ZigBee Alliance
Milan   March 2006

ZigBee Architecture Overview
ZigBee Overview
ZigBee Architecture Objectives

- **Enable low cost, low power, reliable devices for monitoring and control**
  - ZigBee’s architecture needs to be suitable to support all target environments and applications that are in the scope of ZigBee
    - Ensure that devices are efficient in their use of the available bandwidth
  - Provide a platform and implementation for wirelessly networked devices
    - Make it easy to design and develop ZigBee devices
    - Reduce today’s cost of building wireless solutions

- **Ensure interoperability through the definition of application profiles**
  - Enable “out-of-the-box” interoperable devices where desired by manufacturers

- **Define the ZigBee network and stack models**
  - Define ZigBee device types and core functions
  - Define layers / modules with their interfaces, and services

- **Provide the framework to allow a separation of concerns for the specification, design, and implementation of ZigBee devices**
ZigBee Alliance Leadership Map

Organization Chart

Board of Directors

Outsourced Management
Global Ventures, Inc.

Vice Chairmen
Jon Adams
Graham Martin

Secretary
Patrick Kinney

Treasurer
Jon Rosdahl

Technical Steering Committee
Chair Bob Heile

Program Management Office
Rolf Bienert

Chairman
Bob Heile

Change Board Control
Chair: Phil Jamieson

Architecture Work Group
Chair: Don Sturek

Application Framework Work Group
Chair: Phil Jamieson
Vice Chair/PM: Clinton Powell
Editor: Don Sturek
Secretary: DREW GISLAES

Network Work Group
Chair: Ian Marsden
Vice Chair: Myung Lee
Project Manager: Paul O`Call
Technical Editor: Zachary Smith
Secretary: C.C. Huang

Security Work Group
Chair: Joseph Soma Rei
Technical Editor: Renzo Gruik

Gateway Work Group
Chair: Pat Kinney
Vice Chair: Gene Dragotta
Technical Editor: Jay Werb
Project Manager: Jeff Ollis

IEEE 802.15.4

Marketing Work Group
Chair: Bill Craig
Secretary: Vicki McCann
PR Task Group Chair: Shannon Reid

Qualifications Work Group
Chair: Bill Wood
Vice Chair: Dmitri Grigorov
Secretary: Clinton Powell
Technical Editor: John Lin
ZigBee Feature Set

- ZigBee Features
  - Ad-hoc self forming networks
    - Mesh, Cluster Tree and Star Topologies
    - Reliable broadcast messaging
    - Non-guaranteed message delivery
  - Logical Device Types
    - Coordinator, Router and End Device
  - Applications
    - Device and Service Discovery
    - Optional acknowledged service
    - Messaging with optional responses
    - Mechanism to support mix of Public and Private profiles in the same network, all supported by standard ZigBee network and application features
ZigBee Feature Set

- ZigBee Features
  - Security
    - Symmetric Key with AES-128
    - Authentication and Encryption at MAC, NWK and Application levels.
    - Key Hierarchy: Master Keys, Network Keys and Link Keys
  - Qualification
    - Conformance Certification (Platform and Logo)
    - Interoperability Events
ZigBee Deployment Schedule

- Specifications and Conformance Test Plans
  - v0.92 Complete  DONE
  - Ready for Board of Directors  DONE
  - IP Review  DONE
  - Platform Conformance Test Plan  DONE

- Interop Events
  - BeeFest#1  Dec. 2003  ✓
  - BeeFest#2  April 2004  ✓
  - “Field of Dreams 1”  May 2004  ✓
  - BeeFest#3  July 2004  ✓
  - “Field of Dreams 2”  August 2004  ✓
  - “Security Field of Dreams 1”  September 2004  ✓
  - ZigFest#1  October 2004  ✓
  - Conformance Dry Run #1-#3  November 2004  ✓
  - ZigFest#2  January 2005  ✓
  - ZigFest#3  April 2005  ✓
  - ZigFest#4  July 2005  ✓
  - ZigFest#5  October 2005  ✓
  - ZigFest#6  January 2006  ✓
  - ZigFest#7  April 2006  coming soon…….
ZigBee Protocol Stack
ZigBee Stack Architecture

