Module 3: Chap 5

# IP as the IoT Network Layer

- **The Business Case for IP:** This section discusses the **advantages of IP from an IoT perspective** and **introduces the concepts of adoption and adaptation.**

# 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 (for example, fog computing).

- These lightweight applications communicate with the data center servers.

# Explain the key advantages of IP suite
# The Key Advantages of Internet Protocol

- One of the main differences between traditional information technology (IT) and operational technology (OT) is the **lifetime of the underlying technologies and products.**

- An entire industrial workflow generally mandates smooth, incremental steps that evolve, **with operations itself being the most time- and mission-critical factor for an organization.**

- One way to guarantee multi-year lifetimes is to **define a layered architecture such as the 30-year-old IP architecture.**

- It is able to maintain its **operations for large numbers of devices and users, such as the 3 billion Internet users**

# The key advantages of the IP suite for the Internet of Things are:

1) **Open and standards-based:**
2) **Versatile:**
3) **Ubiquitous:**
4) **Scalable**
5) **Manageable and highly secure:**
6) **Stable and resilient:**
7) **Consumers' market adoption:**
8) **The innovation factor:**

# 1.Open and standards-based:

- ***The Internet of Things creates a new paradigm in which devices, applications, and users can leverage a large set of devices and functionalities while guaranteeing interchangeability and interoperability, security, and management***.
- This calls for implementation, validation, and deployment of open, standards-based solutions.
- While many **standards development organizations (SDOs) are working on Internet of Things definitions, frameworks, applications, and technologies,** none are questioning the role of the Internet Engineering Task Force (IETF) as the foundation for specifying and optimizing the network and transport layers.
- **The IETF is an open standards body that focuses on the development of the Internet Protocol suite and related Internet technologies and protocols**

**2. Versatile:**

- A large spectrum of access technologies is available to offer connectivity of “things” in the last mile.
- Additional protocols and technologies are also used to transport IoT data through backhaul links and in the data center.
- Even if physical and data link layers such as Ethernet, Wi-Fi, and cellular are widely adopted, the history of data communications demonstrates that no given wired or wireless technology fits all deployment criteria.
- communication technologies evolve at a pace faster than the expected 10- to 20-year lifetime of OT solutions. So, the layered IP architecture is well equipped to cope with any type of physical and data link layers.
- This makes IP ideal as a 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.

- **3) Ubiquitous:**
- All recent operating system 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.**
- In addition, IoT application protocols in many industrial OT solutions have been updated in recent years to run over IP.
- While these updates have mostly consisted of IPv4 to this point, recent standardization efforts in several areas are adding IPv6.
- In fact, IP is the most pervasive protocol when you look at what is supported across the various IoT solutions and industry verticals.

- **4) Scalable:**
- As the common protocol of the Internet, IP has been massively deployed and tested for robust scalability.
- Millions of private and public IP infrastructure nodes have been operational for years, offering strong foundations for those not familiar with IP network management.
- Adding huge numbers of “things” to private and public infrastructures may require optimizations and design rules specific to the new devices.
- However, you should realize that this is not very different from the recent evolution of voice and video endpoints integrated over IP.
- IP has proven before that scalability is one of its strengths.

**5) Manageable and highly secure:**

- Communications infrastructure requires appropriate management and security capabilities for proper operations.
- One of the benefits that comes from 30 years of operational IP networks is the 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.
- Well-known network and security management tools are easily leveraged with an IP network layer.
- However, you should be aware that despite the secure nature of IP, real challenges exist in this area.
- The industry is challenged in securing constrained nodes, handling legacy OT protocols, and scaling operations

**6) Stable and resilient:**

- IP has been around for 30 years, and it is clear that IP is a workable solution.
- IP has a large and well-established knowledge base and, more importantly, it has been used for years in critical infrastructures, such as financial and defense networks.

- In addition, IP has been deployed for critical services, such as voice and video, which have already transitioned from closed environments to open IP standards.

- **Finally, its stability and resiliency benefit from the large ecosystem of IT professionals who can help design, deploy, and operate IP-based solutions.**

**7) Consumers' market adoption:**

- When developing IoT solutions and products targeting the consumer market, vendors know ***that consumers' access to applications and devices will occur predominantly over broadband 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.**

**8) The innovation factor:**

- The past two decades have largely established the adoption of IP as a factor for increased innovation.
- IP is **the underlying protocol for applications** *ranging from file transfer and e-mail to the World Wide Web, e-commerce, social networking, mobility, and more.*
- Even the recent computing evolution from PC to mobile and mainframes to cloud services are perfect demonstrations of the innovative ground enabled by IP.
- Innovations in IoT can also leverage an **IP underpinning.**

- The adoption of IP provides a solid foundation for the Internet of Things by allowing secured and manageable **bidirectional data communication capabilities between all devices in a network.**

- IP is a standards-based protocol that is **ubiquitous, scalable, versatile, and stable.**

- Network services such as ***naming***, ***time distribution***, ***traffic prioritization, isolation,*** and so on are well-known and developed techniques that can be leveraged with IP.

