Guide to Wireless Communications, Third Edition

Chapter 11
Radio Frequency Identification

Objectives

- Define Radio Frequency Identification (RFID) and Near Field Communication (NFC)
- Explain the need for RFID
- Describe how RFID and NFC work
- List the components of an RFID or NFC system
- Explain the challenges of RFID

What is RFID?

- Radio frequency identification (RFID)
  - Technology similar to barcode labels
  - Uses RF waves instead of laser light to read the product code
  - Stores product information in electronic tags
    - That contain an antenna and a chip
- EPCglobal Inc.
  - Establishes RFID standards and services for real-time, automatic identification of information
    - In the supply chain of any company

What is RFID?

- EPCglobal Inc. (cont'd)
  - Adopts the ISO 18000 series of standards for RFID
    - Including the frequencies and PHY and MAC layer specifications
  - Concentrates on defining services and higher layer functions of the standards

RFID System Components

- Components required to implement an RFID system:
  - Tags
  - Antennas
  - Readers
  - Software
  - EPCglobal Network services

Electronic Product Code (EPC)

- Electronic Product Code (EPC)
  - Standardized numbering scheme
  - Can be programmed in a tag and attached to any physical product
  - Unique number or code associated with each item
    - So that it can be identified electronically
  - EPCs usually represented in hexadecimal notation
  - EPC is either 64 or 96 bits long

Figure 11-1 96-bit Electronic Product Code (EPC)

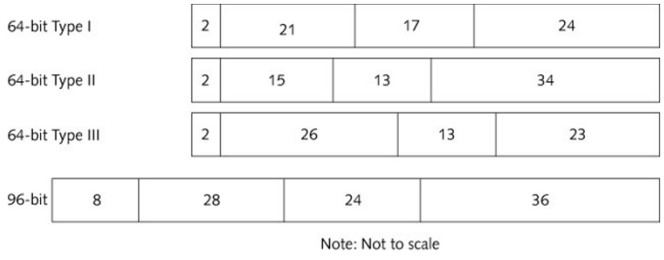

Figure 11-2 Structure of EPC

RFID Tags

- RFID tags
  - Commonly known as **transponders**
    - A combination of *transmitter* and *responder*
  - Includes an integrated circuit
    - Contains some non-volatile memory and a simple microprocessor
  - Can store data that is transmitted in response to an interrogation from a **reader**
    - Device that captures and processes the data received from the tags

RFID Tags

- Basic types of tags
  - Passive tags (most common type)
    - They are small, can be produced in large quantities at low cost, and do not require battery power
    - Use the electromagnetic energy in the RF waves
  - Active tags
    - Equipped with a battery
    - Can transmit the signal farther away
    - Have a limited life due to the battery
    - Beacons transmit on a periodic basis

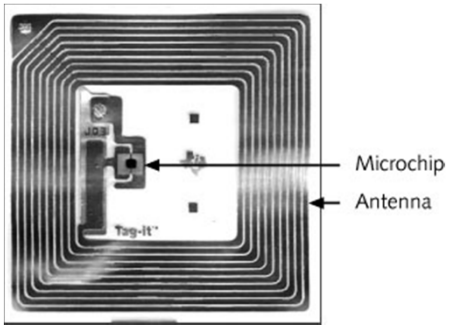

Figure 11-3 A typical RFID passive tag

RFID Tags

- Basic types of tags (cont'd)
  - Semi-active tags
    - Uses a built-in battery to power the circuit only when a reader first energizes the tag
- Size of the memory in a tag varies between 16 bits and hundreds of kilobits
- Tags are initially programmed with a unique identification code obtained from EPCglobal
- Smart labels
  - Flexible RFID tag packages

RFID Tags

- Smart labels (cont'd)
  - Can be read regardless of their position or orientation
    - Major advantage of RFID over bar codes
- 1-bit tags
  - Passive devices used in retail stores
  - Do not contain a unique identification code, a chip, or any memory
  - Simply used to activate an alarm
- Chipless tags (known as RF fibers)
  - Use fibers or materials that reflect a portion of the reader's signal back

RFID Tags

- Sensory tags
  - Can be equipped with various kinds of sensors to monitor and record environmental information
    - Can monitor attempts to tamper with a product
- Cost of a tag can vary greatly
  - Depending on type and number of tags purchased
- There are four classes of tags
  - See table on following slide