IEEE 802.15.4 defined
ZigBee™ Alliance defined
End manufacturer defined
Layer function
Layer interface
ZigBee Devices Type Model

**Application Device Type**
- e.g. Light Sensor
- e.g. Lighting Controller

**ZigBee Logical Device Type**
- ZigBee Coordinator
- ZigBee Router
- ZigBee End Device

**802.15.4 Device Type**
- FFD – Full Function Device
- RFD – Reduced Function Device

- Distinguishes the type of device from an end-user perspective
- Distinguishes the Logical Device Types deployed in a specific ZigBee network
- Distinguishes the type of ZigBee hardware platform

- ZigBee products are a combination of Application, ZigBee Logical, and ZigBee Physical device types
- Profiles may define specific requirements for this combination, but can also leave this up to manufacturers
ZigBee Network Communication Model (Mesh)

- ZigBee Coordinator (FFD)
- ZigBee Router (FFD)
- ZigBee End Device (RFD or FFD)
- Mesh Link
ZigBee Network Communication Model (Tree)

- ZigBee Coordinator (FFD)
- ZigBee Router (FFD)
- ZigBee End Device (RFD or FFD)
ZigBee Network Topologies

- **Star** networks support a single ZigBee coordinator with one or more ZigBee End Devices (up to 65,536 in theory)

- **Cluster tree** networks provide for a beaconing multi-hop network
  - Permits battery management of coordinator and routers
  - Must tolerate high latency due to beacon collision avoidance
  - Must use “netmask” type tree routing

- **Mesh** network routing permits path formation from any source device to any destination device
  - Radio Receivers on coordinator and routers must be on at all times
  - Employs ZigBee joint routing solution including tree and table driven routing
  - Table routing employs a simplified version of Ad Hoc On Demand Distance Vector Routing (AODV). This is an Internet Engineering Task Force (IETF) Mobile Ad Hoc Networking (MANET) submission
ZigBee Networking Concepts

- **Network Scan**
  - Ability to detect active networks within a local Personal Operating Space (POS)
  - Desired networks are identified via ZigBee extensions to the beacon payload

- **Creating/Joining a PAN**
  - Ability to create a network on an unused channel or to join an existing network within the POS
  - Device receives a short (NWK) address

- **Stack Profiles**
  - Multiple stack configurations supported (beaconed, non-beaconed)

- **Device and Service Discovery**
  - Ability to discover identity of devices on within the PAN
  - Ability to determine supported services on given devices within the PAN

- **Binding (Indirect or Direct messaging)**
  - Tagging of devices for application level command/control messaging
ZigBee Application Model

- Devices are modeled through Application Objects
- Application Objects communicate through the exchange of Clusters and Attributes
- Each Profile Object can contain single or multiple Clusters and Attributes
- Binding mechanism ensures interoperable exchange of Clusters/Attributes
- Clusters/Attributes are sent either
  - Directly to destination application objects (thereby to target device)
  - To ZigBee coordinator, ZigBee coordinator reflects Cluster/Attributes to single or multiple target objects
- Generic ZigBee device functions are provided through ZigBee Device Objects
Profiles are an agreement on a series of messages defining an application space (for example, “Home Controls – Lighting”)

Endpoints are a logical extension added to a single ZigBee radio which permits support for multiple applications, addressed by the Endpoint number (1-240)

Key Relationships:

- Maximum of 240 Endpoints per ZigBee Device (0 is reserved to describe the generic device capabilities and 255 is reserved for broadcasting to all endpoints, 241-254 are reserved for future use)
- One Profile described per Endpoint
Security Services Provider (SSP)

- **Security at each layer:**
  - MAC security for MAC-only frames
  - NWK security for NWK command frames (route request and route reply)
  - APL security for APS frames

- **Security Implementation**
  - Trust Center – assumed to be ZigBee coordinator
  - Holds (or creates) Master Keys (Trust Center to each device) – Commercial mode only
  - Each device derives key with single device – Commercial mode only

- **Two Security Modes**
  - Residential – Single NWK key, APL security via NWK key
  - Commercial – Two NWK keys, separate Link Keys for pairs of communicating devices at APL. Master Keys with the Trust Center for key exchange.
Security Services Provider (SSP)

