كلية الهندسة - جامعة الزقازيق

2021/2022

الفرقة: الرابعة هندسة الحاسبات والمنظومات

المقرر: شبكات الحاسب

الإسم: عبدالعزيز عبدالفتاح عبدالعزيز

الرقم في السكشن: 49

رقم الجروب وإسم الموضوع:

Group 1: Network Threats and Protection Techniques

My part is:

Wireless Security

Contents

1-Overview about wireless network

Network: is a collection of nodes (Devices) connected together by a communication link.

This Communication link can be either wires (coaxial cable, fiber optic cable, etc.) or wireless (Wireless Access Points (WAPs), Routers (wired network)).

Wireless networks:

- allow devices to communicate with each other without any physical communications medium (cables), it usually uses radio waves.
- Are implemented at the physical layer (layer 1) of the OSI or TCP/IP models.

BASIC WLAN COMPONENTS

three basic components must be available:
wireless network cards
wireless access point(s).
wireless bridge

The wireless network cards are built-in the devices, and they connect to an access point.

Wireless bridges (Bridges are layer-2 devices: they forward and filter frames using the LAN destination address),
Supporting high-speed long-range outdoor links between buildings (different LAN technologies). Based on line-of-sight.

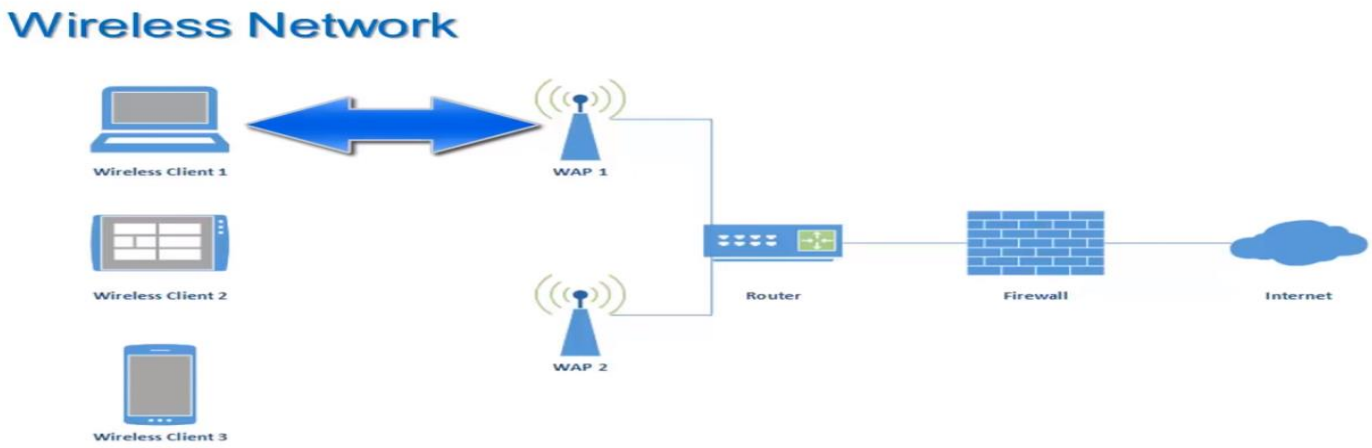
Wireless Access Point (WAP): it is a device that allows end devices like PCs to connect to a wireless network.

- it is considered as central connection point for all nodes (computers) that have wireless network adapter cards.
- the WAP performs the same function as a hub (All LAN segments belong to the same collision domain, all segments must use the same ethernet technology) or switch (switches are available with various combinations of 10 Mbps, 100Mbps and 1 Gbps interfaces, many switches operate in a full-duplex mode) performs for a wired network.

- the WAP is Physically connected to a wired network ”DSL”(Land line Network) via a router and links a wireless network to an existing wired network. I explained the difference between router and WAP in detailed here

- it is Commonly working upon Wi-Fi (IEEE 802.11) standards
- Identified using a Service Set Identifier (SSID)

SSID (name of your network) is a string between 1 and 32 characters in length that is intended to provide a human readable way of uniquely identifying a wireless network.



Types of wireless network:

Type	Range	Applications	Standards
Personal area network (PAN)	Within reach of a person	Cable replacement for peripherals	Bluetooth, ZigBee, NFC
Local area network (LAN)	Within a building or campus	Wireless extension of wired network	IEEE 802.11 (WiFi)
Metropolitan area network (MAN)	Within a city	Wireless inter-network connectivity	IEEE 802.15 (WiMAX)
Wide area network (WAN)	Worldwide	Wireless network access	Cellular (UMTS, LTE, etc.)

Table1: types of w

Wireless Data Frames:

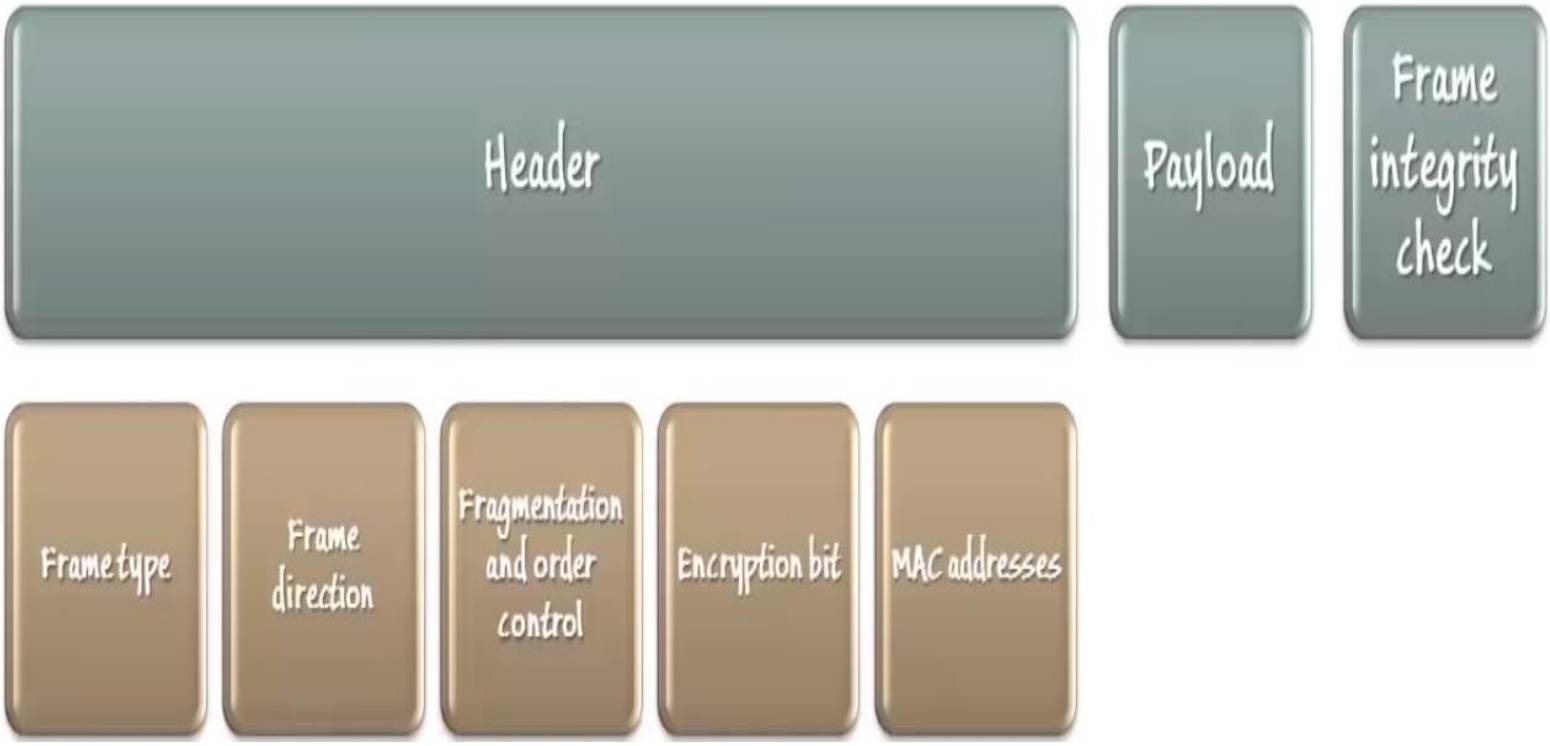
Wireless data are transmitted in blocks called " Wireless data frames"

A Wireless data frame consists of 3 major parts:

1- Frame header
   - Frame type
   - Frame direction (to/from WAP)
   - Fragmentation and order control
   - Encryption bit
   - MAC addresses (sender/receiver)

2- Payload
   - Actual Data

3- Frame check sequences
   Used to verify the safety of the frame.