Tag Class	Type	Characteristics and Options
Class-1	Passive; identity tags	Includes EPC, tag identifier (ID), and a destroy password (discussed later in the chapter) May include optional password-protected access control and user memory
Class-2	Passive; higher functionality	Includes all features of Class-1 plus: extended tag ID, extended user memory, authenticated access control, and additional features to be defined in Class-2 specification (see EPCglobal)
Class-3	Battery-assisted passive (also called semi-active or semi-passive)	Includes all features of Class-2 plus: a power source May include sensors with optional data-logging capabilities
Class-4	Active	Includes EPC, extended tag ID, authenticated access control, power source, autonomous transmitter (can initiate communications with a reader if the protocol in use permits, but must not interfere with Class-1, Class-2, and Class-3 communication protocols) May optionally include user memory and optional sensors with or without data logging

Table 11-1 EPCglobal tag specifications

Readers

- Readers (also called interrogators)
  - Devices that connect with the company's network and transfer data obtained from the tags to a computer
  - Some readers can also write data onto tags
  - Readers that work with passive tags also provide energy that activates the tags
  - Read distance is determined by the size and location of the tag and the reader antennas
    - As well as the amount of power transmitted

Frequency Band	Common Applications
Low Frequency (LF)—135 KHz	Animal identification, access control, industrial automation
High Frequency (HF)—13.56 MHz	Smart cards, books, clothing, luggage, and various other individual-item-racking applications
Ultra High Frequency (UHF)—433 MHz and 860–930 MHz	Asset tracking, inventory control, warehouse management
Microwaves—2.45 and 5.8 GHz (ISM band)	Electronic toll collection, access control, industrial automation

Table 11-2 RFID frequencies and common applications

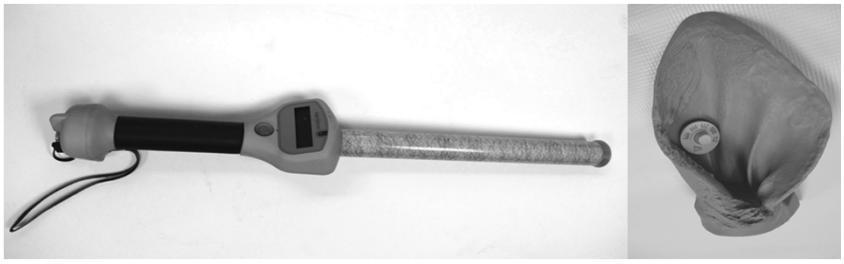

Figure 11-5 LF RFID reader and tag used by cattle farmers to track animals

Antennas

- RFID antennas used in tags may be limited in size due to the dimensions of the tag itself
- Types of antennas
  - Linear: offer greater range but less accurate reads
  - Circular: have greater read accuracy, especially in applications in which the orientation of the antenna varies
    - Have a more limited range

Antennas

- Larger antennas allow the tags to be read at greater distances
  - As frequency increases, the wavelength gets smaller as does the antenna
- Higher frequency antennas can be made relatively small
  - And still allow the tags to be read at greater distances
- Reader antennas have to be designed for the specific type of application
- No “typical” style of RFID antenna exists

Figure 11-7 RFID tags in many shapes and sizes

Software

- Type of software depends on the specific RFID application
- Categories of software components
  - System software: used to control hardware functions, implement communication protocols, and control data flow between tags and readers
  - Middleware: responsible for reformatting data from readers to business applications
  - Business application software: responsible for processing orders, inventory, shipments, invoices, etc…

EPCglobal Network Service

- EPCglobal Network Service
  - EPC reduces need for cross-referencing
- Object Name Service (ONS)
  - A mechanism for discovering information about a product and related services
  - When a reader gets the EPC from a tag:
    - Passes it to the company's servers, which send it to ONS via the Internet
    - ONS identifies the manufacturer and responds with the URL of the server where product information is stored

EPCglobal Network Service

- EPC Information Services (EPCIS)
  - Will enable large organizations to purchase, invoice, and track product orders over the Internet
  - Will eliminate the need to send paper documents by mail or fax
  - Similar to the Electronic Data Interchange (EDI) specifications that many large companies use to complete paperless transactions

