Understanding the Zigbee stack

By Rogelio Reyna Garcia
Applications Engineer
Freescale Semiconductor Inc.
E-mail: rogelio.reyna
@freescale.com

The Zigbee specification is a standard that defines a stack protocol enabling the interoperability of wireless devices in a low-cost, low-power consumption and low-data-rate network. The Zigbee stack is founded over the IEEE 802.15.4 standard, which defines the multiply accumulate (MAC) and physical (PHY) layers of the protocol.

MAC and PHY layers define the RF and communications components of neighboring devices. Zigbee stack layers, on the other hand, include a network layer, an application layer and a security service provider (SSP). **Figure 1** outlines the Zigbee stack architecture.

Each Zigbee device should adhere to a specific profile that can be either public or private. Profiles define the environment of the application, the type of devices and the clusters used for them to communicate. Public profiles guarantee the interoperability of different vendors for the same application space.

Devices are defined by the profiles and are implemented as application objects. Each application object is connected to the rest of the Zigbee stack by an endpoint, which is an addressable component within a device.

Communication is made from endpoint to endpoint and through data structures called clusters. Clusters contain a set of attributes needed to share information between application objects. Clusters used in a specific application are defined within its profile. Each interface can receive or send data in the form of a cluster.

There are two special endpoints: 0 and 255. Endpoint 0 is used for the configuration and management of the entire Zigbee device. Through this endpoint, the application can communicate with other layers of the Zigbee stack to initialize and configure them. Attached to endpoint 0 is the Zigbee device object (ZDO). Endpoint 255, on the other hand, is used to broadcast to all endpoints, while endpoints 241-254 are reserved.

The application support sublayer connects the endpoints with the network layer and SSP. It also aids all the endpoints with data transmission, security and binding. Binding is the ability to match different but compatible devices together, such as a switch and lamp.

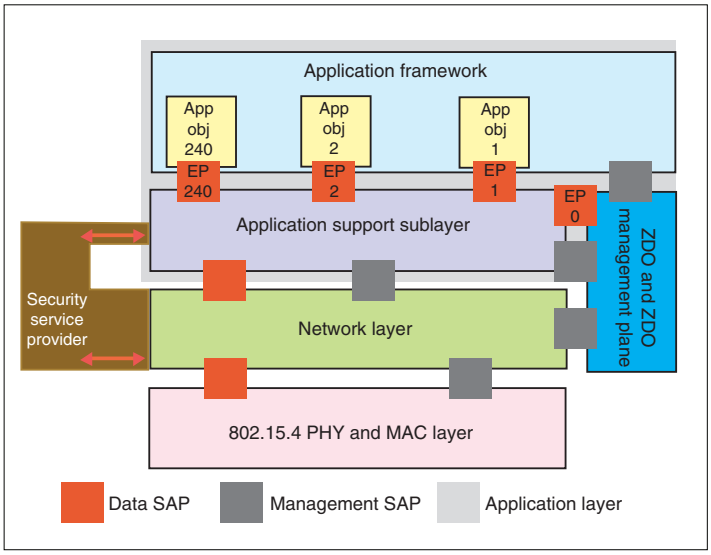

Figure 1: Final implementation of a Zigbee device should include the MAC and PHY layers of IEEE 802.15.4, as well as the Zigbee stack layers.

The network layer enables devices to communicate with one another. It is involved in the initialization of the device within a network, routing of messages and network discovery. The application support sublayer also provides these services. The application can configure and access the parameters of the network layer through the ZDO.

802.15.4 MAC layers

The IEEE 802.15.4 standard defines the first two layers of the Open Systems Interconnection (OSI) model for a low-rate wireless personal area network (LR-WPAN).

The PHY layer defines radio characteristics and supports the 2.45GHz and 868/915MHz radio bands. The 2.45GHz radio band has a data rate of 250Kbps and supports 16 different channels. Meanwhile, the 868/915MHz radio band supports one channel for 868MHz with a data rate of 20Kbps and 10 channels for 915MHz with a data rate of 40Kbps.

The MAC layer is responsible for single-hop data communication between neighboring devices. It synchronizes the network, supports association/disassociation and MAC-level security, and provides a reliable link between two devices.

The different layers of the Zigbee stack and the 802.15.4 MAC communicate with each other using SAPs, which are interfaces to the services provided by a specific layer to the upper layers. Most layers of the Zigbee stack define data- and management-entity interfaces.

The objective of the data-entity interface is to provide the upper layer with the required normal data services. On the other hand, the objective of the management-entity interface is to provide the upper layer with mechanisms for accessing internal layer parameters, configuration and management data.

Security

As the name implies, SSP offers security mechanisms. However, the overall security of the system is defined at the profile level, which defines the kind of security implemented within a specific network.

Each layer–MAC, network and application layers–can be secured and share security keys to reduce the required storage. The SSP is initialized and configured through the ZDO and requires the implementation of the Advanced Encryption Standard.

The Zigbee specification defines the use of a "trust center" as a device within the network that distributes the security keys.

Stack size, devices

The specification defines three types of devices–the coordinator, router and end device. The Zigbee coordinator is a device that starts and configures the network. It supports associations, holds the binding table for indirect addressing and designs the trust center. In every Zigbee network, there should only be one coordinator.

Meanwhile, the Zigbee router is a device that can support associations and forward messages to other devices. Unlike the coordinator, a Zigbee

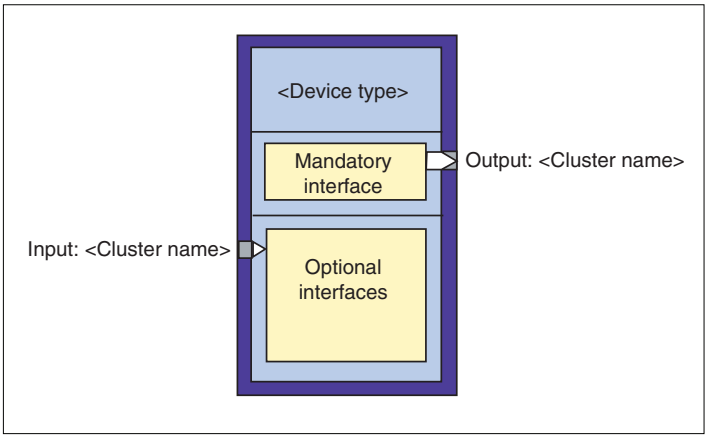

Figure 2: Each interface can receive or send data in the form of a cluster.

mesh or tree network can have multiple Zigbee routers. However, a Zigbee star network does not support Zigbee routers.

Lastly, the Zigbee end-device uses the Zigbee network to communicate with other devices. It also has the least memory size requirement.

The specific architecture of the network impacts the resources required by the devices. The network topologies supported by network layers are star, tree and mesh. Among these topologies, the star network is the least resource-demanding.

A Zigbee stack provides all the functionality required by the Zigbee specification so that manufacturers can focus on developing their product applications. If the manufacturer uses one of the public profiles, most of the configuration is already done. If none of the public profiles fits the manufacturer's needs, a new profile can be created, taking advantage of the job already done by other profiles. □