



ZigBee™ Alliance

Wireless Control That Simply Works



ZigBee Alliance

BuilConn

Palm Springs, California

May 2006

ZigBee Architecture Overview



ZigBee™ Alliance

Wireless Control That Simply Works

ZigBee Overview

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
 - ▶ Standardized Applications and Services
 - ◆ 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 Features (continued)
 - ▶ 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 by accredited test housed (Platform and Logo)
 - ◆ Quarterly Interoperability Events

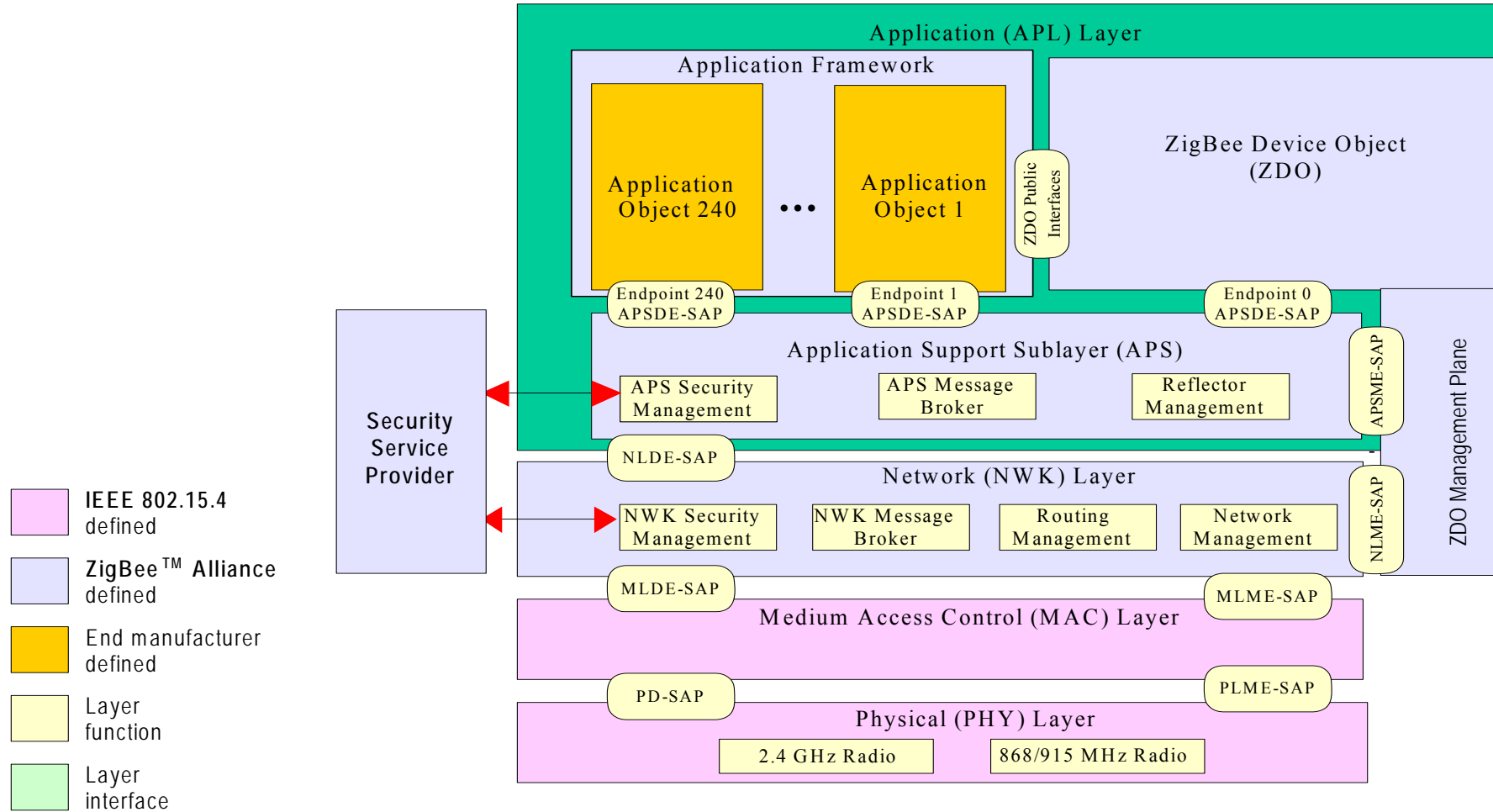


ZigBee™ Alliance

Wireless Control That Simply Works

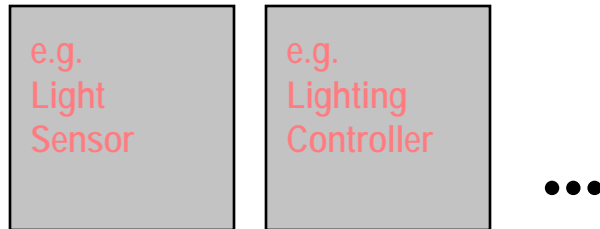
ZigBee Protocol Stack

ZigBee Stack Architecture



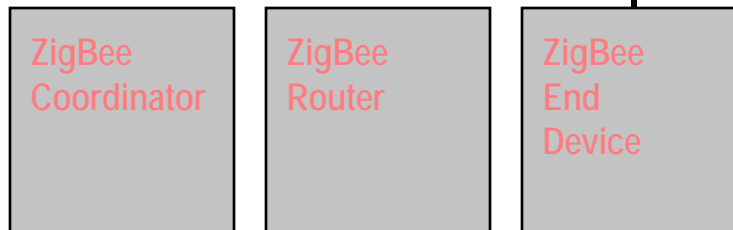
ZigBee Devices Type Model

Application Device Type



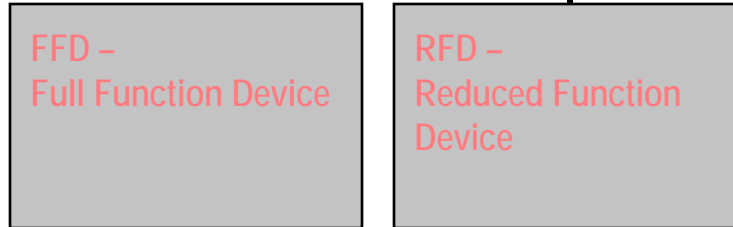
- Distinguishes the type of device from an end-user perspective

