Sensors

- Sensors come in all shapes and sizes
- Example: Smart Farming
- uses a variety of technical advances to improve the
  - efficiency, sustainability, and profitability of traditional farming practices.
- most significant impacts of precision agriculture are those dealing with sensor measurement of a variety of soil characteristics include
  - real-time measurement of soil quality,
  - pH levels,
  - salinity,
  - toxicity levels,
  - moisture levels for irrigation planning,
  - nutrient levels for fertilization planning etc.,

Sensors

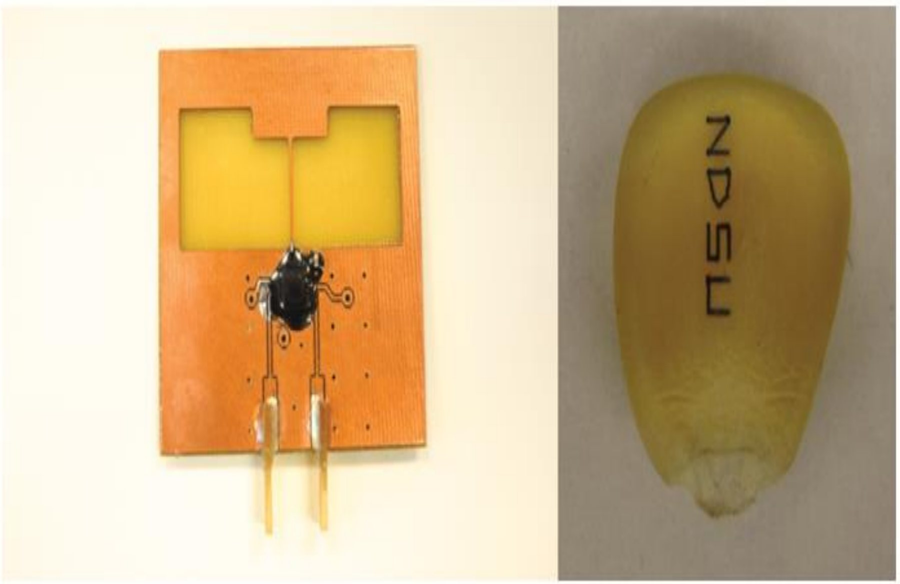


Figure 3-1 *Biodegradable Sensors Developed by NDSU for Smart Farming (Reprinted with permission from NDSU.)*

- shows biodegradable, passive microsensors to measure soil and crop and conditions. These sensors, developed at North Dakota State University (NDSU), can be planted directly in the soil and left in the ground to biodegrade without any harm to soil quality.

