6LoWPAN demystified

Jonas Olsson
System Applications Engineer
Texas Instruments

Introduction

6LoWPAN is connecting more things to the cloud. Low-power, IP-driven nodes and large mesh network support make this technology a great option for Internet of Things (IoT) applications. As the full name implies – "IPv6 over Low-Power Wireless Personal Area Networks" – 6LoWPAN is a networking technology or adaptation layer that allows IPv6 packets to be carried efficiently within small link layer frames, such as those defined by IEEE 802.15.4. The use of an end-to-end, IP-based infrastructure takes full advantage of 30+ years of IP technology development, facilitating open standards and interoperability as largely demonstrated through the daily use of the Internet and its almost 3 billion users.

6LoWPAN is an open standard defined in RFC 6282 by the Internet Engineering Task Force (IETF), the standards body that defines many of the open standards used on the Internet such as UDP, TCP and HTTP to name a few. A powerful feature of 6LoWPAN is that while originally conceived to support IEEE 802.15.4 low-power wireless networks in the 2.4-GHz band, it is now being adapted and used over a variety of other networking media including Sub-1 GHz low-power RF, *Bluetooth*® Smart, power line control (PLC) and low-power Wi-Fi®.

This white paper discusses key 6LoWPAN concepts to demonstrate how it enables the use of IPv6 over IEEE 802.15.4 radio links.

6LoWPAN network architecture

Figure 1 on the following page shows an example of an IPv6 network, including a 6LoWPAN mesh network. The uplink to the Internet is handled by the Access Point (AP) acting as an IPv6 router. Several different devices are connected to the AP in a typical setup, such as PCs, servers, etc. The 6LoWPAN network is connected to the IPv6 network using an edge router. The edge router handles three actions: 1) the data exchange between 6LoWPAN devices and the Internet (or other IPv6 network); 2) local data exchange between devices inside the 6LoWPAN; and 3) the generation and maintenance of the radio subnet (the 6LoWPAN network).

By communicating natively with IP, 6LoWPAN networks are connected to other networks simply using IP routers. As shown in Figure 1, 6LoWPAN networks will typically operate on the edge, acting as stub networks. This means data going into the network is destined for one of the devices inside the 6LoWPAN. One 6LoWPAN network may be connected to other IP networks through one or more edge routers that forward IP datagrams between different media. Connectivity to other IP networks may be provided through any arbitrary link, such as Ethernet, Wi-Fi or 3G/4G. Because 6LoWPAN only specifies operation of IPv6 over the IEEE 802.15.4 standard, edge routers may also support IPv6 transition mechanisms to connect 6LoWPAN networks to IPv4 networks, such as NAT64 defined in RFC 6146. These IPv6 transition mechanisms do not require the 6LoWPAN nodes to implement IPv4 in whole or in part.

By communicating natively with IP, 6LoWPAN networks are connected to other networks simply using IP routers

