This ZigBee Overview provides you with an introduction to ZigBee™ technology.

In this module, we will discuss the ZigBee Alliance and its goals, target markets and applications. We will see how ZigBee compares to other wireless standards and explore the technology which underlies the standard. In particular, we will examine the IEEE 802.15.4 Wireless Personal Area Network (WPAN) standard and the ZigBee Network standard.
The Buzz of ZigBee

<table>
<thead>
<tr>
<th>What is ZigBee?</th>
<th>What makes ZigBee different?</th>
<th>What is the ZigBee architecture?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ZigBee Alliance: Consortium of 70+ companies</td>
<td>• Diverse market penetration</td>
<td>• Based on the IEEE 802.15.4 standard</td>
</tr>
<tr>
<td>• Emerging standardized protocol for Ultra Low Power Wireless Personal Area Networks (WPANs)</td>
<td>• Low cost, low power, sophisticated networking</td>
<td>• Incorporates all layers of software including the Application Layer and below: NWK, MAC, and PHY</td>
</tr>
<tr>
<td></td>
<td>• Standardization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interoperability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Focuses on low data rate, low duty cycle connectivity</td>
<td></td>
</tr>
</tbody>
</table>

The term ZigBee is used to describe a standardized wireless protocol for personal area networking, or “WPAN.” The protocol is the work of and property of the ZigBee Alliance, a consortium of more than 70 companies who have joined together to create and promote the new standard.

ZigBee is different from other wireless standards in that it has been designed to serve a diverse market of applications that require low cost, low power wireless connectivity with more sophistication than previously available at the target price. The standard focuses on low data rate, low duty cycle connectivity, a market segment not serviced well by existing standards. The reason for promoting a new protocol as a standard is to afford interoperability between devices manufactured by different companies.

ZigBee is a hardware and software standard built on the recently ratified IEEE 802.15.4 standard. This important standard defines the hardware and software, which is described in networking terms as the physical (PHY), and Medium Access Control (MAC) layers. The ZigBee Alliance has added Network (NWK) and application (APL) layer specifications to complete what is called the ZigBee stack.
The ZigBee Alliance has two classes of membership. The promoters are the leaders of the alliance. As you can see, the promoters represent a cross section of the wireless industry with semiconductor, software, and system providers.
Participants have a less committed stake in ZigBee. Participants can attend the alliance meetings and have access to all preliminary specifications. As with promoters, ZigBee Alliance participants represent a cross section of the wireless industry.
Solutions based on the ZigBee networking standard target specific markets and applications. The ZigBee standard is tailor-made for monitoring and control applications.

Therefore, such markets as building automation, personal health care, industrial control and lighting and commercial control are perfect fits.

Additionally, because of their low data rates and demand driven nature, high-end remote controls for consumer electronics and human interface devices such as keyboards, mice and joysticks are also good fits. In all cases, the target markets require only low data rates but demand long battery life, sophisticated networking or both.

Move your mouse pointer over the circles to learn more about ZigBee applications.
**Question**

Is the following statement true or false? Click Done when you are finished.

“Building automation, personal health care, and industrial control are good markets for the ZigBee networking standard.”

True

False

Consider this question regarding the ZigBee networking standard.

Correct.
The ZigBee networking standard is tailor-made for monitoring and control applications. Therefore, markets such as building automation, personal health care, and industrial control are perfect fits.
ZigBee Market Goals

- Global band operation, 2.4 GHz, 915 MHz, 868 MHz
- Unrestricted geographic use
- RF penetration through walls and ceilings
- Automatic or semi-automatic installation
- Ability to add or remove devices
- Cost advantageous

Let's summarize the market goals of the ZigBee alliance.

ZigBee is implemented in either the globally assigned 2.4 GHz unlicensed band or one of the 900 MHz regional bands. Unlicensed radio spectrum is designated by international agreement and puts the burden of specification adherence on the equipment manufacturer. Users are not required to have a license demonstrating their technical competence, hence the term unlicensed.

Since unrestricted geographic use is a goal, the 2.4 GHz band is the preferred band due to its international allocation. There are many unlicensed bands at higher and lower frequencies. The 2.4 GHz and 900 MHz bands were chosen by the IEEE 802.15.4 standard because of their propagation characteristics. Propagation refers to the way radio waves behave in the environment.