Sensors

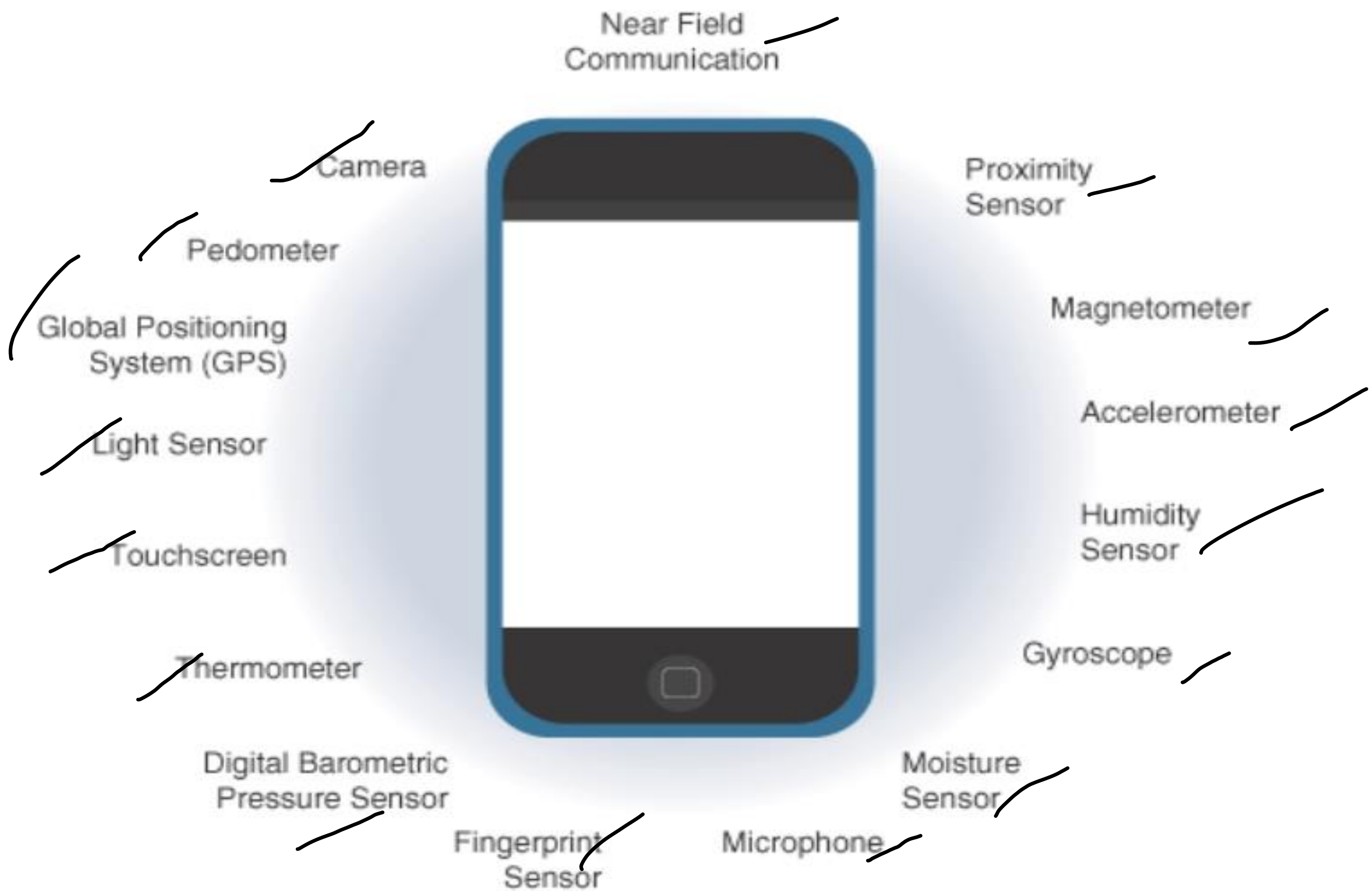


Figure 3-2 *Sensors in a Smart Phone*

Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter

Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Radiation	Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger-Müller counter, scintillator, neutron detector
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO_2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smoke detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

Module 4

Chapter 5: IP as the IoT Network Layer

IP as the IoT Network Layer

Objectives

- **The Business Case for IP:**
  - Discusses the advantages of IP from an IoT perspective and introduces the concepts of adoption and adaptation.
- **The Need for Optimization:**
  - The challenges of constrained nodes and devices when deploying IP. And discusses the migration from IPv4 to IPv6 and how it affects IoT networks.
- **Optimizing IP for IoT:**
  - Explores the common protocols and technologies in IoT networks utilizing IP, including 6LoWPAN, 6TiSCH, and RPL.
- **Profiles and Compliances:**
  - Provides a summary of some of the most significant organizations and standards bodies involved with IP connectivity and IoT.

The Business Case for IP

- Data flowing from or to “things” is consumed, controlled, or monitored by data center servers either in the cloud or in locations that may be distributed or centralized.

- Dedicated applications are then run over virtualized or traditional operating systems or on network edge platforms

- These lightweight applications communicate with the data center servers.

The Key Advantages of Internet Protocol

IP has the ability to integrate small and large evolutions and able to maintain large numbers of devices and users.

Open and standards-based Versatile Ubiquitous Scalable Manageable and highly secure Stable and resilient Consumers market adoption The innovation factor:

Key advantages of the IP suite for the IoT:

***Open and standards-based*:**

- The IETF (Internet Engineering Task Force) is an open standards body that focuses on the development of the IP suite and related Internet technologies and protocols.

***Versatile*:**

- A large spectrum of access technologies is available to offer connectivity of "things" .
- The layered IP architecture is well equipped to cope with any type of physical and data link layers.
- IP is ideal for long-term investment because various protocols at these layers can be used in a deployment now and over time, without requiring changes to the whole solution architecture and data flow.

The Key Advantages of Internet Protocol

Ubiquitous:

- All recent OS releases, from general-purpose computers and servers to lightweight embedded systems (TinyOS, Contiki, and so on), have an integrated dual (IPv4 and IPv6) IP stack that gets enhanced over time.
- IP is the most pervasive protocol as it supports across the various IoT solutions and industry verticals.

***Scalable*:**

- Common Internet protocol and has been massively deployed and tested for robust scalability.

The Key Advantages of Internet Protocol

Manageable and highly secure:

- Well-understood network management and security protocols, mechanisms and toolsets that are widely available. Adopting IP network management also brings an operational business application to OT.

Stable and resilient:

- IP is a workable solution from around for 30 years.
- IP has a large and well-established knowledge base and has been used for years in critical infrastructures, such as financial and defense networks.
- Its stability and resiliency benefit from the large ecosystem of IT professionals who can help design, deploy and operate IP-based solutions.