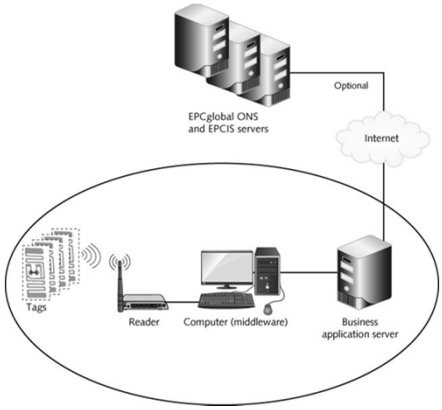

Figure 11-8 Fundamental EPCglobal system components

How RFID Works

- Tags and readers use different transmission mechanisms in each frequency band
- This section of the text introduces the technical details of how two of the most common types of passive tags and readers communicate
  - UHF (400 to 900 MHz)
  - HF (13.56 MHz)

PHY Layer

- Coupling
  - The connection between a passive tag and reader
- Two types of coupling
  - Inductive or magnetic coupling: designed for tags that touch the surface of the antenna or are inserted in a slot in reader's case
  - Backscatter coupling: designed for tags that can be read at distances from 3.3 feet up to 330 feet
- Backscatter is a reflection of radiation

PHY Layer

- Continuous wave (CW)
  - An unmodulated sine wave
  - Used to supply power to the tag
- Backscatter modulation
  - Based on ASK or a combination of ASK and PSK
- Reader has separate transmitter and receiver circuits
- Reader and tag modulate the signal in amplitude
  - By as much as 100% or by as little as 10%

PHY Layer

- Communications are always half-duplex (do not transmit and receive data simultaneously)
  - To prevent interference issues
  - To allow for environments in which multiple readers are installed in the same area
    - Called dense interrogator environments
- EPCglobal standards also specify the use of:
  - Frequency hopping spread spectrum (FHSS)
  - Direct sequence spread spectrum (DSSS)
    - Generally only used for advanced active tags

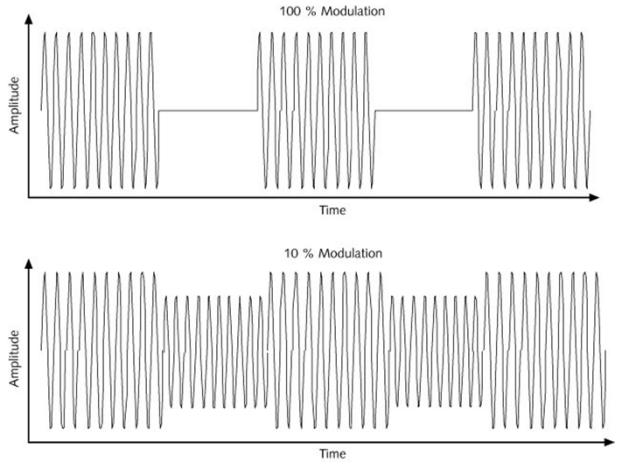

Figure 11-9 ASK modulation

HF Tag Communication

- HF RFID transmission uses a protocol called Slotted Terminating Adaptive Collection (STAC)
  - Tags reply within randomly selected positions or time intervals (slots)
  - Interrogator transmits signals to mark the beginning and end of each slot
- Slots are not equal in size
- Number of slots is regulated by the interrogator
  - And is always a power of two

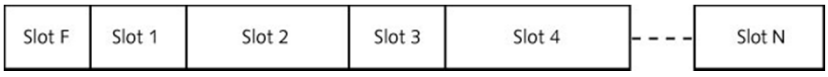

Figure 11-10 Reply intervals in the STAC protocol

UHF Tag Communication

- UHF readers today support Generation 2 (Gen2) protocols
- The Gen2 protocol defines three techniques for communication between tags and readers
  - First technique: reader selects tags by transmitting a bit mask that isolates a tag or group of tags
  - Second technique: reader can inventory tags by isolating them using a repetitive process
  - Third technique: reader can alternatively access each tag individually (once the EPC for a particular tag is known to the system)

Tag Identification Layer

- Defines three methods to manage the population of tags within reach of reader's signal
  - Select
    - Interrogator can send a series of commands to select a particular segment
  - Inventory
    - Interrogator sends out a series of query commands to get information from one tag at a time
  - Access
    - Interrogator can send one or more commands to multiple tags or a single tag at a time

