Interrogation Zone Basics

Terms you need to understand:

- ✓ Interrogator
- ✓ Hybrid interrogator
- ✓ Tethered interrogator
- ✓ Interrogation signal
- ✓ Read range
- ✓ Write range
- ✓ COM ports
- ✓ Host computer
- ✓ Multiplexor
- ✓ Tag's UID
- ✓ ALOHA
- ✓ Binary tree/tree-walking
- ✓ Antenna
- ✓ Polarization
- ✓ Circular polarization
- ✓ Linear polarization
- ✓ Bi-static antenna
- ✓ Mono-static antenna
- ✓ Time in beam/dwell time
- ✓ Faraday cage
- ✓ Antenna field hole
- ✓ Antenna gain
- ✓ Effective radiated power (ERP)
- ✓ Effective isotropically radiated power (EIRP)
- ✓ Front-back ratio
- ✓ Diffraction
- ✓ Free space loss
- ✓ Field density/power density

Techniques and concepts you need to master:

- ✓ Dwell time
- ✓ Interrogation zone
- ✓ Dense interrogator/dense reader mode
- ✓ Frequency hopping
- ✓ Listen Before Talk
- ✓ Software synchronization
- ✓ Multiplexing
- ✓ Shielding
- ✓ Anticollision methods
- ✓ AB Symmetry
- ✓ Calculation of radiated power output
- ✓ Calculation of free space loss
- ✓ Calculation of field (power) density

An RFID interrogator (also called an *RFID reader*) and RFID antennas are two of the major hardware components that make up an RFID system. Depending on the specific application, interrogators and antennas are configured differently to optimize tag read rates. Typical configurations consist of *portals*, *arrays*, and *tunnels*. Power limits can be enhanced by optimizing the radiated signal in a focused manner, to allow for more accuracy and reliability. Various materials can also aid the radiated signal by giving it a better coverage area to enhance the readability of tags. Antenna configurations can also aid the interrogator in reading or writing to tags. When writing to tags, *accuracy* and *time* are the main issues.

The terms *RFID interrogator* and *RFID reader* are used interchangeably in the RFID industry. The CompTIA exam only uses the term *RFID interrogator*.

RFID Interrogator Functionality

An RFID interrogator is an electronic device that generates and receives an interrogation signal (in fact this signal is in its nature a radio signal). These radio signals are radiated or received by an antenna or antennas that are attached to the interrogator. Depending on their type, interrogators can have various capabilities, which include

- Reading and writing data to tags.
- Operating on either a single or on multiple frequencies.
- Performing anticollision processing.
- Reading bar code or other Automatic Data Collection (ADC) capabilities; these are called hybrid interrogators.

RFID Interrogator Components and Their Function

Figure 3.1 shows the components of a basic interrogator. They include

- A receiver that holds an amplifier and a demodulator
- A transmitter that holds a modulator and a power amplifier
- An oscillator

- A controller/processor
- An input/output port to an antenna

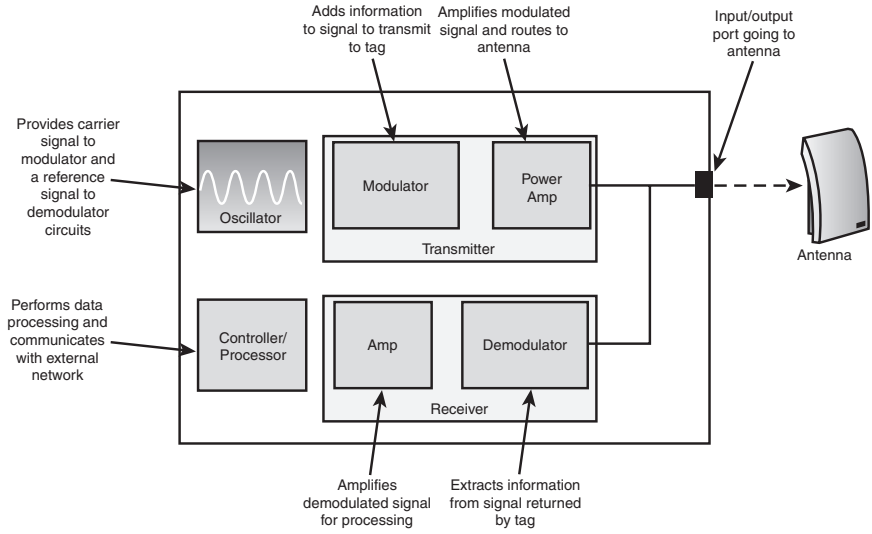

Figure 3.1 Basic RFID interrogator anatomy.

You need to know the component parts that make up an interrogator and what functions they perform.

Receiving

The amplifier "expands" the signal received from the tag through the interrogator's antenna for processing, and the demodulator extracts the information from the signal.

The controller/processor performs the data processing functions and manages the communications with the external network.

Transmitting

The oscillator provides the carrier signal to the modulator and a reference signal to the demodulator circuits. The modulator adds information to the signal to be transmitted to a tag. Then the power amplifier amplifies the modulated signal and routes it to the antenna. The antenna radiates the signal to a tag.

Communication Methods

RFID interrogators use different methods to communicate with RFID tags depending on whether the RFID system is active or passive.

Passive and semi-passive tags use *passive backscatter* to communicate. The signal is generated by the interrogator and radiated through the antenna. The signal is then demodulated by the tag to decode the reader's commands. The reader requested data is reflected back to the interrogator through the modulated signal. This method is also discussed in detail in Chapter 2 on tags.

Active tag communication differs from passive methods in that the tag does not reflect the signal from the interrogator. Because an active tag has its own power source and transmitter, the tag does not have to wait for the interrogator to transmit a signal. This tag can send its data or "beacon" at certain intervals as defined by the system.

Read and Write Range

The capability of an RFID interrogator to communicate successfully with a tag is heavily dependent on two factors:

- The distance between the interrogator and the tag
- The tag and the tag's dwell time

The tag's *dwell time* is the time a tag is in the interrogator's RF field.

An RFID interrogator's *read range* is the distance between the interrogator and the RFID tag at which the signals from the tag can be read properly.