ZigBee Logical Device Type



- Distinguishes the Logical Device Types deployed in a specific ZigBee network

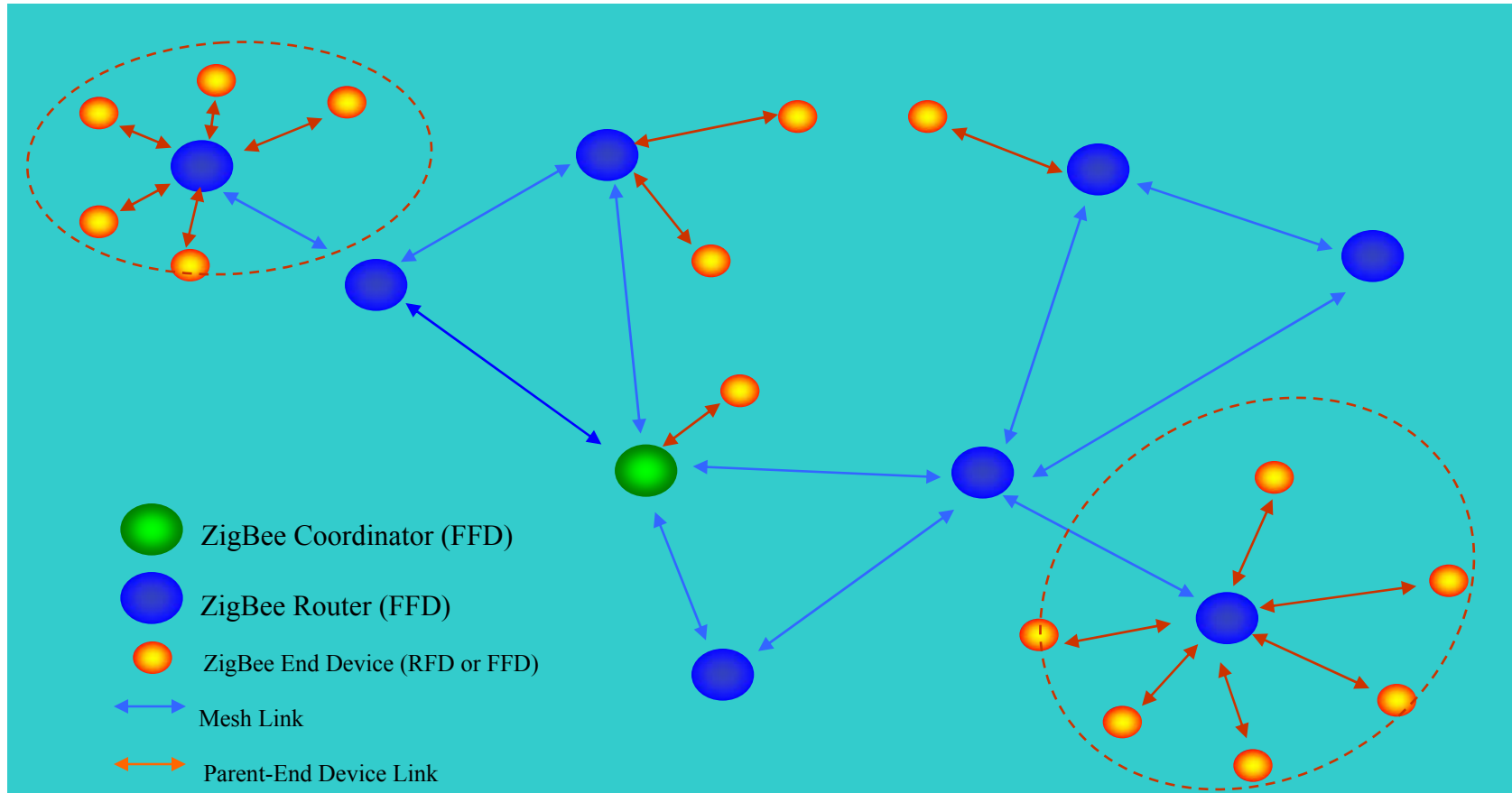