The Key Advantages of Internet Protocol

Consumers market adoption:

- Consumers access to applications and devices will occur predominantly over broad band and mobile wireless infrastructure.
- The main consumer devices range from smart phones to tablets and PCs.
- The common protocol that links IoT in the consumer space to these devices is IP.

The innovation factor:

- Adoption of IP is very clear from past 2 decades.
- IP is the underlying protocol for applications ranging from file transfer and e-mail to the www, e-commerce, social networking, mobility, and more.

Adoption or Adaptation of the Internet Protocol

- The use of numerous network layer protocols along with IP two models, adaptation or adoption, is proposed:

- ***Adaptation*** means application layered gateways (ALGs) must be implemented to ensure the translation between non-IP and IP layers.

- ***Adoption*** involves replacing all non-IP layers with their IP layer counterparts, simplifying the deployment model and operations.

The Need for Optimization

Optimizations are needed at various layers of the IP stack to handle the restrictions that are present in IoT networks.

1)Constrained Nodes

- Limit of network protocol stack on an IoT node may be required to communicate through an unreliable path.
- This causes problems such as limited or unpredictable throughput and low convergence when a topology change occurs.
- Power consumption is a key characteristic of constrained nodes as most of IoT devices are battery powered.
  - To help extend battery life, you could enable a "low-power" mode instead of one that is "always on."
  - Another option is "always off," which means communications are enabled only when needed to send data.

IoT constrained nodes can be classified as follows:

- **Devices that are very constrained in resources, may communicate infrequently to transmit a few bytes, and may have limited security and management capabilities:**

  adaption model, less power and resources

  This drives the need for the IP adaptation model, where nodes communicate through gateways and proxies.

- **Devices with enough power and capacities to implement a stripped-down IP stack or non-IP stack:**

  You may implement either an optimized IP stack and directly communicate with application servers (adoption model) or go for an IP or non-IP stack and communicate through gateways and proxies (adaptation model).

  both adaption (gateways and proxies) and adoption model, more power and resources

- **Devices that are similar to generic PCs in terms of computing and power resources but have constrained networking capacities, such as bandwidth:**

  These nodes implement a full IP stack (adoption model), but network design and application behaviors must cope with the bandwidth constraints.

adoption model, basic power and resources, less networking capacties

2) Constrained Networks

- Constrained networks are referred to as low-power and lossy networks (LLNs).
- *Lossy* in this context refers to network unreliability that is caused by disruptions in the data flow or packet loss.
- Constrained networks are limited by low power, low-bandwidth links (wireless and wired).
- They operate between a few kbps and a few hundred kbps and may utilize a star, mesh, or combined network topologies, ensuring proper operations.
- In a constrained network, with limited bandwidth, it is not unusual for the packet delivery rate (PDR) to oscillate between low and high percentages.

- Large bursts of unpredictable errors and even loss of connectivity at times may occur.
- Constrained nodes and networks pose major challenges for IoT connectivity in the last mile.
- This in turn has led various standards organizations to work on optimizing protocols for IoT.

3) IP Versions

- IETF has been working on transitioning the Internet from IP version 4 to IP version 6.
- This is due to the lack of address space in IPv4 as the Internet has grown.
- IPv6 has a much larger range of addresses that should not be exhausted for the foreseeable future.
- There are variety of factors that influence the use of IPv4, IPv6, or on IoT solution.

The following are some of the main factors applicable to IPv4 and IPv6 support in an IoT solution:

- ***Application Protocol***: IoT devices implementing Ethernet or Wi-Fi interfaces can communicate over both IPv4 and IPv6, but the application protocol may dictate the choice of the IP version.

Cellular Provider and Technology:

- IoT devices with cellular modems are dependent on the generation of the cellular technology and data services offered by the provider.