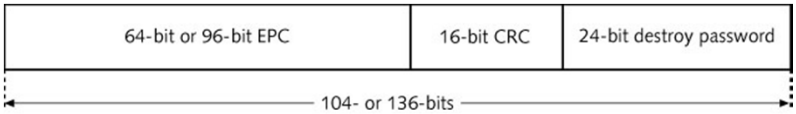

Figure 11-11 Structure of tag information

Tag Identification Layer

- Minimum amount of information contained in a tag's memory:
  - EPC
  - 16-bit cyclic redundancy check (CRC)
  - Destroy password
- Destroy password
  - Code programmed into the tag during manufacturing
  - Once transmitted, tag is permanently disabled and can never be read or written to again

Tag and Reader Collisions

- Tags may respond to a reader at the same time
  - Would result in collisions
- LF tags and readers do not support any collision-handling mechanism
- Tag collision handling in UHF
  - Reader sends a VerifyID command
  - Tags reply with EPC, CRC, and destroy password
  - Reader proceeds to select a range of tags
  - Process repeats until the reader has identified every group of tags

Tag and Reader Collisions

- Tag collision handling in HF
  - Each tag uses its EPC, CRC, and destroy password
    - To calculate a number that becomes the slot number in which each particular tag will reply
  - Calculation based on parameters sent by the reader
- Reader collisions
  - If a reader does not receive any replies:
    - It assumes a reader collision has occurred
    - Backs off for a random period of time

MAC Layer

- Responsible for establishing and communicating the transmission parameters, such as:
  - Transmission bit rate
  - Modulation type
  - Operating frequency range
  - Frequency hop channel sequence
- MAC layer parameters for different types of tags differ

Data Rates

- Amount of data stored in a typical passive RFID tag is relatively small
- Data transmission rates for the tags are also low
- HF tag readers can read 200 tags per second
  - For tags containing just an EPC, the actual rates will likely be between 500 and 800 tags per second
- UHF specifications define the tag-to-reader data rate as twice that of the reader-to-tag
  - Tag-to-reader data rate can be up to 140.35 Kbps

Near-Field Communications

- Near Field Communications (NFC)
  - Technology that provides short-range wireless connectivity between devices such as smartphones and tablet computers
  - Based on the ISO 18092 RFID technology standard
  - Requires little or no configuration by users
    - Devices connect automatically as soon as they are brought to within a minimum of 1.6 inches of each other
  - Able to transfer data between devices or read passive tags at rates of 106 to 424 Kbps

Near-Field Communications

- Examples of NFC uses with handheld devices:
  - MasterCard PayPass and Visa payWave transactions
  - Electronic discount coupons
  - Exchanging business cards, schedules, and maps
  - Transferring images, videos, and other files
  - Debit card or prepaid card transactions
  - Electronic public transport system tickets
  - Airline tickets
  - Pairing Bluetooth devices without entering a PIN

NFC Operation Modes

- Listen mode – initial mode of an NFC device
- Poll mode – probes for other devices within range
- Reader/writer mode – when an NFC device in Poll mode behaves like an interrogator
- Card emulator mode – when an NFC device in Listen mode behaves like a smart card
- Initiator mode – when an NFC device in Poll mode changes the communication protocol to talk to another device
- Target mode – when an NFC device is the target of an initiator that can only use half-duplex mode

NFC Communications

- NFC-capable devices transmit in the 13.56 MHz unlicensed frequency band
  - Modulate the signal using ASK or a combination of ASK and PSK
  - Modulation varies between 10 percent and 100 percent
- To transfer data between two smartphones or tablet computers, NFC employs the Data Exchange Protocol (NFC-DEP)

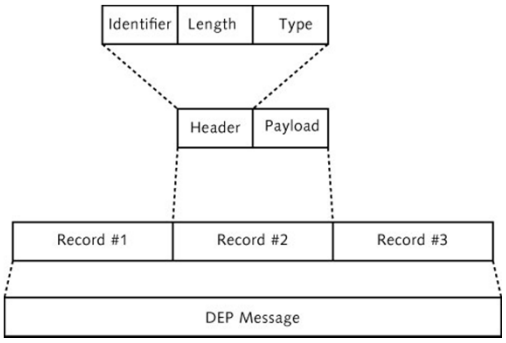

Figure 11-12 Structure of a DEP message

RFID Applications

- The potential uses for RFID are practically unlimited
- The following section outlines a few interesting RFID applications