- From ***cloud, centralized, or distributed architectures***, **IP data flow can be developed and implemented according to business requirements**

# Adoption or Adaptation of the Internet Protocol

- How to implement IP in data center, cloud services, and operation centers hosting IoT applications may seem obvious, but the **adoption of IP in the last mile is more complicated and often makes running IP end-to-end more difficult**.

- Before IPv4 was widely accepted and deployed in IT networks, many different protocol stacks overlapped with IP.

- For example, X.25/X.75 was standardized and promoted by service providers, while computer manufacturers implemented their own proprietary protocols, such as SNA, DECnet, IPX, and AppleTalk.

- **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.

- *Supervisory control and data acquisition (SCADA)* applications are typical examples of vertical market deployments *that operate both the IP adaptation model and the adoption model.*
- Found at the core of many modern industries, *SCADA is an automation control system for remote monitoring and control of equipment.*

- Implementations that make use of **IP adaptation have SCADA devices** *attached through serial interfaces to a gateway tunneling or translating the traffic.*
- **With the IP adoption model**, *SCADA devices are attached via Ethernet to switches and routers forwarding their IPv4 traffic*.

- You should consider the following factors when trying to determine which model is best suited for last-mile connectivity:

**Explain the factors considered to determine select a model for last-mile connectivity**

1)Bidirectional versus unidirectional data flow:

2) Overhead for last-mile communications paths:

3) Data flow model:

4) Network diversity:

**1. Bidirectional versus unidirectional data flow:**

- While **bidirectional** communications are generally **expected**, some last-mile technologies offer **optimization for unidirectional communication.**
- **IoT devices may only infrequently need to report a few bytes of data to an application**.
- These sorts of devices, particularly ones that communicate through LPWA technologies, *include fire alarms sending alerts or daily test reports, electrical switches being pushed on or off, and water or gas meters sending weekly indexes.*
- For these cases, it is **not necessarily worth implementing a full IP stack.**
- It **requires the overall end-to-end architecture** to solve potential drawbacks; ***for example, if there is only one-way communication to upload data to an application,*** then ***it is not possible to download new software or firmware to the devices.***

**2) Overhead for last-mile communications paths:**

- IP adoption implies a **layered architecture** with a **per-packet overhead that varies depending on the IP version.**

- **IPv4 has 20 bytes** of header at a minimum, and **IPv6 has 40 bytes** at the IP network layer. ***For the IP transport layer***, ***UDP has 8 bytes*** of header overhead, while ***TCP has a minimum of 20 bytes.***

- If the data to be forwarded by a device ***is infrequent and only a few bytes***, you can potentially ***have more header overhead than device data***—again, particularly in the case of LPWA technologies.

- Consequently, you need to decide whether the IP adoption model is necessary and, if it is, how it can be optimized.
- This same consideration applies to control plane traffic that is run over IP for low-bandwidth, last-mile links.

**3) Data flow model:**

- One benefit of the ***IP adoption model*** is the ***end-to-end nature of communications.***

- ***Any node can easily exchange data with any other node in a network,*** although security, privacy, and other factors may put controls and limits on the "end-to-end" concept.

- In many IoT solutions***, a device's data flow is limited to one or two applications.***

- In this case***, the adaptation model can work because translation of traffic needs to occur only between the end device and one or two application servers.***

**4) Network diversity:**

- One of the ***drawbacks*** of the ***adaptation model*** is ***a general dependency on single PHY and MAC layers***. For example, ***ZigBee devices*** must only be deployed in **ZigBee network islands.**
- This same restriction holds for ITU G.9903 G3-PLC nodes.
- Therefore, *a deployment must consider which applications have to run on the gateway connecting these islands and the rest of the world.*
- Integration and coexistence of new physical and MAC layers or new applications impact how deployment and operations have to be planned.

# The Need for Optimization

- In addition to coping with the integration of non-IP devices, *you may need to deal with the limits at the device and network levels that IoT often imposes.*
- Therefore, optimizations are needed at various layers of the IP stack to handle the restrictions that are present in IoT networks.

# Constrained Nodes

- Another limit is that this network protocol stack on an IoT node may be required to communicate through an **unreliable path.**

- Even if a full IP stack is available on the node, this causes problems such as **limited or unpredictable throughput and low convergence when a topology change occurs.**

- Finally, **power consumption** is a key characteristic of constrained nodes.

