UNIT-3

Security Considerations to Wireless Devices: Wireless Device Security Issues, Physical Security, Information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistants (PDAS), Wireless Infrastructure **Wireless Technologies and Applications:** Introduction to Cellular Networks- FDMA, TDMA, CDMA, Spread Spectrum Primer, Analogy, TDMA Vs CDMA, PDC, Security Threats.

Security Considerations to Wireless Devices:

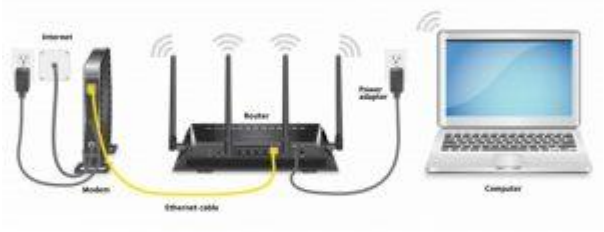
Wireless device security Issues, Physical Security, information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistance, Wireless Infrastructure

Wireless Standards and Technologies:

Introduction to Cellular Networks: FDMA, TDMA, CDMA, Spread Spectrum, OFDM, CURRENT and FUTURE Standards—IEEE 802 Standards, ETSI, Home RF, Ultra-Wide band Radio(UWB)

WHAT IS A WIRELESS DEVICE?

A wireless device is a device that uses radio waves to send or receive information. Wireless devices can be used for communication, such as in phones, tablets, and computers. They can also be used for entertainment, such as in gaming systems and home theater systems. Wireless devices use different frequencies to send and receive information.



THE WIRELESS REVOLUTION

Wireless technology has revolutionized the way we communicate and access information. Wireless devices allow us to connect to the internet, share files, and stay in touch with friends without having to be connected to a cable or phone line. Wireless devices are also becoming increasingly popular for gaming and entertainment purposes.

The wireless revolution

WIRELESS NETWORKING AND WI-FI

Wireless networking is the process of using radio waves to connect devices that are too far apart to be directly connected with cables. Wireless networking is common in homes and small offices, where it’s more convenient and less expensive than using cables.

Wireless Networking and Wi-Fi

Wi-Fi is a type of wireless networking that uses radio waves to connect devices that are within range of each other. Wi-Fi networks use the same frequency as the radios in your computer, phone, or other devices. This means that you can easily connect to a Wi-Fi network without installing any extra software.

WHAT ARE THE DIFFERENT TYPES OF WIRELESS DEVICES?

Wireless devices use radio waves to send and receive information. There are different types of wireless devices, each with its own advantages and disadvantages.

What Are the Different Types of Wireless Devices

WIRELESS ROUTER

A wireless router is a device that allows users to connect to the internet wirelessly. Wireless routers are often found in homes, offices, and schools. They come in a variety of shapes and sizes and can be used for a variety of purposes, such as connecting devices such as laptops, tablets, and smartphones to the internet, sharing files between devices on the same network, or extending the range of a wireless network.

WIRELESS REPEATER

A wireless repeater is a device that amplifies or retransmits signals over a short distance using radio waves. Repeaters are used to extend the range of wireless devices, such as cell phones, laptops and PDAs, in an area where the signal is weak or nonexistent. They can also be used to amplify transmissions from one location to another.

WIRELESS ADAPTERS

Wireless adapters are hardware devices that allow a computer to connect to a wireless network. Wireless adapters come in several different types, including card-based and USB adapters. Card-based adapters are inserted into the computer's PCI or PCIe slots and connect to the computer's networking ports. USB adapters connect directly to the computer's USB ports.

Wireless networks use radio waves to transmit data. Most wireless networks use2 GHz frequency bands because they’re less congested than other frequency bands and they travel farther than networks using5 GHz frequencies. 2 GHz frequency bands are also used by the 802.11b, g, n, and ac standards for wireless networking devices.

WIRELESS PHONES

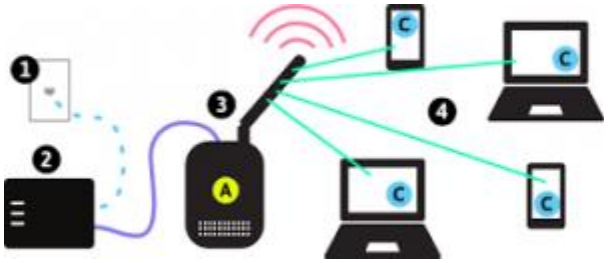
Wireless devices use radio waves to communicate without the need for a physical connection. Cell phone networks, Wi-Fi networks, and Bluetooth signals are all examples of wireless technologies.

Wireless devices can be used for a variety of purposes, including communication, gaming, navigation, and music streaming. Many wireless devices also have capabilities that are unique to that particular device. For example, a cell phone can be used to make calls and text messages, but it can also be used for navigation purposes thanks to its built-in GPS system.

Wireless technology is constantly evolving and improving. New wireless technologies are being developed all the time, and existing ones are becoming more powerful and versatile. Wireless devices will continue to become more popular as they become increasingly versatile and practical.

WIRELESS DEVICES EXAMPLES

Wireless devices are devices that use wireless technology to send and receive data. Wireless technologies can include radio waves, microwaves, infrared signals, and light waves. Wireless devices can be used for a variety of purposes, including communication, navigation, security, and entertainment. Wireless devices can be powered by batteries or by a nearby electrical outlet.



Wireless Devices Examples

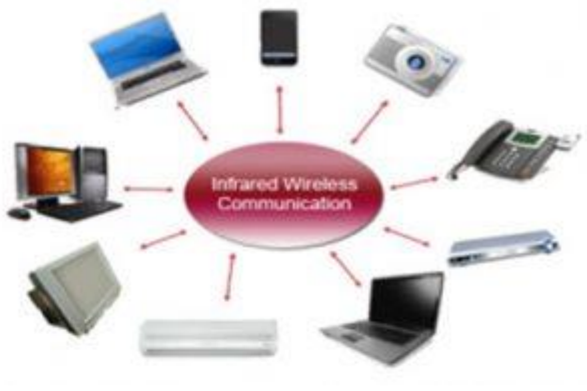
HOW DO WIRELESS DEVICES WORK?

When you think about electronics, you likely think about wires. But there are other ways to connect devices, like with radio waves. Wireless devices use radio waves to transmit data without having to use cables.

Radio waves are invisible, so they travel through walls and other objects without being blocked. That means wireless devices can be placed anywhere in a room without worrying about obstructions.

There are a few different types of wireless signals: Wi-Fi (which is used in homes and businesses), Bluetooth (which is used for connecting accessories like speakers and headphones), and cellular (for connecting phones to the internet). Each type of signal has its own strengths and weaknesses, so it's important to choose the right one for the task at hand.

LIST OF WIRELESS DEVICES



List of Wireless Devices

Wireless devices use radio waves to connect to devices without having to plug in. Wireless devices can be used for a variety of things, like connecting your phone to the internet, streaming music, or checking your email. There are a lot of different wireless devices out there, so it can be hard to decide which one is right for you. Here are some examples:

COMUNICATION EQUIPMENT

A wireless communication device is an electronic device that allows two or more devices to communicate with each other wirelessly. Wireless devices include cell phones, laptops, tablets, and other portable electronics. Wireless devices are often used to communicate with people in faraway places, as well as with people who are nearby.

HOUSEHOLD ITEMS

When it comes to household items, there are a few that come to mind that use wireless technology. One example is a hair dryer. Most hair dryers now come with a wireless connection so you can control the settings from anywhere in the house. Another example is a remote control for your television. These days, most televisions have remotes that use wireless technology to send commands from across the room.

Computer Peripherals

Computer peripherals include devices that are used to input or output data, such as keyboards, mice, touchpad’s, and trackballs. Many computer peripherals also have buttons or switches that allow the user to control how the device works. Peripherals can be connected to a computer using a cable or wireless connection.

Security Concerns

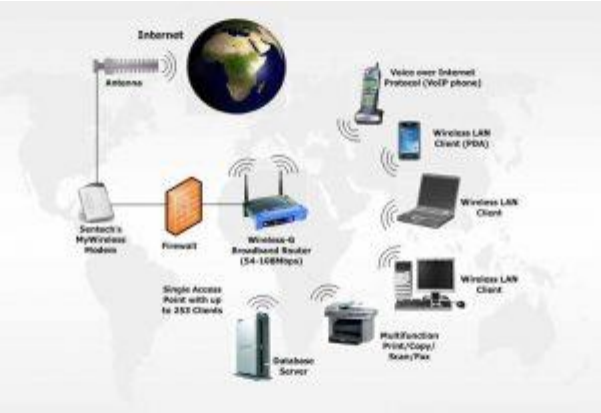
A wireless device is susceptible to security concerns. Wireless devices are vulnerable to being hacked and are often targets for thieves. This is because a wireless device does not require a physical connection to the internet in order to work, which makes it an easy target for thieves. Additionally, wireless devices can be monitored by third parties without the user’s knowledge or consent, which can be intrusive and scary.

What are The Advantages of Wireless Devices?

Wireless devices are advantageous because they do not require an outlet or cord to work. They can be placed anywhere in a room without taking up any space, and they are very easy to use. Wireless devices allow for more freedom in movement because there is no need to worry about getting tangled up in cords. They also have a longer battery life than traditional devices, which means that you can use them for longer periods of time without having to recharge them.

What are The Disadvantages of Wireless Devices?

Wireless devices present a number of security and privacy concerns. Wireless networks are notoriously insecure, as anyone within range can access your data. In addition, wireless devices can be tracked by third parties, even when they are not connected to the internet. Finally, many wireless devices emit electromagnetic radiation that may be harmful to your health.