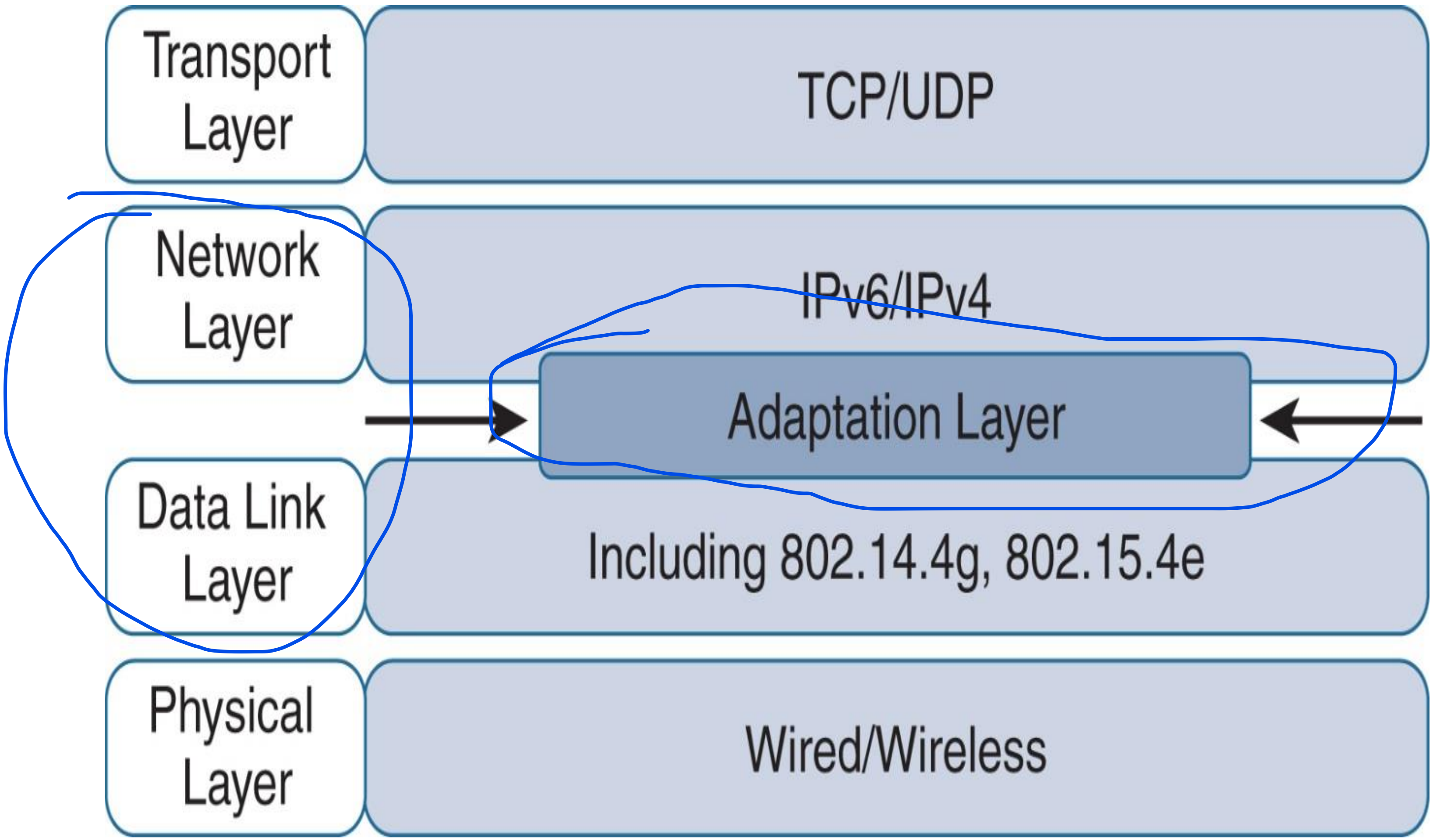
Serial Communications:

- Many legacy devices in certain industries, such as manufacturing and utilities, communicate through serial lines. Encapsulation of serial protocols over IP leverages mechanisms such as raw socket TCP or UDP are implemented.

IPv6 Adaptation Layer:

- IPv6-only adaptation layers for some physical and data link layers for recently standardized IoT protocols support only IPv6. LLNS, RPL are IPv6 only .

Optimizing IP for IoT



Optimizing IP for IoT: From 6LoWPAN to 6Lo

- The model for packaging IP into lower-layer protocols is often referred to as an *adaptation layer*.
- IP adaptation layers are defined by an IETF working group and released as a Request for Comments (RFC).
- An RFC is a publication from the IETF that officially documents Internet standards, specifications, protocols, procedures, and events.
- The main examples of adaptation layers optimized for constrained nodes or "things" are the ones under the 6LoWPAN working group and its successor, the 6Lo working group.
- The initial focus of the 6LoWPAN working group was to optimize the transmission of IPv6 packets over constrained networks such as IEEE 802.15.4.