- 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:** 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:** In this case, you may implement either anoptimized 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).

- **Devices that are similar to generic PCs in terms of computing and power resources but have constrained networking capacities, such as bandwidth:** These nodes usually implement a full IP stack (adoption model), but network design and application behaviors must cope with the bandwidth constraints.

# Constrained Networks

- In the early years of the Internet, network bandwidth capacity was restrained due to technical limitations.
- Connections often depended on low-speed modems for transferring data.
- However, these low-speed connections demonstrated that IP could run over low-bandwidth networks.

- Fast forward to today, and the evolution of networking has seen the emergence of high-speed infrastructures. However, high-speed connections are not usable by some IoT devices in the last mile

- A constrained network can have **high latency and a high potential for packet loss.**

- **Note**

- Constrained networks are often 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***.

- LLNs were defined by ***the IETF's Routing over Low-Power and Lossy Networks (RoLL) working group when developing the IPv6 RPL protocol.***

- An IETF working group is an open discussion group of individuals in a particular technology area. They have a charter that defines their focus and what they are expected to produce.

- Constrained networks have unique characteristics and requirements.

- In contrast with typical IP networks, where highly stable and fast links are available, 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.

- With a constrained network, in addition to 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.***

- These behaviors can be observed on both wireless and narrowband power-line communication links, where packet delivery variation may fluctuate greatly during the course of a day.

- Unstable link layer environments create other challenges in terms of **latency and control plane reactivity**.

- One of the golden rules in a constrained network is to **“underreact to failure.”** Due to the low bandwidth, a constrained network that overreacts can lead to a ***network collapse—which makes the existing problem worse.***

- **Control plane traffic** must also be kept at a minimum; otherwise, it consumes the bandwidth that is needed by the data traffic.
- Finally, you have to consider **the power consumption in battery-powered nodes.** Any failure or verbose control plane protocol may reduce the lifetime of the batteries

- In summary, **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

# IP Versions

- 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. For example, SCADA protocols such as DNP3/IP (IEEE 1815), Modbus TCP, or the IEC 60870- 5-104 standards are specified only for IPv4,So, there are no known production implementations by vendors of these protocols over IPv6 today.
- For IoT devices with application protocols defined by the IETF, such as HTTP/HTTPS, CoAP, MQTT, and XMPP, both IP versions are supported.

**2) Cellular Provider and Technology:**

- IoT devices with cellular modems are dependent on the generation of the cellular technology as well as the data services offered by the provider.
- *For the first three generations of data services—GPRS, Edge, and 3G—IPv4 is the base protocol version*.
- Consequently, if IPv6 is used with these generations, it must be tunneled over IPv4.
- *On 4G/LTE networks, data services can use IPv4 or IPv6 as a base protocol, depending on the provider.*