Internet
Antenna
Voice over Internet Protocol (VoIP phone)
Wireless LAN Client (PDA)
Sentech's MyWireless Modem
Firewall
Wireless-G Broadband Router (54-108Mbps)
Wireless LAN Client
Wireless LAN Client
Single Access Point with up to 253 Clients
Multifunction Print/Copy/ Scan/Fax
Database Server

Introduction to Physical Security

These days, tips on how to strengthen your cyber security follow the announcement of every another cyber attack. Don’t forget to backup your data, apply patches over vulnerabilities, monitor firewalls, etc. It is very important to remember that software is not your only weapon when it comes to cyber security. Physical Cyber Security is another tier in your line of defense.

According to Goldstein(2016), Physical Security is critical, especially for small business that does not have many resources to devote to security personnel and tools as opposed to larger firms. When it comes to Physical Security, the same principles apply here:

- Identify and classify your assets and resources.
- Identify plausible threats.
- Identify probable vulnerabilities that threats may exploit.
- Identify the expected cost in case if an attack occurs.

Factors on which Physical Security Depends

1. How many workplaces, buildings or sites are there in an organization?
2. Size of the building of the organization?
3. How many employees are employed in the organization?
4. How many entry and exit points are there in the organization?
5. Points of placement of data centers and other confidential information.

Layers of Physical Security

Layers in Physical Security are implemented at the perimeter and are moving towards an asset. The layers are as follows:

1. Deterrence

The goal of Deterrence methods is to convince a potential attacker that a successful attack is not possible due to strong defenses. For example: By placing your keys inside a highly secure key control system made up of heavy metal like steel, you can help prevent attackers from gaining access to assets. *Deterrence methods are classified into 4 categories:*

- **Physical Barriers:** These include fences, walls, vehicle barriers, etc. They also act as a Psychological deterrent by defining the perimeter of the facility and making intrusion seem more difficult.
- **Combination Barriers:** These are designed to defeat defined threats. This is a part of building codes as well as fire codes.
- **Natural Surveillance:** In this architects seek to build places that are more open and visible to authorized users and security personnel so that attackers are unable to perform the unauthorized activity without being seen. For example- decreasing the amount of dense and tall vegetation.
- **Security Lighting:** Doors, gates or other means of the entrance should be well lit as Intruders are less likely to enter well-lit areas. Keep mind to place lighting in a manner, that is difficult to tamper.

2. Detection

If you are using the manual key control system, you have no way of knowing the exact timestamp of when an unauthorized user requested a key or has exceeded its time limit. Detection methods can of the following types:

- **Alarm Systems and Sensors:** Alarm systems can be installed to alert security personnel in case of an attempt of unauthorized access. They consist of sensors like perimeter sensors, motion sensors, etc.
- **Video Surveillance:** Surveillance cameras can be used for detection if an attack has already occurred and a camera is placed at the point of attack. Recorded video can be used

3. Access Control

These methods are used to monitor and control the traffic through specific access points. Access Control includes the following methods:

- **Mechanical Access Control Systems:** These includes gates, doors, locks, etc.
- **Electronic Access Control:** These are used to monitor and control larger populations, controlling for user life cycles, dates and individual access points.
- **Identification System and access policies:** These includes the use of policies, procedures and processes to manage the access into the restricted area.

4. Security Personnel

They play a central role in all layers of security. They perform many functions like:

- Administering electronic access control.
- Responding to alarms.
- Monitoring and analyzing video footage and many more

Countermeasures and Protection Techniques

1. Protection against Dumpster Diving

Dumpster Diving is the process of finding some useful information about the person or business from the trash that can later be used for hacking purpose. Since the information is in the trash, it is not useful for the owner but deemed useful to the picker. To protect against it, you need to follow certain measures:

- Ensure all important documents are shredded and they are still secure.
- Destroy any CDs/ DVDs containing personal data.
- Make sure that nobody can walk into your building and simply steal your garbage and should have safe disposal policy.
- Firewalls can be used to prevent suspicious users from accessing the discarded data.

2. Employee Awareness Training

A negligent employee can be one of the major causes of a Cyber security breach. Employee awareness training sessions can help in such cases. Employee awareness training should focus on one underlying theme- *avoid the SEP- Somebody else’s problem field.*

3. Site Access Control

Lack of Access Control can be highly devastating if a wrong person gets in and gets access to sensitive information. Fortunately nowadays, you have a number of modern tools that will help you to optimize your access control.

- **Envoy** is a tool that will help you to expand access to guests in controlled manner.
- **Open Path** is a mobile system that allows access to only a limited set of people within the directory using smart phones and other devices.

4. Securing Your Windows

If you have the data that hackers would love to get their hands on, they will try any method and might just look through the window. Make sure you are aware of the sight angles to position your screens and other devices. Overlooking from different sight angles to see your credentials is known as *Shoulder Surfing.*

5. Secure Network-Enabled Printers

Network Printers are a very convenient option allowing anyone in the office to get connected, without a need of extra wiring. Unfortunately, they have underlying security risks also. Sometimes, due to default settings, they offer open WiFi access, thus allowing anyone to get in and open vulnerabilities in the process.

- Only connect those to the Internet that actually needs to be.
- Remote access is not necessary for scenarios where only people from your office use the printer.
- You can add passwords to the connection if necessary.

6. Securing Your Backups

Physical backups are critical for business continuity, helping you prevent data loss in the event of disasters, outages, and more. Most businesses secure their servers but they forget that backups are equally important. They are holding the same level of sensitive data as servers. Treat your backups as you treat your sensitive information and secure them.

7. Building Secure Guest Wi-Fi

Guest Wi-Fi is a natural solution when you have guests or visitors. Here are a few tricks to help protect your resources from the external users:

- Segment your network- In this way, it isolates Guest Wi-Fi from your internal devices and data.
- Encrypt your wireless signals and change the default passwords of all devices on the network.

8. Locking up your Servers

Any area in your organization that stores data need to be secured. Locking doors and making sure server area gets extra protection.

9. Accounting for Loss or Stolen Devices

As devices are becoming more mobile, chances for them being stolen or falling out of someone’s pocket becomes more frequent. Mobile Device Management can help you to manage such situations and take the necessary precautions. The best solution in such cases is to simply lock down and potentially wipe any lost or stolen devices from the organization remotely.

10. Implementing video systems

To achieve more secure premises, it is advisable to use a Video Surveillance system.

- Mere presence of cameras can deter potential attackers.
- Availability of video footage allows you to have continuous monitoring over the entire premises.
- If an attack happens, you can check the recorded video, easily reconcile the process and catch the perpetrator.

What is Data Leakage?

Data leakage, also referred to as low-profile data theft, involves the unauthorized transfer of electronic or physical data from an organization to external recipients or destinations. Threat actors often leak data using email accounts or the web. They may also use mobile data storage devices like USB keys, laptops, and optical media.

Data leakage can result from purposeful insider action meant to cause harm to the organization, or as part of a bigger scheme to commit payment fraud. It can also be accidental. Cybercriminals look for various types of information in data leaks, including customer information and trade secrets. The scope and the type of leak determines the damage caused to the organization.

This article is part of our series of articles about endpoint security.

Causes of Information Leakage

Here are common causes of information leaks at organizations:

Insider Threats

Insider threats include dissatisfied employees, former employees with access to sensitive systems, or business partners. Their motive may be economic gain, theft of valuable data, or a desire for revenge. Insiders can steal an organization's sensitive data for financial or personal gain.

Payment Fraud

Payment fraud is an attempt to make a fraudulent or illegal transaction. Common scenarios include credit card scams, false returns, and triangle scams. A triangle scam involves an attacker opening an online store with very low prices, tricking customers into providing their payment information, and then using this payment information to buy products at other stores.

Social Engineering

When data leaks are initiated by cybercriminals, they are usually the result of social engineering tactics. Social engineering is the use of psychological manipulation to trick victims into giving over sensitive information. Phishing is the most common type of social engineering attack. Traditionally phishing takes the form of a written message asking the user to provide confidential information or perform an action favorable to the attacker. Increasingly, phishing is performed over the phone (this is known as vishing).

Very often, attackers are after data that does not appear sensitive on its own, but can expand the list of potential victims. This poses a serious threat to data security, because attackers can easily deceive unsuspecting employees, by requesting seemingly harmless information such as phone numbers and social security numbers.

Physical Theft of Sensitive Devices

Company devices contain sensitive information, and misuse of these devices can lead to security breaches and theft of company information.

For example, a cybercriminal can use a stolen device to contact an IT administrator and claim that they have forgotten their login information. With a convincing strategy, attackers can breach the device and gain access to the corporate network.

Unintended Disclosure

Many data breaches are not caused by an attack, but rather by unintentional exposure of sensitive information. For example, employees might view sensitive data and save it to a non-secure location, or IT staff might mistakenly expose a sensitive internal server or cloud system to the Internet.

Malicious Electronic Communications

Many organizations give employees access to the Internet, email, and instant messaging, as part of their role. The problem is that all of these mediums are capable of file transfer or accessing external sources over public networks.

Attackers often target these communication channels and achieve a high success rate. For example, a cybercriminal could spoof a legitimate business email and simply ask an employee to send them sensitive data. If the user is fooled by the message, they could attach the requested files to the email and send them to the attacker.

What Do Cyber Criminals Look for in Data Leaks?

The majority of data leaks involve either personally identifiable information (PII) or protected health information (PHI). Examples of PII are names, social security numbers, and other personal details. PHI is defined in the US HIPAA regulation as any information about an individual’s health, now, in the past, or in the future.

Below are a few types of sensitive data that are commonly targeted in data leaks.

