Chapter 5
IP as the IoT Network Layer

In this chapter, we move up the protocol stack and extend the conversation to network layer connectivity, which is commonly referred to as Layer 3.

Summary of this Chapter

This chapter looks at the following

The Business Case for IP: A discussion of advantages of IP from an IoT perspective and introduces the concepts of adoption and adaptation.

The Need for Optimization: This section dives into the challenges of constrained nodes and devices when deploying IP.

Optimizing IP for IoT: It explorers the common protocols and technologies

Profiles and Compliance: A summary of 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 (for example, fog computing)

These lightweight applications communicate with the data center servers. Therefore, the system solutions combining various physical and data link layers call for an architectural approach with a common layer(s) independent from the lower (connectivity) and/or upper (application) layers

The Key Advantages of Internet Protocol

1. Open and standards-based: The IETF is an open standards body that focuses on the development of the Internet Protocol suite and related Internet technologies and protocols. This ensures that standards are followed while deployment in various technologies.

2. Versatile

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.

…. Key Advantages of Internet Protocol

3. Ubiquitous; refers to IoT application protocols in many industrial OT solutions have been updated in recent years to run over IP which is a pervasive protocol that is supported across the various IoT solutions and industry verticals.

4. **Scalable;** 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. Most of the new devices have been influenced in a way that they have to include support of IP.

…. Key Advantages of Internet Protocol

5. Manageable and highly secure: 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

6. Stable and resilient; 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. There are many IT professionals who can help design, deploy, and operate IP-based solutions.

.... Key Advantages of Internet Protocol

6.Consumers´ market adoption: IP protocol links the consumer´s access application and devices(smart phones, tablets and PCs to the world of IoT. The access to applications is through broadband and wireless mobile infrastructure which is supported by IP.

7. The innovation factor: IP is the underlying protocol for applica-

tions ranging from file transfer and e-mail to the World Wide Web, e-commerce,social networking, mobility, and more.

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.

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.

Examples of Adaption and Adoption

1. In manufacturing industry; Over 10 years now, the initial versions of serial communication protocols, IP and Ethernet were not emphasized but now they have been integrated both Ethernet and IPv4.

2. Supervisory control and data acquisition (SCADA) is an automation control system for remote monitoring and control of equipment.

Adoption: Serial interfaces are attached to the gateways for traffic translation.

Adaption: Ethernet to switches and routers forwarding their IPv4 traffic

3. A ZigBee gateway often acts as a translator between the ZigBee

and IP protocol stacks. It runs a non-IP stack between devices and gateway

Factors to consider when choosing a model for last-mile connectivity

The **last mile** of the IoT network is the access network in the Access Network Sublayer. The link between the topology and the connectivity you choose for the IoT. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g as discussed in chapter 2

1. **Bidirectional versus unidirectional data flow:** some devices infrequently need to report a few bytes of data to an application such as fire alarms sending daily reports,they don´t need full stack IP

2. **Overhead for last-mile communications paths:** There´s need need to decide whether the IP adoption model is necessary and, if it is, how it can be optimized.

3. **Data flow model:** In many IoT solutions, a device´s data flow is limited to one or two applications thus 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:** In cases where deployment is dependent on single PHY and MAC layers, adoption model is used to solve these limitations during deployment

Confinements in the IoT solution.

An IoT Solution is a seamlessly integrated bundle of technologies, including many sensors, that companies can purchase to solve a problem and/or create new organizational value

Both the nodes and the network itself can often be constrained in IoT solutions. Also, IP is transitioning from version 4 to version 6, which can add further confinements in the IoT space.

1.Constrained Nodes

2.Constrained Networks

3.IP versioning

The Need for Optimization

1. **Constrained Nodes**

Devices with limited resources like memory, processing capacity, and power are called constrained nodes.

Optimizations are necessary to address these limitations on constrained nodes;

- A thing architecture may or may not offer similar characteristics compared to a generic PC or server in an IT environment.

- The node may be required to communicate through an unreliable path thus causing unpredictable throughput and low convergence when topology changes.

- Power Consumption; Many IoT devices are battery powered

Classification of IoT constrained nodes

Classification of these nodes helps when evaluating the IP adoption versus adaptation model selection.

1. Devices that are very constrained in resources, may communicate infrequently to transmit a few bytes, and may have limited security and management capabilities. This calls for IP adaptation model.

2. Devices with enough power and capacities to implement a stripped-down IP stack or non-IP stack. Either adoption model for application to server communication or adaptation model communicate through gateways for non-IP stacks.

