Q53 Theory of Operation

Introduction

ZigBee is a mesh networking protocol for control devices with IEEE 802.15.4 radios, such as switches, dimmers, volume controls, and sensor devices such as thermostats, humidistats and motion detectors. Devices in a mesh network directly communicate only with nearby neighbour devices at low RF power levels. To communicate with more distant devices, packets are hopped across the mesh from device to device using the most reliable route.

A general purpose computer with an 802.15.4 radio can join a mesh network directly, but it is often necessary to interact with mesh networks over greater distances than radio links can reach. A device with an Ethernet interface and an 802.15.4 radio is therefore useful in the topology shown in Figure 1.
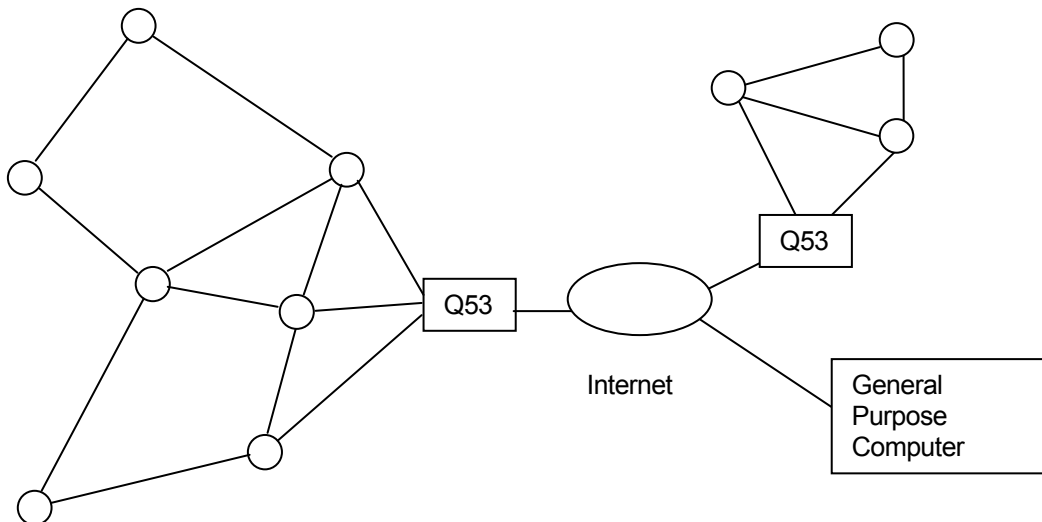

Figure 1 – Mesh Network with Gateway

The Q53s in Figure 1 provide communication links between their respective nearest neighbours by radio link and to a distant general purpose computer.

Operation

The Q53 hardware has the architecture shown in Figure 2. Software consists of a real-time operating system, a TCP/IP stack, a ZigBee stack (see Figure 3) and application software, such as a web browser, a telnet interface, and applications software.

Data Flow

A Q53 joins the network advertised by its nearest neighbours using a radio link. It advertises routes to devices at the other end of its internet connection. Packets received from its neighbours destined for remote devices are optionally encrypted then forwarded across the Ethernet connection using UDP datagrams or TCP sessions as defined by the bridge and gateway protocols of the ZigBee Alliance. These datagrams are received by the computer or Q53 at the other end of the internet link, optionally decrypted, and retransmitted to its neighbours.

Packets are checked at each interface for data integrity and dropped if errors are detected.

Each Q53 includes its own ZigBee network stack in order to appear to its neighbours as any other ZigBee device with routes to remote devices. The bridged routes are indistinguishable from any radio links that might exist between ordinary devices.
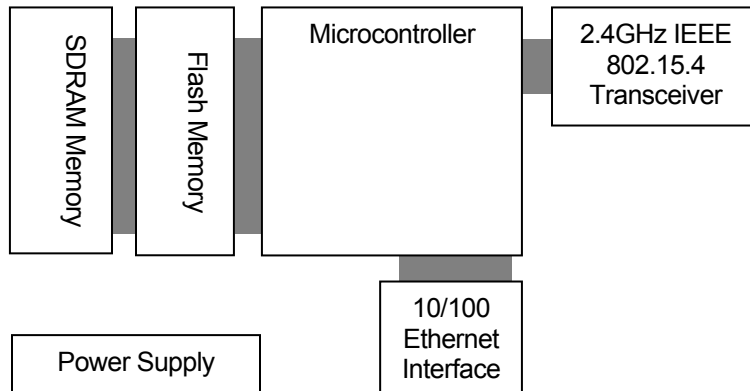