Customer Information

This is information about a company’s customers, including their names and contact details, credentials, activity history, and payment details.

What damage can it cause?

Exposure of customer information can damage both the company and its customers, cause harm to reputation, and in many cases expose a company to compliance violations and lawsuits.

Company Information

This is information revealing the company’s internal operations. It can include emails and internal documents; strategy, marketing, and business plans; and business metrics or forecasts.

What damage can it cause?

Exposure of company information can provide competitors, rivals, or attackers valuable data about a company’s operations. This can give third parties an unfair advantage over the company or help them cause direct damage to its operations. Attackers can also use it to plan secondary attacks.

Trade Secrets

This is possibly the most sensitive information a company can lose in a data leak, including intellectual property, plans for future products, source code, and details about proprietary technologies.

What damage can it cause?

Exposure of trade secrets can cause a company to lose large investments in research and development and make its market offering less valuable.

Analytics

This is data used by a business to derive insights about its customers or environment. This can include historical data about customers or prospects in the industry, demographic data, and models that can generate useful predictions in the company’s industry.

What damage can it cause?

Analytics is valuable to the business and so is equally valuable to an attacker. Like other types of data leaks it can give third parties an unfair advantage by exposing internal knowledge. If analytics data is not anonymized, it can have the additional impact of exposing PII.

How to Prevent Data Leakage

Ensure Timely Detection

You can avoid or reduce the fallout from a data leak by detecting improper activity fast. Ensure you receive alerts on changes to critical access or configuration parameters, and act quickly to investigate and remediate anomalies. Put in place monitoring for unusual data transfers, such as data loss prevention (DLP), and intervene early on if you discover users copying unusual amounts of data.

Classify Data according to Sensitivity and Value

To prevent data leaks, the first step is to identify which data employees are able to freely share. You should then decide who should have permission to access this data. Using data identification and classification, you can organize your data into categories, protecting sensitive data as required.

Here are a few technologies commonly used to protect sensitive data:

- Data Loss Prevention (DLP)
- Identity and access management (IAM)
- Encryption
- Privileged Access solutions
- Change management and auditing
- User and entity behavior analytics (UEBA)

Discover and Mitigate IT Risks

You can't discover your most vulnerable areas unless you periodically assess your risk. To implement successful risk management and risk assessment, you may wish to use an industry standard such as the National Institute of Standards and Technology (NIST). The NIST SP 800-30 document specifies the protocols for vulnerability assessment, which can help mitigate many risks leading to data leakage.

Discover more best practices in our detailed guide to data leakage prevention (coming soon)

Data Leakage Prevention with Perception Point

Perception Point provides enterprise-grade security to protect email, web browsers, cloud collaboration platforms and proprietary apps from all types of cyber attacks.

Enhanced browser-level DLP capabilities deter malicious insiders, partners and contractors and include:

- Clipboard controls (preventing copy and paste);
- Printing controls;
- Configurable download/upload restrictions;
- Watermarking;

- Smart blur of sensitive web apps/data to prevent accidental external screen capture and shoulder surfing
- User activity monitoring and visibility into all installed browser extensions across the organization
- SaaS app login visibility, enabling the organization's admins and security teams to view the usage of unsanctioned web apps

The all-included managed Incident Response service is available for all customers 24/7. Perception Point's team of cyber security experts will manage incidents, provide analysis and reporting, and optimize detection on-the-fly. The service drastically minimizes the need for internal IT or SOC team resources, reducing the time required to react and mitigate web-borne attacks by up to 75%.

Customers deploying the solution will experience fewer breaches, while providing their users with a better experience as they have the freedom to browse the web, use SaaS applications that they require, and access privileged corporate data, confidently, securely, and without added latency.

Wireless Network Infrastructure definition

Wireless Network Infrastructure (© vege / Fotolia.com)

Wireless networks are networks of computers and other smart devices that utilize a wireless data connection between nodes. This infrastructure today powers a great many of the services, entertainment and products that we rely on and so it pays to have a solid understanding of how it works and of the impact of wireless network infrastructures on your life and your business.

What is a Wireless Network?

Wireless networks are networks that allow for multiple devices to communicate with one another wirelessly and with no need for cables or connections. This is an incredibly useful and important tool and much of modern business, communication and entertainment depends on it.

Most of us have personal wireless networks at home and this depends on the infrastructure that has been put in place. This means that we can have multiple devices connected to the web at any given time, meaning that we might be using a computer upstairs to get work done and answer emails, while still being able to receive online messages through a mobile phone. It also allows us to communicate between devices *on* that wireless network. For instance, you might send a photo to your computer upstairs, or you might stream media to your television from your phone.

Wireless networks become even more important in a range of businesses and industries. Wireless networks are crucial for many companies to communicate internally and conveniently and to exchange information in a manner that is safe and secure. Likewise, wireless networks are used in a range of other institutions and organizations. Hospitals use wireless connections to communicate around the ward and to manage tools and important machinery. Schools and colleges have wireless networks for their students. Police, airlines, government and more all depend on wireless networks.

So with wireless networks being so ubiquitous and fundamental to our way of life, it seems pertinent to understand how they work!

How Do Wireless Networks Work?

So, in any telecommunications network, **nodes** are defined as redistribution points or communication endpoints. In the case of a physical network, nodes might be active electronic devices attached to that network – as long as they are capable of creating, receiving or transmitting information over a communications channel.

Passive distribution points such as patch panels are **therefore** not considered nodes (patch panels are used to connect and route circuits). In the case of **wireless network infrastructure**, nodes are computers, smartphones, games consoles, printers and of course the router itself. Routers, hubs or switches are considered **data communication equipment** whereas **data terminal equipment** includes the devices that we typically interact with.

Networks can be either LAN (**local area network**) or WAN (**wide area network**). WAN networks extend over large geographical distances and essentially allow for multiple LANs to be tied together to transmit communication. Businesses, schools and other organizations use WANs in order to communicate with their members. Likewise, leased telecommunication circuits can be used to form WANs. Even the internet itself can be considered WAN!

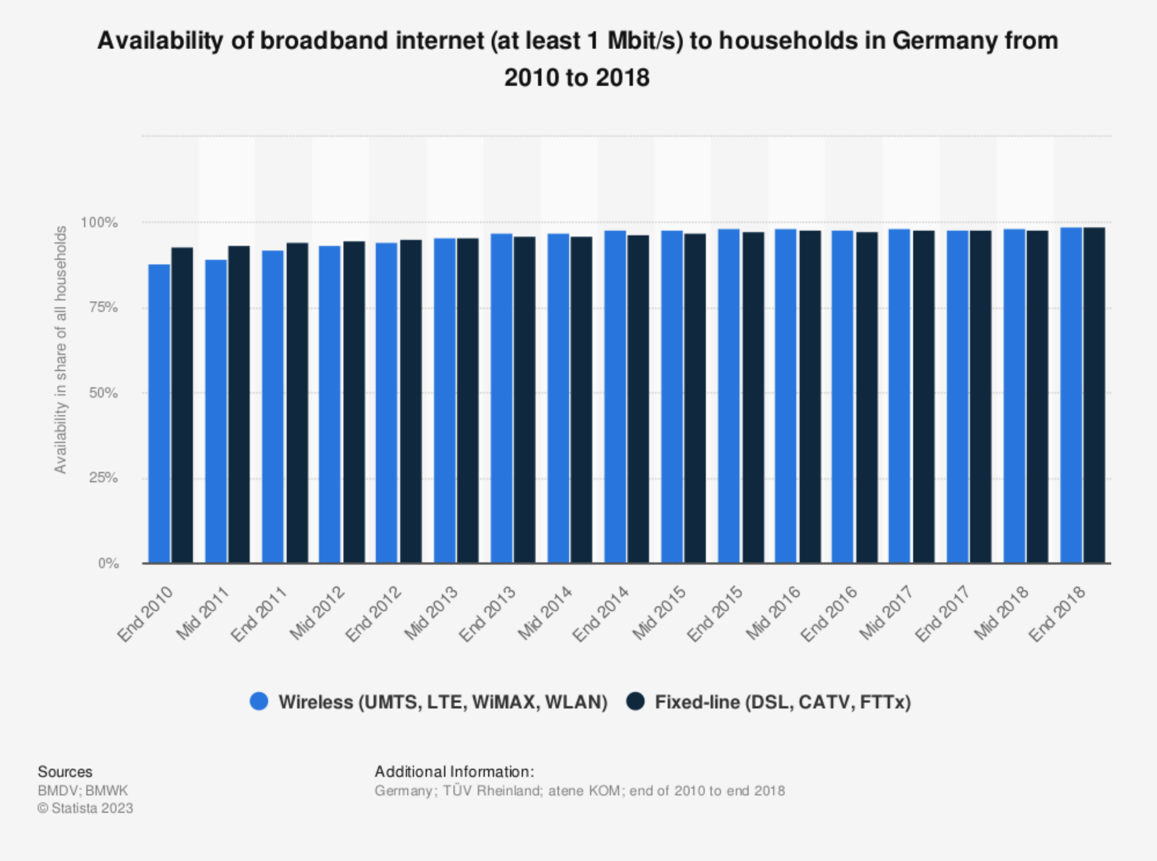
The internet network in your home is most likely a LAN network (for those devices plugged into ethernet ports or powerline adaptors) or a WLAN network (wireless LAN). These use OFDM or spread-spectrum technologies to provide connectivity to the network with no need for a wired connection.

The computers on these networks are described as **host computers** or **internet nodes** and will be given their own IP addresses. These IP addresses are unique to the private network and are called ‘private IP’ addresses. The router itself also has an IP, which is referred to as the ‘public IP address’.