900 MHz and 2.4 GHz both have good penetration through walls and ceilings but have a limited range. Range limitation is desirable to reduce interference. After all, ZigBee is based on 802.15.4, which is a PAN standard.

Moving to desirable features of ZigBee-based systems, installation should be automatic or semi-automatic so that consumers can easily set up wireless networks. Additionally, adding new hardware to an existing system should be straightforward. Since ZigBee replaces wires and other wireless systems, cost must be kept low to make the change to ZigBee advantageous.
ZigBee Technical Market Goals

- 10 kbps to 115 kbps data throughput
- 10 to 75 m coverage range
- Up to 100 collocated networks
- Up to 2 years of battery life on standard alkaline batteries

Continuing with some technical market goals, ZigBee hardware and networks must be able to accomplish 10 to 115 kbps data throughput. This represents the actual amount of data that can be transferred once the protocol overhead is removed.

ZigBee hardware must be able to communicate over a 10 to 75 meter range. Typical 2.4 GHz hardware has demonstrated 30 meters indoors and over 100 meters outdoors.

Up to 100 ZigBee networks should be able to be co-located and still function.

Network end points as they are called should give up to 2 years of battery life from standard AA and AAA batteries. End points are typified by such devices as wireless sensors, monitors or controllers.
Let’s examine a typical ZigBee network model.

We mentioned the end point or end device in discussing ZigBee technical market goals. End devices can be full function devices, meaning that they have the capability to perform all of the tasks required in a network or can be reduced function devices.

An end device gets its instructions from a ZigBee Coordinator. All ZigBee networks must include a coordinator, which is a full function device that manages the network.

If the end device is out of range of its coordinator, it can communicate through a router. The diagram shows what is called a mesh network. The term mesh is used because of the routers and coordinator have multiple communication path options.

End devices are arranged in what is called a star network around a router or coordinator. This star arrangement is the typical way that low-cost wireless networks operate. ZigBee maintains the low cost while adding the power of mesh networking, a feature not found in most wireless networking standards.
How Does ZigBee Compare?

<table>
<thead>
<tr>
<th>ZigBee (WPAN)</th>
<th>Bluetooth (WLAN/WPAN)</th>
<th>Wi-Fi (WLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 802.15.4 standard</td>
<td>• 802.15.1 standard</td>
<td>• 802.11 standard</td>
</tr>
<tr>
<td>• 250 kbps</td>
<td>• 1 Mbps</td>
<td>• Up to 54 Mbps</td>
</tr>
<tr>
<td>• TX: 35 mA</td>
<td>• TX: 40 mA</td>
<td>• TX: 400+ mA</td>
</tr>
<tr>
<td>• Standby: 3 uA</td>
<td>• Standby: 200 uA</td>
<td>• Standby: 20 mA</td>
</tr>
<tr>
<td>• 32-60 KB memory</td>
<td>• 100+ KB memory</td>
<td>• 100+KB memory</td>
</tr>
<tr>
<td>• Lighting, sensors, RC peripherals</td>
<td>• Telecom audio, cable replacement</td>
<td>• Enterprise, home access points</td>
</tr>
<tr>
<td>• Mesh networking</td>
<td>• Point to multi-point</td>
<td>• Point to multi-point</td>
</tr>
</tbody>
</table>

There are many wireless options available to designers. Let's compare ZigBee with some of the more popular standards which share the unlicensed 2.4 GHz band. The parameters listed in the chart include the governing MAC standard, maximum over the air data rate, typical transmit and standby currents, memory requirements for a typical device, target applications and networking options.

Bluetooth is a popular standard applied to wire replacement applications. It too is based on an IEEE PAN standard, 802.15.1. Bluetooth operates with a 1 Mbps data rate. Note that Bluetooth and ZigBee have similar transmit currents, but ZigBee has a significantly lower standby current. This is because devices in Bluetooth networks must frequently report into the network to maintain synchronization, so they cannot easily drop into a “sleep” mode.

Wi-Fi is a wireless LAN standard, so it requires almost continuous activity by devices in the network. The advantage of this standard is the tremendous amount of data that can be moved from point to multi-point. Note the transmit and standby currents. Wi-Fi hardware is designed to operate off a significant power source.

Note that, of the three wireless standards, only ZigBee offers the flexibility of mesh networking.

Also note the reduced memory requirements of ZigBee. ZigBee applications are typically simple. The power is in the networking and the fact that ZigBee end devices can “sleep” while still maintaining network association.