Similarly, an RFID interrogator's write range is the maximum distance at which information within the RF signal from the interrogator can be received correctly and stored within the memory of the tag's microchip.

More power is needed to write to a tag than to read it. As a result, the tags need to be closer to the antenna to write than to read. The general rule is that the write range is 50–70% of the read range of a particular interrogation zone.

Due to the process differences between reading a tag and writing a tag, writing to a tag takes longer to perform than just reading a tag. Therefore, writing to a tag requires longer dwell time.

Types of RFID Interrogators

The three types of RFID interrogators are

- Fixed
- Hand-held
- Mobile interrogators

Table 3.1 highlights the major characteristics of each type of interrogator.

Table 3.1 Interrogator Types and Their Characteristics

Interrogator Type	Characteristics
Fixed Interrogators:	Can read tags as well as write to tags, depending on the type
	Can be mounted to walls, doors, or other structures
	Can be integrated with stationary devices, such as conveyors, door portals, sortation systems, manufacturing lines, and others
	Need an external power source
	Typically can accommodate multiple antennas
	Can be hard-wired or wirelessly connected to the local area network (LAN)
Hand-held Interrogators:	
Hand-held interrogators can be either *tethered* or *wireless*.	Are much smaller than fixed interrogators and usually come in the shape of "a gun" or a tablet
	Have capabilities similar to those of fixed interrogators but are much smaller
	Can be used not only to read from tags but also to write to tags (some models, however, are just read-only)
	Have an antenna built into the unit
	Are primarily used for exception processing due to their portability and capabilities
	Can be used in low-volume applications for tag data verification, case, and pallet association or tag searches
	Can have both barcode and RFID functionality

(continued)

Table 3.1 Interrogator Types and Their Characteristics *(continued)*

Interrogator Type	Characteristics
Tethered interrogators	Are tied directly into the IT infrastructure Don't need their own power because they are typically connected to a power source through the attached tethered cable Have limited mobility due to their wired connections to other devices and to their external power source
Wireless interrogators	Are connected to the network through a wireless LAN protocol or device-specific protocols Need a power source (battery) built into the device Are able to achieve greater mobility due to their wireless capability
Mobile Interrogators:	
These interrogators can come in different forms (for instance mobile phone, PDA, or vehicle mounted).	Can have PCMCIA cards to connect to laptop PCs Differ from hand-held interrogators in size and form factor Usually are powered from their own power source (battery) or by the vehicle they are mounted on Typically have wireless connectivity
Mobile phones and PDAs	Are very small in size but have fairly advanced functionality Are a proven technology Are attractive to industrial applications
Vehicle mounted interrogators	Are typically mounted on forklifts or clamp trucks Are built to withstand environmental extremes Are placed for minimal contact with material being handled

Each RFID application is different. Choosing between a tethered or a wireless interrogator depends on your application objective and the particular environment in which you are deploying. Although you gain mobility by using a wireless interrogator, you trade off power consumption. All of these issues need to be addressed and resolved before you can select the appropriate equipment needed for a particular application.

Interrogator Installation

When installing interrogators, not only is the optimization of the interrogation field important but several other considerations must also be taken into account. They are

- ➤ Ensuring equipment safety
- ➤ Ensuring employee safety
- ➤ Maintaining proper functionality
- ➤ Making proper connections for power and data
- ➤ Understanding the environmental limitations of the equipment

You need to know and are tested on each of these elements and how they affect an RFID implementation.

Equipment Safety

One of the important decisions you have to make is where to locate your interrogator to minimize the risk of damage. In the case of a dock door interrogator, for instance, knowing that a material-handling device, such as a forklift, may miss the door from time to time helps you choose the optimal location to ensure the interrogator is out of harm's way.

Instead of mounting the interrogator low on the portal, you may want to install it on the wall behind the antenna stand or high on the antenna stand. This location helps avoid damage from moving vehicles. Also, consider the potential for water damage caused by flooding, broken liquid products, or the cleaning crew that uses water to hose down an area. Remember to ensure easy access to the interrogator for troubleshooting!

Initial attempts by major RFID manufacturers to build prefabricated door portals showed that these manufacturers had given little thought to these real-world situations. Interrogators in these early solutions were mounted about six inches off the floor, and they were not only difficult to access for troubleshooting, but the devices and their connections were also easily damaged by moving vehicles such as forklifts.

Manufacturers have learned from these early design flaws, and more intelligently designed portals are increasingly becoming available. Some manufacturers now offer portals, where the antennas can be rotated horizontally as well as vertically.

Employee Safety

Careful consideration should be given to employee safety when determining where to place interrogators. Units should not be placed in locations where they can be an obstruction or a trip hazard. If the interrogator is being mounted on a vehicle, neither the interrogator nor its antennas should affect visibility or operator maneuverability during the operation of the vehicle.

Vehicle operators are of great assistance here because they know all the actual scenarios in which the vehicles are used, and not just how the vehicles are intended to be used.

Proper Functionality

Ideal placement of an interrogation zone is vital for proper functionality. To determine this, the intended primary function must be defined; only then can it be determined where the interrogator and antennas must be placed as well as how the antenna must be oriented to achieve maximum accurate reads. Ensuring that the expected read is realized is critical to the success of the operation.

Proper Connections

Clean power and data connections are also important. For a small price you can buy a basic power analyzer at any major retail department store. This tool determines that the power circuit is wired properly and grounded. Usually, this device has a series of three to four LEDs on it that, when plugged in, light up to indicate various conditions in the wiring. These conditions can include

- Ground fault
- Reverse neutral/hot
- Reverse neutral/ground

If more serious problems are suspected, a qualified electrician should be called in. He or she will bring a more advanced power analyzer that detects conditions such as

- RMS voltage quality (sags, swells, flicker)
- Impulsive voltage quality (transient voltage)

- Harmonic voltage quality (harmonic voltage, harmonic current, harmonic power, inter-harmonic voltage, inter-harmonic current, harmonic phase angle, total harmonic voltage distortion, total inter-harmonic current distortion)

Normally, this level of investigation is not required. Most sites already have certified wiring. However, in the odd situation in which the equipment repeatedly fails, it might be a power issue. When this happens, a certified professional should be consulted.