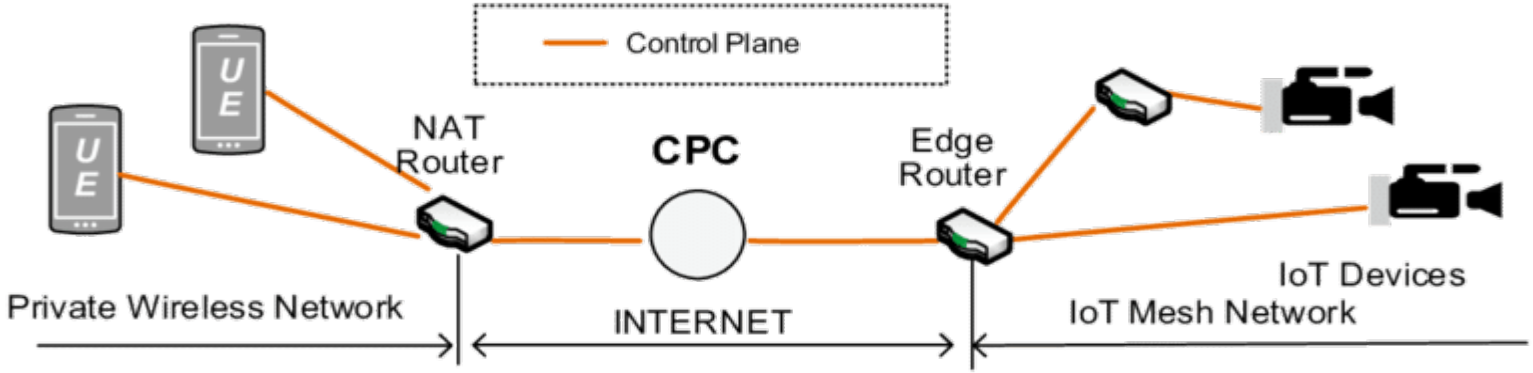
3. Devices that are similar to generic PCs in terms of computing and power resources but have constrained networking capacities, such as bandwidth: These nodes usually implement a full IP stack (adoption model)

2. Constrained Networks

A constrained network is composed of a significant portion of constrained nodes. Mostly, these constrained node networks are deployed in the edge network of an IoT system.

UEs and IoT devices behind constrained access networks

UE-User Equipments



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

A constrained network exhibits below characteristics:

- Low bit-rate/throughput
- High packet loss and high variability of packet loss
- Highly asymmetric link characteristics
- Lack of advanced network services like multi-cast

Control plane traffic must also be kept at a minimum; otherwise, it consumes the bandwidth that is needed by the data traffic.

3. IP Versioning

Internet Protocol: Which version?

There are currently two versions of the Internet Protocol in use for the Internet

- **IPv4 (IP Version 4)**
  - Specified in 1980/81 (RFC 760, 791)
  - Four byte addresses
  - Universally deployed
  - **Problem**: Address space almost exhausted
- **IPv6 (IP Version 6)**
  - Specification from 1998 (RFC 2460)
  - Significant differences to IPv4, but not fundamental changes
  - 16-byte addresses
  - **Problem**: Not widely used (yet?)

Factors that dictate whether IPv4 or IPv6 or both 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: For the first three generations of data services—GPRS, Edge, and 3G—IPv4 is the base protocol version but IPv6 can be used on 4G/LTE networks.

Serial Communications: Many legacy devices in certain industries, such as manufacturing and utilities, communicate through serial lines. MAP-T enables older, industrial end devices and applications to continue running IPv4 even though the network providing connectivity is IPv6

IPv6 Adaptation Layer:Some physical and data link layers stipulate the use of only IPv6 while physical and data link layers (Ethernet, Wi-Fi, and so on) use both IPv4 and IPv6. New techs such as WPAN and NPLC have only IPv6 adaptation layer.

Optimizing IP for IoT

The IoT network optimization offers a lot of benefits for improving traffic management, operating efficiency, energy conservation, reduction in latency, higher throughput and faster rate in scaling up or deploying IoT services and devices in the network.

Adaptation Layer - translation between non-IP and IP layers.