One of the key points of this chart is to show that wireless standards are built around what are called “use models” or “applications.” No one standard meets the requirement of all use models. Designers should choose the standard that most closely meets their application requirements.
Let’s examine the comparison of Bluetooth and ZigBee more closely. Both standards are in the personal area networking category. As you learned previously, both have similar radios, as evidenced by their transmit currents. The difference between the two standards is in their target applications.

Bluetooth targets medium data rate, continuous duty applications like file transfer and streaming telecom audio.

ZigBee on the other hand, targets low data rate, low duty cycle applications. End point devices do not transmit or receive as frequently in these applications, resulting in exceptional battery life.

Based on battery life calculations, the crossover point for Bluetooth and ZigBee applications is at around a 1 second data rep rate. Put another way, if ZigBee and a Bluetooth device were to transmit the same data once every second, the battery life would be about the same for both.
Let's review the 2.4 GHz wireless options available to designers.

Correct.

Bluetooth (WLAN/WPAN) operates with a 1 Mbps data rate and targets medium data rate and continuous duty applications. ZigBee (WPAN) targets low data rate, low duty cycle applications, offers the flexibility of mesh networking, and devices can sleep and still maintain network association. Wi-Fi (WLAN) supports high data rates but has a standby current of 20 mA, requiring a significant power source.
Let’s look at two battery life examples, one high-duty cycle and one low, to understand where ZigBee demonstrates extended battery life. This scenario analysis is based on published data for a typical Bluetooth Radio and Freescale’s ZigBee solution RFIC and GB60 MCU.

In the first example, we will transfer 5 bytes of data once every 1.28 seconds. In this scenario, assuming a 200 milliAmp-hour (mAh) battery, a Bluetooth device will last 15 days. An equivalent ZigBee device will last about 33 days.

In the second example, we have the event driven scenario of a security system sensor. The sensor transmits once a minute to report its status and another 10 times a day when there is some sort of event such as a door opening. In this case, the Bluetooth device will last 100 days. The ZigBee device will last 9.8 years, exceeding the shelf life of the battery! Clearly, ZigBee is a better choice for such an event driven application.
As a final point of comparison, let’s look at 2.4 GHz radio performance. ZigBee, as defined by the underlying 802.15.4 specification, uses Direct Sequence Spread Spectrum (DSSS), coding, and half-sine filtered Offset Quadrature Phase Shift Keying (QPSK) modulation.

This chart shows the Bit Error Rate (BER) performance of various radio technologies versus Signal to Noise Ratio (SNR).

The BER performance of Bluetooth, with its Frequency shift keying, is shown by the blue line.

ZigBee, with its DSSS and Offset QPSK modulation is shown by the green line.

Note that ZigBee BER is 12 dB better than the Bluetooth BER that can be obtained at a given signal-to-noise ratio. This translates directly to range, with ZigBee giving 3 to 5 times the range for the same output power. This is yet another way the ZigBee conserves battery life.
The Challenge of Coexistence

- Potential for interference exists in every unlicensed band
- IEEE 802.11 and 802.15.2 committees are addressing coexistence issues

Mouse over the bulleted text below to learn more.

- ZigBee/802.15.4 Protocol is very robust
  - Clear channel checking before transmission
  - Back off and retry if no acknowledgment received
  - Duty cycle of ZigBee-compliant device usually extremely low

Coexistence inevitably comes up in discussions of unlicensed band standards.

Both the 802.11 and 802.15.2 committees are reviewing the situation.

ZigBee and 802.15.4 networks are in better shape than most due to their low data rate and low duty cycle. ZigBee devices will typically operate at 0.1 to 1% duty cycles. This allows the Carrier Sense Multiple Access (CSMA) scheme to produce robust results. ZigBee or 802.15.4 devices listen for a clear channel before they transmit. The CSMA algorithm is part of the 802.15.4 software so the user is relieved of the burden of creating a collision avoidance scheme.

Move your mouse pointer over the third bulleted point for more information.
We have discussed ZigBee performance attributes and mentioned the underlying 802.15.4 MAC. Let’s look in more detail at the ZigBee software stack architecture.

If you are familiar with other communications protocol software stacks you will note some familiar terms: PHY for the physical, or hardware, layer, MAC for the medium access control layer and NWK for the network layer.

