was developed by Modicon Inc.
Bacnet is used for communication across devices.	Modbus is used for communication between devices.
Its transmission modes are; IP, Ethernet, Zigbee & MS/TP.	Its transmission modes are; ASCII, RTU, and TCP/IP.
Its standards are; ANSI/ASHRAE Standard 185; ISO-16484-5; ISO-16484-6.	Its standards are; IEC 61158.
It is used in different markets like Industrial, Energy Management, Transportation, Building Automation, Regulatory, health & security.	It is used in different markets like Lighting, Life Safety, Access Controls, HVAC, transportation & maintenance.

Network Interfaces: Existing LANs &LANs infrastructure.	Network Interfaces: Traditional serial & Ethernet protocols.
Examples: Measurements of Tank Level. Boiler Control.	Examples: Tasks like fan schedule, sending a status alarm, and requesting temperature reading.