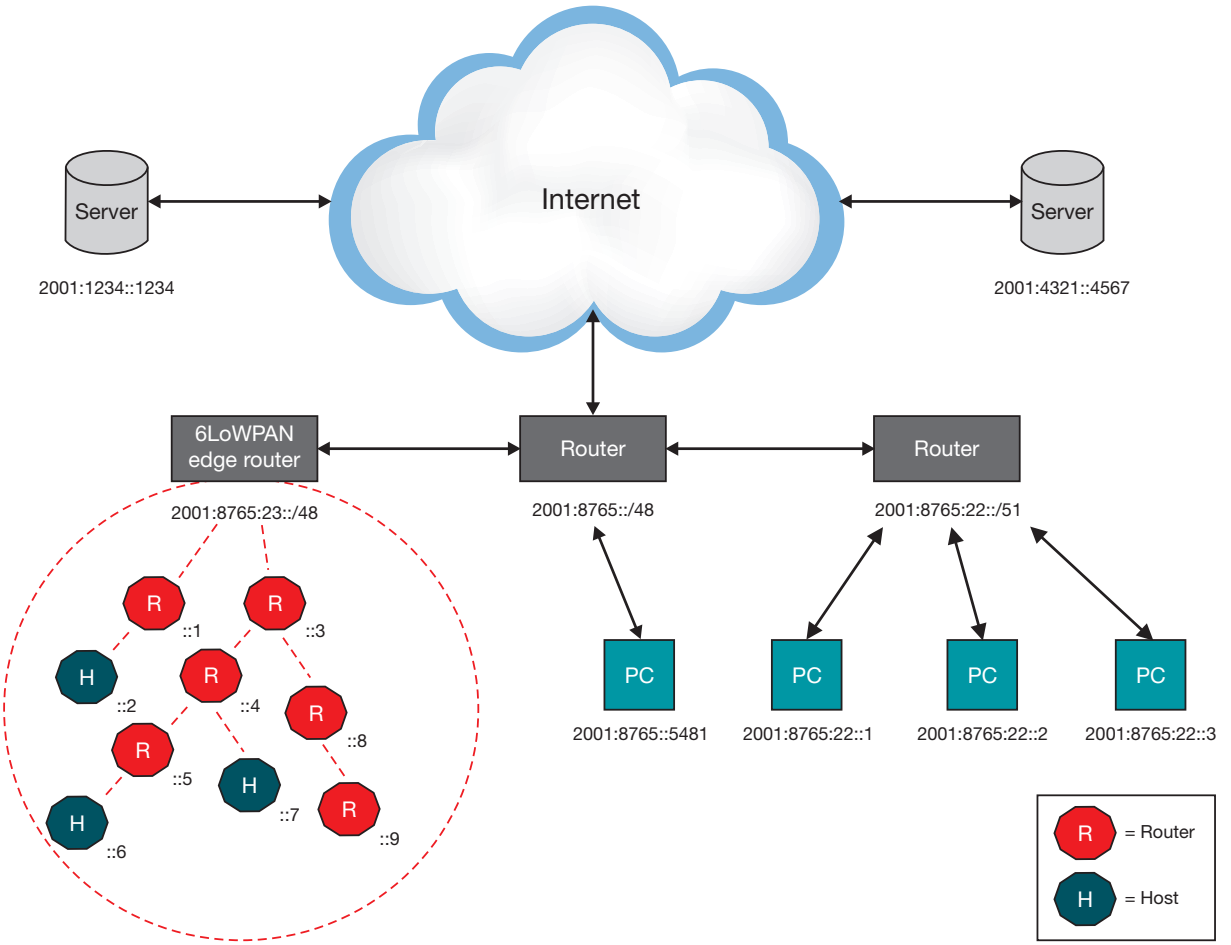

Figure 1. An example of an IPv6 network with a 6LoWPAN mesh network

Because edge routers forward datagrams at the network layer (see the next section about communications layers), they do not maintain any application-layer state. Other network architectures such as ZigBee®, Z-wave, *Bluetooth*® or proprietary networks require stateful and sometimes complex application gateways to connect to IP-based networks, such as the Internet. These application gateways must understand any application profiles that may be used in the network, and any changes to application protocols on the wireless nodes must also be accompanied by changes on the gateway. In contrast, IP-based border routers, like the edge router, remain agnostic to application protocols used in the 6LoWPAN. This lowers the burden put on the edge router in terms of processing power, thus making it possible to use embedded devices that are lower cost, runs simpler software and has less complex hardware. However, the IP architecture does not preclude the use of proxies and caches to optimize network performance, both of which are widely used in the Internet today.

Two other device types are included inside a typical 6LoWPAN network: routers and hosts. Routers can, as the name implies, route data destined to another node in the 6LoWPAN network. Hosts are also known as end devices and are not able to route data to other devices in the network. Host can also be a sleepy device, waking up periodically to check its parent (a router) for data, enabling very low power consumption.

System stack overview

6LoWPAN radically changes the IoT landscape. As discussed, up until now a complex application-layer gateway was needed to make devices such as ZigBee, *Bluetooth* and proprietary systems connect to the Internet. 6LoWPAN solves this dilemma by introducing an adaptation layer between the IP stack's link and network layers to enable transmission of IPv6 datagrams over IEEE 802.15.4 radio links.

All communications systems use a set of rules or standards to format data and control the exchange. The most common model in data communication systems is the Open Systems Interconnect (OSI) model, which in a simplified model, breaks the communication into five fundamental layers. Figure 2 shows this simplified OSI model alongside two typical examples of stacks used in IoT devices. One is a device running the Wi-Fi stack, the other device is an IoT-connected device based on 6LoWPAN.