ZigBee is simpler than many protocol stacks, so it requires less software code. The MAC and PHY are defined by the IEEE 802.15.4 standard, as mentioned before. The NWK and application layers are defined by the ZigBee Alliance with the actual application code being supplied by the equipment designer. Let’s look in more detail at the MAC and PHY as defined by the IEEE standard.
IEEE 802.15.4 Standard Basics

- Channel access is via CSMA with collision avoidance and optional time slotting
- Three bands, 27 channels specified
  - 2.4 GHz: 16 channels, 250 kbps
  - 868.3 MHz: 1 channel, 20 kbps
  - 902-928 MHz: 10 channels, 40 kbps
- Message acknowledgment and an optional beacon structure
- Multi-level security
- Works well for selectable latency for controllers, sensors, remote monitoring and portable electronics
- Configured for maximum battery life
  - has the potential to last as long as the shelf life of most batteries

802.15.4 is a simple packet data protocol for lightweight wireless networks. Many of the aspects of the design have been used for years in packet radio networks.

Since ZigBee focuses on low data rate and low data rep rate applications, as mentioned earlier, CSMA is employed to avoid interferers. Simply put, 802.15.4 devices listen before they transmit. If there is interference, the device either waits for a period of time and tries again or moves to another channel.

There are 16 channels defined for the 2.4 GHz band. Note that this band can support significantly higher data rate than the two lower bands.

Message acknowledgment is also available for improved data delivery reliability, and beacon structures are available to improve latency.

The IEEE 802.15.4 standard defines multiple levels of security.

The 802.15.4 protocol is designed for monitoring and control applications where battery life is important. 802.15.4 is the source of ZigBee’s excellent battery life.
IEEE 802.15.4 MAC Features

- Employs 64-bit IEEE & 16-bit short addresses
  - Ultimate network size can be $2^{64}$ nodes (more than probably needed)
  - Using local addressing, simple networks of more than 65,000 ($2^{16}$) nodes can be configured, with reduced address overhead
- Three devices specified
  - Reduced Function Device (RFD)
  - Full Function Device (FFD)
  - Network coordinator (FFDC)
- Simple frame structure
- Reliable delivery of data
- Supports association/disassociation
- Supports AES-128 security
- Employs CSMA-CA channel access for better coexistence
- Offers Optional superframe structure with beacons, GTS mechanism

802.15.4 employs both IEEE long and short addressing. Short addressing is used in network management where network IDs are assigned ad hoc. This results in reduced memory requirements but still allows more than 65,000 network nodes.

As mentioned earlier, three device types are specified: the Reduced Function Device (RFD), the Full Function Device (FFD), and the network coordinator. These map to the ZigBee device definitions where an end device is either an RFD or FFD, a router is an FFD, and a ZigBee coordinator is a network coordinator.

802.15.4 employs a simple frame structure which we will discuss in more detail later. This structure combined with acknowledgment results in reliable data delivery.

Network association and disassociation are supported as is AES-128 encryption if desired.

As mentioned, the CSMA scheme allows for good coexistence with other equipment. An optional superframe structure is available for improved latency.
Consider this question regarding the IEEE 802.15.4 standard.

**Correct.**

16 channels are defined for the 2.4 GHz band and CSMA is employed to avoid interferers. Message acknowledgment is available to improve data delivery reliability, and beacon structures are also available to improve latency. Multiple levels of security are defined. 802.15.4 is configured for maximum battery life, which makes it an excellent protocol for monitoring and control applications where battery life is important.
MAC Options

- Non-beacon network
  - Standard ALOHA CSMA-CA communications
  - Positive acknowledgment for successfully received packets

Mouse over the bulleted point below for more information.

- Optional beacon-enabled network
  - Superframe structure
    - For dedicated bandwidth and low latency
    - Set up by network coordinator to transmit beacons at predetermined intervals
      » 15ms to 252sec (15.38ms + 2n where 0 ≤ n ≤ 14)
      » 16 equal-width time slots between beacons
      » Channel access in each time slot is contention free

Let’s examine the MAC optional features. There are two channel access mechanisms. Non-beacon operation implies reliance on the CSMA and acknowledgment features for successful communications.

If better latency is desired, beacon operation can be used. In this mode, devices are assigned one of 16 time slots between beacons. Beacon intervals can be from 15 ms up to 252 seconds.

Three security levels are specified. Security options include none, the network access control list, and AES-128. The later option involves extra software, which will add to the code size.