## 3. Serial Communications

## 4. IPv6 Adaptation Layer

# Optimizing IP for IoT

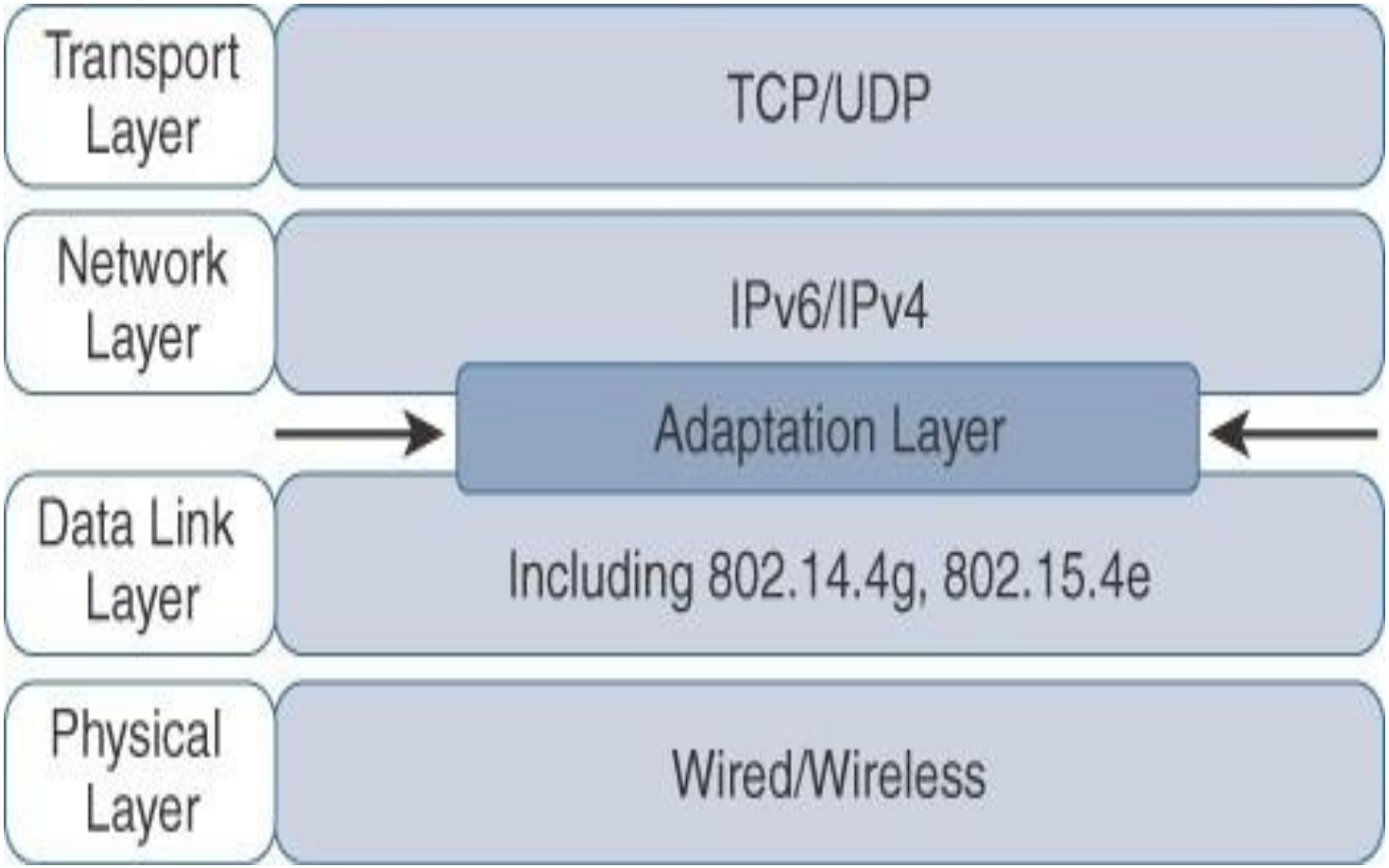



**Figure 5-1** *Optimizing IP for IoT Using an Adaptation Layer*

- **From 6LoWPAN to 6Lo**
- In the IP architecture, the transport of IP packets over any given Layer 1 (PHY) and Layer 2 (MAC) protocol **must be defined and documented.**

- The model for packaging IP into lower-layer protocols is often referred to as an ***adaptation layer***.

- Unless the technology is proprietary, IP adaptation layers are typically 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.
- For example, **RFC 864** describes ***how an IPv4 packet gets encapsulated over an Ethernet frame***, and

- **RFC 2464** describes how the same function is performed for an ***IPv6 packet.***

- IoT-related protocols follow a similar process. The main difference is that an adaptation layer designed for IoT may include some optimizations to deal with constrained nodes and networks

- 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***.