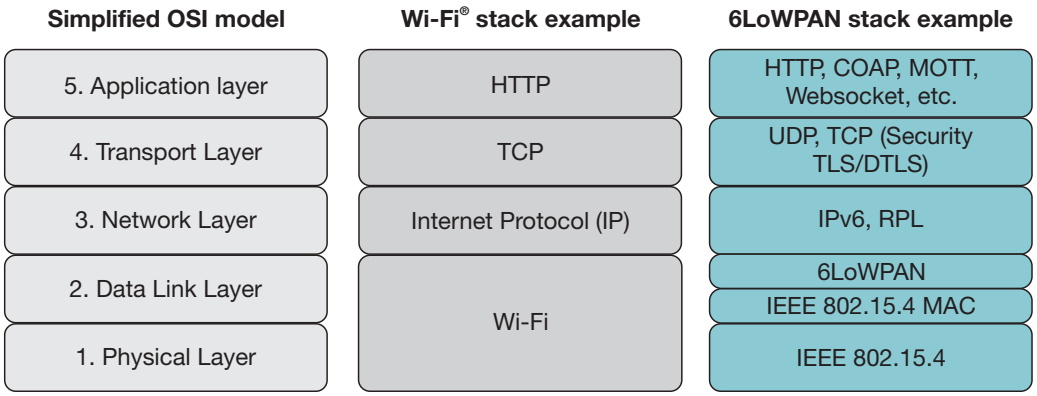

Figure 2. The OSI model, a Wi-Fi® stack example and the 6LoWPAN stack

The physical layer converts data bits into signals that are transmitted and received over the air. In the 6LoWPAN example, IEEE 802.15.4 is used. In addition to the well-rounded 2006 version of the standard, two important amendments exist: e and g. IEEE 802.15.4e is a MAC amendment and provides enhancements such as time slotted channel hopping (TSCH) and coordinated sampled listening (CSL). Both enhancements aim to further lower the power consumption and make the interface more robust. The IEEE 802.15.4g is a PHY (or physical layer) amendment and aims to provide an additional range of radio frequency bands to enable worldwide use even in the Sub-1 GHz frequency bands.

The data link layer provides a reliable link between two directly connected nodes by detecting and correcting errors that may occur in the physical layer during transmission and receiving. The data link layer includes the media access layer (MAC) which provides access to the media, using features like carrier sense multiple access – collision avoidance (CSMA-CA) where the radio listens that no one else is transmitting before actually sending data over the air. This layer also handles data framing. In the 6LoWPAN example, the MAC layer is IEEE 802.15.4. The 6LoWPAN adaptation layer, providing adaptation from IPv6 to IEEE 802.15.4, also resides in the link layer.

The network layer addresses and routes data through the network, if needed over several hops. IP (or Internet Protocol) is the networking protocol used to provide all devices with an IP address to transport packets from one device to another.

The transport layer generates communication sessions between applications running on end devices. The transport layer allows multiple applications on each device to have their own communications channel. TCP is the dominant transport protocol on the Internet. However, TCP is a connection-based protocol (including packet ordering) with large overhead and therefore not always suitable for devices demanding ultra-low power consumption. For those types of systems, UDP, a lower overhead, connectionless protocol, can be a better option. Secure transport layers examples include TLS (transport layer security) running atop TCP and DTLS, which is based on UDP.

Finally, the application layer is responsible for data formatting. It also makes sure that data is transported in application-optimal schemes. A broadly used application layer on the Internet is HTTP running over TCP. HTTP uses XML, which is a text-based language with a large overhead. Therefore, it is not optimal to use HTTP in many 6LoWPAN systems. However, HTTP can still be very useful for communications between 6LoWPAN and the Internet. For this reason, the industry and community have developed alternative application layer protocols, such as the constrained application protocol (COAP), a message protocol running over UDP with a bit-optimized REST mechanism very similar to HTTP. COAP is defined by IETF in RFC 7252 and defines retransmissions, confirmable and non-confirmable messages, support for sleepy devices, block transfers, subscription support and resource discovery. COAP is also easy to map to HTTP via proxies.

Another application layer protocol that should be mentioned is message queue telemetry transport (MQTT), an open-source protocol that was invented by IBM. MQTT is a publish/subscribe type of protocol running over TCP. Data is not transported directly between end points. Instead a broker (i.e., server) is used to relay messages. MQTT introduces the "topic" entity; devices can publish and subscribe to different topics. Once a topic is updated that a specific device has subscribed to, the device will get notified and receive the data via the broker. Devices can use wildcards like # and * to subscribe to a hierarchy of topics. MQTT supports several layers of quality of service (QoS) making sure that messages are delivered. The broker can run both locally in an IP intranet and on the Internet and multiple brokers are supported interacting in the same system. Several public brokers are available and many of the cloud service providers provide MQTT access. There are many more application layer protocols available that can run over the TCP/UDP. Those listed here specifically target low-power IoT applications.

Internet Protocol version 6 (IPv6) over IEEE 802.15.4

Today's Internet (and many standalone IP networks) is mainly based on IPv4 and uses 32-bit addresses, which limits the address space to 4,294,967,296 unique addresses. As addresses were assigned to users (and devices), the number of unassigned addresses naturally decreased. IPv4 address exhaustion occurred on Feb. 3, 2011, although it had been significantly delayed by address changes such as network address translation (NAT).