Optimizing IP for IoT: From 6LoWPAN to 6Lo

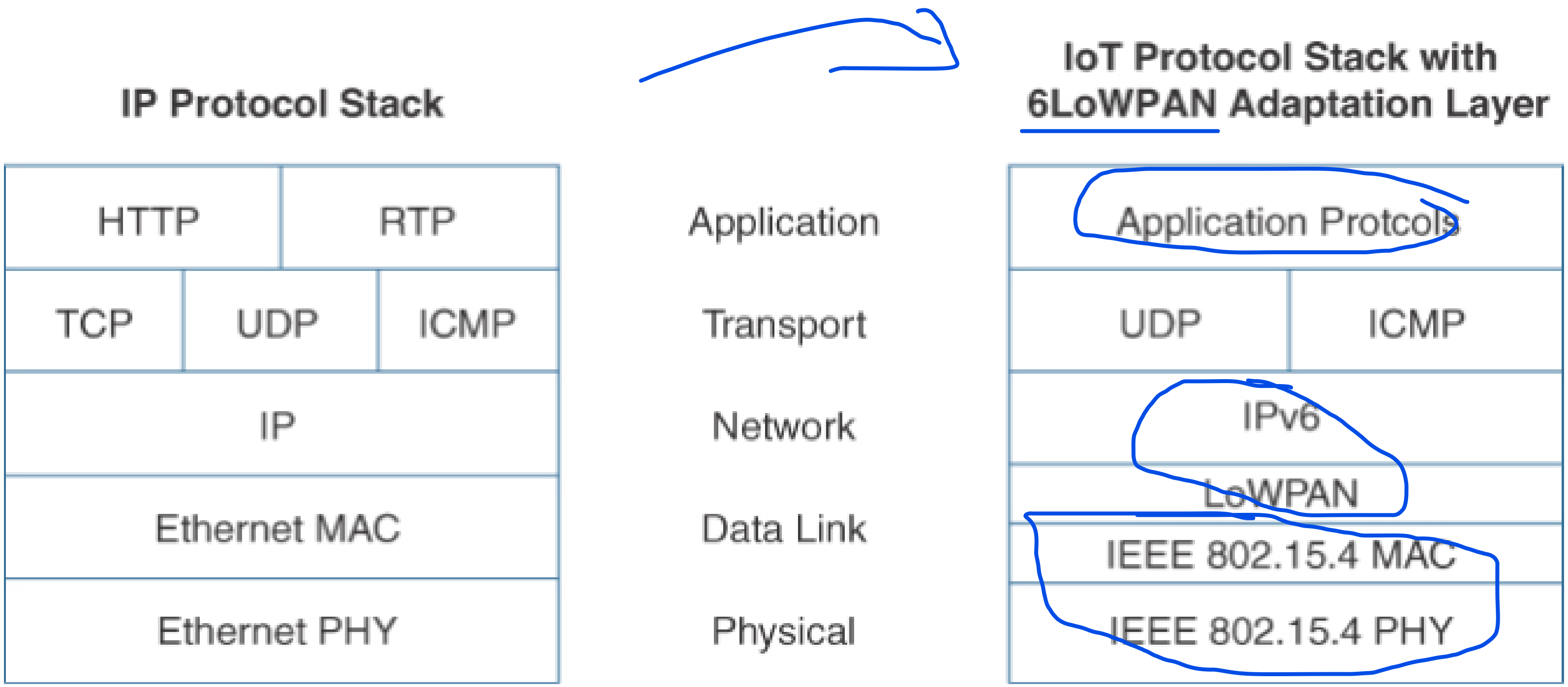
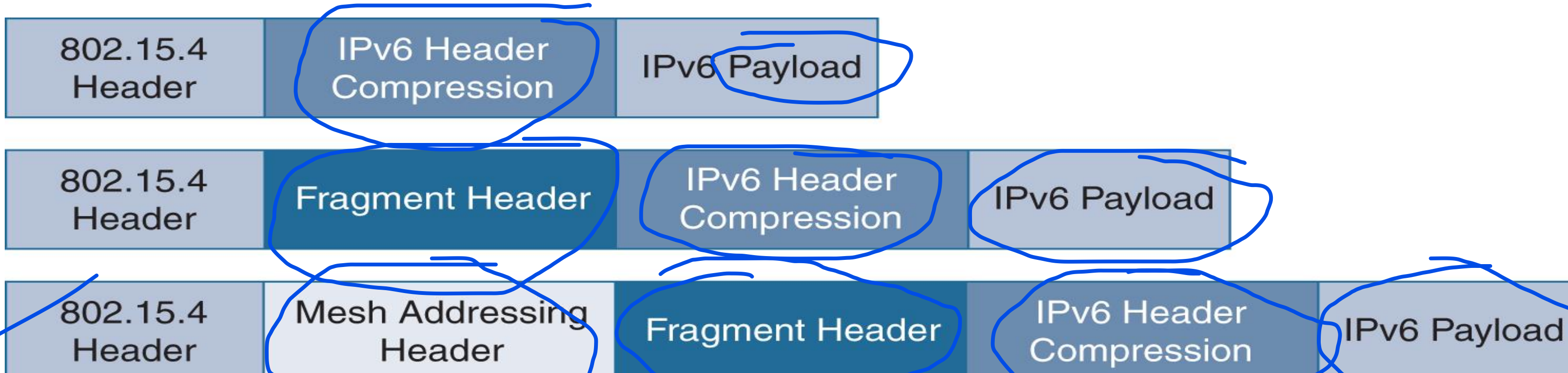