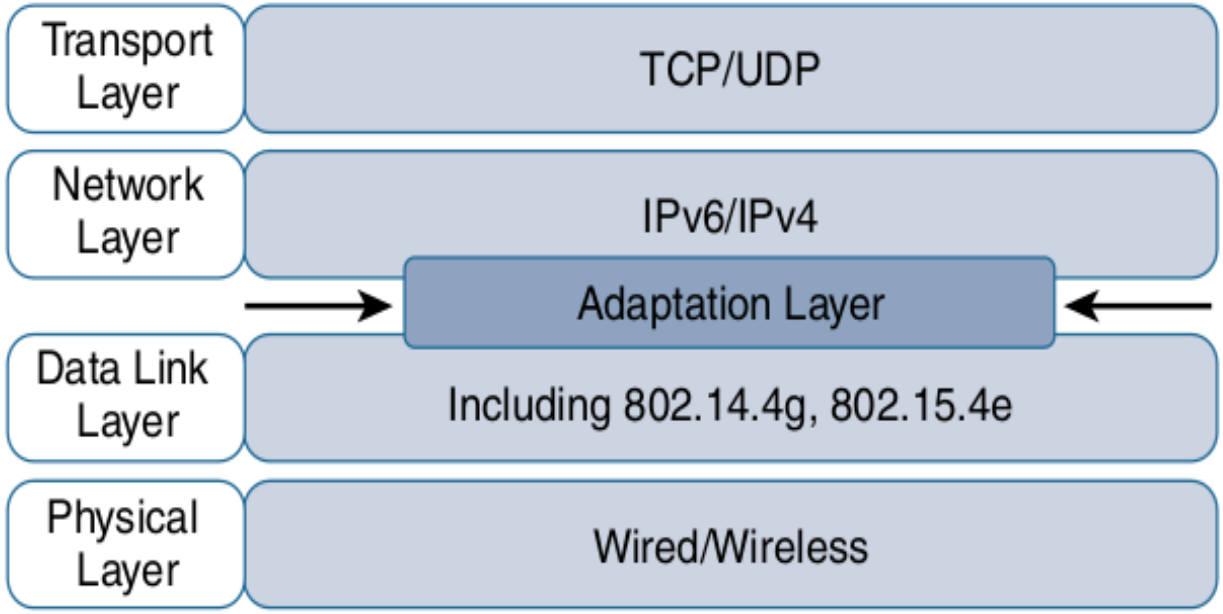


Figure 5-1 *Optimizing IP for IoT Using an Adaptation Layer*

From 6LoWPAN to 6Lo

Expanding the Universe of IPv6-Supported Technologies for the Internet of Things.

The 6lo (IPv6 over Networks of Resource-constrained Nodes) is a successor of the 6LoWPAN

The primary difference is that 6lo defines specifications for running IPv6 over multiple constrained technologies that use a base 6LoWPAN stack or the IPv6 low-power adaptation, stateless header compression and Neighbor

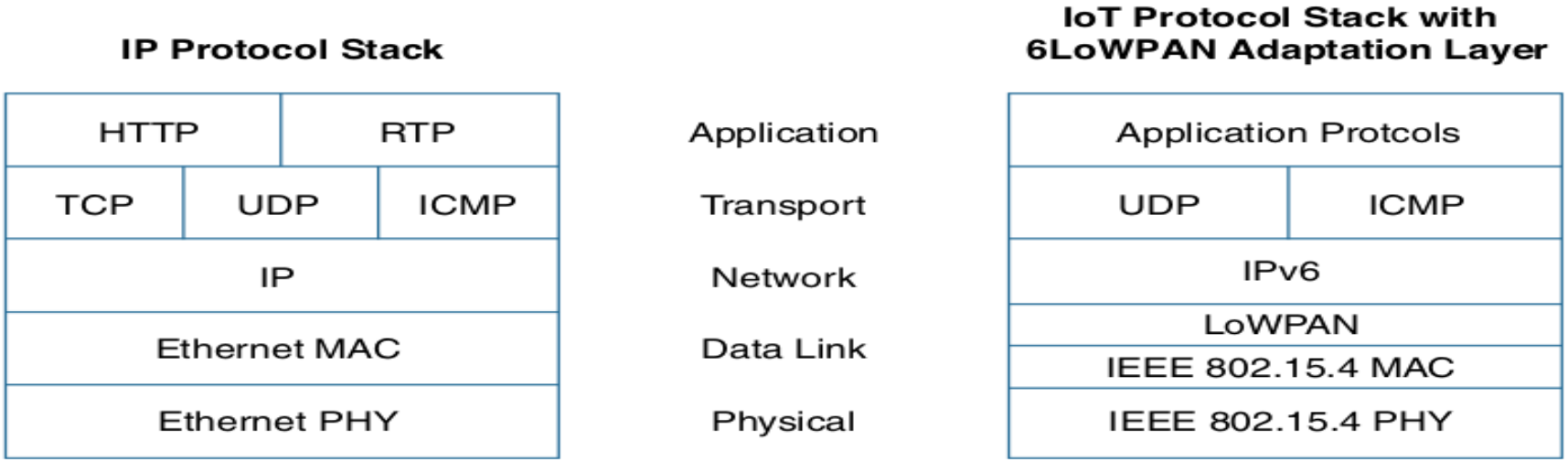


Figure 5-2 *Comparison of an IoT Protocol Stack Utilizing 6LoWPAN and an IP Protocol Stack*

Example of a typical 6LoWPAN header stacks.

The 6LoWPAN working group is foundational because it defines frame headers for the capabilities of header compression, fragmentation, and mesh addressing.