This limitation of IPv4 stimulated the development of IPv6 in the 1990s, which has been in commercial deployment since 2006. IPv6 covers an address space of 2^{128} and $3.4*10^{38}$ unique addresses. This should be enough for Internet to scale for decades to come – even with the promise of the Internet of Things, which according to estimates might include 50 billion connected devices by the year 2020.

To recognize the increase in bandwidth, IPv6 increases the minimum maximum transmission unit (MTU) from 576 to 1280 bytes. IPv6 also reflects changes and advances in link layer technologies the Internet uses. Ethernet is the dominant link technology and its throughput has increased over the years. Wi-Fi mirrors Ethernet capabilities supporting similar-sized MTU and very high link rates. Both Ethernet and Wi-Fi operate in the context of ample power and highly capable devices. On the other hand, IEEE 802.15.4 was designed to serve a different market; long-lived applications that require large numbers of low-cost, ultra-low-power devices. The throughput under this standard is limited to 250 kbps, and the frame length is limited to 127 bytes to ensure low packet and bit error rates in a lossy RF environment. Additionally, IEEE 802.15.4 uses two addresses: a 16-bit short address and an EUI-64 extended address. These addresses reduce header overhead and minimize memory requirements. In addition, 6LoWPAN operates most commonly over multiple hops forming a low-power mesh network, a fundamental difference from Ethernet- or Wi-Fi-based networks. Finally, devices used to implement 6LoWPAN are typically constrained in terms of resources, having about 16 kB RAM and 128 kB ROM.

Due to the above resource constraints and 6LoWPAN multi-hop topology, supporting IPv6 over IEEE 802.15.4 networks present several challenges;

1. IPv6 datagrams are not a natural fit for IEEE 802.15.4 networks. Low throughput, limited buffering and datagrams that are one-tenth of IPv6 minimum MTU make header compression and data fragmentation a necessity. For example IEEE 802.15.4 link headers can limit the effective possible payload to 81 bytes. This makes IPv6 (40 bytes), TCP (20 bytes) and UDP (8 bytes) headers seem way too large.
2. Since IEEE 802.15.4 is both low power and low throughput, in addition to the use of RF as media, it is more prone to spurious interference, link failures and asymmetric links (A can hear B, but B cannot hear A). Those characteristics require the network layer to be adaptive and responsive at the same time as low power and efficient.
3. The most common network topology for 6LoWPAN is a low-power mesh network. This negates the assumption that a link is a single broadcast domain, something that is very important since the very foundation of IPv6 such as neighbor discovery relies on it.

The above issues are all addressed in the 6LoWPAN standard.

The 6LoWPAN adaptation layer

When sending data over MAC and PHY layers, an adaptation layer is always used. For example, RFC 2464 defines how an IPv6 packet is encapsulated in an Ethernet frame. The same is also used for IEEE 802.11 Wi-Fi. For 6LoWPAN, RFC 6282 defines how an IPv6 data frame is encapsulated over an IEEE 802.15.4 radio link.

The main focus of the IETF working group, 6LoWPAN WG, was to optimize the transmission of IPv6 packets over low-power and lossy networks (LLNs) such as IEEE 802.15.4 and led to the publication of RFC 6282 specifying;

- **Header compression**, which compresses the 40-byte IPv6 and 8-byte UDP headers by assuming the usage of common fields. Header fields are elided when they can be derived from the link layer. The way the headers can be compressed is one of the factors that led to the standard only supporting IPv6 and not IPv4. Note that there is nothing stopping one from running TCP in a 6LoWPAN system, but TCP header compression is not part of RFC 6282.

- **Fragmentation and reassembly.** The data link of IEEE 802.15.4 with a frame length of maximum 127 bytes does not match the MTU of IPv6, which is 1280 bytes. It should be noted that the frame format of IEEE 802.15.4g does not have the same limitation.
- **Stateless auto configuration.** Stateless auto configuration is the process where devices inside the 6LoWPAN network automatically generate their own IPv6 address. There are methods to avoid the case where two devices get the same address; this is called duplicate address detection (DAD).

Throughout the 6LoWPAN adaptation layer, the key concept is to use stateless or shared-context compression to elide header fields. This can compress all headers (adaptation, network and transport layers) down to a few bytes. It is possible to compress header fields since they often carry common values. Common values occur due to frequent use of a subset of IPv6 functionality, namely UDP, TCP and ICMP. Assumptions regarding shared context can also be made, such as a common network prefix for the whole 6LoWPAN system. The 6LoWPAN adaptation layer also removes duplicated information that can be derived from other layers, such as the IPv6 addresses and UDP/IPv6 length fields.