When installing RFID systems, best practice is to use an uninterruptible power supply. This will prevent system failures in case of power shut downs.

Using a network analyzer to ensure connectivity and throughput are consistent and reliable is also always a good idea. A network analyzer enables you to capture and examine data from your network. You can browse the captured data and view detailed information for each packet that has been captured. A network analyzer also provides detailed information about current traffic, as well as overall protocol statistics and more. Many network analyzers support various protocols including IP4, TCP, UDP, IEEE 802.2 frame, Ethernet II frame, NetBIOS, IPX, and others. In addition to real-time monitoring, most network monitors include an extensive array of filter options that allow you to limit capture based on IP address, port, protocol, MAC address, packet size, and other criteria.

If the interrogator is not communicating with the network systems, the data that is critical to the business will be lost; this is why using a network analyzer is important.

Environmental Considerations

Consideration should be given to the environmental conditions of the physical site where you will be locating the interrogators. Several factors need to be evaluated when assessing the environmental conditions, such as

- Temperature minimum/maximum
- Humidity
- Shock
- Vibration
- Chemical exposure
- Splash conditions
- Dust

Not many of the "off the shelf" interrogators will survive all these extreme conditions. Making the choice of a proper interrogator for your specific environment is critical in reducing the costs involved with replacing frequently damaged equipment and the downtime associated with hardware failure. A thorough environmental study is always recommended even if the conditions seem to be readily apparent.

Interrogation Zone Considerations

Special considerations should be addressed when setting up an RFID system with multiple interrogators that have overlapping interrogation zones. You can deal with these types of situations in several ways, such as using dense interrogator mode, interrogator synchronization, arbitration, and anticollision protocols. Some of these features are only available with Generation 2 devices.

Dense Interrogator Mode

Dense interrogator mode, also called *dense reader mode*, provides each interrogator the capability to operate at a slightly different frequency, which helps reduce the radio interference between interrogators. Other techniques are used as well, such as *Listen Before Talk (LBT)*, *frequency hopping*, or a combination of the two.

Listen Before Talk

Using the LBT technique, an interrogator tries to "listen or hear" whether another interrogator is using a channel. If it learns that another interrogator operates on that channel, it rolls to another channel to avoid interfering with the other interrogator.

Frequency Hopping

Interrogation signals hop between channels within a certain frequency spectrum. In the United States, they can hop between 902 MHz and 928 MHz, and they can be required to listen for a signal before using a channel. These guidelines are supplied by the FCC and are discussed in Chapter 9, "Standards and Regulations."

Interrogator Synchronization

In certain applications that require multiple interrogators operating at the same time and in the same proximity, it is necessary to coordinate their

transmitting and receiving functions. The radio transmissions from the interrogator's antennas may interfere with other interrogators, so much so that the tags are unable to completely understand the information being read or written and the interrogator may misread the tag. The level of interference depends on a number of factors, which include

- The sizes and types of the antennas
- The output power of the antennas
- The distances between antennas
- The presence (or absence) of shielding

Variations in local conditions can affect the general noise background. For example, radio frequency interference (RFI) and electrical noise can travel from one interrogator zone to another via conducted metal structures. Metal structures can include the frames of metal buildings, reinforcing bars in concrete floors, and power or data cables.

Several synchronization methods are used; we discuss the main three:

- Software synchronization
- Multiplexing
- Shielding

Software Synchronization

The software synchronization method can be used when multiple interrogators are connected to the same communication bus. As interrogators are individually addressable, the controlling (host) computer is able to command each interrogator to transmit at a separate time so that it is not possible for more than one interrogator to be transmitting at the same time.

Multiplexing

In the multiplexing method, a single interrogator is connected through a switching box (MUX) to multiple antennas. The interrogator output is directed to each antenna in turn, again ensuring that only one antenna is transmitting at a time.

Multiplexers need to take advantage of solid state circuitry for switching versus mechanical switching. Because solid state switching introduces signal loss, the interrogator power output is normally increased to compensate for the discrepancy. Mechanical switches or relays are not feasible due to their construction and use of moving parts. The moving parts undergo high levels

of wear, which reduce their functionality during high loads or peaks. Ultimately, the constant switching will result in failure of the mechanical switch.

Multiplexing divides the time available to read a tag by the number of channels on the multiplexer. Because of this timing issue, the interrogator needs additional time to ensure a complete read has been achieved, especially if the tags are moving quickly through an interrogation field.

Shielding

Shielding prevents interference between interrogators. It also prevents tags that are passing outside the interrogating system from being interrogated by an adjacent system, and when antennas are close together, shielding prevents the same tag from being interrogated by an adjacent antenna.

Shielding can also act as a barrier to prevent metal sheets or other objects that have been left next to an antenna from affecting the performance of tags and interrogators.

Shielding can also be used when a large concentration of other devices operating in the 902–928 MHz spectrum is present, such as older 900 MHz wireless systems or cordless phones.

Because of the shape of an antenna's RF field (that is, side lobes), the shielding has to be larger than the antenna. The metal mesh or sheet used for shielding needs to be approximately twice as high and wide as the antenna. Anechoic material also works well for shielding since it absorbs scattered RF and does not reflect. It is not recommended to have the shielding too close to an antenna (less than 8 inches or 0.2 meter) because the antenna can be detuned, and the metal can reflect some of the power that should be radiating. You can retune the antenna to compensate to some extent for the detuning, but metal reflection is harder to fix.

Arbitration

Arbitration is a method of identifying all of the transponders in the reader's field. Arbitration precedes the anticollision mechanism.

Arbitration works differently in Generation 1 and Generation 2 protocols. In Generation 1 all the tags have to communicate their nth bit to the reader. If the received signal (consisting of nth bits of all tags) is composed of 1 and 0, the read/write module assigns 0 to the nth bit. If the received signal is composed of 0 only, the read/write module assigns 0 to the nth bit. If the received signal is composed of 1 only, the read/write module assigns 1 to the nth bit. Then the tags communicate bit n-1 to the reader and it goes through the same process as the nth bit. The same way is identified bit n-2 until bit 1. At

the end of this process, a whole tag has been identified. This tag is disabled so that it does not answer any longer during subsequent arbitrations. Each time a whole tag is identified, it is "put to sleep" and the whole process starts all over until all of the tags are identified.