Move your mouse pointer over “Optional beacon-enabled network” for more information.
Let’s examine the three device types in more detail.

The network coordinator is the most sophisticated device. It must manage the network and, therefore, generally requires the most memory.

The FFD has full 802.15.4 functionality. While an FFD can be an end device, more often it will be a router. FFD can also be employed as a bridge to other networks. In this case, it may require more memory and computing power than the network coordinator. Such a device will generally not be powered by a small battery.

Finally, the RFD carries, as its name implies, a reduced feature set. It only needs to know of its network coordinator and its closest router. This class of device targets battery operated end device applications.
Let’s examine the 802.15.4 packet structures. The most basic structure is the Data Frame packet. This structure is used for sending and receiving data.

Note the nesting of the MAC Packet Data Unit, or MPDU, within the PHY Packet Data Unit, PPDU. The MPDU is also called the PHY Service Data Unit (PSDU).

The PSDU is a maximum of 127 bytes in length. 2 bytes are for the Frame Check Sequence, FCS.

In addition to the PSDU, the PPDU includes a 4-byte preamble, a 1-byte start of frame delimiter and a 1-byte frame length.

The MPDU includes 2 bytes of frame control, a 1 byte data sequence number used for acknowledgment. 4 to 20 bytes are used for address information, which can include both source and destination information. This leaves a maximum of 104 bytes of actual data.

While the MAC software does the parsing of the data and managing of the address info and data sequence numbers, it is useful to understand this structure.

Move your mouse pointer over the diagram for more information.
Acknowledgment Frame Format

Mouse over the diagram for more information.

The acknowledgment frame, or ACK, confirms that the data is received successfully. Frame control and Data sequence are taken from the original packet. A transmission is considered successful if the ACK frame contains the same sequence number as the transmitted frame.

Move your mouse pointer over the diagram for more information.
The command frame is used for remote control. Instead of data as the payload, this frame contains command information. A command type byte is added as well. The MPDU must still be 127 bytes or less as with the Data frame.

Move your mouse pointer over the diagram for more information.
Beacon Frame Format

Mouse over the diagram for more information.

- Beacons add a new level of functionality to a network.
- Client devices can wake up only when a beacon is to be broadcast, listen for their address, and if not heard, return to sleep.
- Beacons are important for mesh and cluster tree networks to keep all of the nodes synchronized without requiring nodes to consume precious battery energy listening for long periods of time.

The beacon frame is much more complex as it must convey the synchronization and guaranteed time slot (GTS) information to all of the devices in the network.

Move your mouse pointer over the diagram for more information.
Question

Match the frame formats to their functions by dragging the letters on the left to their appropriate locations on the right. Click Done when you are finished.

A Data Frame Format  D Beacon Frame Format
B ACK Frame Format  B Conveys synchronization and GTS information to all the devices in the network
C MAC Command Frame Format  A Sends data
C Contains information that is used for remote control

Consider this question regarding the frame formats.

Correct.
The Data Frame Format is used for sending data. The ACK Frame Format confirms that data is received successfully. The MAC Command Frame Format contains command information that is used for remote control. The Beacon Frame Format conveys synchronization and GTS information to all the devices in the network.
You may recall from the ZigBee Stack block diagram that the NWK layer resides above the MAC and PHY.

Since the ZigBee protocol stack is relatively simple compared with other communications protocol stacks, what is called the ZigBee Network layer often refers to the application layer (APL) as well. This architecture is the starting point for discussion of the network layer.
ZigBee Architecture Objectives

Mouse over the bulleted text for more information.

- 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 and modules with their interfaces, and services
- Provide the framework to allow a separation of concerns for the specification, design, and implementation of ZigBee devices:
  - Help to create and coordinate consistent use of terms in ZigBee
- Allow future extension of ZigBee:
  - Enable both extension of the basic ZigBee platform as well as ZigBee application profiles

The ZigBee architecture has other objectives beyond simply enabling low cost, low power, reliable devices for monitoring and control.

The architecture must support all the target applications and environments within the scope of the marketing requirements.

The architecture must allow for the easy design and development of the low cost and low power devices promised.

Interoperability must be addressed as it is one of the main reasons for standardization.

The architecture should define the stack in such a way that terminology is standardized.