2- Advantages of wireless network:

1-For users

- **Convenience:**
  Because it allows a user to connect a network without a cable to be attached in the connected devices and without needing to assign any network configuration settings like IP addresses, DNS servers.

- **Mobility:**
  Rather than forced to stay in one location as with a wired network.

- **Accessibility:**
  Users can easily access the network

- **Expandability:**
  Easily to grow the network and adding new users

2-For providers:

- **There is no need of cables**

- **Lower installation and maintenance costs**

3- Weaknesses (threats) of the wireless networks:

Many security vulnerabilities:

1- No physical access required:

With an Ethernet LAN, attacking the network from the inside requires physical access to the network infrastructure components such as routers or network cables. A hacker must be able to connect a machine to in the network somewhere.
WLANs have no physical boundary to protect the data, WLANs use radio waves over the air as the medium (carrier signal).
After a radio signal (carrier signal) transmitted from the source, the signal travels through the air in many directions, and you have no control over the signal propagation. Any hacker with an antenna that is adjusted to the right frequency and in the range of the WLAN can “Eavesdropping”. A hacker can use software programs like (wireshark) to eavesdrop on a wireless network.

2-Ad-hoc networks could be a security threat:

A network of end devices that do not have any access points (central control) in between them like (Public hotspot networks). These networks usually have low protection, encryption methods.
Any attacker can create an ad hoc network with a trusted client then stealing his information.

3- Vulnerabilities Inherent to Mobility:

Suppose that you've a secure WLAN, using the strongest authentication and encryption technologies available. You are confident in your WLAN security. But then, how do you secure the devices of the other users in your WLAN when they connect to public hotspot WLAN networks in airports or coffee shops (Ad-hoc networks)?

4-Vulnerabilities Inherent to the Standards Definitions

- **Unauthenticated Management Frames:**

  No authentication for management frames allow the hackers to hack your WLAN.

What is meant by the Management frames? This section is explained deeply in "**Authentication & Encryption**"
The access point sends out frames continuously to the nearby WLAN users.
The user specifies an access point to be connected on WLAN by entering the SSID (Name of the network) and if there a password the user should enter it to be connected and then:
The AP will send an authentication reply to the client.
Upon successful authentication, the user will send an association request frame to the access point.
The AP will send back an association response.
The user now can pass a payload(traffic) to the access point.

- **Authentication and encryption weaknesses:**

  There are some protocols that no longer been used because of their Authentication and encryption weaknesses like (WEP).
  Authentication is very important to restrict the ability to send and receive on the network. It is the first step for a device attempting to connect to an 802.11 WLAN. As mentioned above "Authentication is handled by a request/response exchange of management packets between the user and the access point"

5- Unknown network boundary:

In a wired network; networking and security personnel can know precisely where the network ends (the real location of the destination), this isn't usually possible in a wireless network because users usually establish or drop connections on an ad-hoc networks.

6-Rogue Aps (Access points):

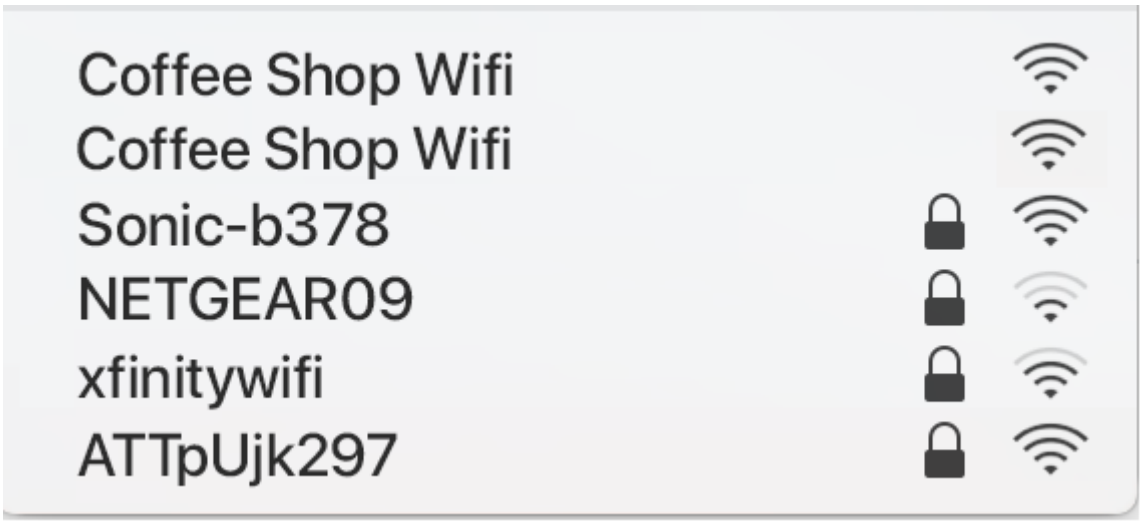
Access points:
Nowadays homes often connect to the internet using an access point instead of a wired connection. If you are wondering why you've never heard of access points but have heard of routers? it's because most routers include access points. Routers are responsible for transporting packets (using routing protocols), but access points are used to providing wireless internet access to the pcs connected to them as I mentioned above.

Access point

routers

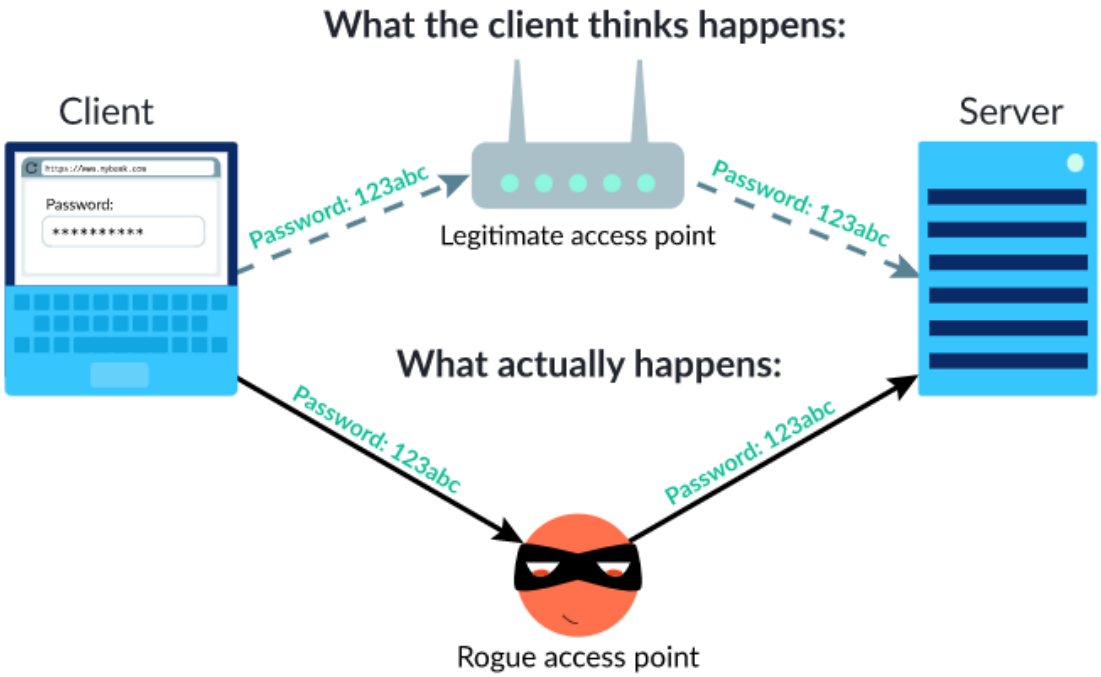
A rogue AP network Is any WAP that has been installed on a network's wired infrastructure without the network's administrator's permission.