Figure 5-2 *Comparison of an IoT Protocol Stack Utilizing 6LoWPAN and an IP Protocol Stack*

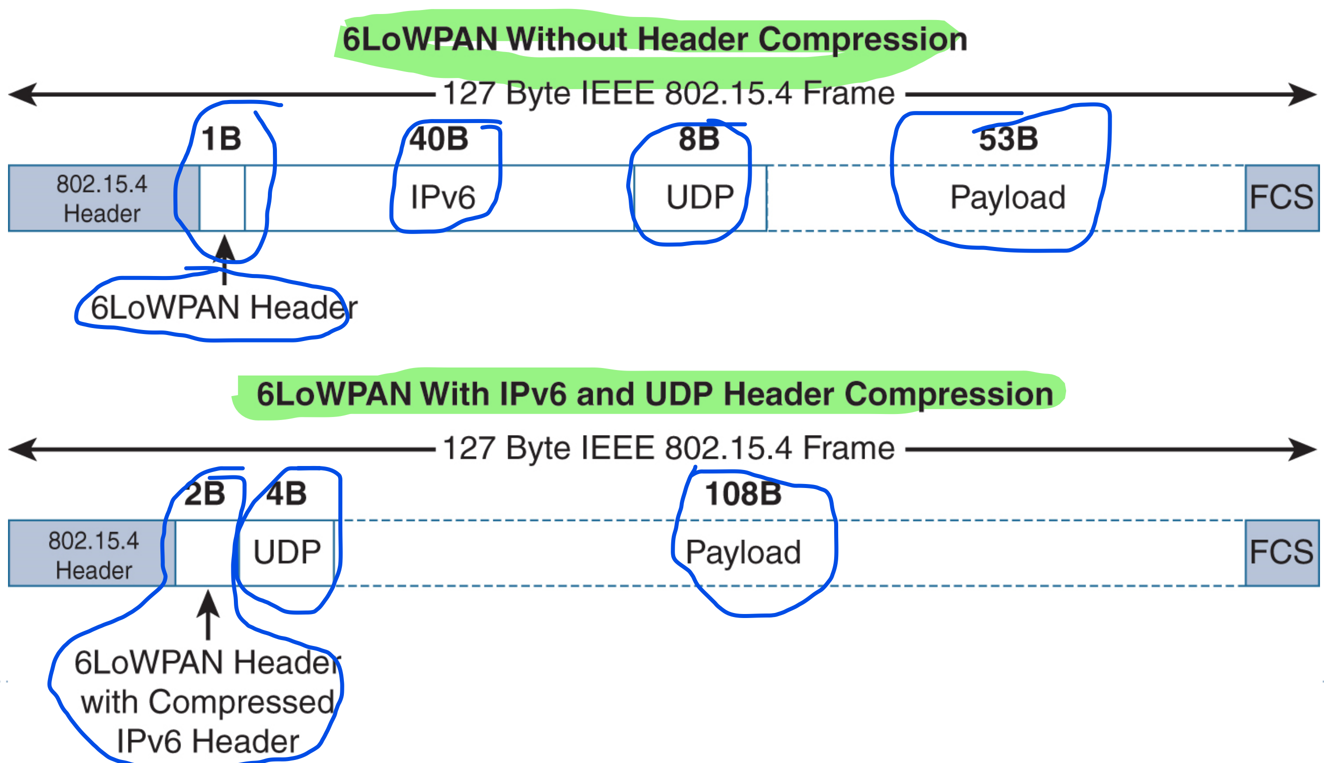
Optimizing IP for IoT: From 6LoWPAN to 6Lo

- RFC 4994 defined frame headers for the capabilities of header compression, fragmentation, and mesh addressing.
- These headers can be stacked in the adaptation layer to keep these concepts separate while enforcing a structured method for expressing each capability.
- Depending on the implementation, all, none, or any combination of these capabilities and their corresponding headers can be enabled.