From time to time, the private IPs of your devices will change around. This is handled by the DHCP or ‘**Dynamic Host Configuration Protocol**’. The public IP however will remain constant. This way, the router acts as a kind of conduit between the devices on your home private network and the internet outside. The router will be connected to a wired cable (perhaps fiber optic) and will then transmit and receive wireless signals to help you communicate with the outside world.

Services are used via specific ‘**ports**’ on the network, which are bound to IP addresses. Because computers are capable of running multiple programs at a time, multiple ports allow for a range of different data services to be carried out simultaneously.

DHCP I just one of several protocols that make up the standardised conceptual model that is the **internet protocol suite.** This series of protocols together provides a ‘model’ for how networks should be handled and managed on the web and on other computer networks. It is sometimes referred to as **TCP/IP** because the original protocols are the transmission control protocol and internet protocol.


Availability of broadband internet (at least 1 Mbit/s) to households in Germany from 2010 to 2018

Sources
BMDV; BMWK
© Statista 2023

Additional Information:
Germany; TÜV Rheinland; atene KOM; end of 2010 to end 2018

Find more statistics at Statista

Infrastructure

So, while the WLANs that you experience in your home are wireless by name, they still rely on a wired connection that connects the router to the wider internet (the WAN). The infrastructure provided by the local service providers and the council then, will almost certainly provide the limit or bottleneck for your connection speeds and stability.

Some of this will be outside of your control, but other aspects of your wireless infrastructure are your responsibility. For instance, making sure that you have the best router, using wired connections where convenient and tweaking the advanced settings of your router can help you to increase your speed and stability.

openPR-Tip: More importantly, it is up to you to protect your data and to keep your connections as private as possible. Recognize the danger of being on a public network such as coffee shop WiFi and don't access sensitive private information during this time.

Better yet, consider setting up a VPN or '**virtual private network**'. This works just like a LAN except it is entirely digitized and conceptual. Nevertheless, the IP address you put out to the world will be that of your VPN and *not* the physical location. This is called **spoofing** the physical location.

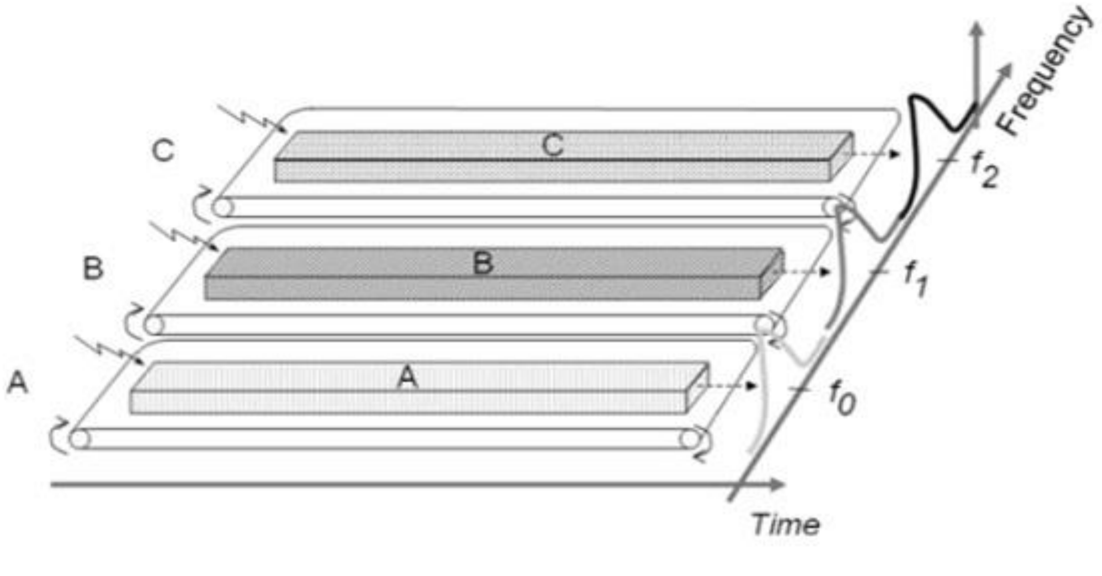
Wireless infrastructure has helped to bring us into the digital age and it will continue to have a transformative impact on our culture and economy. It's up to us to ensure the infrastructure is there and we are using it in a safe and responsibly manner.

Frequency Division Multiple Access (FDMA) is one of the most common analogue multiple access

methods. The frequency band is divided into channels of equal bandwidth so that each conversation is carried on a different frequency (*as shown in the figure below*).

FDMA Overview

In FDMA method, guard bands are used between the adjacent signal spectra to minimize crosstalk between the channels. A specific frequency band is given to one person, and it will received by identifying each of the frequency on the receiving end. It is often used in the first generation of analog mobile phone.



Advantages of FDMA

As FDMA systems use low bit rates (large symbol time) compared to average delay spread, it offers the following advantages −

- Reduces the bit rate information and the use of efficient numerical codes increases the capacity.

- It reduces the cost and lowers the inter symbol interference (ISI)
- Equalization is not necessary.
- An FDMA system can be easily implemented. A system can be configured so that the improvements in terms of speech encoder and bit rate reduction may be easily incorporated.
- Since the transmission is continuous, less number of bits are required for synchronization and framing.

Disadvantages of FDMA

Although FDMA offers several advantages, it has a few drawbacks as well, which are listed below −

- It does not differ significantly from analog systems; improving the capacity depends on the signal-to-interference reduction, or a signal-to-noise ratio (SNR).
- The maximum flow rate per channel is fixed and small.
- Guard bands lead to a waste of capacity.
- Hardware implies narrowband filters, which cannot be realized in VLSI and therefore increases the cost.

TDMA - Technology

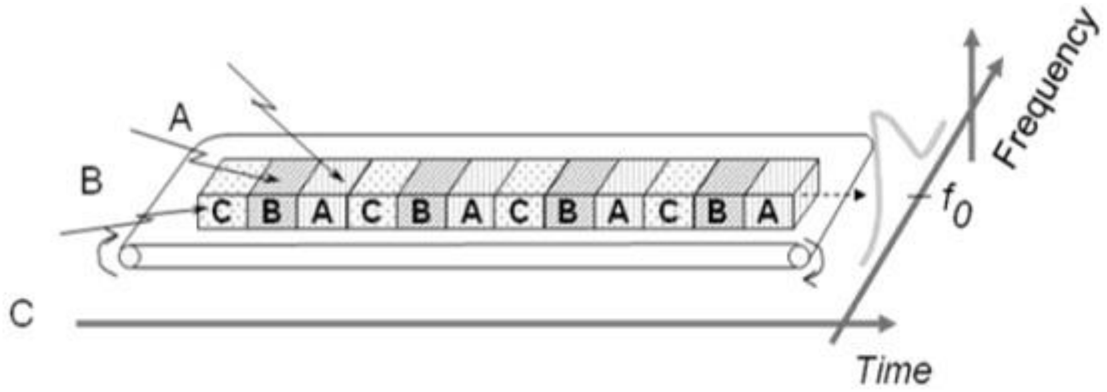
Time Division Multiple Access (TDMA) is a digital cellular telephone communication technology. It facilitates many users to share the same frequency without interference. Its technology divides a signal into different timeslots, and increases the data carrying capacity.

TDMA Overview

Time Division Multiple Access (TDMA) is a complex technology, because it requires an accurate synchronization between the transmitter and the receiver. TDMA is used in digital mobile radio systems. The individual mobile stations cyclically assign a frequency for the exclusive use of a time interval.

In most of the cases, the entire system bandwidth for an interval of time is not assigned to a station. However, the frequency of the system is divided into sub-bands, and TDMA is used for the multiple access in each sub-band. Sub-bands are known as **carrier frequencies**. The mobile system that uses this technique is referred as the **multi-carrier systems**.

In the following example, the frequency band has been shared by three users. Each user is assigned definite **timeslots** to send and receive data. In this example, user **'B'** sends after user **'A,'** and user **'C'** sends thereafter. In this way, the peak power becomes a problem and larger by the burst communication.



FDMA and TDMA

This is a multi-carrier TDMA system. A 25 MHz frequency range holds 124 single chains (carrier frequencies 200) bandwidth of each kHz; each of these frequency channels contains 8 TDMA conversation channels. Thus, the sequence of timeslots and frequencies assigned to a mobile station is the physical channels of a TDMA system. In each timeslot, the mobile station transmits a data packet.

The period of time assigned to a timeslot for a mobile station also determines the number of TDMA channels on a carrier frequency. The period of timeslots are combined in a so-called TDMA frame. TDMA signal transmitted on a carrier frequency usually requires more bandwidth than FDMA signal. Due to the use of multiple times, the gross data rate should be even higher.

Advantages of TDMA

Here is a list of few notable advantages of TDMA −

- Permits flexible rates (i.e. several slots can be assigned to a user, for example, each time interval translates 32Kbps, a user is assigned two 64 Kbps slots per frame).
- Can withstand gusty or variable bit rate traffic. Number of slots allocated to a user can be changed frame by frame (for example, two slots in the frame 1, three slots in the frame 2, one slot in the frame 3, frame 0 of the notches 4, etc.).
- No guard band required for the wideband system.

- No narrowband filter required for the wideband system.

Disadvantages of TDMA

The disadvantages of TDMA are as follow −

- High data rates of broadband systems require complex equalization.
- Due to the burst mode, a large number of additional bits are required for synchronization and supervision.
- Call time is needed in each slot to accommodate time to inaccuracies (due to clock instability).
- Electronics operating at high bit rates increase energy consumption.
- Complex signal processing is required to synchronize within short slots.

CDMA - Introduction

What is CDMA?