The attacker uses the rogue access point with a network ssid like yours, so when you want to connect to the network you will see a duplicating ssid like the picture.



There are to "Coffee Shop wifi" networks one is real and the other is a rogue access point network. If you connect to the fake one the attacker will see your ip and your

mac addresses, and not only this he can intercept the data flowing through the network.



There are two ways for interception:

1- Passive interception: a rogue AP can read your data but can't manipulate it. Ex if you connect to a network with a rogue access point and enter your password on a site over HTTP, the rogue access point can read your password.
2- Active interception: a rouge AP can also manipulate the data. Reading the incoming user data, modify the data and send the modified data to the destination.

So next time be careful when connecting to a free hotspot in public locations such as coffee shops or airports or anywhere, to protect yourself you can use VPNs and only visit sites with HTTPS not HTTP, cause even if a rogue access points intercept it, it won't be able to unscramble it.

7-Client Mis association (Misconfigured):

When a user connects to an Access point, the OS usually automatically save the SSID. Once that SSID is detected again, the user's PC automatically is connected to the network and the user maybe unaware of the connection. If the SSID is being spoofed, the user could connect to an unsafe network.

8-The nebulous and unprotected nature of wireless networks;

introduces threats to the (privacy) and Integrity and the Availability of data traveling over those wireless networks, because of interferences and hacks that wouldn't be happen if the same data were traveling over a wired.

9- The most substantial threats to information security emerge in the context of (Unsecured wireless networks);

unencrypted wireless data frames can be easily sniffed and analyzed using software.

10- Wireless Attacks:

Networks in general are constantly under attacks.
Some of these attacks are unique to wireless networks, as is the case with management frame spoofing (a rogue AP declare an SSID known to the user to make the user connect to the rogue AP.

4- Securing the Wireless Network

1- To overcome the "**No physical access required and the radio transmission medium"** issue, we must use strong authentication and privacy, and use the latest version of the encrypt and authentication techniques.

2- To overcome the "**Vulnerabilities Inherent to Mobility**" issue, we must use secure roaming, secure management and policies, and take care of who are connected to the network and use strong password to the network, and use the **MAC Filtering** property. As mentioned below.

3- To overcome the "**Ad-hoc networks and Rogue Aps and Client Mis association**" issues: You shouldn't connect to any free hotspot in public locations such as coffee shops or airports or anywhere, to protect yourself you can use VPNs and only visit sites with HTTPS not HTTP, cause even if a rogue access points intercept it, it won't be able to unscramble it, also if you are outside you must turn the "the automatically connection to the wifi" off.

4- To overcome the "**Vulnerabilities Inherent to the standards Definitions**" issue: we must use strong authentication and management frame protection as mentioned above in "the management frame"

- **Authentication & Encryption:**
  - ❖ Open Authentication: doesn't require a WEP key (username, password)
  - ❖ Pre-shared key (PSK): A user provides credentials, such as a username and a password, to access a network.

Client and AP are shared (configured) with a key (PSK), this PSK is used to create encryption key (4-way handshake)

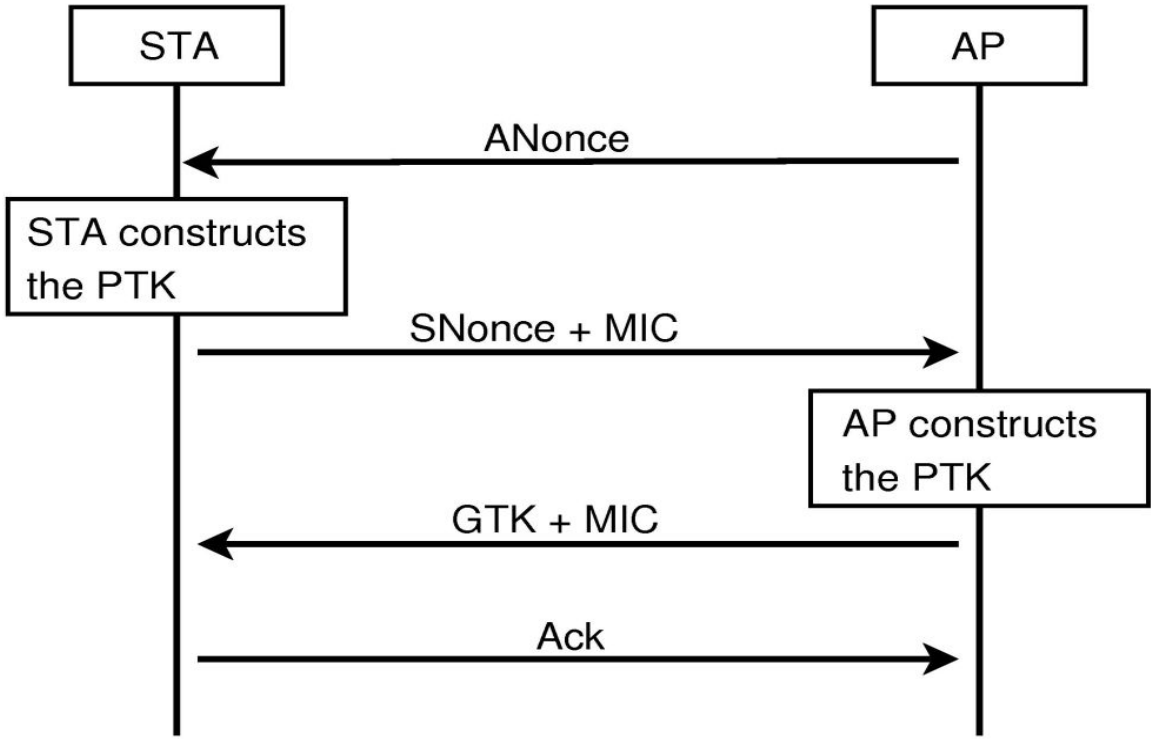
PSK is used in personal WLAN mode

4- way handshake

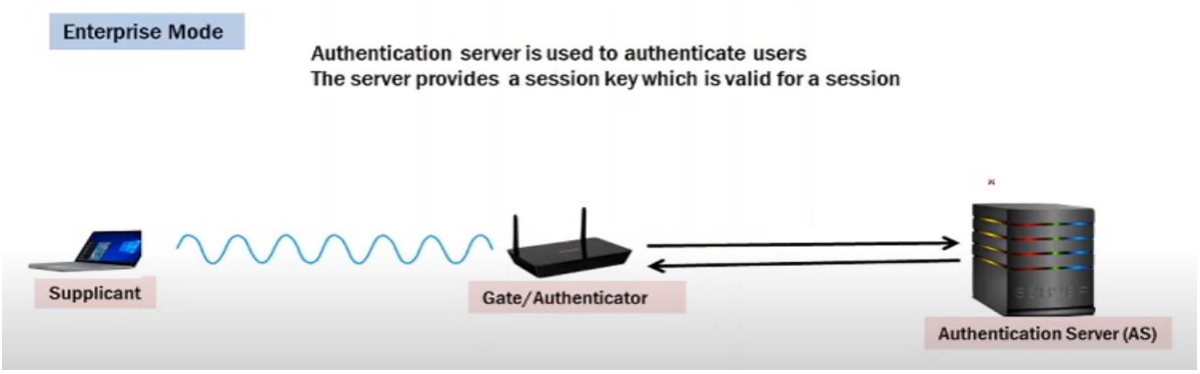
4-way handshake process:

1- A PMK (Pairwise Master Key) is installed in the client device (station) and the Access Point (AP)
2- AP sends an Anonce (a random Authenticator number used once) to the client
3- Then client sends a Snonce and MIC (Message Integrity Check) to the AP
4- Then AP prepares a PTC (Pairwise Transient Key) and sends a GTK (Group Temporal Key) and MIC to the client. PTC (is a set of encryption keys used for different functions unicast encryption and data protection)
5- Then the client sends an Acknowledge (ACK).