802.15.4 Device Type



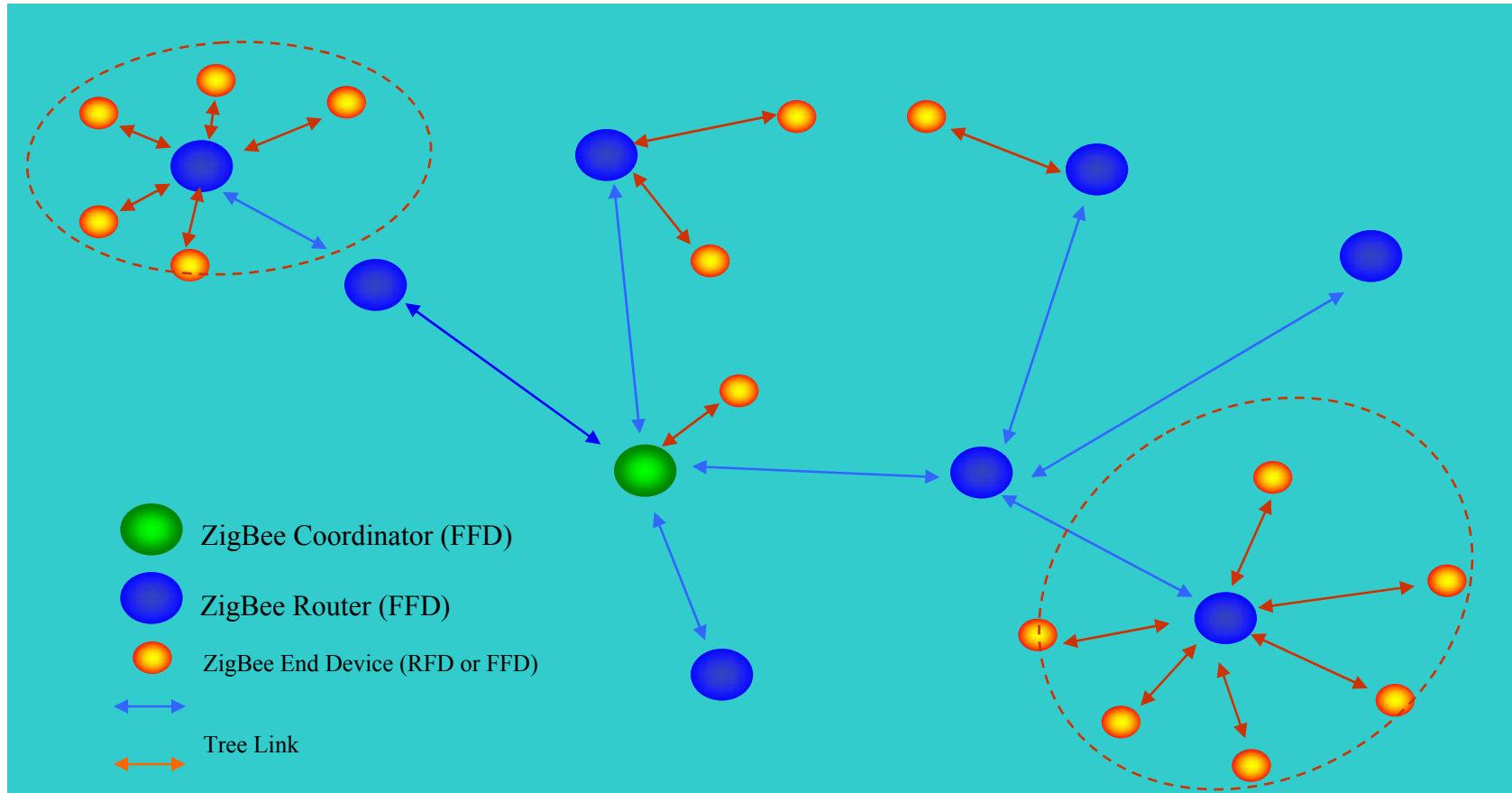
- Distinguishes the type of ZigBee hardware platform