Sometimes the tag may take tag longer to wake up or it can never wake up. To avoid this problem, Generation 2 does not use the sleep or quiet state, but two states—A and B. If the reader decides to interrogate only A tags, as it interrogates them it changes their state to B. Now it reads all B tags and changes their state to A. That way the reader knows how many tags it read. This method is called AB Symmetry.

To identify each tag, Generation 2 uses Q algorithm. Gen 2 tags have the ability to generate random numbers. The reader will tell the tags the range in which they should generate a random number by issuing a query command with a Q value ranging from 0 to 15. If it gets back no response to its queries, it will automatically decrease the Q value. If it gets more than one tag responding, it will increase the Q value, thereby increasing the range of numbers that can be generated by the tags. This method is quite complex to be explained in detail in this book but it is good to know that it assures that the reader is talking only to the tags that it intends to.

Collisions and Anticollision Methods

When two or more tags respond simultaneously, this is known as a collision. Anticollision processing is the means by which the interrogator distinguishes one tag from the others so only one tag is processed at a time.

It is important to know when collisions occur and the methods the interrogators use to avoid collisions.

Anticollision algorithms are commonly classified as either *probabilistic* or *deterministic*.

In probabilistic algorithms (also called *asynchronous*), the tags respond at randomly generated times. There are several variations of probabilistic algorithms, depending on the amount of control the interrogator has over the tags. Many of them are based on the ALOHA scheme in networking. This scheme involves a node transmitting a data packet after receiving a data packet. If a collision occurs, a node becomes saturated and transmits the packet again after a random delay. The interrogator keeps transmitting until the collision does not happen. The times at which interrogators can respond

can be slotted or continuous. This mode makes slight restriction in the transmission independence of individual data packets. If packet collisions happen under slotted ALOHA mode, the packets overlap completely, and that considerably increases the data transfer.

In deterministic algorithms (also called *synchronous*), the interrogator sorts through the tags based on their unique identification number (UID). The tags do not have to rely on a complete collision-free transmission and do not have to take turns communicating to the interrogator. The simplest deterministic scheme is the binary tree/tree-walking scheme, in which the interrogator searches the tree of all possible identification numbers. This search is quite time consuming, and it is based on the knowledge of the tag's UID. At each node in the tree, the interrogator checks for responses. Only tags whose identifier is a child of the checked node respond. The lack of a response implies that the subtree is empty. The presence of a response gives the interrogator an indication as to where to search next.

There are two other common types of anticollision algorithms, FM0 and Miller Subcarrier.

- FM0 is currently used in ISO standards. This algorithm is fast but more susceptible to interference.
- Miller Subcarrier is slower but better in RF noisy environments and is supported by Generation 2 readers. This algorithm uses narrow spectrum for the tags to send back their signal and fits it between the channels used by the reader. That way the RF signals coming from the reader do not cover the signals coming back from the tags. Miller Subcarrier uses advanced filtering techniques to separate the tag's response from the reader's transmissions and other noise compared to FM0.

Reader Commands

The five basic command operations to manage tag populations are

- **Select**—This command is used to determine which groups of tags will respond. Prior to conduction of an inventory, a Select command makes it possible to conditionally isolate only tags with desired characteristics such as a particular date code, manufacturer code, or others. By targeting only a certain segment of EPC memory containing this description, readers can easily sort through the tag population and access just a certain group of tags within its field.

For the tag data and parts of tag memory, refer to the Chapter 9, where these topics are discussed in detail.

- **Inventory**—This command is used to identify (singulate) individual tags from a group.
- **Access**—This command is used after the tags have been singulated and individual commands can now be addressed to those tags. Access commands allow the interrogator to write individual tag memory fields directly (with EPC and/or password data), lock the tag, or kill the tag.
- **Lock**—This command allows a reader to lock individual passwords, preventing subsequent reads or writes, or lock individual memory banks, preventing subsequent writes.
- **Kill**—This command permanently disables a tag from talking back to a reader, which renders the tag inoperative. This feature can be used to address privacy concerns; however, the Kill command also can be issued maliciously. To prevent unauthorized kills, this command will become password protected as soon as the specifications have been defined for killing a tag.

All of the above mentioned commands should be supported by Generation 2 readers. Generation 1 readers usually do not support certain commands such as Kill and Lock. That differs, however, by manufacturer and version.

RFID Antennas

RFID antennas are always connected to an interrogator. This allows for the transmission of signals to and from the tag.

Antenna Design

Depending on the design, antennas can be either *mono-static* or *bi-static:*

- **Mono-static antennas** are based on a principle by which a single antenna transmits a signal coming from the interrogator to the area as well as receives a signal coming from tags and these functions are switched in fractions of seconds. This requires use of a circulator in a reader that multiplexes the receive and transmit signals through a single port. There is some loss and phase distortion due to the use of a circulator.

- **Bi-static antennas** include two antennas, where one antenna is dedicated to transmitting, and the other antenna is dedicated to receiving. Both dedicated antennas can be but do not have to be in the same casing. In bi-static antenna, a circulator is not required, which improves the performance and sensitivity of the antenna.

Antenna Polarity

Antenna polarity is very important because it affects the quality of communication between the interrogator and tag.

The interrogator's antenna and the tag's antenna should have the same polarization. If polarization is not realized, a severe loss in signal, along with a drastic decrease in a read range, which results in unsuccessful communication with a tag, can be experienced.

Polarization can be either circular or linear. Linear polarization is relative to the surface of the earth. Linear polarization can also be either *horizontal* or *vertical:*

- Horizontally polarized signals propagate parallel to the earth.
- Vertically polarized signals propagate perpendicular to the earth.

Antennas with circular polarization can receive signals from both the vertical and horizontal planes by injecting the signal at two points on the antenna radiated slightly out of phase creating a rotating effect on the field. However, there is a slight loss of signal strength, due to the constructive and deconstructive effect of the field being slightly out of phase.