Automobile Security

- Immobilizer
  - Car antitheft device
- Vehicle's ignition key head contains a tiny Class 1 RFID chip
  - Transmits in the 135 KHz frequency band
  - Only the original key can start the vehicle

Health Care

- RFID tags in a patient's identification bracelet
  - Provides vital information that cannot be easily misplaced
    - Patient's admission history
    - Blood type
    - Medications and prescribed dosages
  - Can sound alarm if patient leaves a designated area
- Newborn babies and their mothers can wear bracelets that contain matching information

Transportation and Military

- RFID tags embedded in standard courier packages
  - Can speed up and help automate sorting, in addition to preventing errors
- The U.S. Department of Defense (DoD)
  - Uses RFID tags to control, handle and ship its inventory

Sports and Entertainment

- RFID tags are used for monitoring tire pressure in race cars
  - Can be used in transport trucks and interstate buses
- Monitoring participants in marathons and triathlons is another common use for RFID tags
- Passive tags can be installed inside golf balls
  - In case they are lost during a game
- In 2004, the Golden Globe awards used RFID tags in the event invitations

People Monitoring, Crowds, and Access

- Parents of children wearing special bracelets containing RFID tags
  - Can instantly locate their kids if they become separated
- RFID-tagged concert and sports event tickets can simplify the jobs of security personnel

Pharmaceuticals

- Pharmaceutical industry is vulnerable to counterfeit drugs
  - RFID tags can help track products
  - Tracking can help isolate the exact location of counterfeiting activity
- Tags in over-the-counter and prescription medication
  - Allow vision-impaired people using a special device to listen to a description of their drugs and dosages

RFID and NFC Challenges

- RFID and NFC technologies face some challenges
- You will learn about some of these challenges in the following section

RFID Impact on Corporate Networks

- One of the major challenges for the implementation of RFID systems:
  - The impact of the volume of data on a company's network
- RFID systems are usually implemented so that inventory can be counted by simply activating the tags
- Some systems may direct readers to interrogate all RFID tags every 5 minutes or so
  - This scanning can add a lot of traffic to a network

Network Availability in RFID

- Network availability is a serious factor in the store's ability to serve its customers
  - To increase service and reduce costs, greater network bandwidth must be available
    - And the network must be reliable

Storage Requirements for RFID

- The huge volume of data that can be generated by RFID systems significantly increases the need to store information accurately and reliably
  - Large banks and corporations have to archive tremendous amounts of historical data
  - New laws designed to protect investors and consumers require companies to accumulate and store even more information

Device Management

- Even without RFID in place, businesses find it a challenge to manage the huge numbers of devices on their networks
- The need to remotely monitor and manage RFID readers from a central location becomes a critical factor
  - Add to this the task of managing and tracking millions of RFID tags

Security Considerations for RFID and NFC

- Use of RFID devices has generated a large number of security and privacy concerns
  - In the United States, in particular, the concerns are centered on privacy
- Security related to RFID readers falls under the wired network security policy
  - Reader-to-tag communications have the same vulnerabilities as any wireless network
- Passive tags do not support authorization or encryption security methods

Security Considerations for RFID and NFC

- Data in tags can be locked
  - Require a password for the tag to be used again
- Blocker tag
  - Device that can be used to simulate the presence of a virtually infinite number of tags
  - Can disable unauthorized readers from accessing the information from a selective group of tags

Summary

- Radio frequency identification (RFID) stores information in electronic tags
- Standards being published by EPCglobal Inc. will allow RFID to be used worldwide
- RFID systems components: electronic tags, readers, antennas, software, and EPCglobal network services
- RFID tags are also known as transponders
- Tags can be produced in flexible packages called smart labels

Summary

- 1-bit tags are passive devices used in retail stores to prevent theft
- Sensory tags are equipped with thermal, smoke, or other type of sensors
- A reader or interrogator communicates with both the tags and the corporate network
- Two types of tag antennas: linear and circular
- RFID software includes system software, middleware, and business applications

Summary

- RFID has a multitude of uses ranging from healthcare to entertainment-related applications
- Coupling: connection between a reader and a tag
- In HF, the tags use time slots to communicate with the reader
- RFID has the potential for significantly increasing the amount of traffic and storage requirements
- NFC allows enabled devices to communicate in short distances
- There are many security and privacy concerns with RFID and NFC