- 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)



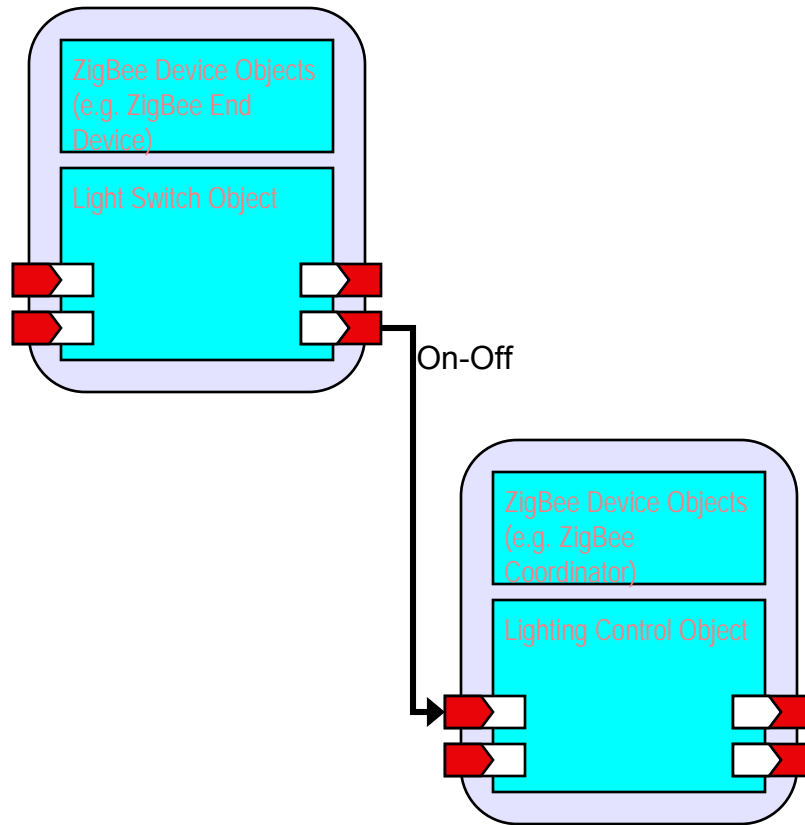
ZigBee Network Communication Model (Tree)