Where the tag's orientation can be assured, using a linear polarized antenna is better because the coherent wave of the signal and lack of phase distortion increases the likelihood of communicating with the tag.

Antenna Installation Considerations

Because RFID tags are subject to RF anomalies and orientation issues, it is often desirable to use several antennas grouped together and controlled by a common interrogator.

In supply chain applications, portals and tunnels are the commonly used configurations. Energizing and reading RFID tags are exercises in probability, in which the probability has to be maximized to increase the likelihood that a

given RFID tag will be in the field of an interrogator's signal long enough that it can be read.

RFID Portals

The best way to understand how an RFID portal works is through its typical application—for instance, in a warehouse where a forklift is moving inventory through a dock door. As the fork truck removes a pallet of goods from a truck at a receiving dock, the antennas on the portal are positioned such that the RFID tags on the pallet pass through the signal from the interrogator. The antennas of the portal may be connected to a single RFID interrogator, or each antenna can connect to its own individual interrogator. They are application dependent. An example of an antenna portal is shown in Figure 3.2.

In Figure 3.3, notice the four antennas. There are gaps in the coverage. These gaps may be acceptable if you are positive of the tag's placement relative to the antennas of the portal—for example, if you are certain that the tags on all the products that go through the portal are at the same height and location every time they go through the portal.

When RFID antennas are installed, the installation efforts should aim to create a *sweet spot*. A sweet spot is a volume of space where the likelihood of communication with RFID tags is maximized. Ensure that you create a portal sweet spot when designing your portal.

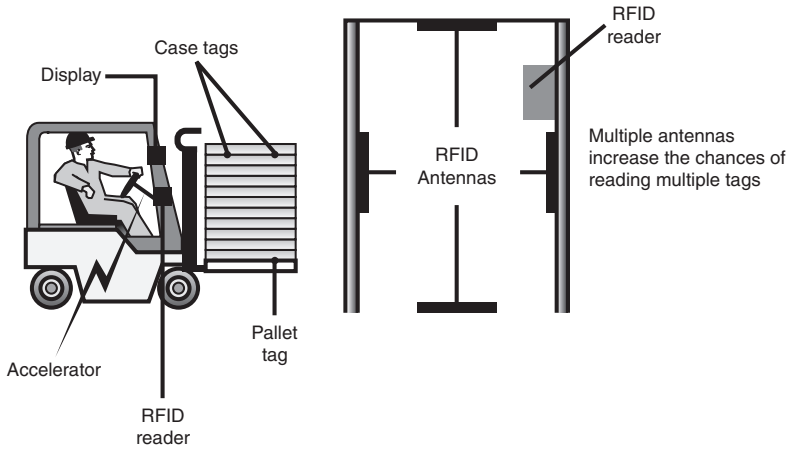

Figure 3.2 RFID antenna portal.

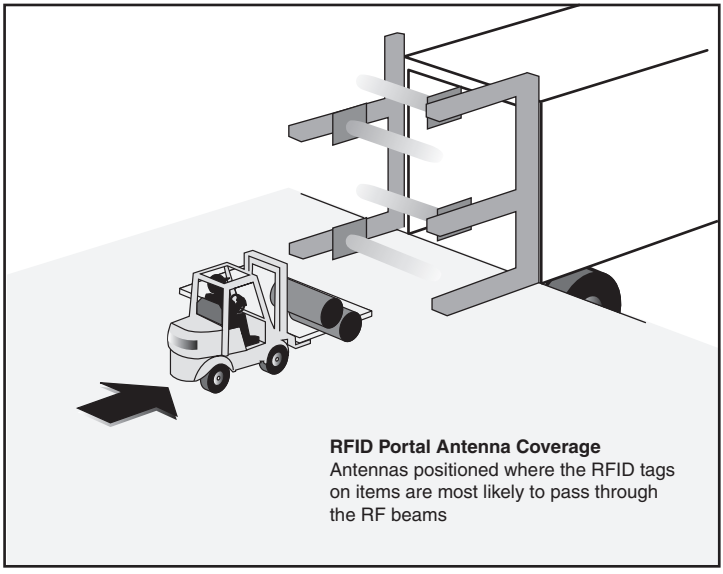

Figure 3.3 Dock door RFID antenna portal.

As discussed earlier, an RFID tag, once energized, requires a certain amount of time to power up and respond. It is important that the RF energy that is energizing the tag remain at a level sufficient to sustain the tag's functionality until it has successfully retrieved data from or to store data in to its memory. Because the tag can be powered only when it is in the beam of the RFID antenna(s), the tag must remain in the beam long enough for the required operations to occur. This is known as *dwell time* or *time in beam*. If the dwell time is too short, the tag may power down prematurely, and the read or write operation will not be completed. One way to maximize the tag's time in beam is to position the antennas so that the sweet spot is as large as is practical.

Dwell times differ, depending on the operation being performed. Read operations are completed quickly, but writing to tags can take much longer. The time required for write operations in contrast to the time needed for read operations can be as much as 5 times longer.

RFID Tunnels

RFID tunnels are a variation on the portal theme and are typically used with conveyor systems.

Tunnels are often enclosed in RF-absorptive material, such as anechoic material. This is called a *Faraday cage*. Enclosing the tunnel this way helps contain the RF signal that is concentrating the RF energy.

A tunnel reduces the power output requirement of the interrogator. However, it can accidentally energize a tag on an item on a different conveyor by mistake. Therefore, care must be taken when planning and constructing a tunnel.

As with portals, multiple antennas increase the read probability in a tunnel. The enclosure helps to contain and concentrate the RF energy. Properly constructed enclosures also help keep the interrogators on one conveyor from interfering with the interrogators on another conveyor.

If you choose not to use a tunnel, proper antenna placement and attenuation in conjunction with a conveyor can produce similar results.

When you are installing interrogation zones, it is important to consider all the factors that are involved so that the best choice of antenna arrays can be made to maximize the number of tags that are successfully interrogated when passing through the interrogation zone.

Imperfections in an Antenna's Coverage

Holes can be caused by a number of factors:

- Reflections of RF energy interfering with the radiated wave field (multipath)
- Imperfections in the antenna's reflector
- Interference from external sources

By using several overlapping wave fields, you can counter interference with any one wave, which is called multi-path interference. This can cause null points (holes) as well as points with very strong RF signal or noise.