Code **D**ivision **M**ultiple **A**ccess (CDMA) is a digital cellular technology used for mobile

communication. CDMA is the base on which access methods such as cdmaOne, CDMA2000, and WCDMA are built. CDMA cellular systems are deemed superior to FDMA and TDMA, which is why CDMA plays a critical role in building efficient, robust, and secure radio communication systems.

A Simple Analogy

Let's take a simple analogy to understand the concept of CDMA. Assume we have a few students gathered in a classroom who would like to talk to each other simultaneously. Nothing would be audible if everyone starts speaking at the same time. Either they must take turns to speak or use different languages to communicate.

The second option is quite similar to CDMA — students speaking the same language can understand each other, while other languages are perceived as noise and rejected. Similarly, in radio CDMA, each group of users is given a shared code. Many codes occupy the same channel, but only those users associated with a particular code can communicate.

Salient Features of CDMA

CDMA, which is based on the spread spectrum technique has following salient features −

- In CDMA, every channel uses the full available spectrum.
- Individual conversations are encoded with a pseudo-random digital sequence and then transmitted using a wide frequency range.
- CDMA consistently provides better capacity for voice and data communications, allowing more subscribers to connect at any given time.
- CDMA is the common platform on which 3G technologies are built. For 3G, CDMA uses 1x EV-DO and EV-DV.

Third Generation Standards

CDMA2000 uses Frequency Division Duplexing-Multicarrier (FDD-MC) mode. Here, multicarrier implies N × 1.25 MHz channels overlaid on N existing IS-95 carriers or deployed on unoccupied spectrum. CDMA2000 includes −

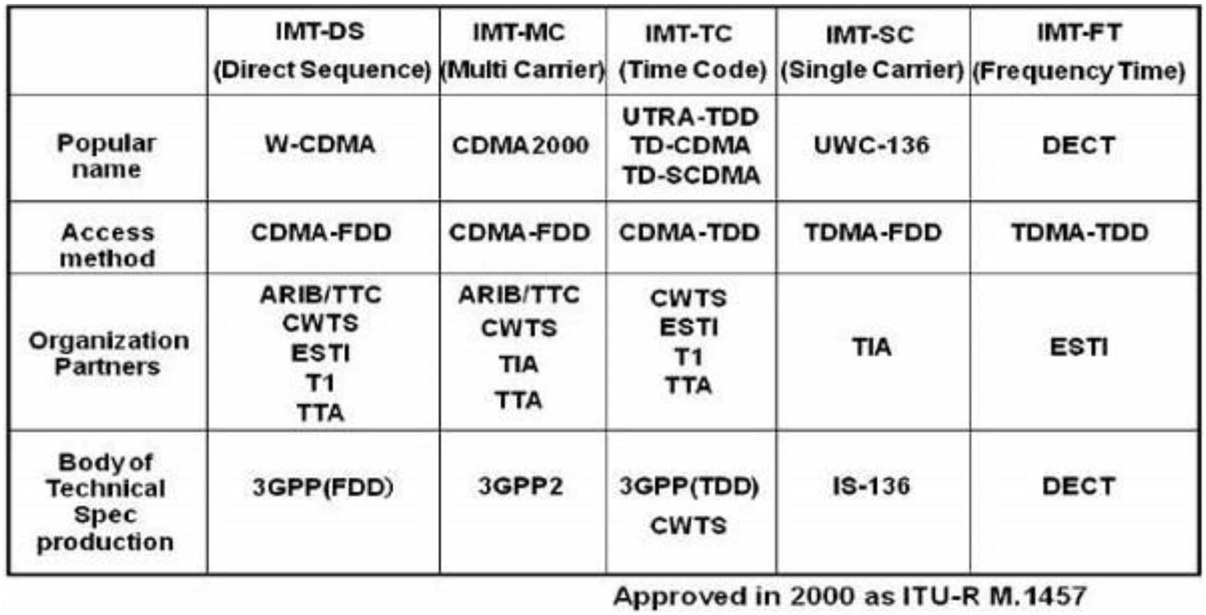
- 1x — uses a spreading rate of 1.2288 Mcps.
- 3x — uses a spreading rate of 3 × 1.2288 Mcps or 3.6864 Mcps.
- 1xEV-DO (1x Evolution – Data Optimized) — uses a spreading rate of 1.2288 Mcps, optimized for the data.
- WCDMA/FDD-DS — Wideband CDMA (WCDMA) Frequency Division Duplexing-Direct Sequence spreading (FDD-DS) mode. This has a single 5 MHz channel. WCDMA uses a single carrier per channel and employs a spreading rate of 3.84 Mcps.

CDMA Development Group (CDG)

The CDMA Development Group (CDG), founded in December 1993, is an international consortium of companies. It works together to lead the growth and evolution of advanced wireless telecommunication systems.

CDG is comprised of service providers, infrastructure manufacturers, device vendors, test equipment vendors, application developers, and content providers. Its members jointly define the technical requirements for the development of complementary systems CDMA2000 and 4G. Further, the interoperability with other emerging wireless technologies are meant to increase the availability of wireless products and services to consumers and businesses worldwide.

IMT-2000 System



	IMT-DS (Direct Sequence)	IMT-MC (Multi Carrier)	IMT-TC (Time Code)	IMT-SC (Single Carrier)	IMT-FT (Frequency Time)
Popular name	W-CDMA	CDMA2000	UTRA-TDD TD-CDMA TD-SCDMA	UWC-136	DECT
Access method	CDMA-FDD	CDMA-FDD	CDMA-TDD	TDMA-FDD	TDMA-TDD
Organization Partners	ARIB/TTC CWTS ESTI T1 TTA	ARIB/TTC CWTS TIA TTA	CWTS ESTI T1 TTA	TIA	ESTI
Body of Technical Spec production	3GPP(FDD)	3GPP2	3GPP(TDD) CWTS	IS-136	DECT

Approved in 2000 as ITU-R M.1457

CDMA - Channels

CDMA channels can be broadly categorized as Forward channel and Reverse channel. This chapter explains the functionalities of these channels.

Forward Channel

The Forward channel is the direction of the communication or mobile-to-cell downlink path. It includes the following channels −

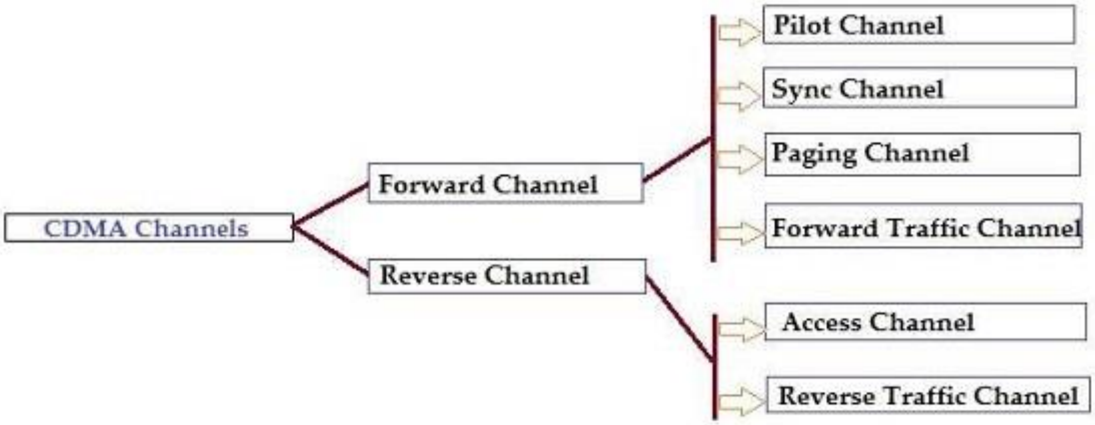
- **Pilot Channel** − Pilot channel is a reference channel. It uses the mobile station to acquire the time and as a phase reference for coherent demodulation. It is continuously transmitted by each base station on each active CDMA frequency. And, each mobile station tracks this signal continuously.
- **Sync Channel** − Synchronization channel carries a single, repeating message, which gives the information about the time and system configuration to the mobile station. Likewise, the mobile station can have the exact system time by the means of synchronizing to the short code.

- **Paging Channel** − Paging Channel's main objective is to send out pages, that is, notifications of incoming calls, to the mobile stations. The base station uses these pages to transmit system overhead information and mobile station specific messages.
- **Forward Traffic Channel** − Forward Traffic Channels are code channels. It is used to assign calls, usually voice and signaling traffic to the individual users.

Reverse Channel

The Reverse channel is the mobile-to-cell direction of communication or the uplink path. It consists of the following channels −

- **Access Channel** − Access channel is used by mobile stations to establish a communication with the base station or to answer Paging Channel messages. The access channel is used for short signaling message exchanges such as call-ups, responses to pages and registrations.
- **Reverse Traffic Channel** − Reverse traffic channel is used by the individual users in their actual calls to transmit traffic from a single mobile station to one or more base stations.



CDMA - Multiple Access Methods

The possibility to operate in either FDD or TDD mode is allowed for efficient use of available spectrum according to frequency allocation in different regions.

Frequency Division Duplex

A duplex method whereby the Uplink and the Downlink transmissions use two separate frequency bands −

- **Uplink** − 1920 MHz to 1980 MHz
- **Downlink** − 2110 MHz to 2170 MHz
- **Bandwidth** − Each carrier is located on the center of a 5 MHz wide band

Channel Separation

Nominal value of 5 MHz that can be adjusted.

Channel Raster

200 kHz (center frequency must be a multiple of 200 kHz).

Tx-Rx Frequency Separation

Nominal value of 190 MHz. This value can be either fixed or variable (minimum of 134.8 and maximum of 245.2 MHz).