Before the 4-way handshake process the client and AP know the MAC (Authentication Address) of each other, as soon as the client enters the password and connects to the WLAN.



❖ 802.1X (enterprise mode): used in companies, authentication (Radius) server, this server is the administrator which can permit or deny the user to access the network, and gives the user a temporary key to be used just for one time just for this session and same for the access point.



if packets are intercepted by an attacker, an attacker cannot make sense of them, if they are encrypted.

❖ Techniques to authenticate and encrypt WLANs:

- **Wired Equivalent Privacy (WEP):**

the security standard designated by the original IEEE 802.11 Wireless standard (WI-FI)
Not recommended because it uses a very weak algorithm called "RC4 encryption algorithm" it encrypts the data with a 64-bit encrypted key (initialization vector) and these keys are static.
it uses the hashing method as an encryption + shared key and uses CRC (Cyclic Redundancy Check for MIC (Message Integrity Check).

How WEP Is Broken

WEP for data privacy. WEP keys have the following properties:

- They are static: It means that They can't be changed except by reconfiguring all access points.
- They are shared: All access points share the same WEP keys.

- **WI-FI Protected Access (WPA):**

- it encrypts the data with a 64-bit encrypted key but, It uses Temporal Key Integrity Protocol (TKIP) (improved encryption compared to RC4), it is dynamic which it changes the key so quickly that a hacker wouldn't have time to learn that key before a new key is created.

- It uses a longer initialization vector to reduce the number of collisions (a collision happens when the same initialization vector is reused)

Has discovered security weakness (it is not considered to be a secure protocol any longer)

- **WI-FI protected Access version2 (WPA2):**

  - Requires supporting AES (Advanced-Encryption-Standard) (uses 128-bit) and CCMP (Counter-Mode-with-Cipher-Block-Chaining-Message-Authentication-Code) "in addition to AES's powerful encryption by making it challenging for a malware user to spot repeated sequences and also uses hashing to verify messages haven't been modified in transit" protocols.
    The AES is stronger encryption compared to TKIP
    WPA2 can also support TKIP (128 bits encrypted key) from the WPA

  - Has a discovered security weakness (it is not considered to be a secure protocol any longer).

- **WI-FI protected Access version3 (WPA3):**

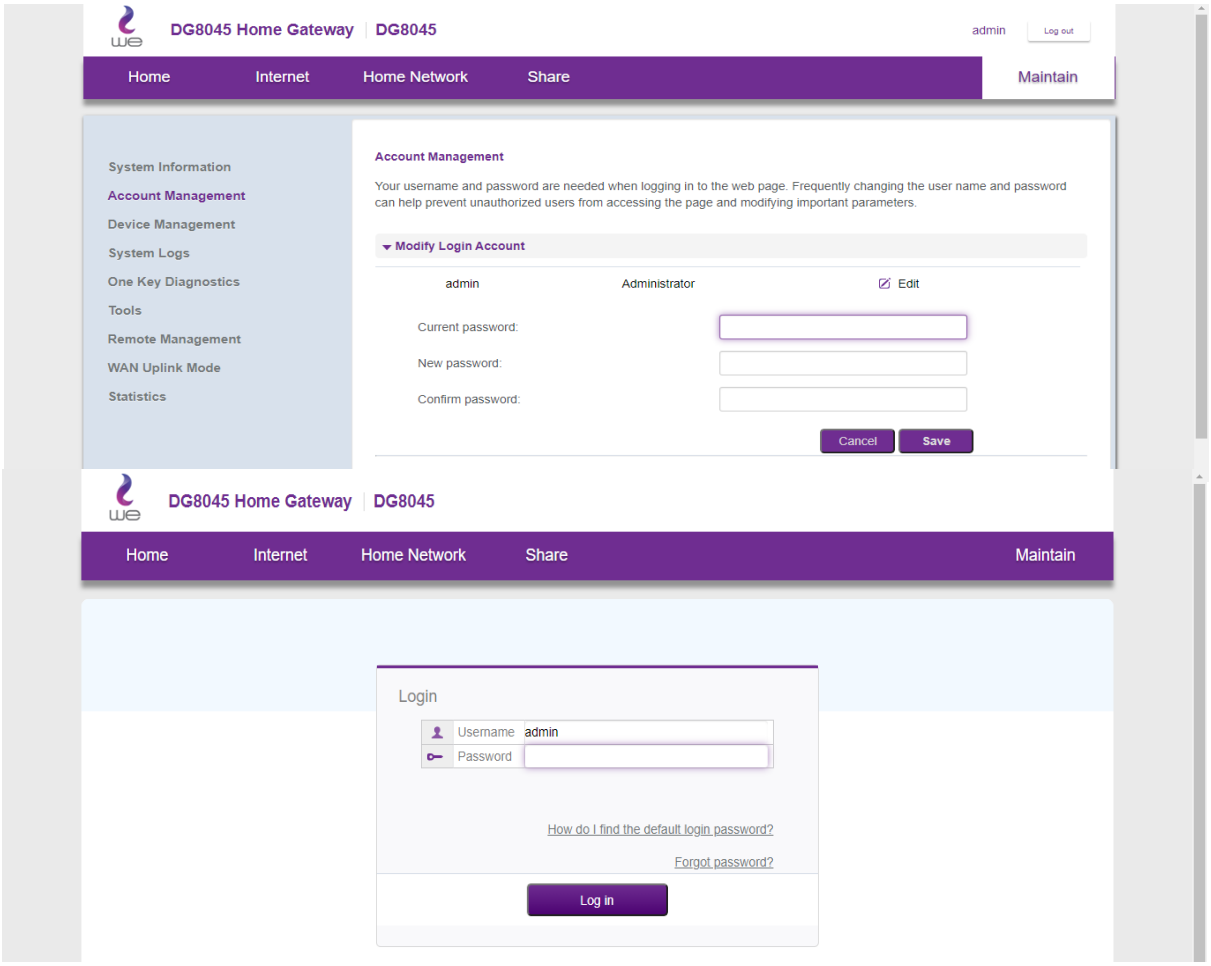
  - Announced as the replacement for WPA2

  - It uses 192-bit encryption key

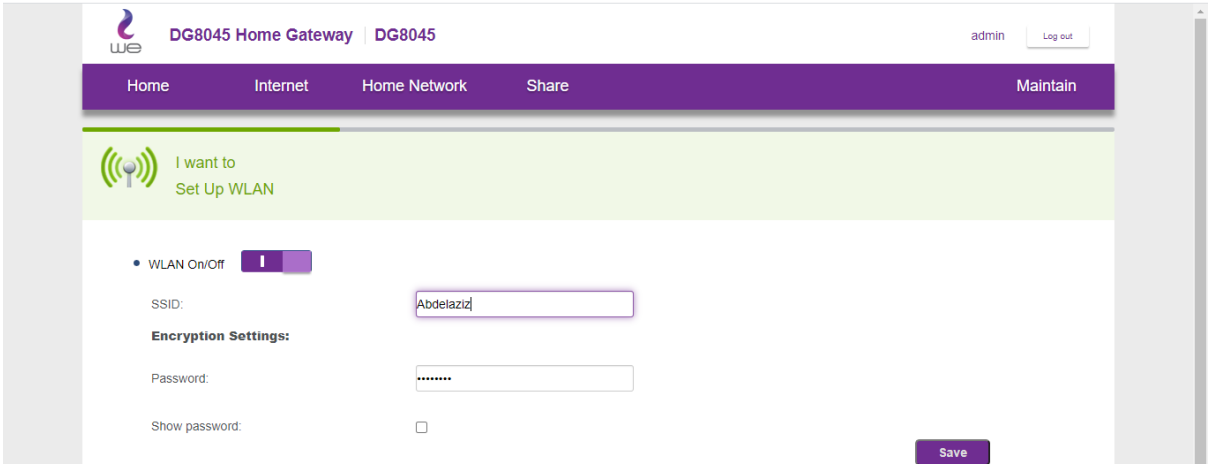
  - It will help with the adoption of IOT devices due to easier setup for devices without displays like in smart homes (smart TV, smart refrigerators and security cameras)

we can do this technique in our home network from the router configuration page.