Moving the tagged item through the wave field ensures that the tag does not stay in a hole for very long.

Antenna Field Calculations

There are several calculations regarding the antenna field that you may perform to understand the antenna performance based on power input and other variables. In this section, we discuss antenna gain and loss calculations, free space loss, effective radiated power, and field density calculations.

Antenna Gain and Loss

An *antenna gain* is achieved by focusing the radiated RF into narrower patterns to get more power coming from the antenna in the required direction, as illustrated in Figure 3.4.

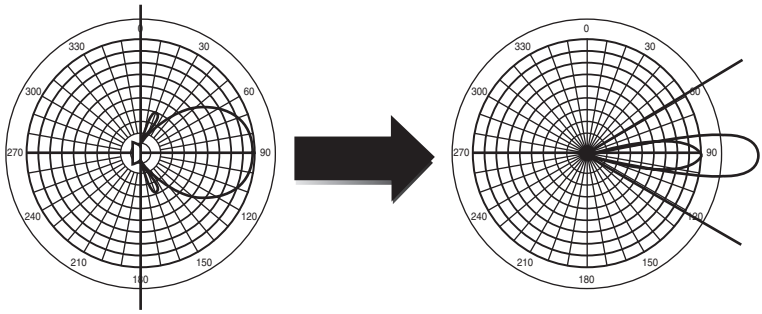

Figure 3.4 Antenna gain.

Antenna gain is the relative increase in radiation at the maximum point expressed as a value in decibels (dB) above a reference—in this case, the basic antenna, a half-wavelength dipole by which all other antennas are measured. The reference is known as 0 dBD (zero decibels referenced to dipole):

Antenna gain in dBD = 10**log* (*Power output/Power input*)

An antenna with the effective radiated power of twice the input power would therefore have a gain of 10**log* (2/1) = 3dBD. Therefore, if you know the power output and input, you can find out the gain or "efficiency" of an antenna.

Another reference used in antenna gain figures helps to give an antenna an appearance of higher gain than what the antenna is truly rated. It is known as *dBi* and represents a gain of an antenna over the value rate of an isotropic antenna. An isotropic antenna radiates equally in a spherical pattern, or equally radiated in all directions. It gives an antenna a 2.14 dB boost:

Antenna gain in dBi = antenna gain in dBd + 2.14

Effective Radiated Power (ERP)

There are several definitions of effective radiated power from an antenna. The most common definition of effective radiated power is the power supplied to an antenna multiplied by the antenna gain in a given direction,

or as the product of the power supplied to the antenna and its gain relative to a half-wave dipole in a given direction:

ERP (dBm) = Power of transmitter (dBm) – loss in transmission line (dB) + antenna gain in dBd

Note that if the direction is not specified, the direction of maximum gain is assumed. The type of reference antenna also must be specified. A reference antenna can be real, virtual, or theoretical. Antenna examples are unit dipoles, half-wave dipoles, or isotropic, that is, omnidirectional antennas. If the cable loss is not specified, you should consider it zero.

The ERP value is frequently measured in watts.

Effective Isotropically Radiated Power (EIRP)

Effective isotropically radiated power is the arithmetic product of the power supplied to an antenna and its gain relative to an isotropic source:

EIRP (dBm) = Power of transmitter (dBm) – loss in transmission line (dB) + antenna gain in dBi

dBm = 10 *log(power out / 1mW)

Example: An antenna has a gain of 16 dBi, and the power delivered to the antenna is 100 milliwatts (0.1 watt). What is the effective isotropic radiated power?

100 mW equals to 20 dBm.

10 *log (100 mW/1 mW) = 10*2 = 20 dBm

EIRP = 20 + 16 = 36 dBm = 4 watts

To help you convert between watts and decibels, you can refer to table 3.2.

Table 3.2 RF Power Conversion

dBm = 10*log (x mW/1mW)		
Power in Watts	**Power in mW**	**Power in dBm**
4	4000	36
2	2000	33
1	1000	30
0.100	100	20
0.010	10	10
0.001	1	0

Beam Width

The generally accepted description of beam width is that it is the angle between two points on the same plane where the radiation falls to "half power," that is, 3dB below the point of maximum radiation.

Radiation Pattern

Radiation pattern is a graphical representation of the intensity of the radiation versus the angle from the perpendicular. The graph is usually circular, and the intensity is indicated by the distance from the center of the corresponding angle.

Component materials cannot create power; the only other alternative is to focus wasted energy using reflectors and bounce the radiated signal toward a more useful direction. The method by which an antenna is made to have "gain" is merely focusing the radiation (this is often compared to taking a doughnut and flattening it into a pancake), which makes the radiation more intensified toward one plane.

If a reflector is placed next to a dipole, all the energy that would have radiated in the direction of the reflector is now reflected back in the direction of the dipole. This makes all the energy appear in only one hemisphere and thus results in a doubling of radiated energy in this direction.

Further focusing can be achieved with the use of "directors," and again, by making the angle smaller and smaller (that is, packing all the radiation into one direction), higher gain is achieved. Achieving high gains may be practical in certain applications; however, the effective angle of such an antenna is therefore small.

Front-Back Ratio

In front-back ratio, the doughnut radiation pattern mentioned previously is achieved, and it is squeezed into a beam off the front of the antenna. The reflector used for focusing the beam does not stop all the radiated energy, and some is radiated toward the rear (or, in the case of reception, bypasses the reflector and is intercepted by the dipole). Even a solid sheet of metal as a reflector does not completely isolate the front from the rear because of *diffraction*. The tips of the metal cause some signal to "bend" on the edges of the reflector and toward the rear (or, in the case of reception, from the rear toward the dipole).

You need to be concerned not only about the antenna gain but also about the loss of signal in free space.

Free Space Loss

Free space loss is the power loss of a radio signal as it travels from the transmitter to the receiver through free space without other sources of loss such as reflections, cable, or connector loss. In the case of an RFID system, the free space loss would be the power loss of a radio signal as it travels from the interrogator's antenna to the tag. The gains from particular antennas are not taken into account.