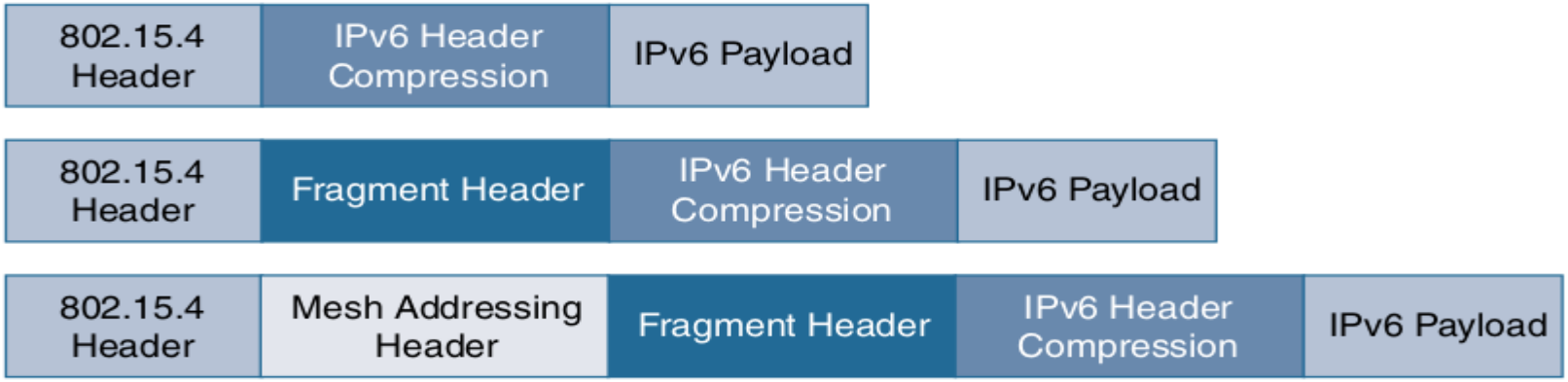


Figure 5-3 *6LoWPAN Header Stacks*

These headers can be stacked in the adaptation layer to keep these

concepts separate while enforcing a structured method for expressing each capability.

6LoWPAN header ….ctd

Capabilities of 6LoWPAN include;

1. Header compression: 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.

2. Fragmentation header: large IPv6 packets must be fragmented across multiple 802.15.4 frames at Layer 2 so that they can fit in the carrier.