The architecture must also allow for upgrades and extensions in the future.
Move your mouse pointer over the bulleted points for more information.
Wireless Networking Basics

- **Network scan**: ability to detect active channels within a local Personal Operating Space (POS)
- **Creating/Joining a PAN**: ability to create a network on an unused channel or to join an existing network within the POS
- **Device discovery**: ability to identify devices on active channels within the PAN
- **Service discovery**: ability to determine supported services on given devices within the PAN
- **Binding**: ability to perform application level command/control messaging

Let’s examine some commonly used terms in wireless networking. These terms relate directly to network layer features.

Network scan is the ability of a device to detect active channels within its communications range. This range is often called, in personal area networking, the Personal Operating Space (POS).

Creating is the ability to form a network on unused channels within the POS. In the case of ZigBee, the network is a PAN. Joining is the ability to join a network within the POS.

Device discovery is the ability to identify the devices on active channels in the PAN.

Service discovery is the ability to determine what features or services are supported on devices within a network.

Binding is the ability to communicate at the application level with other devices in the network.
Network formation and joining is based on some assumptions.

First, devices are pre-programmed for their network function. End devices will always try to join an exiting network. Coordinators will always try to find an unused channel and form a network.

Devices discover other devices and join in the network to provide complementary services. For example, a ZigBee light control device will discover only a ZigBee lighting network because that is all that it understands. Devices can, however, be programmed to function in multiple network types.

The same holds for binding. Devices can only talk to devices in a complementary network.

Move your mouse pointer over the bulleted points for more information.
### ZigBee Network Routing Features

<table>
<thead>
<tr>
<th>Star Network</th>
<th>Cluster Tree</th>
<th>Mesh Network Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Supports a single ZigBee coordinator with one or more ZigBee end devices (up to 65,536 in theory)</td>
<td>- Permits “netmask” style message routing down or up the tree based on the destination address</td>
<td>- 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Flooding is used to determine paths from source to destination in the mesh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Route Replies determine viable paths in the mesh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Routing tables record known paths.</td>
</tr>
</tbody>
</table>

We have mentioned that mesh networking is one of ZigBee’s strong points. Let’s look at the full list of ZigBee network possibilities.

The star network is the most simple network topology. This topology has one coordinator networked with one or more end devices. Remember that an end device communicates only with a router or coordinator, not directly to another end device. A TV remote control is a simple example of a star network.

A more complex network topology is called a cluster tree. This is similar to computer networking where devices branch off of a tree, the network backbone. Star networks can be branches in a cluster tree network.

In mesh networking, routing paths are not as constrained as in the cluster tree topology. Mesh networking permits path formation from any source to any destination device. There can be multiple paths for device communications and the viable paths are maintained in the network routing table.
As we discussed under binding, information exchange can only occur between devices with complementary services. These complementary services are defined by application support features.

Profiles are used to define a device’s application capability and drive the application details. An example of a profile would be Home Control—Lighting.

Endpoints are the physical dimensions added to a ZigBee device which permit multiple application support.

Interfaces are defined per endpoint and allow such things as extra proprietary capability extensions and backwards compatibility.

Move your mouse pointer over the bulleted points for more information.
Let's review some terms that are commonly used in wireless networking.

Correct.

Network scan is the ability for a device to detect active channels within its communications range (local POS). Creating a PAN is the ability to form a network on unused channels within the POS. Device discovery is the ability to identify the devices on active channels in the POS. Service discovery is the ability to determine what features or services are supported on devices within a network. Binding is the ability to communicate at the application level with other devices in the network.
Module Summary

- ZigBee Alliance goals, target markets, and applications
- ZigBee comparisons with other wireless standards
- Basics of the IEEE 802.15.4 standard
- Basics of the ZigBee software stack

This module provided an introduction of the ZigBee Alliance networking standard, its underlying technology, and its target markets.

In this module, we discussed the ZigBee Alliance and examined its goals, target markets, and applications. A major goal of the ZigBee Alliance is to promote the ZigBee standard as a protocol for allowing interoperability between devices manufactured by different companies. The ZigBee standard is tailor-made for monitoring and control applications markets such as building automation, personal health care, industrial control and lighting, and commercial control. Because of their low data rates and demand driven nature, high-end remote controls for consumer electronics and human interface devices such as keyboards, mice and joysticks are also good fits.

We compared ZigBee to other wireless standards and delved into the technology which underlies the standard, in particular, the IEEE 802.15.4 WPAN standard and the ZigBee Network standard. Of the three wireless standards, only ZigBee offers both the flexibility of mesh networking and reduced memory requirements.