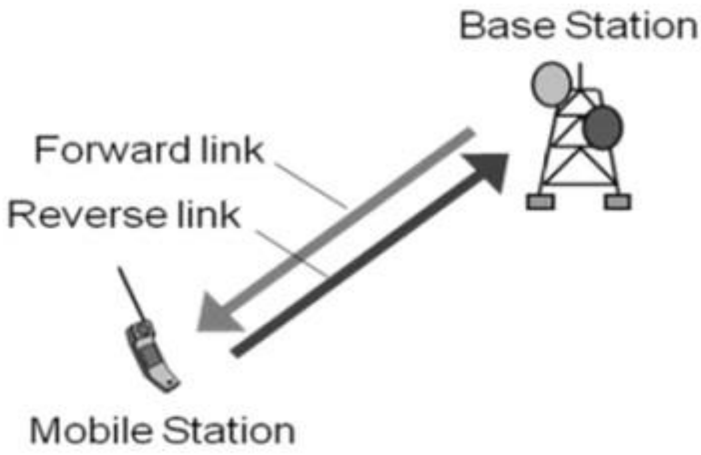
Channel Number

The carrier frequency is designated by the UTRA Absolute Radio Frequency Channel Number (UARFCN). This number is sent by the network (for the uplink and downlink) on the BCCH logical channel and is defined by Nu = 5 * (Frequency uplink MHz) and ND = 5 * (Frequency downlink MHz).

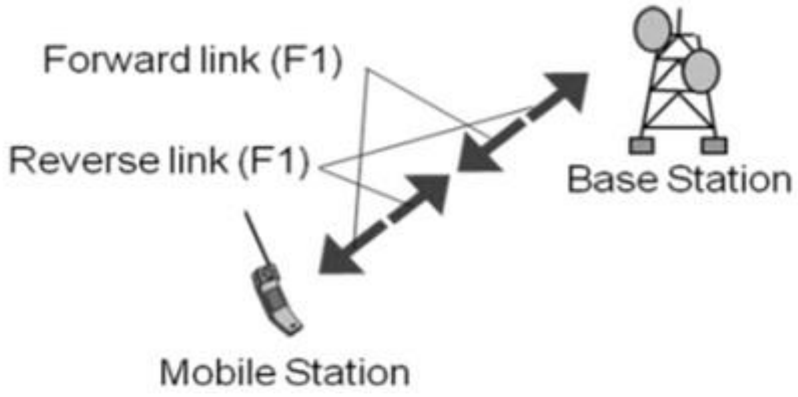
Time Division Duplex

Time division duplex is a technique by which the Uplink and the Downlink transmissions are carried over the same frequency by using synchronized time intervals. The carrier uses a 5 MHz band, although there is a low chip rate solution under study by the 3GPP (1.28 Mcps). The available frequency bands for TDD will be 1900–1920 MHz and 2010 – 2025 MHz.

Duplex Methods of Radio Links



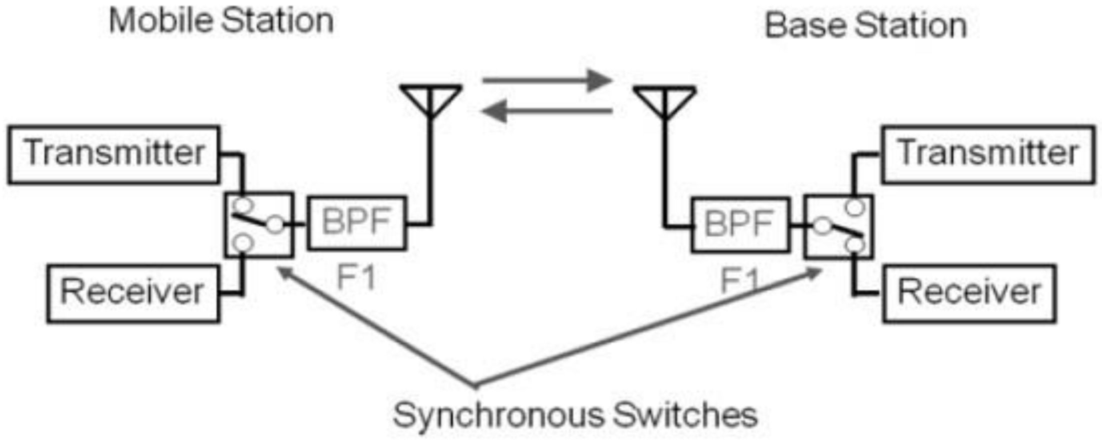
In case of Time Division Duplex, the forward link frequency is same as the reverse link frequency. In each link, signals are transmitted continuously in turns − just like a ping-pong game.



Example of TDD System

TDD uses a single frequency band for both to transmit and to receive. Further, it shares the band by assigning alternate timeslots for transmitting and receiving operations. The information to be transmitted can be voice, video, or computer data in bit-serial format. Each time interval can be 1 byte long or may be a part of several bytes.

TDD alternates the transmission and reception station data over time. Timeslots can be of variable length. Due to the nature of high-speed data, the communicating parties cannot mean that the transmissions are intermittent. Transmissions that appear as simultaneous are actually competing each other. Digitally converted into analog voice, no one can say that it is not a full duplex.



In some TDD systems, alternative time intervals are of same duration or having both DL and UL; however, the system does not need to be symmetric 50/50. The system may be asymmetrical as required.

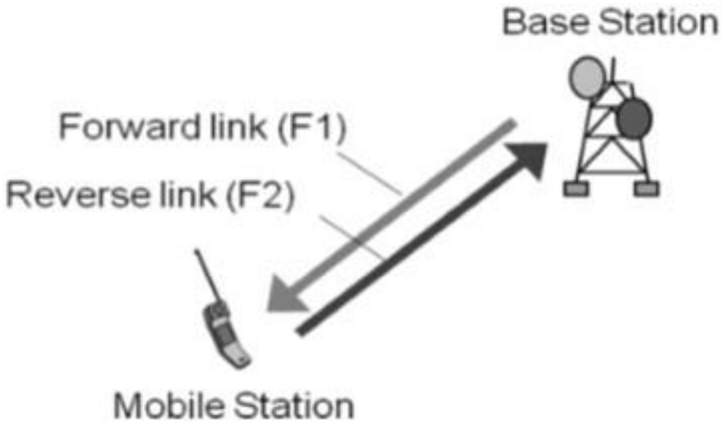
For example, while accessing the Internet, the download speed is usually higher than the upload speed. Most of the equipment work on asynchronous mode where the download speed is higher than the upload speed. When the download speed is higher than the upload speed, less timeslots are needed for uploading. Some TDD formats offer dynamic bandwidth allocation when the number of time intervals or durations is changed on the fly as needed.

The real advantage of TDD is that it is only a single channel of the frequency spectrum and it doesn’t require band guards or channel separations as the intervals take place using timeslots. The disadvantage is that the successful implementation of TDD requires a timing system. The precise timing to both the transmitter and the receiver is needed to ensure that the time intervals do not overlap or interfere with another.

Timing is often synchronized to GPS atomic clock standards specific derivative. The guard time is also needed between timeslots to avoid duplication. This time is generally equal to the transmission-reception processing time (transmission-reception switching time) and the transmission delays (latency) on the communications channel.

Frequency Division Duplex

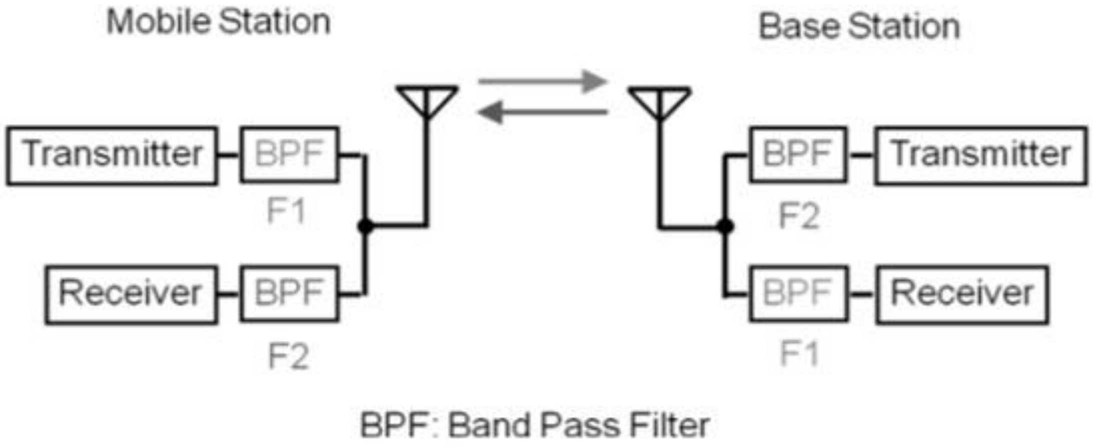
In Frequency Division Duplex (FDD), the forward link frequency is not the same as the reverse link frequency. In each link, signals are continuously transmitted in parallel.



Example of FDD System

FDD requires two symmetrical segments of spectrum for the uplink and downlink channels.

In a cell phone with a transmitter and receiver, operating simultaneously in such close proximity, the receiver has to filter as much of the signal from the transmitter as possible. More separation of the spectrum, the most effective filters.



FDD uses a lot of frequency spectrum, generally twice of the required TDD spectrum. In addition, there must be adequate spectrum separation between transmission and reception of the channels. These bands keep saying − it cannot be used, they are unnecessary. Given the scarcity and cost of the spectrum, they are real disadvantages.

Use of FDD

FDD is widely used in different cellular telephone systems. In some systems, the band 869-894 MHz is used as the downlink (DL) spectrum from the cell site tower to the device. And, the band 824-849 MHz is used as the uplink (UL) spectrum of the handset at the cell site.