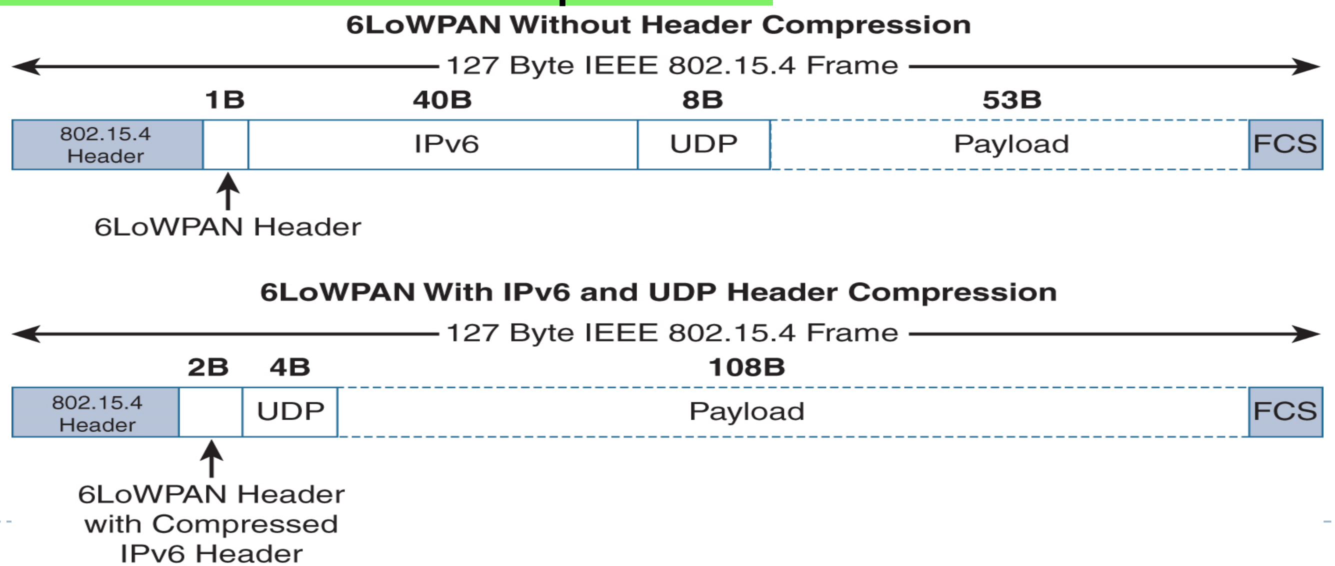
Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Header Compression**
- 6LoWPAN frame without any header compression enabled: The full 40-byte IPv6 header and 8-byte UDP header are visible. The 6LoWPAN header is only a single byte in this case.



Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Header Compression**
- The 6LoWPAN header increases to 2 bytes to accommodate the compressed IPv6 header, and UDP has been reduced in from to 4 bytes from 8.
- The header compression has allowed the payload to more than double, from 53 bytes to 108 bytes, which is much more efficient than with out compression

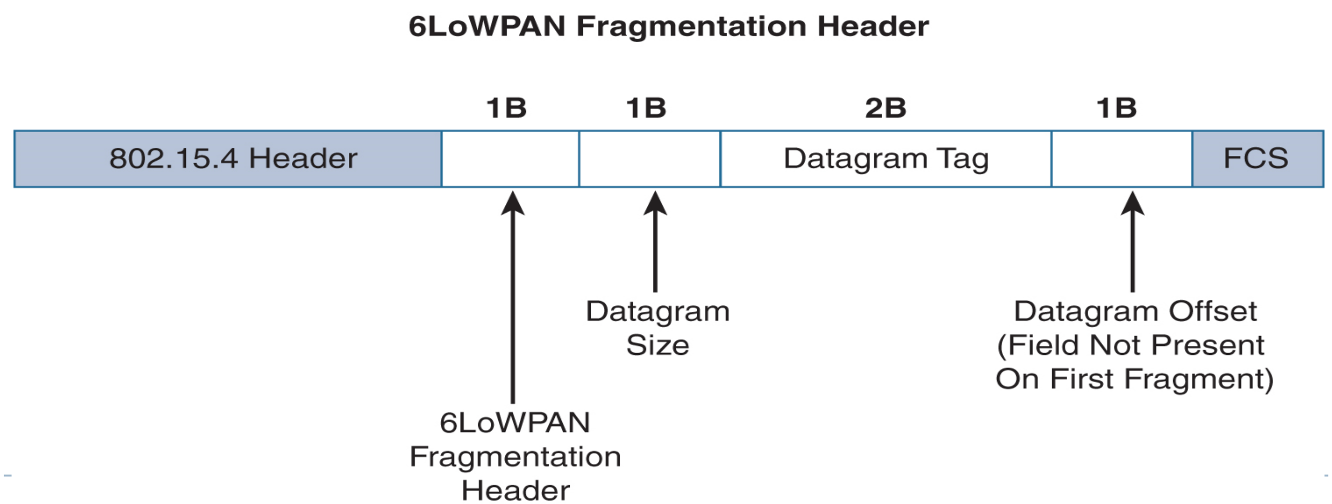


Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Fragmentation**
- Maximum transmission unit (*MTU*) defines the size of the largest protocol data unit that can be passed.
- The MTU for an IPv6 network must be at least 1280 bytes.
- IN IPv6 much larger MTU, is carried inside the 802.15.4 frame with a much smaller one.
- To remedy this situation, large IPv6 packets must be fragmented across multiple 802.15.4 frames at Layer 2.
- The fragment header utilized by 6LoWPAN is composed of three primary fields:
- Datagram Size, Datagram Tag, and Datagram Offset.