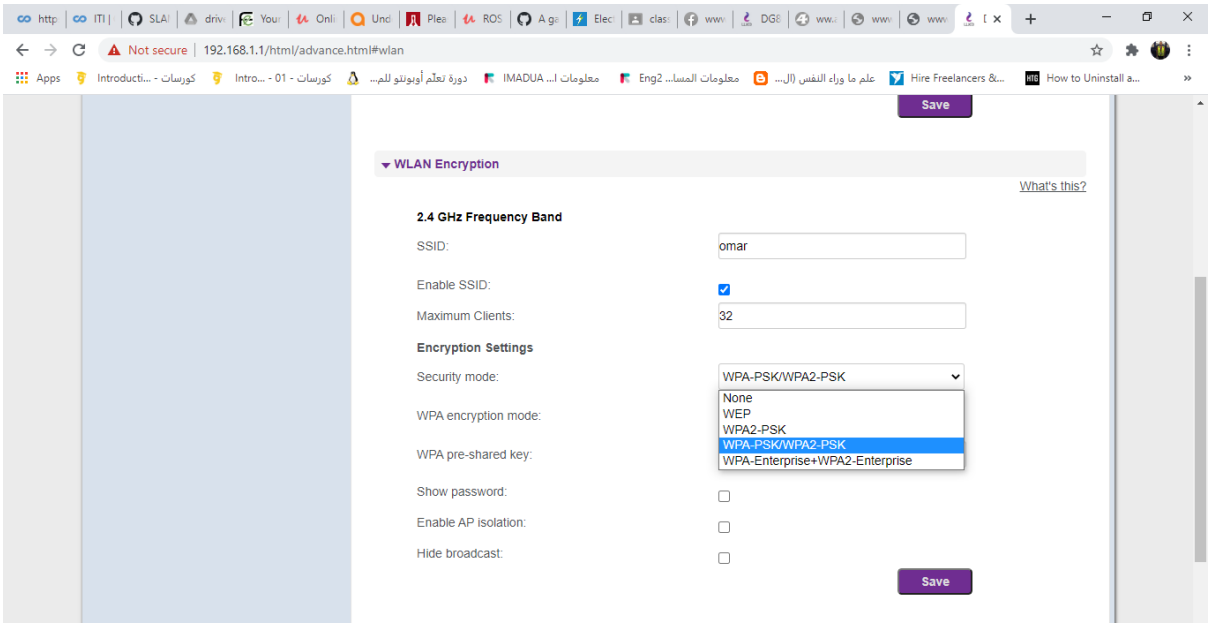
1- Authentication of the router:

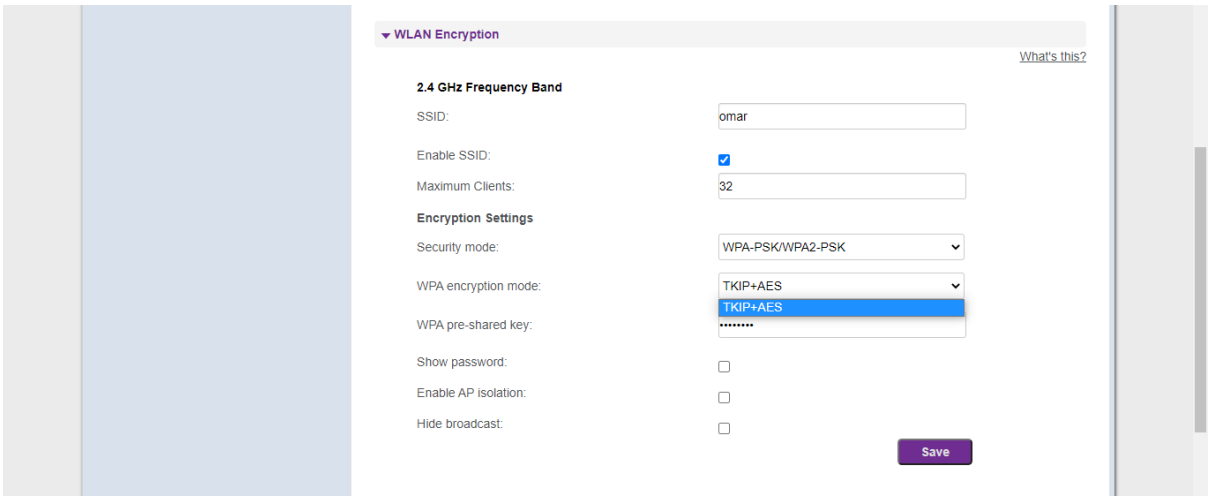


2- Encryption setting of the WLAN:



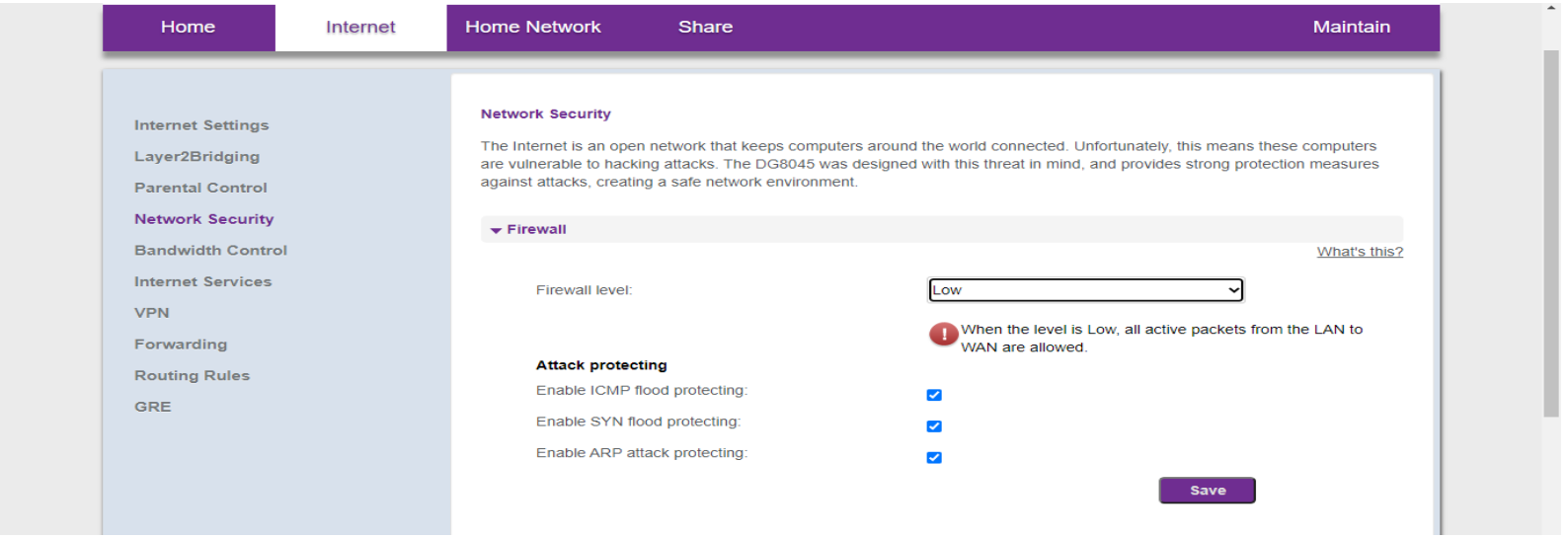
3- Using WPA-PSK/WPA2-PSK Technique to encrypt and authenticate the WLAN (algorithms used are TKIP + AES)