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 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

ZigBee Application Model

- **Application 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)

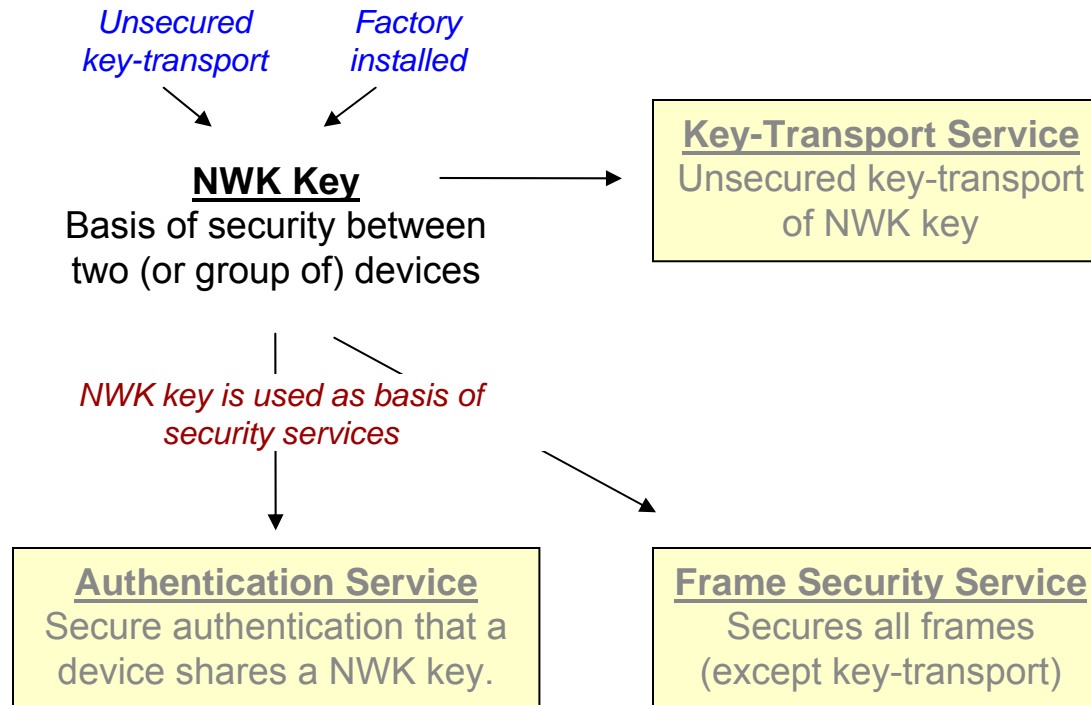
■ Key Structure

- ▶ 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

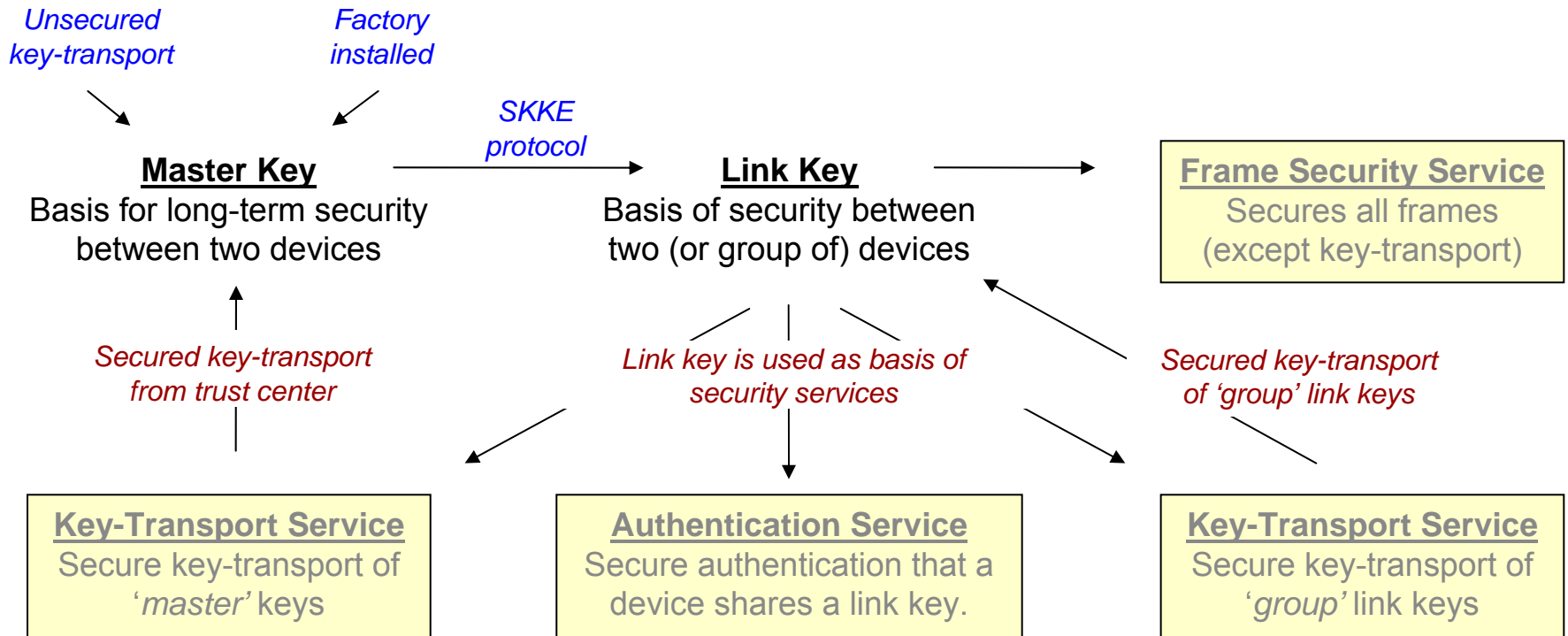
■ Features

- ▶ Authentication and Encryption
- ▶ Freshness (frame counters)
- ▶ Message Integrity

Security Service in Residential Mode



Security Service in Commercial Mode





ZigBee™ Alliance
Wireless Control That Simply Works

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 Controls Lighting and Home Automation application profiles
 - ▶ Commercial, Industrial and Institutional (mesh)
 - ◆ Supports Commercial Building Automation, HVAC and Industrial Plant Monitoring application profiles
- Stack profile identifier supplied in beacon payload. Devices join appropriate networks supporting desired stack profile.
- Additional stack profiles expected: Sensor Networks (cluster tree) and Peripherals (star)



Deployment Considerations

■ 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 Network Deployments

- 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.)