3. Mesh Addressing: This is purposeful in the 6LoWPAN to to forward packets over multiple hops.

6LoWPAN header….ctd

Header Compression

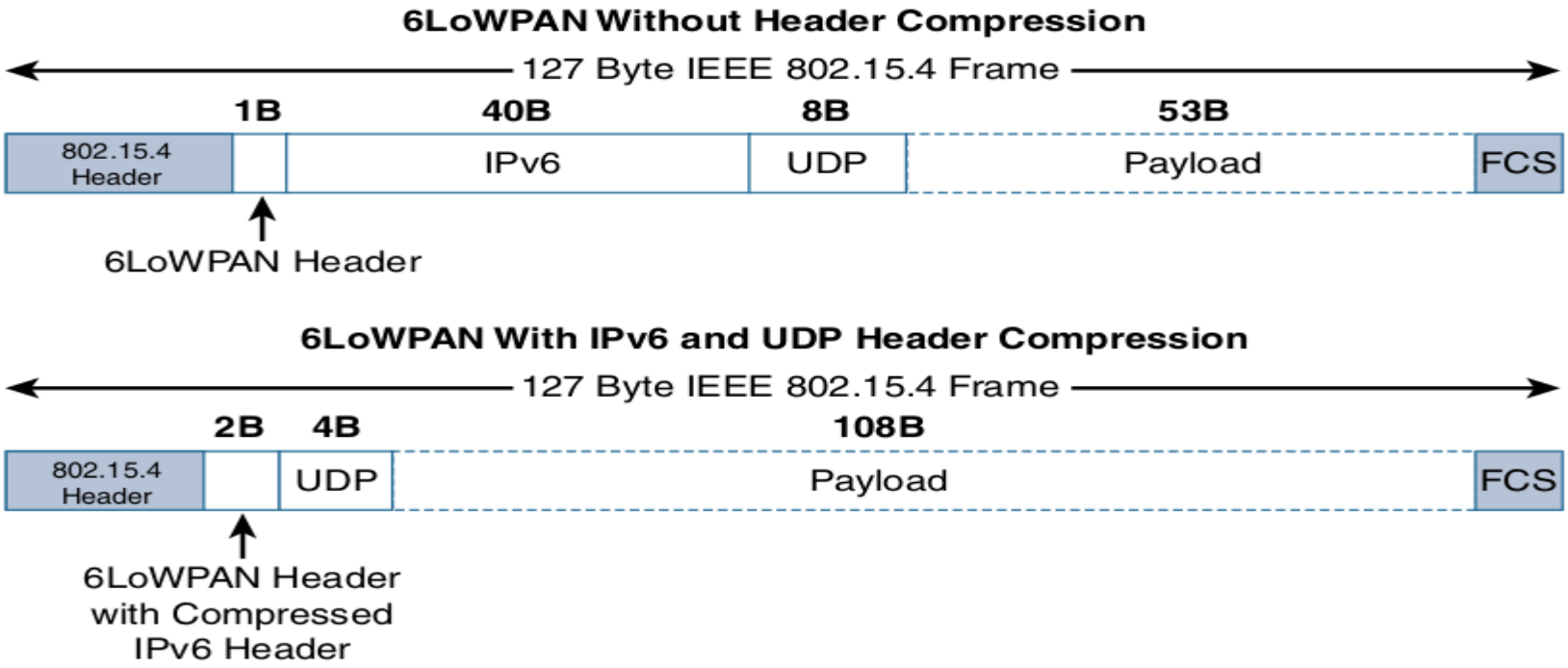


Figure 5-4 *6LoWPAN Header Compression*

6LoWPAN header ….ctd

From the above illustration, the Header compression has been enabled for a best-case scenario. The 6LoWPAN header increases to 2 bytes to accommodate the compressed IPv6 header, and UDP has been reduced in half, to 4 bytes from 8.

Most importantly, the header compression has allowed the payload to more than double, from 53 bytes to 108 bytes, which is obviously much more efficient

While nothing precludes running TCP over IPv6/6LoWPAN, no TCP header compression is defined. The main reason is because TCP´s congestion-avoidance algorithms could overreact to LLN´s packet drops and/or round-trip delay variance.

6LoWPAN header ….ctd

2. Fragmentation The fragment header utilized by 6LoWPAN is composed of three primary fields: Datagram Size, Datagram Tag, and Datagram Offset.

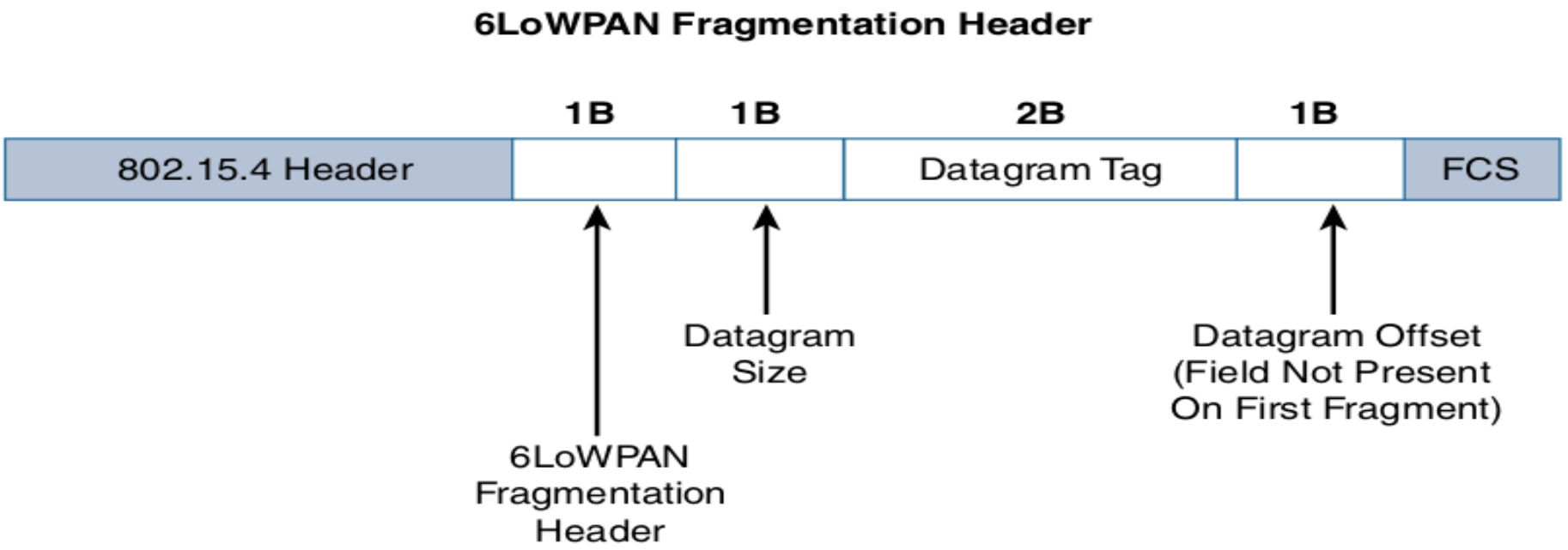


Figure 5-5 *6LoWPAN Fragmentation Header*

6LoWPAN header ….ctd

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.