Header compression

The traditional way of performing IP header compression is status based, which is used at point-to-point connections where a flow between two end points is stable. This implementation is very effective in static networks with stable links. Communication over multiple hops requires hop-by-hop compression/decompression. The routing protocols (e.g., RPL) normally running in 6LoWPAN systems obtain receiver diversity by rerouting, which would require state migration and hence severely reduce the compression efficiency. For dynamically changing networks, with multiple hops and infrequent transmissions like a 6LoWPAN radio network, another method has to be applied. Instead in 6LoWPAN stateless and shared-context compression is used, which does not require any state and lets routing protocols dynamically choose routes without affecting compression ratio.

In the example in Figure 3, three communication scenarios are displayed:

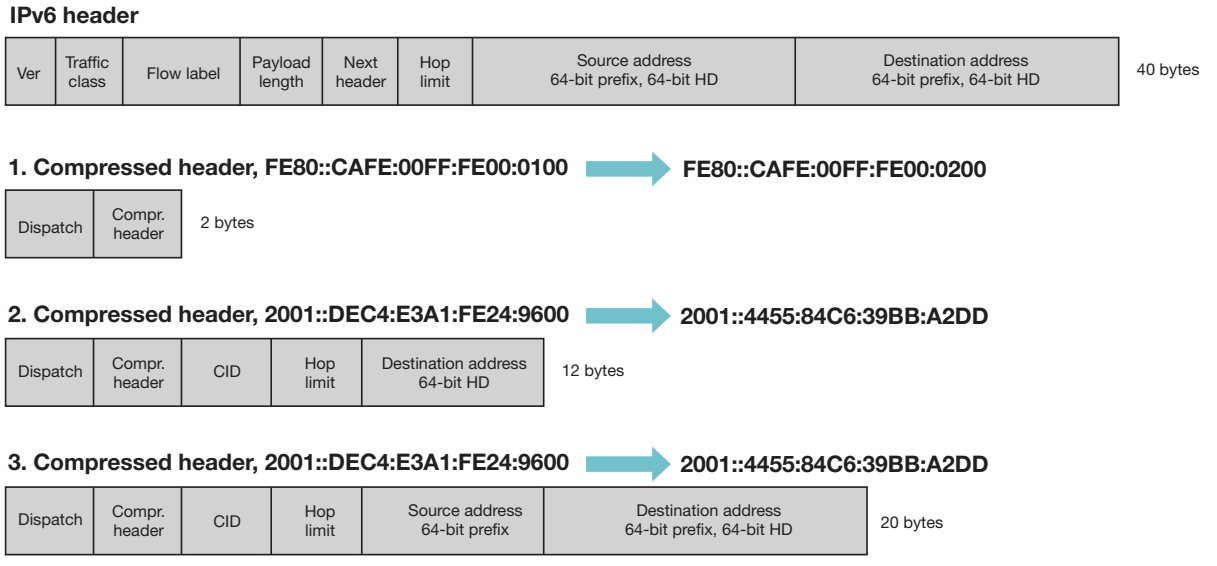

Figure 3. 6LoWPAN IPv6 header compression examples

1. Communication between two devices inside the same 6LoWPAN network, using link-local addresses, the IPv6 header can be compressed to only 2 bytes.
2. Communication destined to a device outside of the 6LoWPAN network and the prefix for the external network is known, where the IPv6 header can be compressed to 12 bytes.
3. Similar to 2, but without knowing the prefix of the external device, that gives an IPv6 header of 20 bytes.

The best case (1) in this example is not useful for sending application data (as it can only be used to send data to direct neighbors), however being able to compress headers on data interchanged between two near-by devices is important especially for the routing protocol. The worst case (3) still gives a 50 percent compression ratio. In the example, it is assumed that the interface ID (IID) is derived from the MAC address of the device. It shall also be noted that UDP header compression is part of the 6LoWPAN standard as stated earlier in this document, but not displayed in this example.

Fragmentation and reassembly

In order to enable the transmission of IPv6 frames over IEEE 802.15.4 radio links, the IPv6 frames need to be divided into several smaller segments. For this purpose, additional data in the headers are generated to reassemble the packets in the correct sequence at the end. When data packets are re-assembled, the additional information added is removed and the packets are restored to their initial IPv6 format. The fragmentation sequence is different based on what type of routing is used (different routing techniques are discussed later). In the case of mesh-under routing, fragments are reassembled at their final destination only, while in the case of route-over networks data packets are reassembled at every hop. Thus in a router-over network each hop has to have enough resources to store all fragments. Whereas in a mesh-under system, a lot of network traffic is generated quickly since all fragments are passed immediately. If any fragments are missing (in a mesh-under system) during the reassemble, the complete packet needs to be re-transmitted. If possible, fragmentation should be avoided as long as possible since it negatively impacts the battery life of a device. Therefore, keeping the payload low (includes selecting the appropriate application level protocols) and using header compression are of the utmost importance.