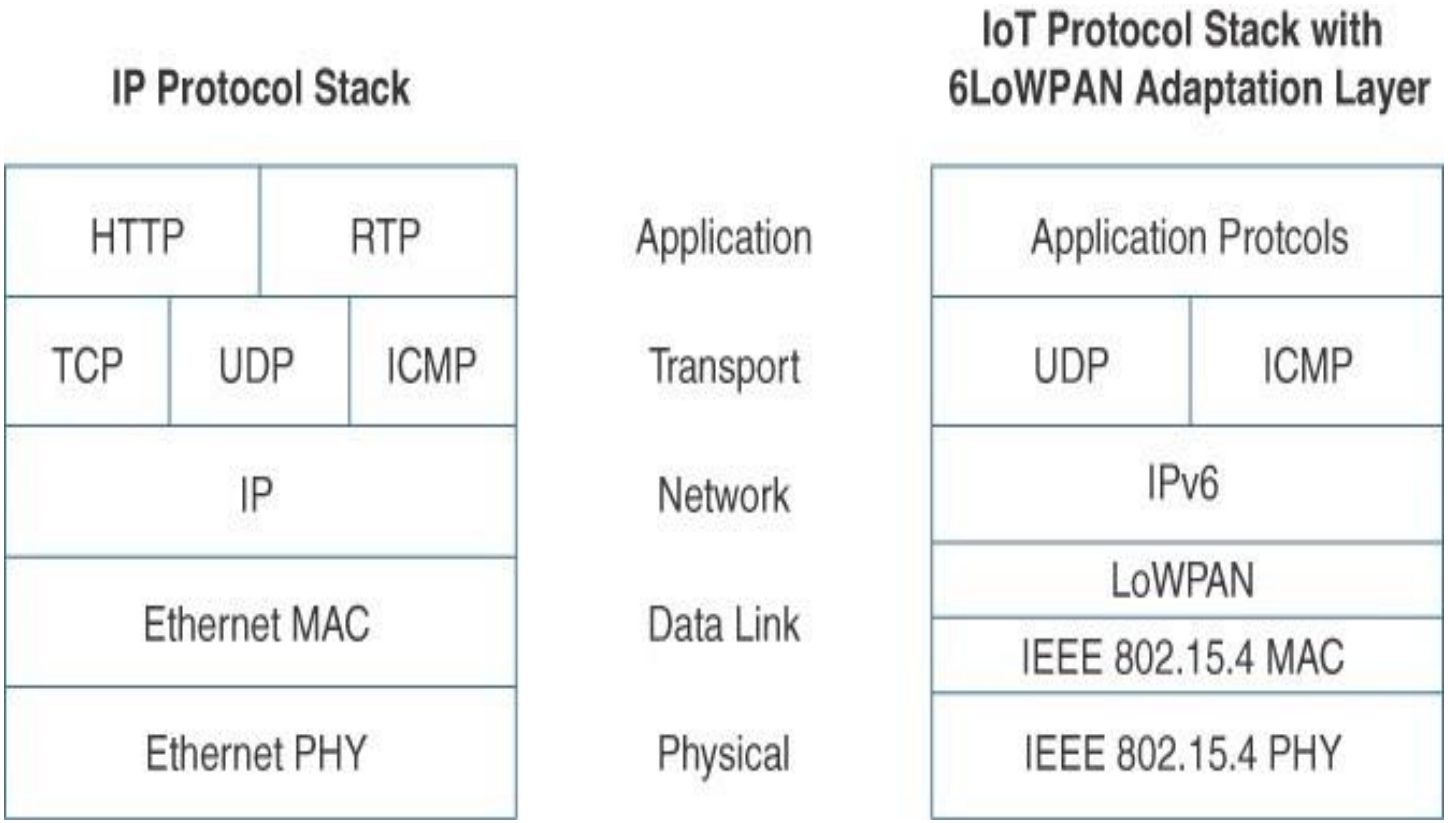



**Figure 5-2** *Comparison of an IoT Protocol Stack Utilizing 6LoWPAN and an IP Protocol Stack*

- The 6LoWPAN working group published several RFCs, but **RFC 4994** is foundational because it defines 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. Figure 5-3 shows some examples of typical 6LoWPAN header stacks.