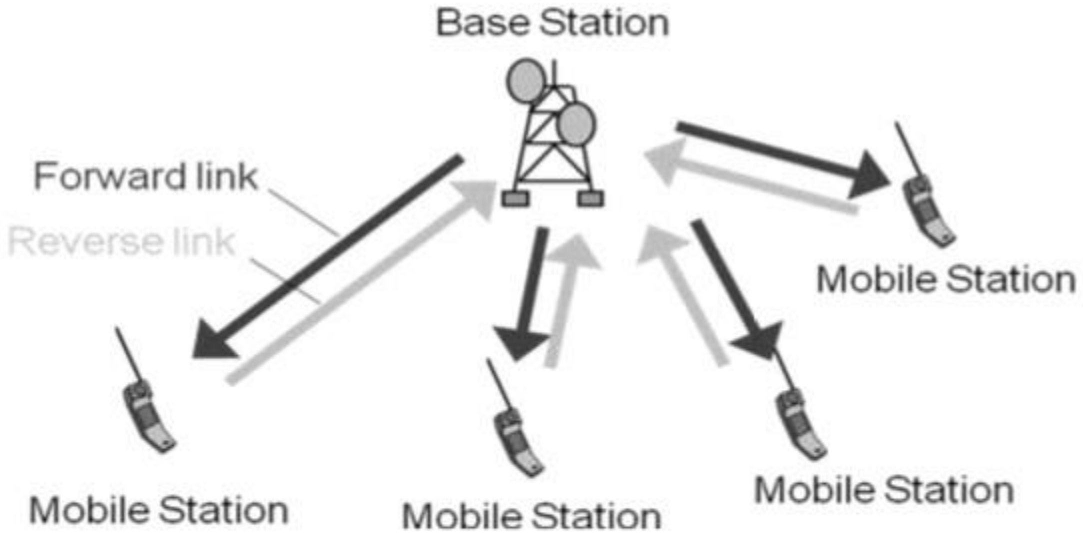
FDD also works on a cable where transmit and receive channels are given different parts of the cable spectrum, as in cable TV systems. And, filters are used to keep the channels separate.

Disadvantage of FDD

The drawback of FDD is that it does not allow special techniques like multiple antennas, multiple input-output (MIMO), and beamforming. These technologies are an essential element of the new strategies Long Term Evolution (LTE) 4G cell phone to increase the data rate. It is difficult to make broad enough bandwidth to cover both sets of antenna spectrum. Circuit complex dynamic adjustment is required.

Multiple Access Methods

The radio channel is a communication medium shared by several users in a geographic area. Mobile stations are in competition with one another for the frequency resource to transmit their information flow. Without other measures to control concurrent access of several users, collisions can occur. Since collisions are undesirable for connection oriented communication such as mobile phones, personal/mobile subscriber stations need to be allocated the dedicated channels on request.

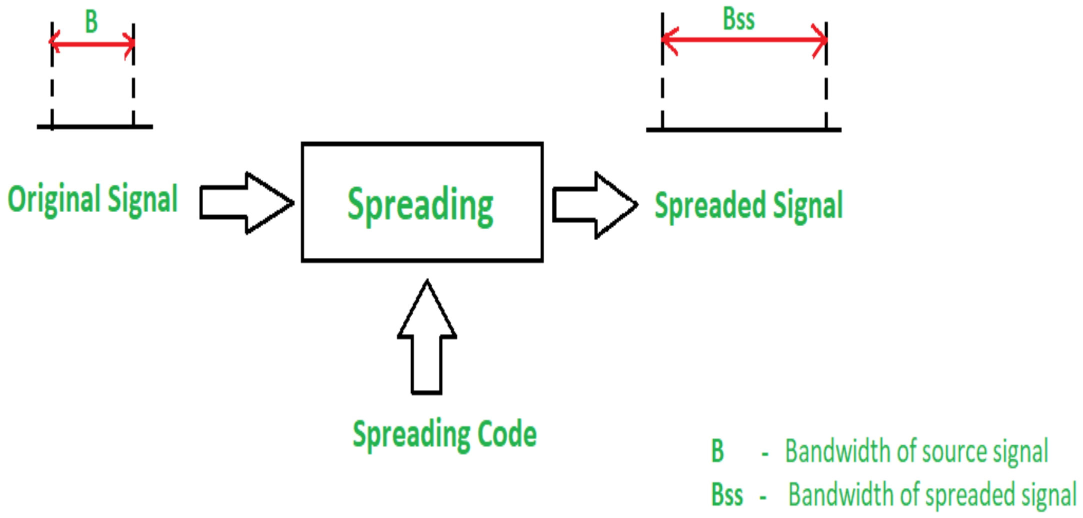


The mobile communication, sharing wireless resources on all users, must be communicated to identify the user. While identifying the user, it is referred to as "multiple access" (Multiple Access) that is receiving a radio wave of a number of transmitting stations in a receiving station (as shown in the following image).

What is Spread Spectrum?

The increasing demand for wireless communications has problems due to limited spectrum efficiency and multipath propagation. The use of spread spectrum communication has simplified these problems. In the spread spectrum, signals from different sources are combined to fit into **larger bandwidth**.

Most stations use air as the medium for communication, stations must be able to share the medium without an interception and without being subject to jamming from a malicious intruder. To achieve this, spread-spectrum techniques add redundancy means it uses **extended bandwidth** to accommodate signals in a protective envelope so that more secure transmission is possible. The spread code is a series of numbers that looks random but are actually a pattern. The original bandwidth of the signal gets **enlarged** (spread) through the spread code as shown in the figure.


B
Bss
Original Signal
Spreading
Spreaded Signal
Spreading Code
B - Bandwidth of source signal
Bss - Bandwidth of spreaded signal

Spread Spectrum

Principles of Spread Spectrum process:

1. To allow redundancy, it is necessary that the bandwidth allocated to each station should be much larger than needed.
2. The spreading process occurs after the signal is created by the source.

Conditions of Spread Spectrum are:

1. The spread spectrum is a type of modulation where modulated signal BW is much larger than the baseband signal BW i.e. spread spectrum is a wide band scheme.
2. A special code (pseudo noise) is used for spectrum spreading and the same code is to be used to despread the signal at the receiver.

Characteristics of the Spread Spectrum are:

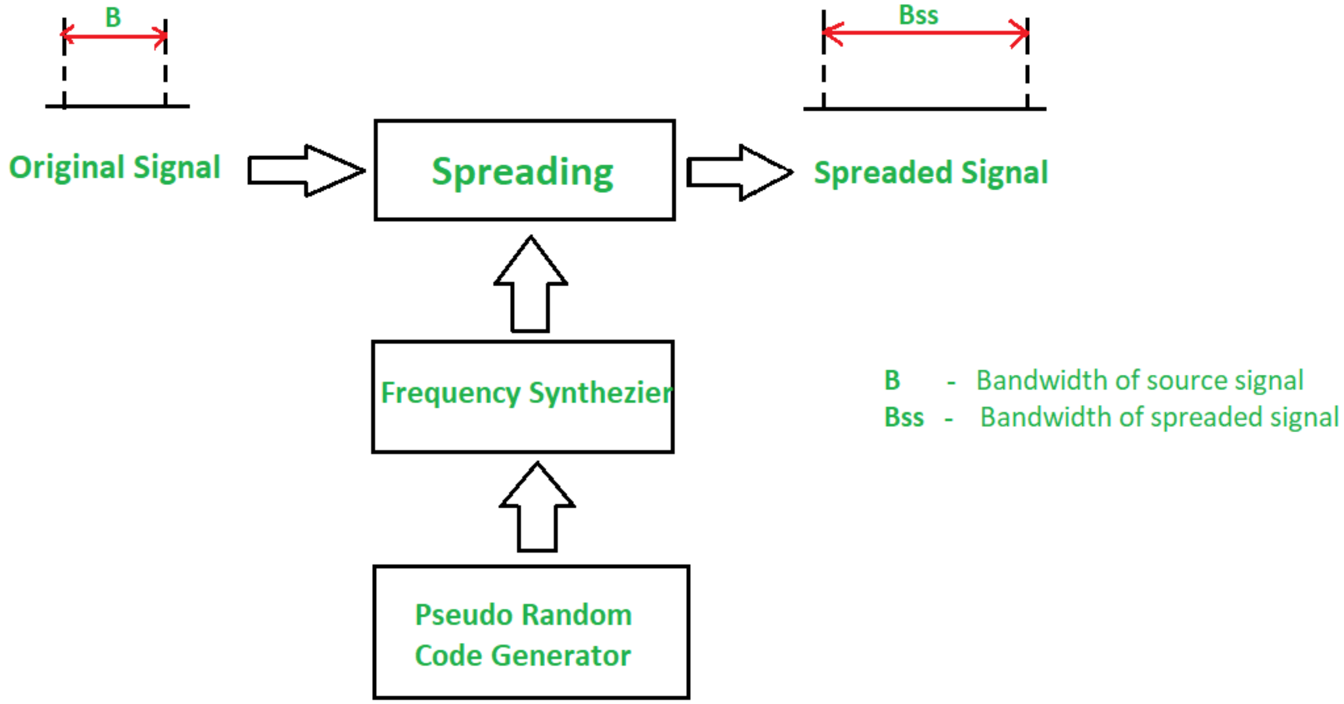
1. Higher channel capacity.
2. Ability to resist multipath propagation.
3. They cannot easily intercept any unauthorized person.
4. They are resistant to jamming.
5. The spread spectrum provides immunity to distortion due to multipath propagation.
6. The spread spectrum offers multiple access capabilities.