- **Tools for securing a Wireless Network:**

  - **Enabling the firewall from the router configuration page as shown:**
    From internet section choose network security category
    From the firewall list (low or high or disable) choose (low or high) but never disable it.
    Also, you can select any protection techniques (ICMP flood, SYN Flood, ARP)



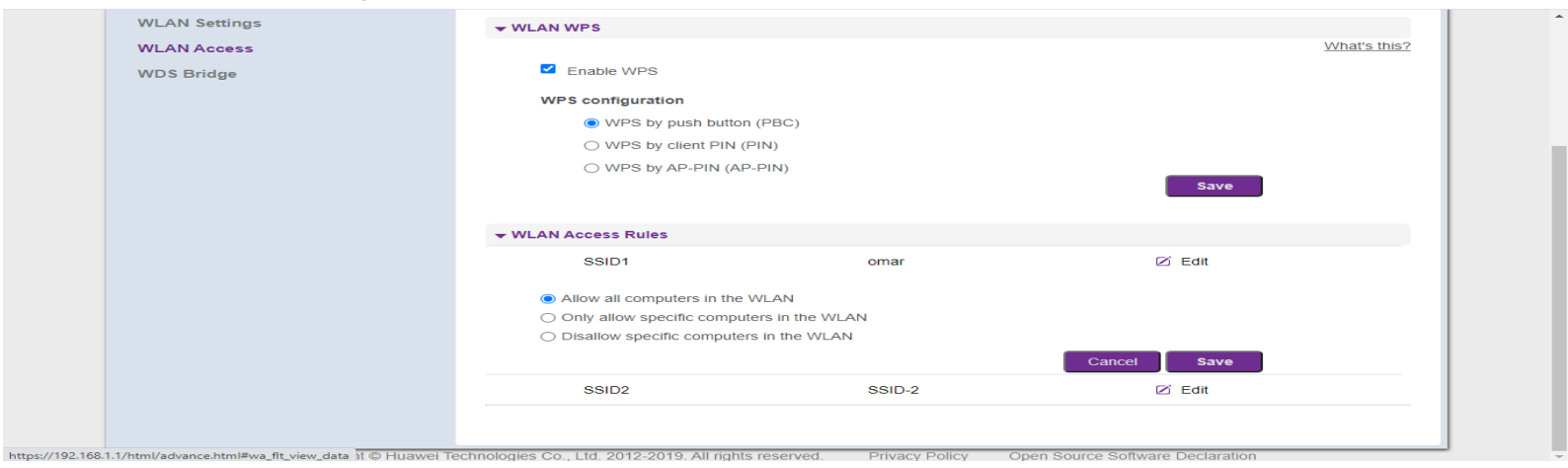
ICMP flood (Ping flood) Attack; is a Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP(Internet Control Msg Protocol) echo requests, also known as pings.

SYN Flood Attack; is a form of (DoS) attack in which an attacker sends a progression of SYN requests to an objective's framework trying to consume enough server assets to make the framework inert to authentic activity because the attacker didn't send the ACK.

ARP Attack (ARP poisoning); ARP spoofing is a cyber-attack that is carried out over a Local Area Network (LAN) when the victim send request to the network to update its ARP table if the attacker is connected to the same LAN it can reply to this request by sending a malicious ARP packets to a default gateway on a LAN

- **MAC Filtering:**

  only allowing specific devices on a network if their MAC Addresses are allowed or blocking specific devices on a network by knowing their MAC addresses. (Not recommended because there are programs that can change the MAC Addresses). As shown in figure



- **Geofencing (using AP):**

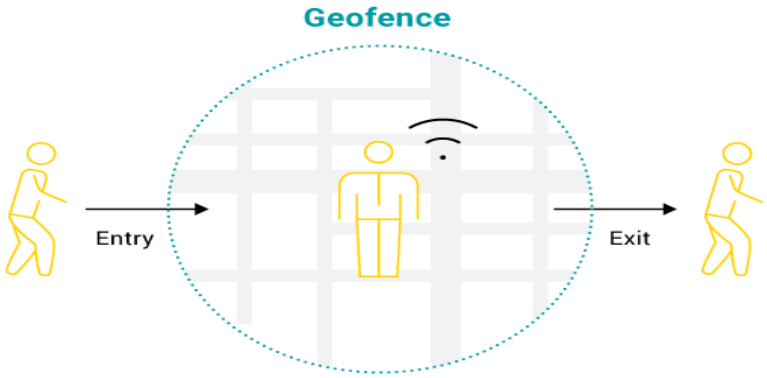
  is a location-based technology, it is created within a certain location. This could be a building or store or a mall or a conference hall.

  It works as a zone where devices are able to access information while within the boundaries of the zone, most popular using of the geofencing is in the shopping malls or public cafes.

  How does it work?

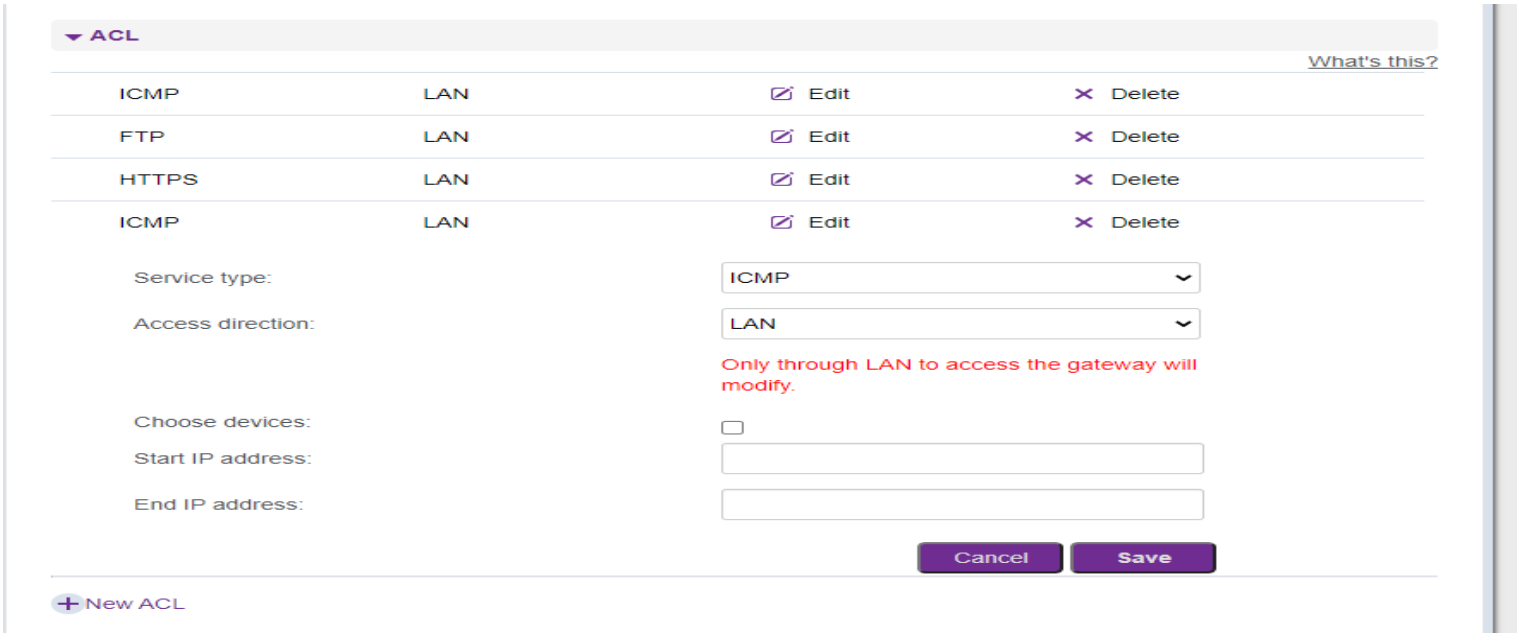
  It is based on predefined coordinates within software, when a user enters the zone, the option to subscribe and use an app or access free WiFi becomes available. When a user accesses free WiFi, the software (with geofencing capabilities) provides the opportunity to make use of or access services within the geofence.