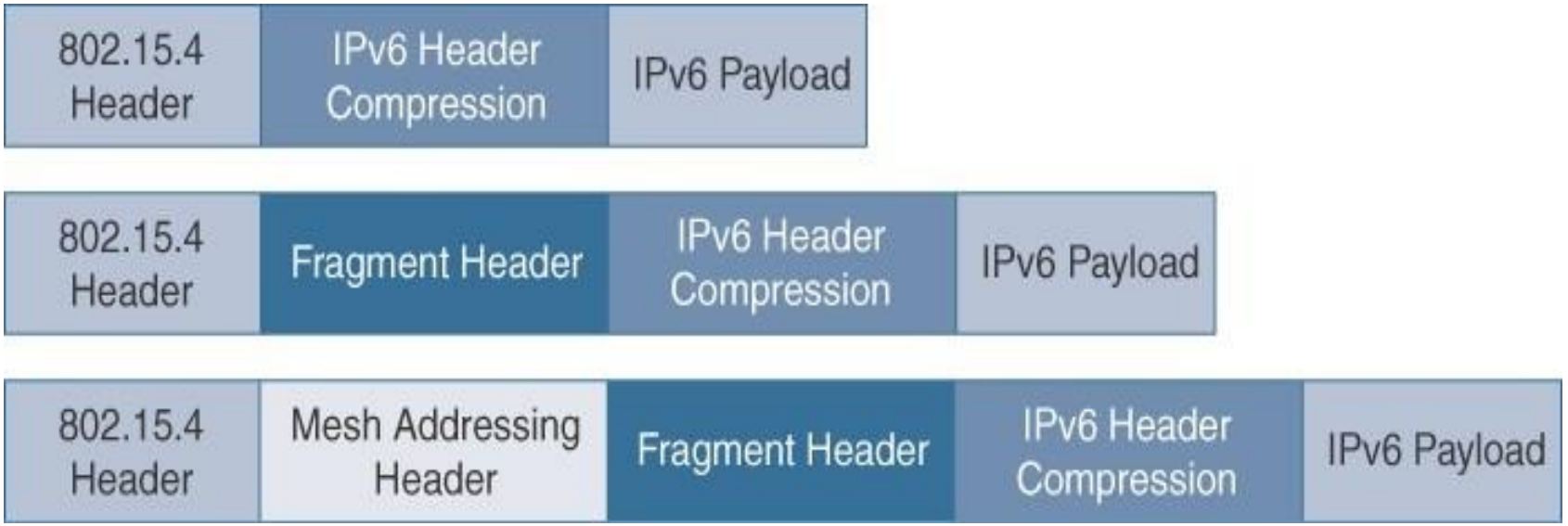



**Figure 5-3** *6LoWPAN Header Stacks*

Figure 5-3 shows the subheaders related to compression, fragmentation, and mesh addressing

- **Header Compression**
- IPv6 header compression for 6LoWPAN was defined initially in RFC **4944 and subsequently updated by RFC 6282**.
- This capability shrinks the size of IPv6's 40-byte headers and User Datagram Protocol's (UDP's) 8-byte headers down as low as 6 bytes combined in some cases.

At a high level, 6LoWPAN works by taking advantage of shared information known by all nodes from their participation in the local network.

In addition, it omits some standard header fields by assuming commonly used values. Figure 5- 4 highlights an example that shows the amount of reduction that is possible with 6LoWPAN header compression.