Two types of techniques for Spread Spectrum are:

1. Frequency Hopping Spread Spectrum (FHSS)
2. Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS):

In Frequency Hopping Spread Spectrum (FHSS), different carrier frequencies are modulated by the source signal i.e. M carrier frequencies are modulated by the signal. At one moment signal modulates one carrier frequency and at the subsequent moments, it modulates other carrier frequencies. The general block diagram of FHSS is shown in the below figure.


B
Bss
Original Signal
Spreading
Spreaded Signal
Frequency Synthezier
Pseudo Random Code Generator
B - Bandwidth of source signal
Bss - Bandwidth of spreaded signal

Frequency Hopping Spread Spectrum

A pseudorandom code generator generates Pseudo-random Noise of some pattern for each hopping period $\mathbf{T_h}$. The frequency corresponding to the pattern is used for the hopping period and is passed to the frequency synthesizer. The synthesizer generates a carrier signal of that frequency. The figure above shows the spread signal via FHSS.

Advantages of FHSS:

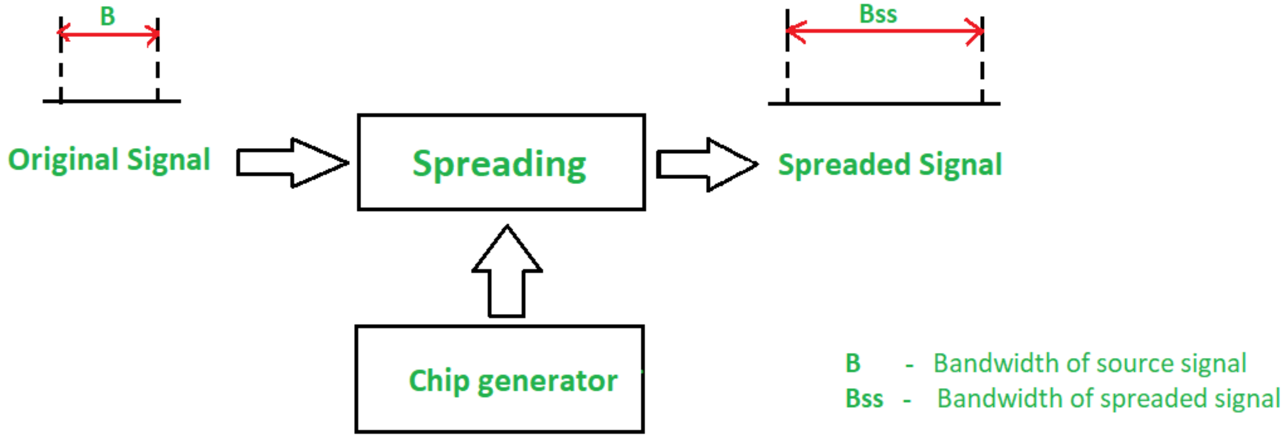
- Synchronization is not greatly dependent on distance.
- Processing Gain is higher than DSSS.

Disadvantages of FHSS:

- The bandwidth of the FHSS system is too large (in GHz).
- Complex and expensive Digital frequency synthesizers are required.

Direct Sequence Spread Spectrum (DSSS):

In DSSS, the bandwidth of the original signal is also expanded by a different technique. Here, each data bit is replaced with n bits using a spreading code called **chips,** and the bit rate of the chip is called as **chip-rate**. The chip rate is n times the bit rate of the original signal. The below Figure shows the DSSS block diagram.


B
Bss
Original Signal
Spreading
Spreaded Signal
Chip generator
B - Bandwidth of source signal
Bss - Bandwidth of spreaded signal

Direct Sequence Spread Spectrum

In wireless LAN, the sequence with n = 11 is used. The original data is multiplied by **chips** (spreading code) to get the spread signal. The required bandwidth of the spread signal is 11 times larger than the bandwidth of the original signal.

Advantages of DSSS:

- The DSSS System combats the jamming most effectively.
- The performance of DSSS in presence of noise is superior to FHSS.
- Interference is minimized against the signals.

Disadvantages of DSSS:

- Processing Gain is lower than DSSS.
- Channel Bandwidth is less than FHSS.
- Synchronization is affected by the variable distance between the transmitter and receiver.

Types Of Attacks

Due to the massive architecture of a cellular network, there are a variety of attacks that the infrastructure is open to.

1. Denial Of Service (DOS): This is probably the most potent attack that can bring down the entire network infrastructure. This is caused by sending excessive data to the network, more than the network can handle, resulting in users being unable to access network resources.
2. Distributed Denial Of Service (DDOS): It might be difficult to launch a large scale DOS attack from a single host. A number of hosts can be used to launch an attack.
3. Channel Jamming: Channel jamming is a technique used by attackers to jam the wireless channel and therefore deny access to any legitimate users in the network.
4. Unauthorized Access: If a proper method of authentication is not deployed then an attacker can gain free access to a network and then can use it for services that he might not be authorized for.
5. Eavesdropping: If the traffic on the wireless link is not encrypted then an attacker can eavesdrop and intercept sensitive communication such as confidential calls, sensitive documents etc.
6. Message Forgery: If the communication channel is not secure, then an attacker can intercept messages in both directions and change the content without the users ever knowing.
7. Message Replay: Even if communication channel is secure, an attacker can intercept an encrypted message and then replay it back at a later time and the user might not know that the packet received is not the right one.
8. Man In The Middle Attack: An attacker can sit in between a cell phone and an access station and intercept messages in between them and change them.
9. Session Hijacking: A malicious user can highjack an already established session, and can act as a legitimate base station.

wireless networks are dependent on other private networks, which are managed by others, so after these issues, the users have less control of security procedures. These security issues are:

Denial of Service (DOS) attacks

The denial of services or DOS attacks is one of the most common attacks of all kinds of networks and especially in a wireless network. It prevents users from using network services because the attacker sends a large amount of unnecessary data or connection requests to the communication server. It causes a slow network, and therefore the users cannot get benefitted from using its service.

Traffic Analysis

Traffic analysis is used to identify and monitor communication between users. In this process, the service provider listens the traffic flowing in the wireless channel to access the private information of users affected by the attacker.

Eavesdropping

It specifies that the attacker can log on to the wireless network and access sensitive data if the wireless network was not secure enough. This can also be done if the information is not encrypted.

Session Interception and Messages Modification

It specifies that the attacker can intercept the session and modify the transmitted data in this session. This scenario is called "man in the middle." It inserts the attacker's host between the sender and receiver host.

Spoofing

In this security issue, the attacker impersonates him as an authorized account of another user and tries to access the sensitive data and unauthorized services.

Captured and Retransmitted Messages

In this security issue, the attacker can get some of the network services by getting unauthorized access. After capturing the message, he/she can reply to it with some modifications to the same destination or another.

PDC (Personal Digital Cellular)

Personal Digital Cellular (PDC) is a digital cellular telecommunications system that was primarily used in Japan. Developed in the 1990s, PDC was designed to offer improved voice quality and enhanced features compared to its predecessor, the analog cellular system. In this article, we will explore the key aspects of PDC, including its technical specifications, network architecture, and impact on the telecommunications industry.

PDC was introduced by the Japanese telecommunications company NTT DoCoMo in 1993 and quickly gained popularity in the country. It was based on the IS-95 standard, which was also used in the United States for the Code Division Multiple Access (CDMA) technology. PDC operated in the 800 MHz frequency band, providing efficient and reliable communication services to mobile phone users.

One of the main advantages of PDC over the analog cellular system was its ability to carry digital voice signals, resulting in improved call quality and reduced background noise. PDC utilized a speech coding algorithm called Adaptive Transform Coding (ATC), which compressed voice signals while maintaining acceptable audio quality. This compression allowed for more efficient use of network resources, enabling higher call capacity within the available frequency spectrum.

PDC also introduced several advanced features that enhanced the user experience. It supported Short Message Service (SMS) for text messaging, enabling users to send and receive text-based messages directly from their mobile phones. PDC also supported data services, allowing users to access basic internet services such as email and basic web browsing. While the data speeds were relatively slow compared to modern standards, it laid the foundation for the future development of mobile data technologies.

In terms of network architecture, PDC utilized a cellular network structure consisting of multiple base stations that provided coverage over specific geographic areas called cells. Each base station was equipped with antennas that transmitted and received signals from mobile devices within its coverage area. The base stations were interconnected through a wired network, allowing seamless communication across the entire PDC network.

To manage the allocation of network resources and ensure efficient call handling, PDC employed a system known as cell selection and handover. When a user moved from one cell to another while making a call, the system automatically transferred the call to a new base station without interrupting the conversation. This feature was critical in maintaining call quality and reducing dropped calls, especially when users were traveling or moving between different coverage areas.

PDC faced some challenges during its deployment and operation. One of the major limitations was its incompatibility with other cellular systems used globally. Since PDC operated on a unique frequency band and utilized different technical specifications, mobile phones designed for PDC were not compatible with networks outside of Japan. This limited the international roaming capabilities of PDC users and hindered its global adoption.

Another challenge was the rapid advancement of mobile technologies during the same period. While PDC provided significant improvements over the analog cellular system, it was soon overshadowed by the emergence of Global System for Mobile Communications (GSM) and its subsequent upgrades, such as General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE). These technologies offered higher data speeds, improved call quality, and global compatibility, eventually becoming the de facto standards for digital cellular communication worldwide.

Despite these challenges, PDC played a crucial role in the development of digital cellular technologies, particularly in Japan. It paved the way for subsequent generations of mobile networks, including 3G, 4G, and 5G, which brought significant advancements in data speeds, capacity, and multimedia capabilities.