Header formats

6LoWPAN uses stacked headers and, analogous to IPv6, extension headers. 6LoWPAN headers define the capability of each sub-header. Three sub-headers are defined: *mesh addressing*, *fragmentation* and *header compression*. Mesh addressing supports layer-two (data link) forwarding and fragmentation supports the transmission of

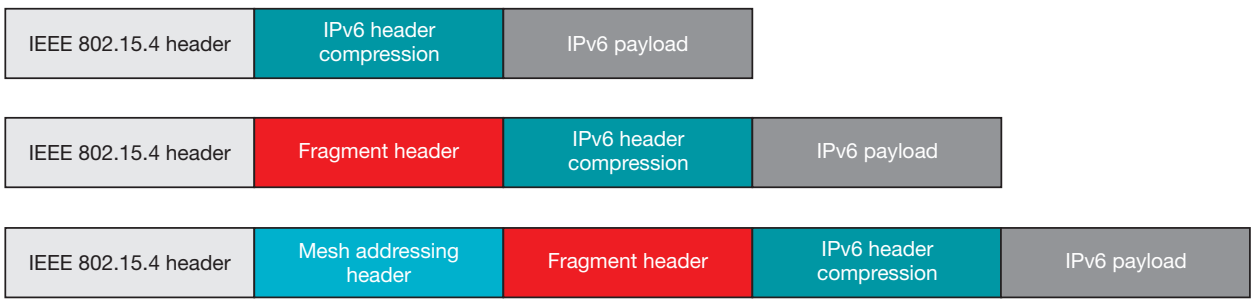

Figure 4. 6LoWPAN stacked headers

IPv6 MTU. The header format is defined by using the header type field placed at the beginning of each header. The header stack is easy to parse and allows for sub-headers to be removed if not needed. The fragmentation header is elided for packets that fit into one single IEEE 802.15.4 frame. The mesh header is not used when sending data over one hop only.

The fragment header is used when the payload is too large to fit in a single IEEE 802.15.4 frame. The fragment header contains three fields; datagram size, datagram tag and datagram offset. Datagram size describes the total (un-fragmented) payload. Datagram tag identifies the set of fragments and is used to match fragments of the same payload. Datagram offset identifies the fragment's offset within the un-fragmented payload. The fragment header length is 4 bytes for the first header and 5 bytes for all subsequent headers.

The mesh address header is used to forward packets of multiple hops inside a 6LoWPAN network. The mesh address header includes three fields: hop limit, source address and destination address. The hop limit field is used to limit the number of hops for forwarding. The field is decremented at each hop. Once the count reaches zero the packet is dropped. The source and destination address fields indicate the IP end points. Both are IEEE 802.15.4 addresses and may be short or extended as defined in the IEEE 802.15.4 standard. The mesh address header's length is between 5 and 17 bytes, depending on the addressing mode in use.

Routing

Routing is the ability to send a data packet from one device to another device, sometimes over multiple hops. Depending on what layer the routing mechanism is located, two categories of routing are defined: mesh-under or route-over. Mesh-under uses the layer-two (link layer) addresses (IEEE 802.15.4 MAC or short address) to forward data