  Geofencing are used to provide a range of services. The most popular are related to marketing. As soon as clients enter a location, sellers can send a push notification to their smartphones. The notification, in the form of an SMS, typically includes a link to download an app or to a website designed for the location. Once the user accesses the app or website, they can begin to receive deals, discounts and special offers. Use AP if you want to expand the zone.



- **Access-Lists (ACL):** Is a group of rules and protocols defined to control the network traffic and reduce network attacks and for providing Application protocol services to deal with the Application Layer such as (HTTPS, FTP, ICMP, Mail, DNS, etc.) ACLs are used to filter traffic based on the set of rules.

  we can do this technique in our home network from the router configuration page.

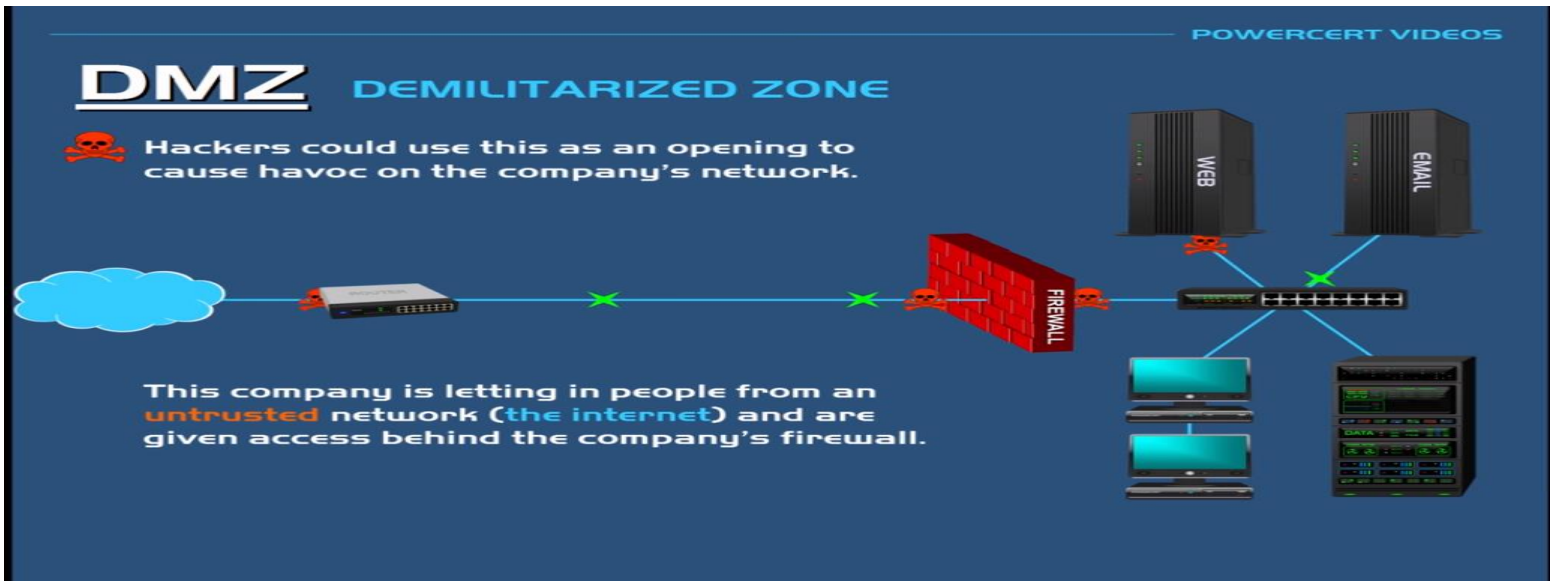


- **DMZ (Demilitarized Zone):**

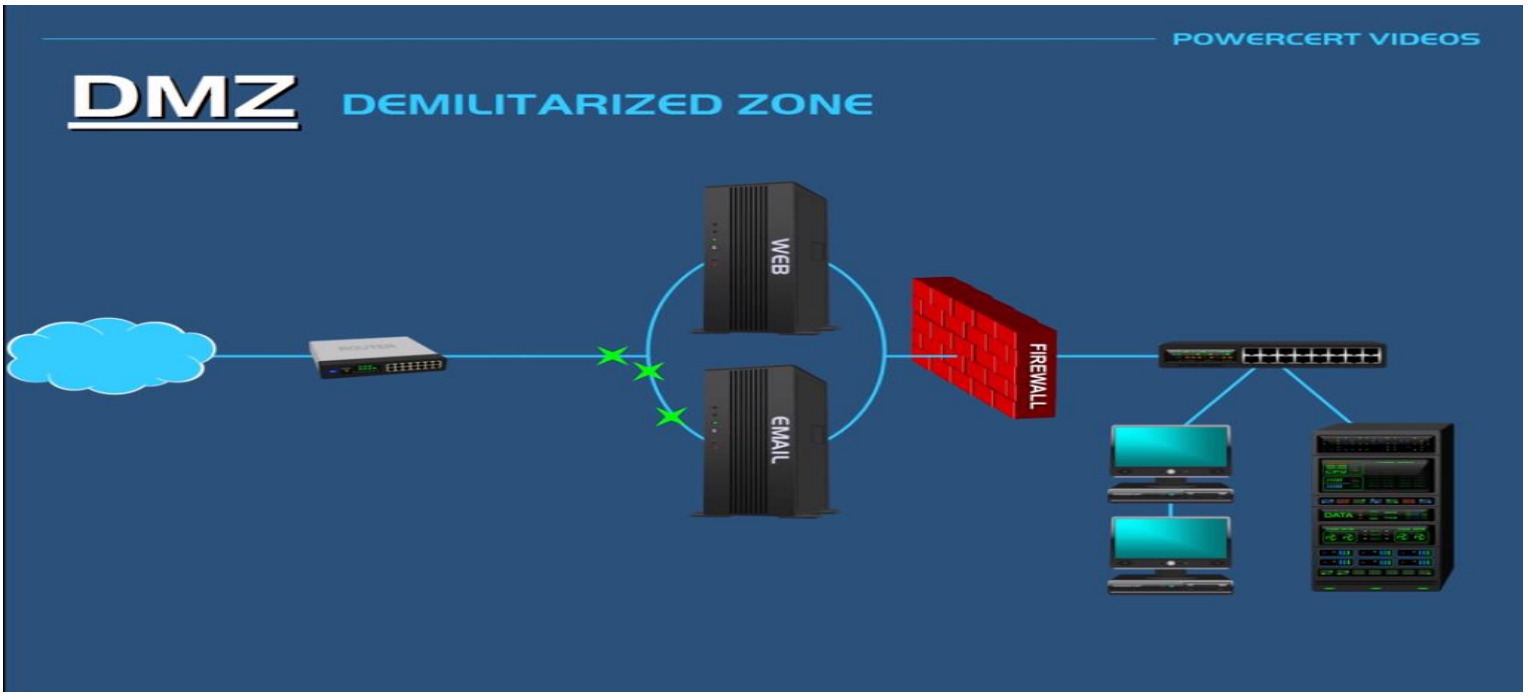
It considered as a subnetwork that it sits before the firewall between the public internet (unsecured networks) and private networks.

It is mostly used to protect the organizations (companies) internal Local-Area-Network (LAN).

Network without the DMZ all the devices and servers connected to this network are behind the firewall. it could create a security concern (issue), as all devices are behind the firewall, hackers could use this as an opening to cause havoc on the company's network, because this network allows people from an untrusted network (internet) to access behind the company's firewall because all the servers are behind the firewall.