6LoWPAN header ….ctd

3. Mess Addressing Header; Three fields are defined for this header:

Hop Limit, Source Address, and Destination Address

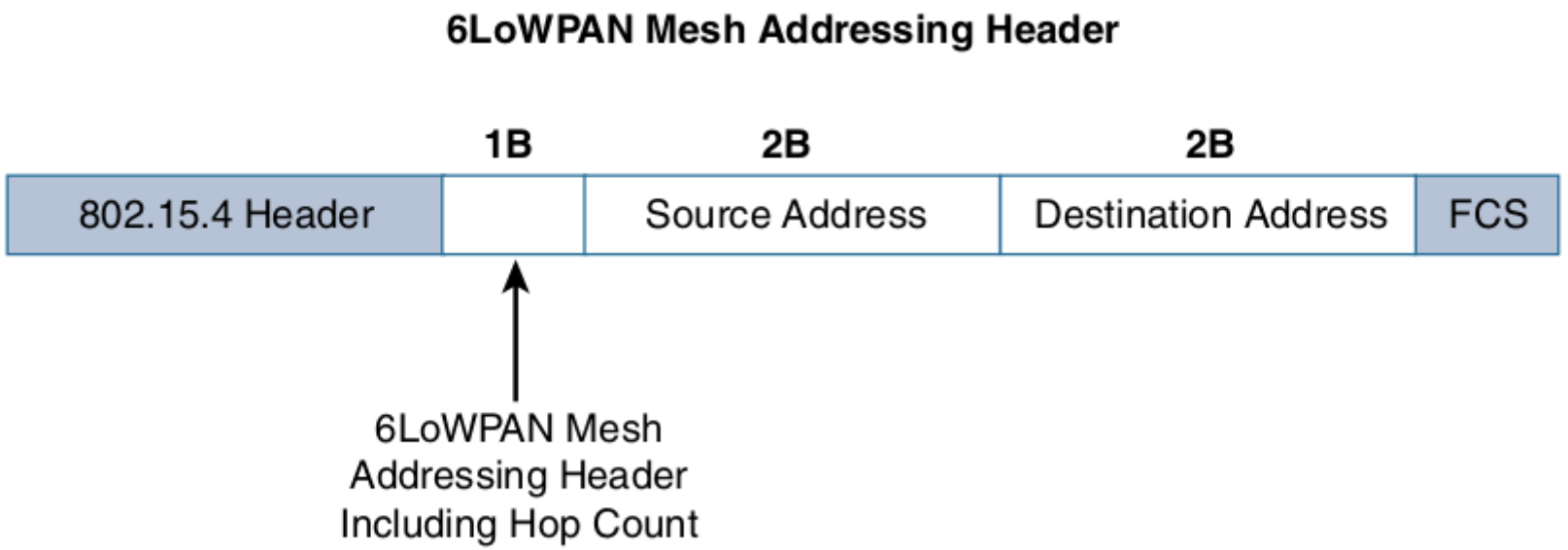


Figure 5-6 *6LoWPAN Mesh Addressing Header*

6LoWPAN header ….ctd

The hop limit for mesh addressing 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.

Mesh-Under Versus Mesh-Over Routing

Mesh-Under Routing

In this routing multiple link layer hops can be used to complete a single IP hop. The routing of packets is handled at the 6LoWPAN adaptation layer.

Mesh-over or Route-over

This routing is utilized for computing reachability and then getting packets forwarded to their destination, either inside or outside the mesh domain. The specialized routing protocol that handles this is called IPv6 Routing Protocol for Low Power and Lossy Networks -RPL

6Lo Working Group

The 6Lo working group seeks to expand on this completed work with a focus on IPv6 connectivity over constrained-node networks.

6lo facilitates the IPv6 connectivity over constrained-node networks.

In particular, this working group is focused on the following

- IPv6-over-foo adaptation layer specifications using 6LoWPAN technologies

(RFC4944, RFC6282, RFC6775) for link layer technologies

- Information and data models such as MIB modules

- Optimizations that are applicable to more than one adaptation layer specification:

- Informational and maintenance publications needed for the IETF specifications in this area

6TiSCH

This refers To standardizing of IPv6 over the Time Slotted Channel Hopping.

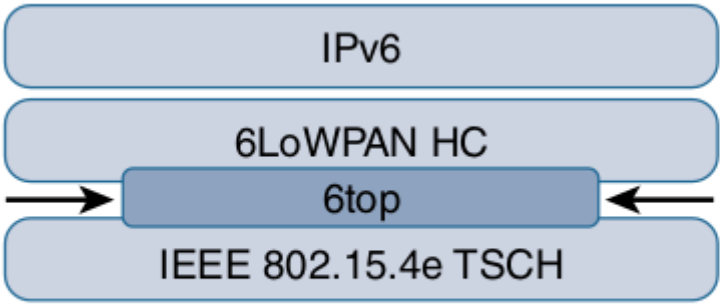


Figure 5-7 *Location of 6TiSCH's 6top Sublayer*

Schedule Management mechanisms for 6TiSCH

- **Static scheduling:**Static scheduling is a simple scheduling mechanism that can be used upon initial implementation or as a fallback in the case of network malfunction.