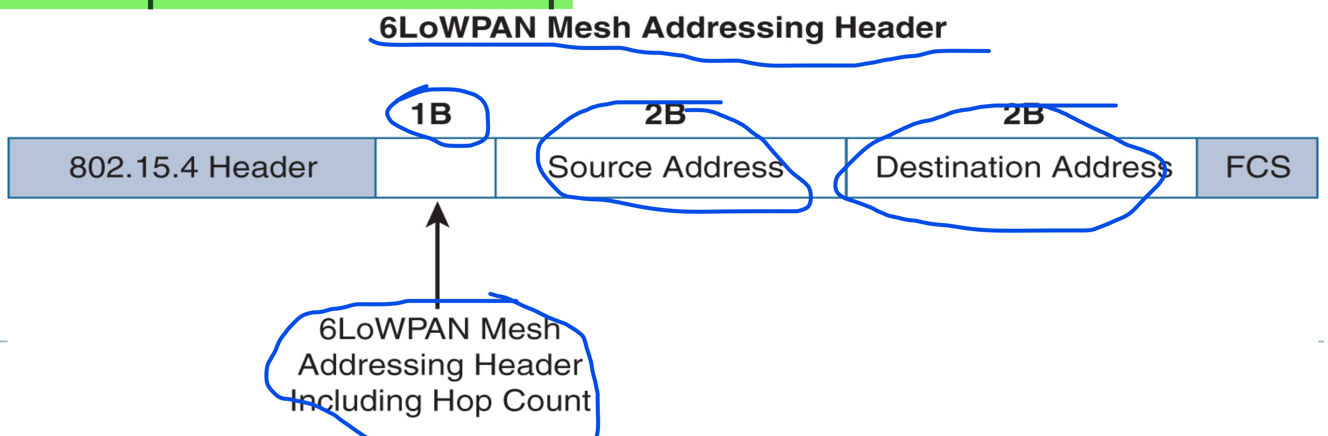
Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Fragmentation**
- Datagram Size,
  - specifies the total size of the unfragmented payload.
- Datagram Tag,
  - identifies the set of fragments for a payload.
- Datagram Offset.
  - delineates how far into a payload a particular fragment occurs.



Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Mesh Addressing**
- The purpose of the 6LoWPAN mesh addressing function is to forward packets over multiple hops.
- Three fields are defined for this header:
- Hop Limit:
  - Provides an upper limit on how many times the frame can be forwarded.
- Source Address, and Destination Address.
  - Indicates the endpoints of an IP hop.



Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Mesh-Under Versus Mesh-Over Routing**
- For network technologies that support mesh topologies and operate at the physical and data link layers, two main options exist for establishing reachability and forwarding packets.
- First option, mesh-under, the routing of packets is handled at the 6LoWPAN adaptation layer.
- Second option, known as "mesh-over" or "route-over," utilizes IP routing for getting packets to their destination.

Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Mesh-Under**
- used because multiple link layer hops can be used to complete a single IP hop.
- Nodes have a Layer 2 forwarding table that they consult to route the packets to their final destination within the mesh.
- An edge gateway terminates the mesh-under domain.
- The edge gateway must also implement a mechanism to translate between the configured Layer 2 protocol and any IP routing mechanism implemented on other Layer 3 IP interfaces.

Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **Mesh-Over**
- routing is utilized for computing reachability and then getting packets forwarded to their destination, either inside or outside the mesh domain.
- Each full-functioning node acts as an IP router, so each link layer hop is an IP hop.
- When a LoWPAN has been implemented using different link layer technologies, a mesh-over routing setup is useful.

Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **6Lo Working Group**
- 6Lo working group seeks to expand on this completed work with a focus on IPv6 connectivity over constrained-node networks. This working group is focused on the following:
- **IPv6-over-foo adaptation layer specifications using 6LoWPAN technologies (RFC4944, RFC6282, RFC6775) for link layer technologies:**
- For example, this includes:
  - IPv6 over Bluetooth Low Energy
  - Transmission of IPv6 packets over near-field communication
  - IPv6 over 802.11ah
  - Transmission of IPv6 packets over DECT Ultra Low Energy
  - Transmission of IPv6 packets on WIA-PA (Wireless Networks for Industrial Automation–Process Automation)
  - Transmission of IPv6 over Master Slave/Token Passing (MS/TP)

Optimizing IP for IoT: From 6LoWPAN to 6Lo

- **6Lo Working Group**
- **Information and data models such as MIB modules:**
- One example is RFC 7388, "Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)."
- **Optimizations that are applicable to more than one adaptation layer specification:**
- For example, this includes RFC 7400, "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)."
- **Informational and maintenance publications needed for the IETF specifications in this area**