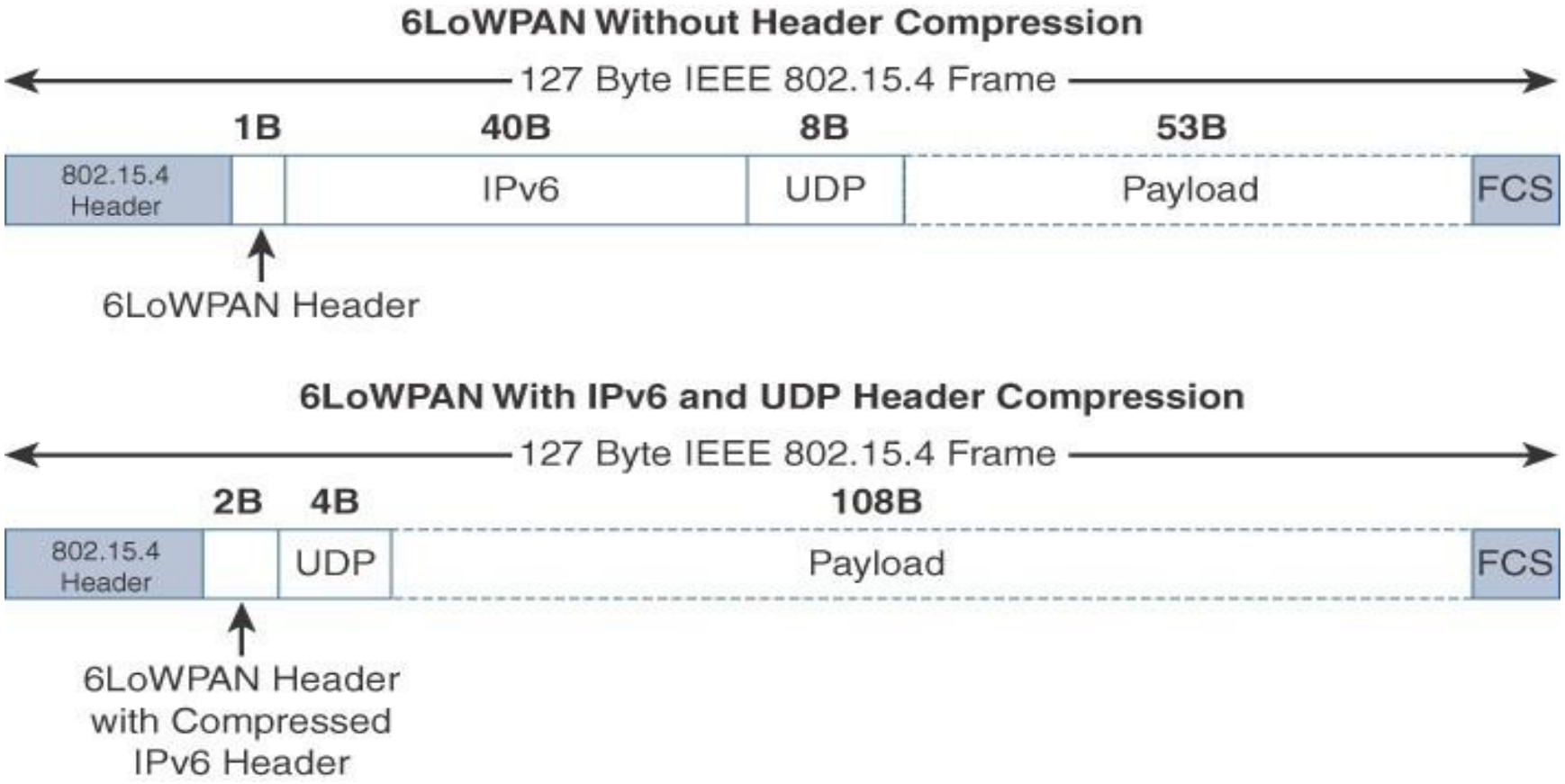



**Figure 5-4** *6LoWPAN Header Compression*

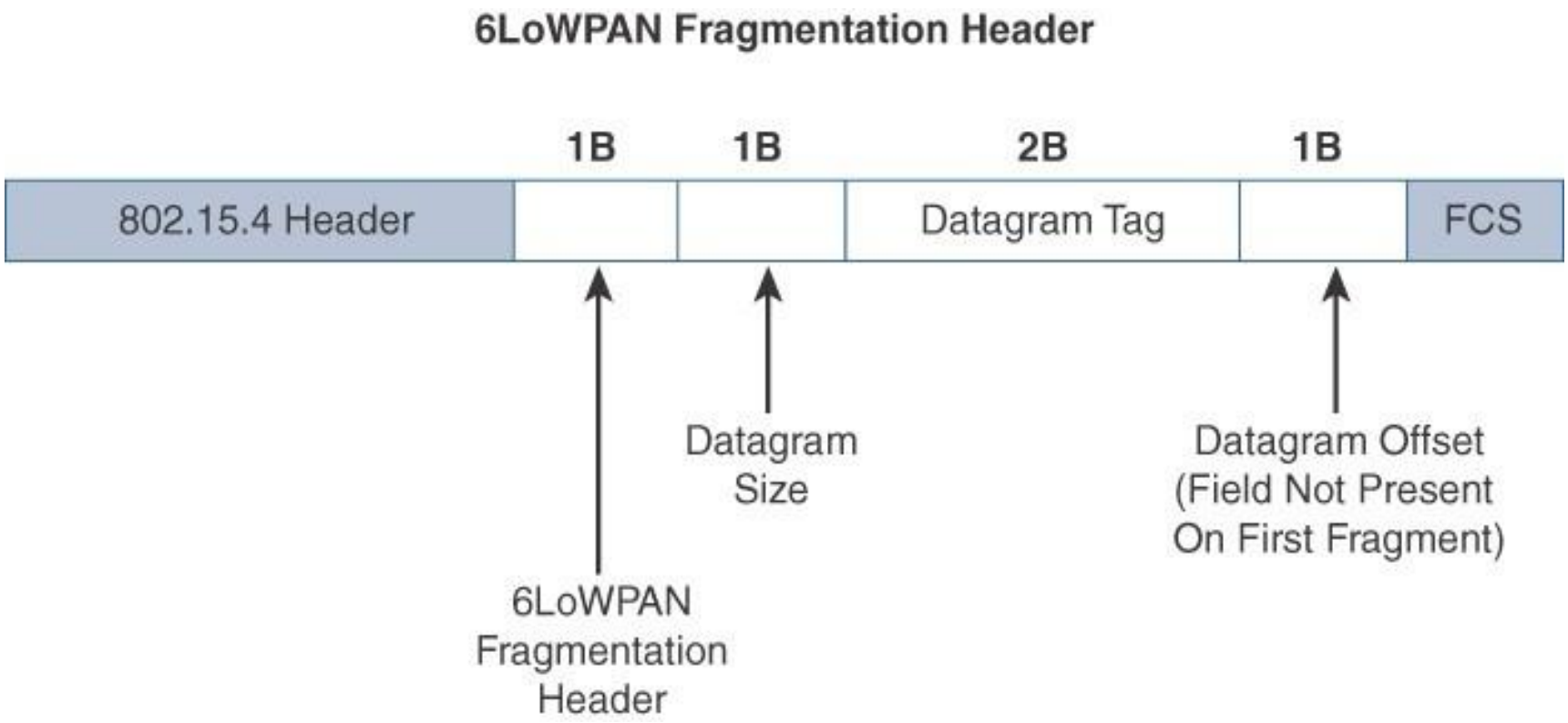
**Note** that the 2-byte header compression applies to intra- cell communications, while communications external to the cell may require some field of the header to not be compressed.