The loss is caused by beam divergence, which is signal energy spreading over larger areas at increased distances from the source.

You do not need to memorize an exact equation to calculate the free space loss; however, it is important to know that the loss is proportional to the square of the distance between the transmitter and receiver (interrogator and tag) and proportional to the square of the frequency of the radio signal.

A free space loss can be expressed in dB as

$$FSL(dB) = 20 * log(d) + 20 * log(f) + K$$

where d is the distance, f is the frequency, *log* is to the base 10, and K is a constant that depends on the units used and details of the radio link.

Example: If d is measured in meters, f in Hz, and if the isotropic antennas are used, the expression becomes

$$FSL(dB) = 20 * log(d) + 20 * log(f) - 147.5$$

As an example, the FSL(dB) of a 1000 meter link operating at 1 gigahertz using isotropic antennas is 92.5 dB.

If d is measured in miles, f in MHz, and the isotropic antennas are used, the expression stays the same, except that the K equals 36.6. If the free space loss is based on nonisotropic antennas (dipole), the K equals 32.3.

A free space loss can be also calculated as

$$FSL\ (dB) = (4\pi R/\lambda)^2 = (4\pi Rf/c)^2$$

where R is the radius or the distance from the source of the signal, λ is signal wavelength, f is frequency. and c is the speed of light.

It is important to use consistent units; therefore, if the distance (d, R) is counted in meters, the speed of light (c) must be in meters per second.

An important concept to understand is that the loss of power over distance is *not* linear. So, for instance, if there is 3 dBi of power loss 2 feet from the antenna, there will not be 6 dBi of loss 4 feet from the antenna; the loss will be greater. Also, the amount of loss for the same distance (2 feet in this example) will be much greater the farther you are from the source because the field becomes less and less dense as you move away from the antenna.

Field Density

Field density or power density can be determined through a very complex mathematical calculation. The power density of an isotropic antenna is

$$P_D = \frac{P_t}{4\pi R^2}$$

where P_D is power density, P_t is transmitted power or power input to the antenna (either average or peak transmitted power depending on the approach), and R is the distance to the center of radiation.

The power density of a directional antenna is

$$P_D = \frac{P_t G_t}{4\pi R^2}$$

where G_t is the antenna gain.

A typical RFID professional does not need to perform these calculations regularly. Instead, you need a clear understanding of what field density is and how it relates to your interrogation zones.

Figure 3.5 depicts an antenna and three measurement areas. The closer to the antenna the measurement is taken, the higher the collected power is, because the RF field is denser at that point. Therefore, at the first point, the radiation collected for the measurement is higher than that collected at points 2 or 3.

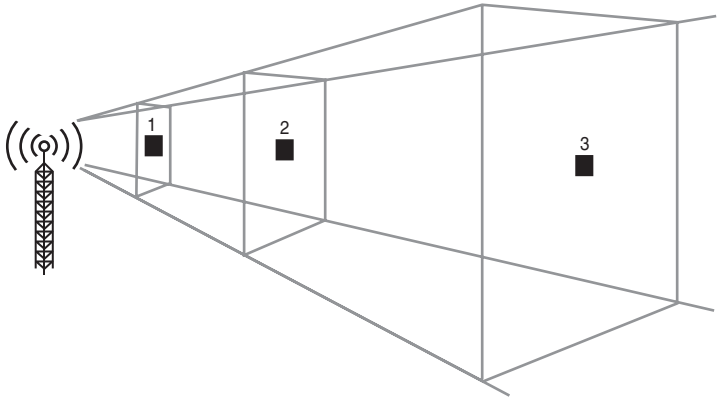

Figure 3.5 Field density.

If you think of this like a garden hose with a spray attachment on the end, 6 inches from the sprayer, the water is very close together, or dense. The farther you get from that sprayer, the wider the water disperses, leaving more and more room for air between the water, making the spray less dense. This is exactly the phenomena seen in RF field density.

Exam Prep Questions

1. An RFID interrogator is also called an
   - ❑ A. RFID radiator
   - ❑ B. RFID tag
   - ❑ C. RFID reader
   - ❑ D. RFID transistor
2. When are the anticollision protocols used?
   - ❑ A. To avoid the collisions between vehicle-mounted interrogators
   - ❑ B. To avoid the collisions that can occur when multiple readers attempt to read the same RFID tag
   - ❑ C. To avoid the collisions that can occur when multiple tags respond to the interrogation at the same time
   - ❑ D. To avoid the collisions between the data sent through the RFID system network
3. Which is not a part of an RFID interrogator?
   - ❑ A. Power amplifier
   - ❑ B. Controller/processor
   - ❑ C. Inlay
   - ❑ D. Oscillator
4. What are the kinds of polarity of RFID antennas?
   - ❑ A. Circular
   - ❑ B. Horizontal linear
   - ❑ C. Vertical circular
   - ❑ D. Vertical linear
5. What is the difference between bi-static and mono-static antennas?
   - ❑ A. A mono-static antenna radiates power only in one direction, whereas a bi-static antenna is omnidirectional.
   - ❑ B. A mono-static antenna performs a transmitting function as well as a receiving function, whereas a bi-static antenna includes two antennas sometimes within one case, including separate receiving and transmitting antennas.
   - ❑ C. A mono-static antenna requires AC power input, whereas a bi-static antenna requires DC power input.
   - ❑ D. A mono-static antenna is only one antenna in a case, whereas a bi-static antenna also includes two side antennas next to the main antenna in the case.
6. What is the relation between reading and writing to a tag?
   - ❑ A. Reading takes less time than writing to a tag.
   - ❑ B. Writing to a tag takes less time than reading the tag.
   - ❑ C. Reading and writing both require the same time.
   - ❑ D. The time ratio of writing to a tag and reading the tag depends on the frequency at which the interrogator operates.