- **Key Structure**
  - Master Key (could be programmed in or provided *in the clear* from the Trust Center) – Commercial mode only
  - Network Key (used for all NWK commands from any device) – Residential or Commercial mode
  - Link Keys (used for each pair of communicating devices) – Commercial mode only

- **Features**
  - Authentication and Encryption
  - Freshness (frame counters)
  - Message Integrity
Security Service in Residential Mode

- **Unsecured key-transport**
- **Factory installed**

**NWK Key**
Basis of security between two (or group of) devices

- **NWK key is used as basis of security services**

- **Key-Transport Service**
Unsecured key-transport of NWK key

- **Authentication Service**
Secure authentication that a device shares a NWK key.

- **Frame Security Service**
Secures all frames (except key-transport)
Security Service in Commercial Mode

- **Master Key**
  - Basis for long-term security between two devices
  - Factory installed
  - Secured key-transport from trust center

- **Link Key**
  - Basis of security between two (or group of) devices
  - Link key is used as basis of security services

- **Frame Security Service**
  - Secures all frames (except key-transport)
  - Secured key-transport of ‘group’ link keys

- **Key-Transport Service**
  - Secure key-transport of ‘master’ keys

- **Authentication Service**
  - Secure authentication that a device shares a link key.
“Stack Profiles” and Deployment
Stack Profiles

- Agreement of stack parameters, settings and policies for a family of application profiles (including private profiles)

- Current stack profiles:
  - Home Controls (mesh)
    - Supports **Home Automation** application profile
  - Commercial, Industrial and Institutional (mesh)
    - Supports **Commercial Building Automation, HVAC** and **Industrial Plant Monitoring** application profiles
  - Wireless Sensor Networks (cluster tree)
    - Will announce new application profiles shortly……..

- Stack profile identifier supplied in beacon payload. Devices join appropriate networks supporting desired stack profile.
Deployment

■ Commissioning
  ▶ Devices are programmed for a specific stack profile
    ♦ However, if multiple networks with the same stack profile are present, need mechanisms to help the device select the correct network
  ▶ Provisioning security keys
  ▶ Establishing command/control relationships in the network

■ Maintenance
  ▶ Adding new devices to an existing network
  ▶ Combining networks
  ▶ Replacing devices in a network
ZigBee Protocol does support a “tool box” approach, however….

► Once the stack profile and application profile are defined, the “tool box” becomes a set of specific deployment features: residential/commercial security, specific stack settings, specific application profiles, etc.

► Left to the implementer: Specifics of commissioning (though there are provisions in ZigBee for specific actions like managing network join, transport of security keys, binding, etc.)
Application Design Considerations
Network Formation Management

- Permit Join can be enabled/disabled on routers and the coordinator (network wide)
- Permit Join can be managed by an application to allow devices to enter the network upon:
  - Button press on a designated device or any other application defined action
  - Security keys may be exchanged upon managed network formation

Deployment examples:

- No commissioning tool
  - Example: Bubble pack purchased at a home improvement store
- Commissioning tool
  - Example: Professional installation
Application Design Considerations (no commissioning tool)

- Three networks: Suite 101, Suite 102, Fire Safety for the floor
- Coordinators are the green dots
- Question: How to commission appropriate devices to their proper coordinators
Some approaches to the previous commissioning problem (without a dedicated commissioning tool):

- Button press sequences to permit joining for a set amount of time and then a second set of button presses to identify the joining devices
- Low power output
  - Though this may affect the topology if the end device children are too far away from their parent
- Remote control device selection
  - Choose all neighbors and then iterate through deducing which device is which
  - Construct the list and permit the user to add/eliminate devices
- Pre-manufactured with information on devices in the pack
Application Design Considerations (commissioning tool)

- Same network topologies as before with addition of commissioning tools
- Commissioning tool works by identifying neighbors and networks, joining appropriate network, populating a list of devices on the network and permitting the installer to identify which one is which
Commissioning tool:

- Scans to find networks, joins the network selected by the installer
- Performs device discovery on neighbor devices or the whole network
- Identifies to the installer which device is which (various solutions to this)
- Once devices are identified, installer may create binding records, groups and scenes with a collection of other specified devices.