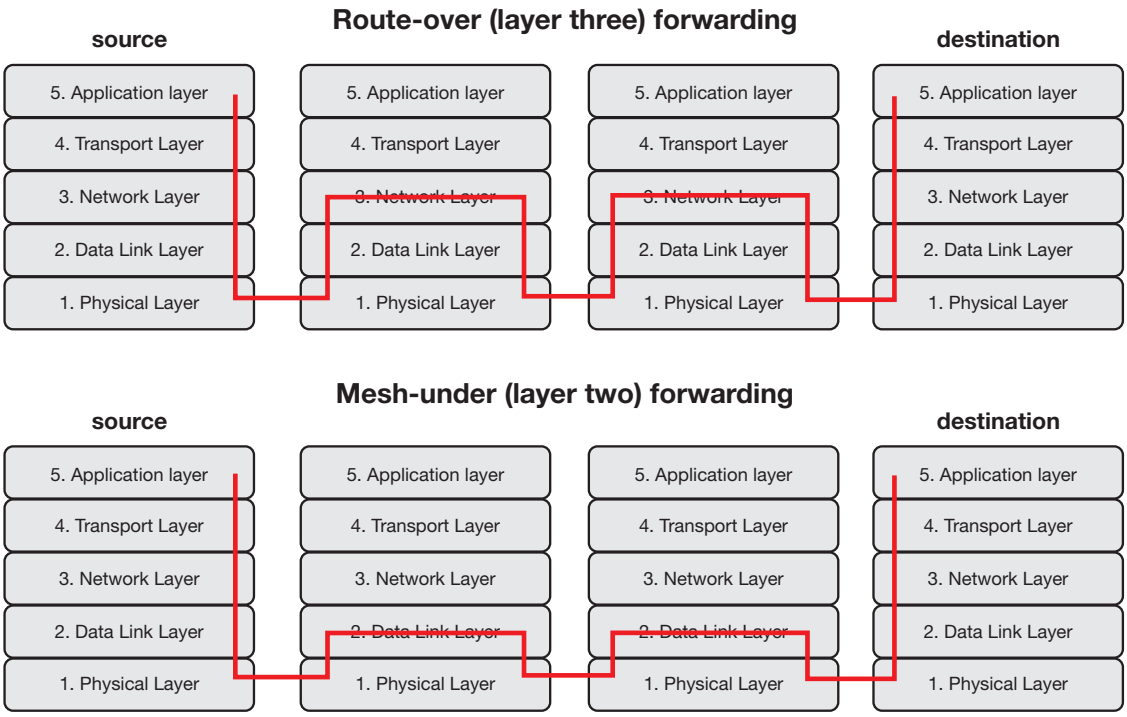

Figure 5. Mesh-under and route-over packet forwarding

packets; while route-over uses layer three (network layer) addresses (IP addresses).

In a mesh-under system, routing of data happens transparently, hence mesh-under networks are considered to be one IP subnet. The only IP router in such a system is the edge router. One broadcast domain is established to ensure compatibility with higher layer IPv6 protocols such as duplicate address detection. These messages have to be sent to all devices in the network, resulting in high network load. Mesh-under networks are best suited for smaller and local networks.

In route-over networks the routing takes place at the IP level as described above, thus each hop in such networks represents one IP router. The usage of IP routing provides the foundation to larger and more powerful and scalable networks, since every router must implement all features supported by a normal IP router such as DAD, etc. The most widely used routing protocol for route-over 6LoWPAN networks today is RPL (pronounced “ripple”) as defined by IETF in RFC 6550. Compared to mesh-under, route-over features the advantage that most of the protocols used on a standard TCP/IP stack today can be implemented and used as is. RFC 6550 specifies the IPv6 routing protocol for low-power and lossy networks (RPL), which provides a mechanism whereby multipoint-to-point traffic from devices inside the 6LoWPAN network towards a central control point (e.g., a server on the Internet) as well as point-to-multipoint traffic from the central control point to the devices inside the 6LoPWAN are supported.

Support for point-to-point traffic is also available. However, RPL is not the optimum choice for such traffic, since the data in many cases needs to be transported via the edge router. RPL supports two different routing modes; storing mode and non-storing mode. In storing mode, all devices in the 6LoWPAN network configured as routers maintain a routing table and a neighbor table. The routing table is used to look up routes to devices, and the neighbor table is used to keep track of a node’s direct neighbors. In non-storing mode the only device with a routing table is the edge router, hence source routing is used. Source routing means that the packet includes the complete route (or hops) it needs to take to reach the destination. For example, when sending data from one device to another device inside the same 6LoWPAN network, data is first sent from the source device to the edge router, the edge router in turn makes a lookup in its routing table and adds the complete route to the destination in the packet. Storing mode imposes higher requirements on the devices acting as routers (i.e., they need to have resources enough to store the routing and neighbor tables), while using non-storing mode the overhead increases with the number of hops a packet needs to traverse to reach the destination.

Auto configuration and neighbor discovery

Auto configuration is the autonomous generation of a device’s IPv6 address. The process is essentially different between IPv4 and IPv6. In IPv6 it allows a device to automatically generate its IPv6 address without any outside interaction with a DHCP server or such. To get an address, a host can communicate via neighbor discovery protocol (NDP), however many of the NDP features are also included in RPL. The procedure described here is valid for RPL also, and involves four message types:

- Router solicitation (RS)
- Router advertisement (RA)
- Neighbor solicitation (NS)
- Neighbor advertisement (NA)

IPv6 neighbor discovery (ND) lets a device discover neighbors, maintain reachability information, configure default routes, and propagate configuration

parameters. The RS message includes, among other things, the IPv6 prefix of the network. All routers in the network periodically send out these messages. If a host wants to participate in a 6LoWPAN network, it assigns itself a link-local unicast address (FE80::IID), then sends this address in an NS message to all other participants in the subnet to check if the address is being used by someone else. If it does not hear an NA message within a defined timeframe, it assumes that the address is unique. This procedure is called duplicate address detection, DAD. Now, to get the network prefix, the host sends out an RS message to the router to get the correct prefix. Using these four messages, a host is able to assign itself a worldwide unique IPv6 address.