Figure 2 – Block Diagram

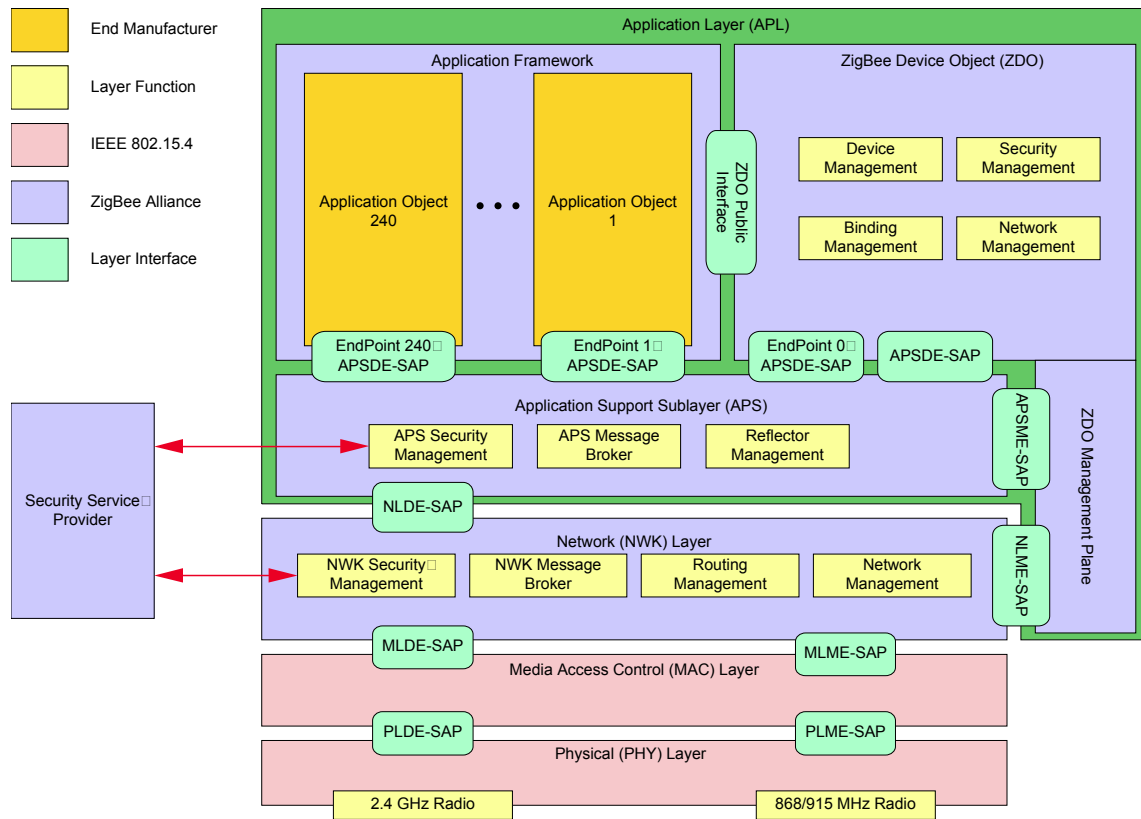In addition to its bridging functionality, a web browser and command line interface allow users to configure, monitor, manage and update the devices over an internet connection.

Figure 3 – ZigBee Stack Diagram

Legend:
- End Manufacturer
- Layer Function
- IEEE 802.15.4
- ZigBee Alliance
- Layer Interface

Application Layer (APL)

Application Framework

Application Object 240 ... Application Object 1

ZigBee Device Object (ZDO)
- Device Management
- Security Management
- Binding Management
- Network Management

ZDO Public Interface

EndPoint 240 APSDE-SAP
EndPoint 1 APSDE-SAP
EndPoint 0 APSDE-SAP
APSDE-SAP

Application Support Sublayer (APS)
- APS Security Management
- APS Message Broker
- Reflector Management

APSME-SAP

ZDO Management Plane

Security Service Provider

NLDE-SAP

Network (NWK) Layer
- NWK Security Management
- NWK Message Broker
- Routing Management
- Network Management

NLME-SAP

MLDE-SAP

Media Access Control (MAC) Layer

MLME-SAP

PLDE-SAP

Physical (PHY) Layer

PLME-SAP

2.4 GHz Radio

868/915 MHz Radio