- **Neighbor-to-neighbor scheduling:**The schedule is established that correlates with the observed number of transmissions between nodes.

- **Remote monitoring and scheduling management:**Time slots and other resource allocation are handled by a management entity that can be multiple hops away

- **Hop-by-hop scheduling**: A node reserves a path to a destination node multiple hops away by requesting the allocation of cells in a schedule at each intermediate node

hop in the path.

Forwarding models for 6TiSCH architecture

Forwarding is the operation performed on each packet by a node that allows it to be delivered to a next hop or an upper-layer protocol.

The three 6TiSCH forwarding models:

Track Forwarding (TF): A track in this model is a unidirectional path between a source and a destination

Fragment forwarding (FF): It is defined where the first fragment is routed based on the IPv6 header present.

IPv6 Forwarding (6F): This model forwards traffic based on its IPv6 routing table.

RPL

Routing Protocol for Low-Power and Lossy Networks (RPL) is an IPv6 routing protocol that is standardized for the Internet of Things (IoT) by Internet-Engineering Task Force (IETF).

Each node examines every received IPv6 packet and determines the next-hop destination based on the information contained in the IPv6 header.

Modes to cope with constrained nodes;

Storing mode: Every node knows how to directly reach every other node.

Non-storing mode: In this mode a node always forwards its packets to the border router, which knows how to ultimately reach the final destination.

RPL ..... continued

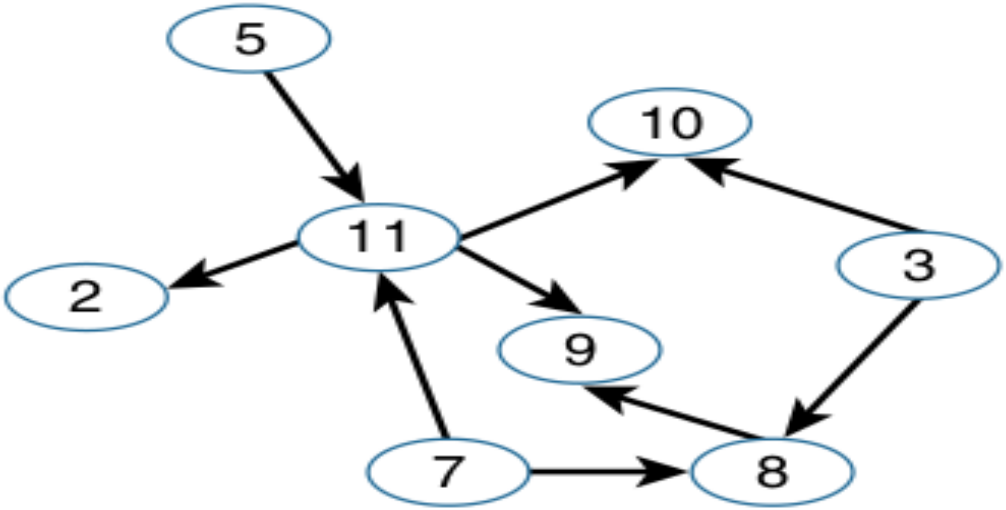
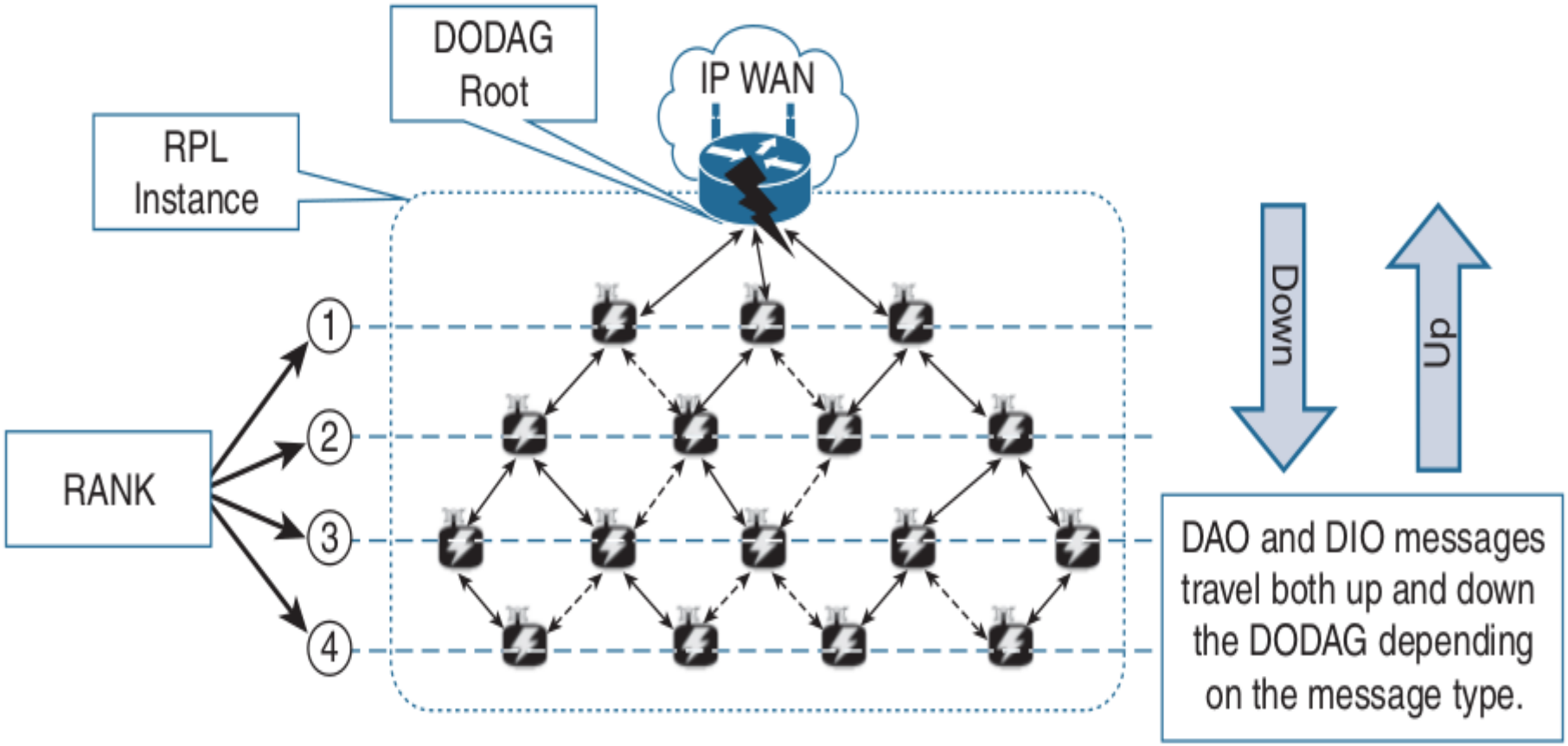