Using source address auto configuration, each host generates a link-local IPv6 address using its IEEE 802.15.4 EUI-64 address, 16-bit short address or both. In a mesh-under configuration, the link-local scope covers the entire 6LoWPAN network, even over multiple hops, and a link-local address is sufficient for communication happening in the 6LoWPAN. The only time a routable IPv6 address is needed is when communicating outside of the 6LoWPAN network. In a route-over configuration, a link-local address is sufficient to communicate with nodes that are within radio coverage, but a routable address is required to communicate with devices several hops away.

For all unicast addresses, it is most efficient to derive them from the local IEEE EUI-64 address. 6LoWPAN's binding between link, adaptation and IP headers allows them to be elided and removes the need for address resolution, thus resulting in smaller headers. Similarly, auto configuration should configure interface addressing to use a common prefix, so that 6LoWPAN can elide the prefix. 6LoWPAN can use a short link address to derive the IPv6 address, resulting in shorter headers.

Security

Security is a must for IoT systems and always presents a challenge. Due to the nature of IoT with many nodes that in many cases have very constrained performance, there are also more entry points for an outside attacker. Another critical aspect is that data flowing in a typical IoT system is not just "data," the damage potential is much higher since the data flowing in the system can be used to open the door to you house or turn on/off alarms remotely, for example.

State-of-the-art security schemes are necessary to be ahead of the pack. 6LoWPAN takes advantage of the strong AES-128 link layer security defined in IEEE 802.15.4. The link layer security provides link authentication and encryption. In addition to link layer security, transport layer security (TLS) mechanisms have been shown to work great in 6LoWPAN systems. TLS, as defined in RFC 5246, runs over TCP. For constrained environments and systems where UDP is chosen as the transport layer protocol, the RFC 6347 (datagram transport layer security) can be used to provide security at the transport layer. However, it should be noted that implementing TLS/DTLS requires the device to have necessary resources, such as a hardware encryption engine to enable the use of advanced cipher suites, etc. A device especially developed for this purpose is TI's **CC2538** wireless MCU, which integrates a powerful ARM® Cortex®-M3 CPU and an IEEE 802.15.4 radio. The device has up to 512kB Flash and 32kB RAM, and also features a hardware encryption engine capable of supporting TLS/DTLS.

Interoperability

Interoperability is the ability for devices from different manufacturers to exchange data. There are many alliances and organizations that

define specifications, testing procedures and interoperability tests to assure interoperability on different layers in the communication stack. Some standards define interoperability on one or two layers in the OSI model, while others define the entire end-to-end system.

The Institute of Electrical and Electronics Engineers (IEEE) focuses on communications and radio engineering by releasing standard specifications. IEEE does not provide interoperability testing or certification programs. To name a few standards coming from the IEEE, 802.3 is used by the Ethernet specification, used by most computers today. 802.11 provides foundation for the Wi-Fi specification, which is also widespread. 802.15.4 defines the wireless personal area networks (PAN) used by ZigBee and 6LoWPAN amongst others. For 802.15.4 IEEE has defined the physical (PHY) and MAC layers.

The Internet Engineering Task Force (IETF) is an open standards organization responsible for many standards used on the Internet today, best known is the TCP/IP suite. IETF standards are, as described in this white paper, published using "Request For Comments" (RFC) documents freely available at **www.ietf.org**. A few examples of popular RFCs are RFC 2616, defining HTTP/1.1, and RFC 791 that defines IPv4. Just as with IEEE, the IETF does not provide certification programs so vendors cannot get recognition that their product complies to the standards.

However, there are several organizations and alliances that adopt standards from IEEE, IETF and others and use them to create a top-to-bottom certification programs to ensure full product interoperability. There are a few organizations working on 6LoWPAN interoperability, including the newly (July 2014) formed Thread Group, which focuses on defining the components up to and including the transport layer (in the OSI model) for a smart home system including a certification program. The Open Interconnect Consortium is seeking to define a common communication framework to wirelessly connect and intelligently manage the flow of information among devices. And there are many others; Wi-SUN, IPSO, ZigBee IP, etc. which all are using 6LoWPAN as part of their system.

Summary

6LoWPAN is fairly new to the market. Its characteristics make the technology ideal for markets such as home automation with sensors and actuators, street light monitoring and control, residential lighting, smart metering and generic IoT applications with Internet connected devices. Today's deployments use both 2.4 GHz and Sub-1 GHz, building on the IEEE 802.15.4 advantages including support for large mesh network topology, robust communication and very-low power consumption. Add to that the benefits of using IP communication with a plethora of applications developed over the last 30+ years, it is easy to understand why 6LoWPAN, with open standards, long lifetime, easy learning curve (since many developers already know IP) and transparent Internet integration, is well positioned to fuel the fast growing Internet of Things market.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265