If the company used the DMZ technique and put the WEB and Email servers and other servers connected to the internet outside the company's internal network (before the firewall) and the important servers such as (database servers where sensitive data is kept) are inside the internal network (behind the firewall). As shown:

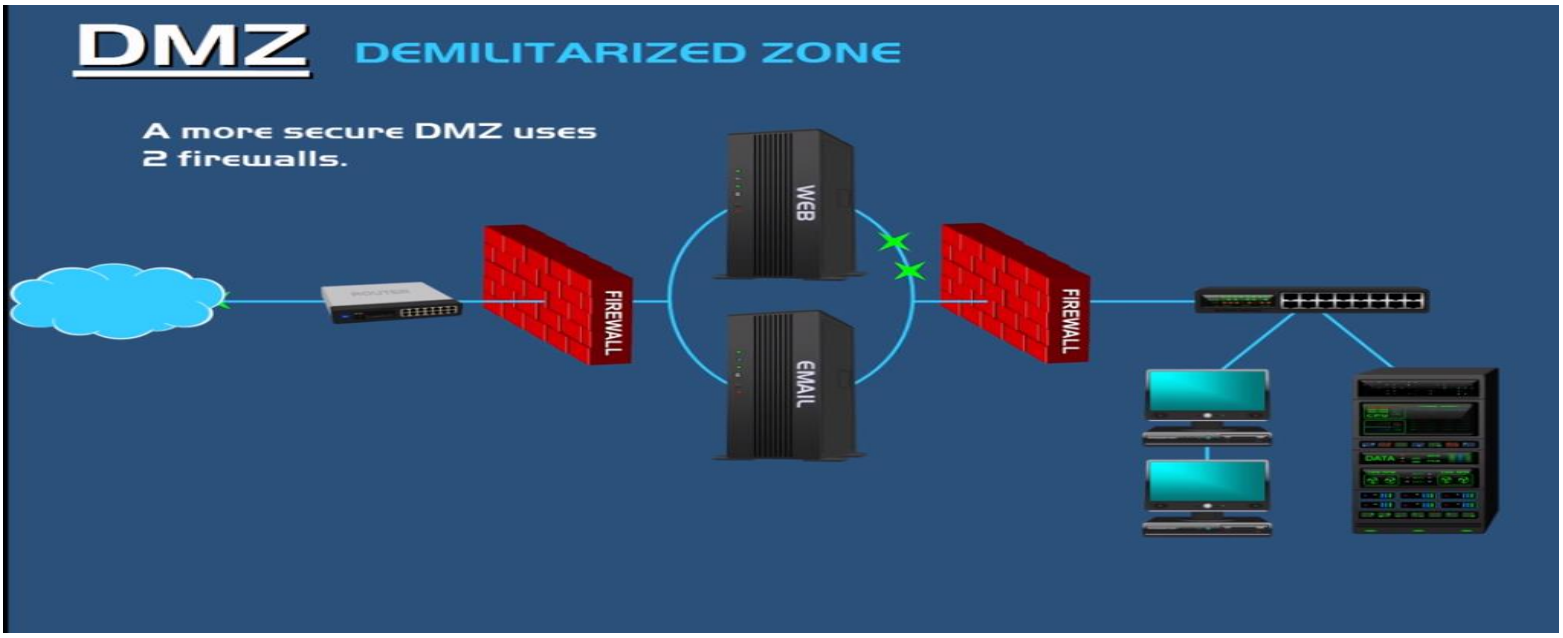


So now, when people access the WEB & Mail servers, the other servers behind the firewall aren't going to be accessing.

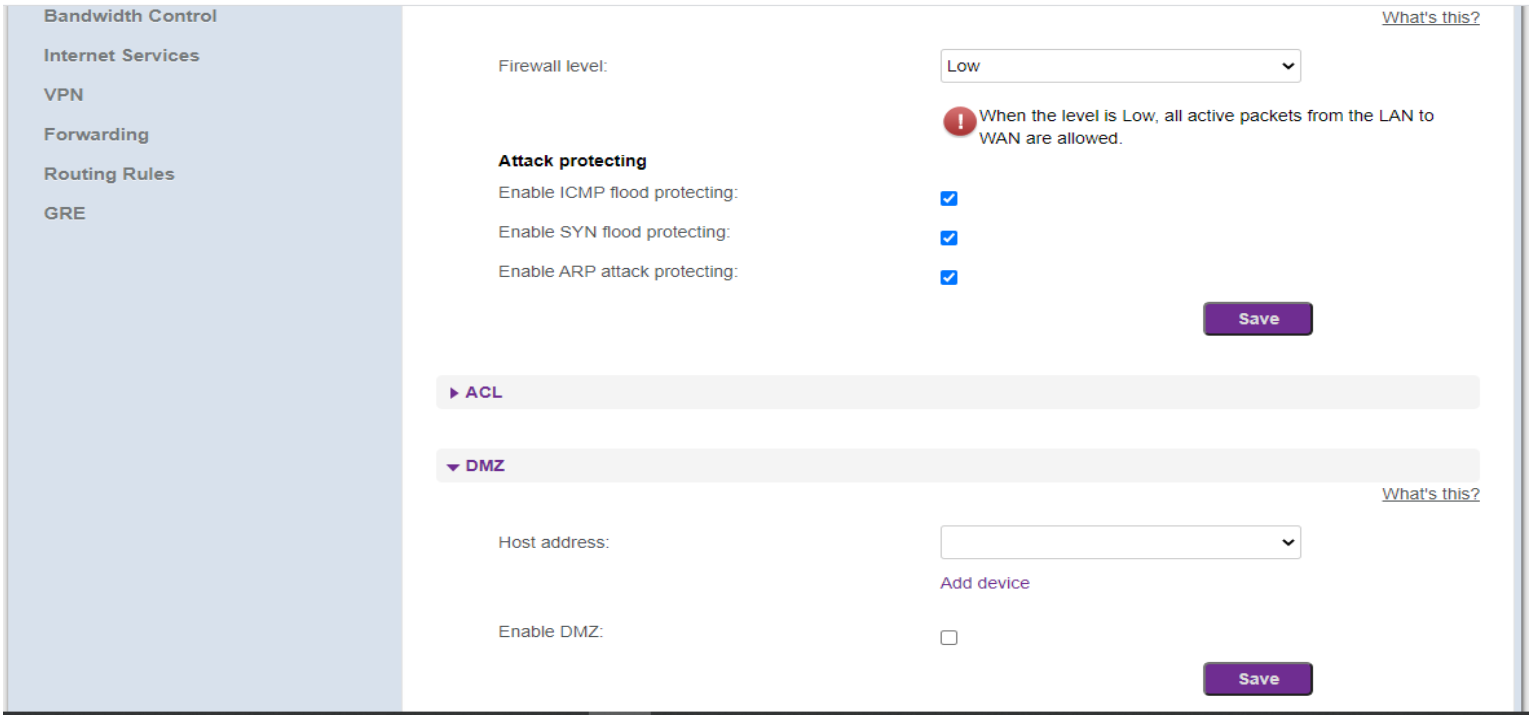
This technique act as a screened network to detect any malicious activity before it can get behind the firewall and into the company's internal network, by dividing a network into 2 parts by taking certain devices from inside the firewall and putting them outside the firewall.

An ordinary DMZ use only one firewall, but a more secure DMZ uses 2 firewalls (an extra firewall is added and then putting in front of the DMZ)

as shown



we can do this from the router configuration page as shown:



References:

1- Chapter 4 Cisco unified Wireless LAN security fundamentals

2- Cisco.Press.CCNA.Wireless.Official.Exam.Certification

3- Wireless_security_techniques_an_overview

4- Wireless LAN security " Kevin wallace " youtube tutorial

5- Abeer hosni CCNA 200-125 youtube Tutorial (WI-FI technology)

6- Tutorials on youtube (what is DMZ, ACL, etc.)