Figure 5-8 *Example of a Directed Acyclic Graph (DAG)*

In RPL, any vertex or point in the graph, you cannot follow an edge or a line back to this same point. All of the edges are arranged in paths oriented toward and terminating at one or more root nodes.

Overview of RPL



RPL Overview ...ctd

Objective Function (OF)

OF defines how metrics are used to select routes and establish a node´s rank.

Rank

The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagram.

The RPL option is carried in the IPv6 Hop-by-Hop header.

Metrics

Developed to support powered and battery-powered nodes, RPL offers a far more

complete set than any other routing protocol.

RPL routing metrics and constraints defined in RFC 6551

- Expected Transmission Count (ETX)
- Hop Coun
- Latency
- Link Quality Level
- Link Color
- Node State and Attribute
- Node Energy
- Throughput

RPL is a new routing protocol that enables an IPv6 standards-based solution to be deployed on a large scale while being operated in a similar way to today´s IP infrastructures. RPL was designed to meet the requirements of constrained nodes and networks, and this has led to it becoming one of the main network layer IPv6-based routing protocols in IoT sensor networks.

Authentication and Encryption on Constrained Nodes

IETF working groups suggest focus on security of Constrained nodes with emphasis on ACE and DICE

ACE

The Authentication and Authorization for Constrained Environments (ACE) working group is tasked with evaluating the applicability of existing authentication and authorization protocols and documenting their suitability for certain constrained-environment use cases.

DICE

The DTLS in Constrained Environments (DICE) working group focuses on implementing the DTLS transport layer security protocol in these environments.

Profiles and Compliances

This includes profile definitions, certifications, and promotion by alliances can help implementers develop solutions that guarantee interoperability and/or interchangeability of devices.

Internet Protocol for Smart Objects (IPSO) Alliance: It is more focused on how to use IP, with the IPSO Alliance organizing interoperability tests between alliance members to validate that IP for smart objects can work together and properly implement industry

Standards.

Wi-SUN Alliance: Wi-SUN's main focus is on the IEEE 802.15.4g protocol and its support for multiservice

and secure IPv6 communications with applications running over the UDP transport layer.

Profiles and Compliances … ctd

Thread: Companies formed thread groups that defined an IPv6-based wireless profile that provides the best way to connect more than 250 devices into a low-power, wireless mesh network.

IPv6 Ready Logo: It was created due to interoperability and certification issues. The IPv6 Ready Logo program has established conformance and interoperability testing

programs with the intent of increasing user confidence when implementing IPv6.