ZigBee™ Alliance

Wireless Control That Simply Works

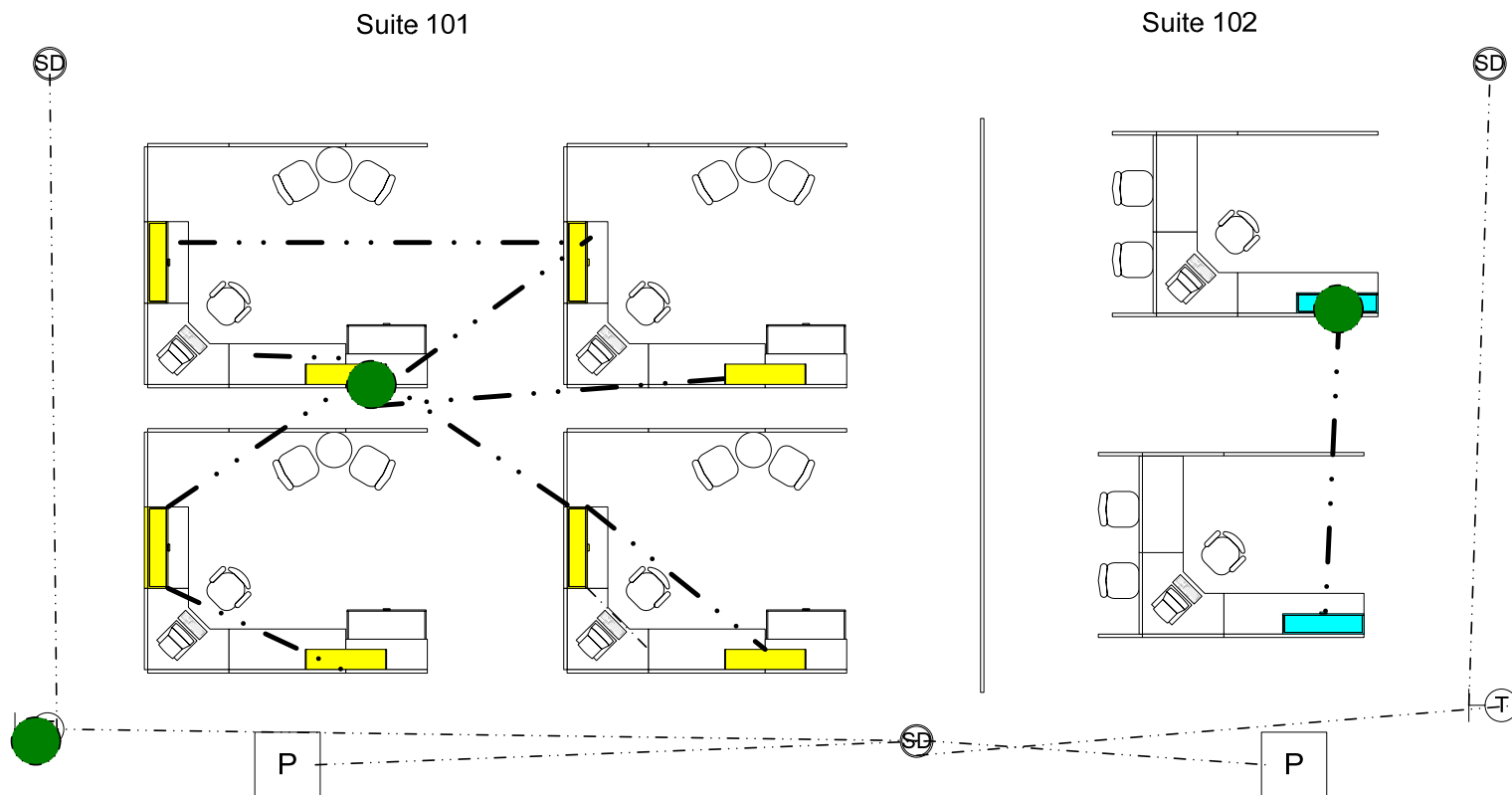
Application Design Considerations

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

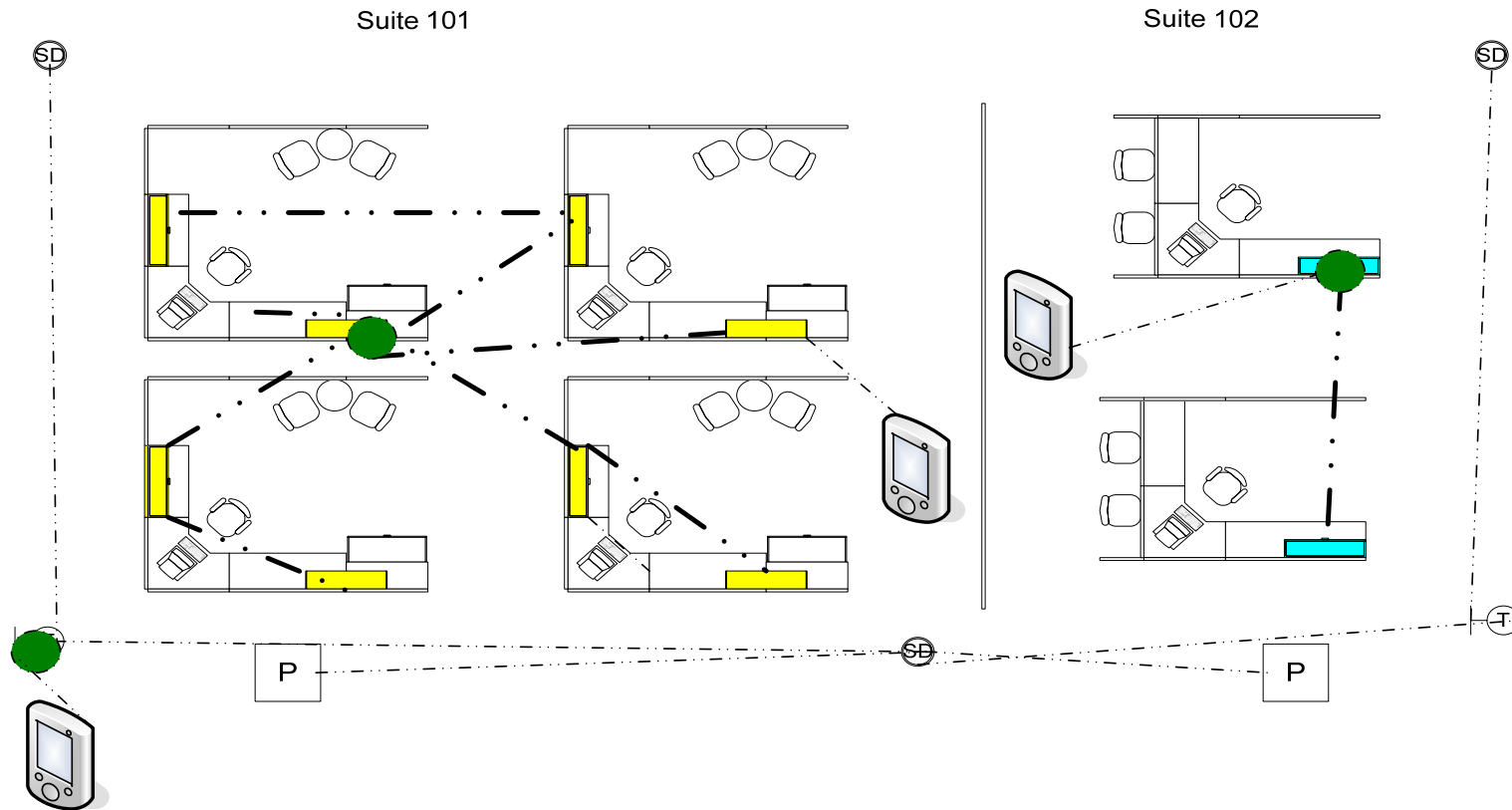


Application Design Considerations (no commissioning tool)

- 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



Application Design Considerations (commissioning tool)

- 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.