# Fragmentation

# Fragmentation

- The maximum transmission unit **(MTU) for an IPv6 network** must be at least **1280 bytes**.
- The term MTU defines the size of the largest protocol data unit that can be passed.
- For IEEE 802.15.4, 127 bytes is the MTU.
- You can see that this is a problem because IPv6, with a 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

**Figure 5-5** *6LoWPAN Fragmentation Header*




three primary fields: Datagram Size, Datagram Tag, and Datagram Offset.
**The 1-byte Datagram Size** field ***specifies the total size of the unfragmented payload***.

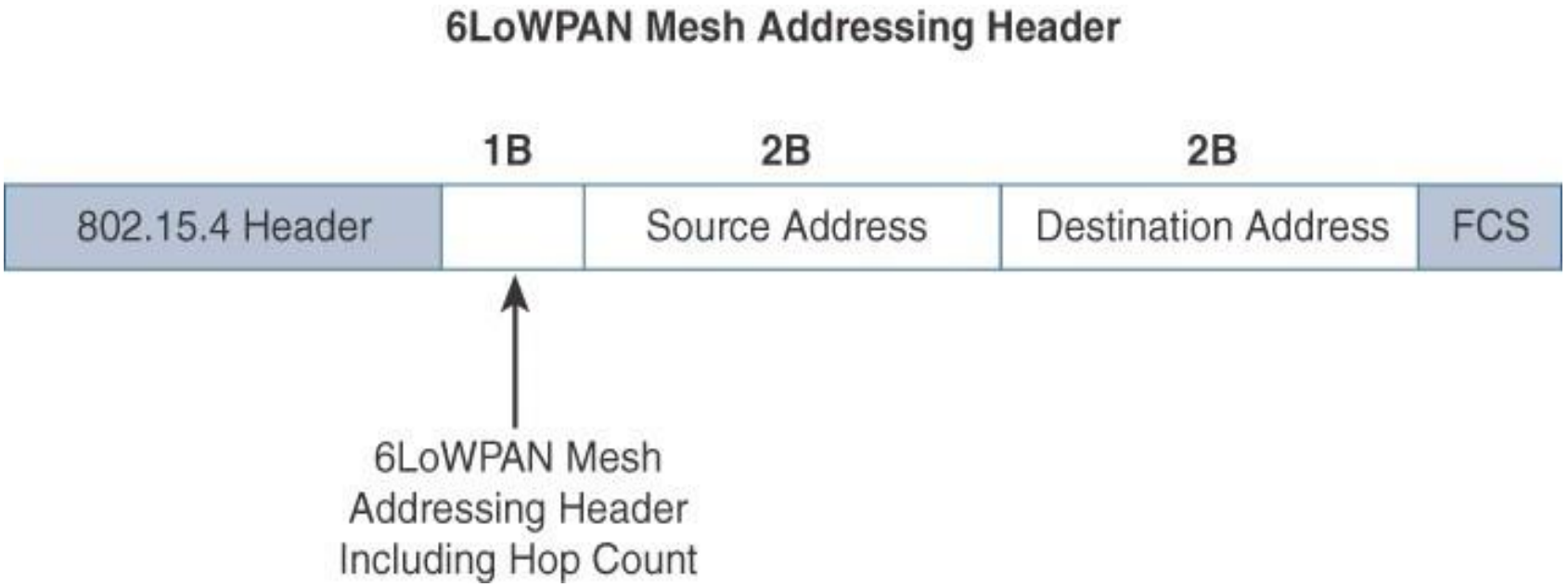
***Datagram Tag identifies the set of fragments for a payload***.

Finally, the **Datagram Offset field** delineates ***how far into a payload a particular fragment occurs***

# 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, Source Address, and Destination Address.**
- Analogous to the IPv6 hop limit field, ***the hop limit for mesh addressing also provides an upper limit on how many times the frame can be forwarded***. Each hop decrements this value by 1 as it is forwarded. Once the value hits 0, it is dropped and no longer forwarded.
- ***The Source Address and Destination Address fields for mesh addressing are IEEE 802.15.4 addresses indicating the endpoints of an IP hop***

- **Figure 5-6** *6LoWPAN Mesh Addressing Header*



# Mesh-Under Versus Mesh-Over Routing

- Two main options exist for ***establishing reachability and forwarding packets.***

- **mesh-under,** the *routing of packets is handled at the 6LoWPAN adaptation layer.*

- **“mesh-over” or “route-over,”** *utilizes IP routing for getting packets to their destination*

- **With mesh-under routing,** the routing of IP packets leverages the *6LoWPAN mesh addressing header* to route and forward packets at the link layer.

- The term *mesh-under* is 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.

- **In mesh-over or route-over scenarios**, *IP Layer 3 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.**

- While traditional IP routing protocols can be used, a specialized routing protocol for smart objects, such as **RPL**, is recommended.

# 6Lo Working Group

- 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)

- **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**