7. What is an antenna gain?
   - ❑ A. An antenna, due to its design, radiates the RF signal stronger than the power input. This is called antenna gain.
   - ❑ B. Antenna gain is calculated as the power gained from the reader multiplied by the operating frequency of the reader.
   - ❑ C. Antenna gain is achieved by focusing the radiated RF signal into narrower patterns to get more power coming from the antenna in the required direction.
   - ❑ D. Antenna gain is achieved by focusing the radiated RF signal into wider patterns because the antenna gain is measured as the size of the area where the signal is present.
8. When is the likelihood of communication with a tag maximized?
   - ❑ A. When the tag is placed as close to the antenna as possible
   - ❑ B. When the tag is placed in the antenna sweet spot
   - ❑ C. When the tag is static and is in the antenna's radiation field
   - ❑ D. When the tag is moving through the antenna's radiation field
9. When using a multiplexer, why use solid state circuitry for switching?
   - ❑ A. Mechanical switching is too costly and requires a huge amount of space.
   - ❑ B. Solid state circuitry is smaller and requires less space.
   - ❑ C. Due to the extreme volume of switching required, a mechanical switch would not be feasible because the switching would occur many times a second; therefore, the wear and stress on the mechanical switch would be too great for reliability.
   - ❑ D. Solid state circuitry can withstand abuse better than a mechanical switch.
10. What is a Faraday cage?
    - ❑ A. The term *Faraday cage* refers to the construction of the portal with the sides and top being made of mesh materials so that the signal can travel in all directions.
    - ❑ B. The meaning of the term *Faraday cage* originated from the town Faraday, Louisiana, where local shipping agents needed to have a way of packaging products that would not be readable by interrogators. The cage was constructed of metal that would reflect the antenna's signal, causing interference.
    - ❑ C. A Faraday cage is a tunnel enclosed in RF-reflective material, such as sheet metal. This helps contain the RF signal inside the tunnel.
    - ❑ D. A Faraday cage is a device that holds a package on a conveyor system in order to be assured of an accurate read.

Answers to Exam Prep Questions

1. Answer C is correct. RFID interrogators are commonly called RFID readers. This name prevails from the past when the function of this device was limited to purely reading the tag's ID. An RFID interrogator is not called an RFID radiator or RFID transistor because these names are not established in RFID but in different technologies. Therefore, answers A and D are incorrect. An RFID interrogator is not called an RFID tag because that is another part of the whole RFID system. Therefore, answer B is also incorrect.

2. Answer C is correct. The anticollision protocols are not used for collisions between vehicle-mounted interrogators. These must be avoided by proper operation of the vehicles on which these devices are mounted. Therefore, answer A is incorrect. The problems created by multiple readers operating in the same environment are solved by a dense interrogation mode or synchronization methods. And data moving through an RFID system is a network management issue. Therefore, answers B and D are incorrect.

3. Answer C is correct. An inlay is not a part of an RFID interrogator but is part of an RFID tag. The power amplifier, controller/processor, and oscillator are parts of the RFID interrogator; therefore, answers A, B, and D are incorrect.

4. Answers A, B, and D are correct. No antenna polarities are classified as vertical circular because the circular polarization is not orientation sensitive and is not referenced to a plane. Therefore, answer C is incorrect.

5. Answer B is correct. The mono-static antenna is based on a principle by which a single antenna works as a transmitter as well as a receiver, and these functions are switched in fractions of seconds. A bi-static antenna includes two antennas that can be within one case or separated. One antenna is dedicated to transmitting, and the other antenna is dedicated to receiving. This implies that answer D is incorrect. Answer A is incorrect because the names of antennas in this case have nothing to do with the radiation direction. Answer C is also incorrect because the antenna gets the power from the reader, and the AC or DC power has nothing to do with the antenna design.

6. Answer A is correct. Reading the data on a tag takes less time than writing the data to a tag; therefore, answers B and C are incorrect. The ratio of the reading and writing time does not depend on the frequency at which the readers operate; therefore, answer D is also incorrect.

7. Answer C is correct. An antenna does not create power to radiate a stronger signal. Therefore, answer A is incorrect. Antenna gain is calculated as 10 times the logarithm of the power output to power input ratio; therefore, answer B is incorrect. Antenna gain is not achieved by focusing the radiated RF signal into wider patterns but narrower patterns; therefore, answer D is incorrect.

8. Answer B is correct. The probability of communication with the tag is in the sweet spot, which is usually not immediately at the antenna. Some interrogators/antennas require a certain distance between the antenna and the tag when reading and writing the tag, to achieve a better communication, or because the tag could be damaged when too close to the antenna. Therefore, answer A is incorrect. It is always better if the tag in the antenna's field moves because this would prevent the possibility of the tag staying in a hole of antenna coverage, where it could not be interrogated. Therefore, answer C is incorrect. Because it is always better for the tag to be moving through the field, this option could be the right answer; however, for successful reading and mainly writing tags, the tag needs to be in the field for a certain time. If it moves too fast and stays in the field for too short a time, the communication could be unsuccessful; therefore, answer D is incorrect.

9. Answer C is correct. The amount of switching required using a multiplexer would render a mechanical switch useless not only because of the wear the switch would undergo, but by the sheer volume of switching required to ascertain accurate reads. Answers A, B, and D are all true but not the correct answers. It is the capability of the solid state circuitry to switch rapidly each time with no moving parts that makes it a better option. Therefore, A, B, and D are not correct answers.

10. Answer C is correct. Although A could be viewed as the correct answer, mesh metal would not give the required advantage of reading the tagged materials on a conveyor system because it would not reflect or focus the radiated signal on the projected area. Answer B is not correct. Answer D also is not correct; if a device was to hold the package until a successful read was achieved, it would not work well with a high-speed conveyor system.

Need to Know More?

Technical notes: http://www.ti.com/rfid/docs/technotes.shtml

Free space field and loss calculations: http://www.softwright.com/faq/engineering/Free%20Space%20Field%20and%20Loss%20Calculations.html

Calculations: Free Space Loss: http://www.terabeam.com/support/calculations/free-space-loss.php

Free Space Loss Calculations: http://www.maxstream.net/helpdesk/article-13

Effective Isotropically Radiated Power (EIRP): http://www.rfcafe.com/references/electrical/eirp.htm

Effective Isotropically-Radiated Power: http://www.answers.com/topic/effective-isotropically-radiated-power?method=6