Mobile and Wireless Technology

Name : Sandesh Subedi 'A'

Intake : BSc. IT (Semester III)

Intake Code : NPI2F1909IT

Student ID : NPI000040

Course Code : CT090-3-2

Exam Type : Test

Date : July 15, 2021

Question no. 1)

a)

Ans.

An access point can be defined as a hardware device that generates a WLAN Network by connecting to any certain type of hardware (eg. Hub or switch).

The three types of Access Points are :

I. Autonomous Access Point

Autonomous Access Point is a standalone device that is organized and configured discretely. These access points are linked through core, distribution and access layers, which then connects to autonomous access points. These Access Points (APs) are independent, meaning without any assistance or information from other access points.

II. Lightweight Access Point

A Lightweight Access Point is a device built specifically to link to constituent that substantiate WLAN controller facilities. The network switch is linked to wireless LAN controller, which is connected to Lightweight AP and eventually among wireless devices.

III. Mess Access Point

Mesh Access Point is different to other APs as they study the surrounding in which they are in. Unlike Autonomous or Lightweight, this access point is configured as a mesh point or portals and the most appropriate path is selected for the portal.

Question no. 1)

b)

Ans.

PIN BASED Security Solution :

In order to keep the WLAN network secure from any sort of threats, the PIN Based system is considered to be a effective solution. PIN stands for 'Personal Identification Number' which avoids unauthorized users to enter and use the WLAN Network with the purpose of maintaining security. A PIN can be set up in a connection through access points by registering it manually or updating it in some case. The PIN method further assists in setting up the WLAN Network with other security functionalities. This way of decryption can guard the network from any unethical authorization or hacking. With this functionality, crucial data can be securely transformed with Extensible Authentication Protocol as well.

PUSH-BUTTON Security Solution :

Push-Button is an inbuilt protection system that allows Wi-Fi warrant gadgets to link to authorized and safe wireless network. It connects with the router having WPS button, which through a medium like TV or phone searches for a Wi-Fi Protected Setup connection. Once the router button is pushed, the waiting guest device generates the communication in between them. For, this to successfully happen, the hardware must be kept within appropriate range so it can get the coverage.

Question no. 2)

a)

Ans.

The three broken down configurations of ad-hoc and wireless LAN modes are :

I. Basic Service Set (BSS) :

The Basic Service Set can be defined as a building batch of Local Area Network IEEE 802.11. It is basically the stock of terminals with an access point being connected, which communicates in the LAN network dynamically. In BSS, all the channels should be connected to network so that the network topology allows all the devices to communicate freely.

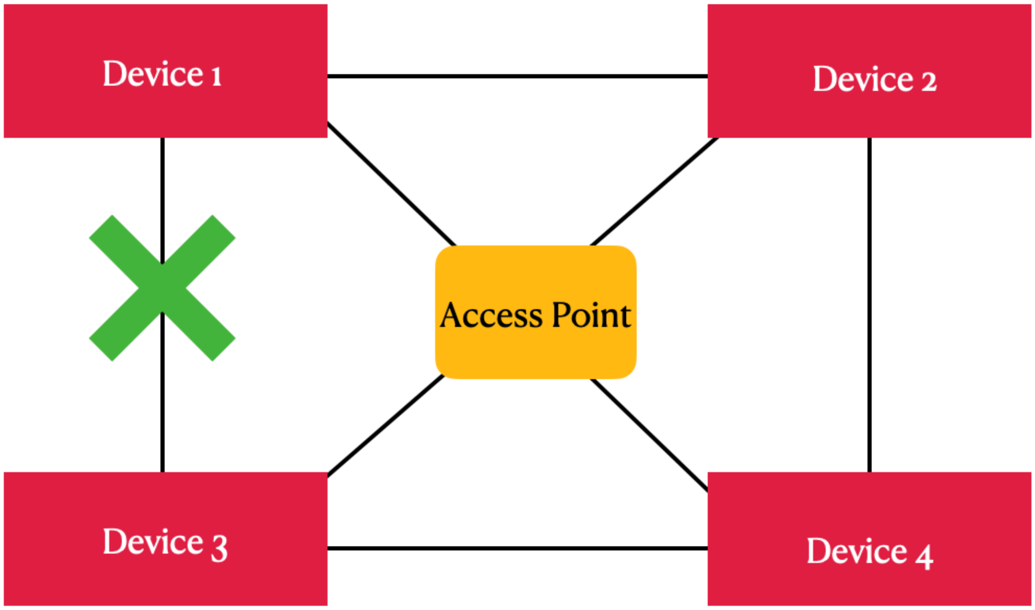

Fig. BSS Diagram

II. Independent Basic Service Set (IBSS)

The IBBS network, also known ad ad-hoc network is considered to be the simplest network among all of 802.11 LAN. Similar to that of BBS, this network also has several stations which communicates to each other freely. However, there is no any medium in between Independent Basic Service Set (IBBS) assistance.

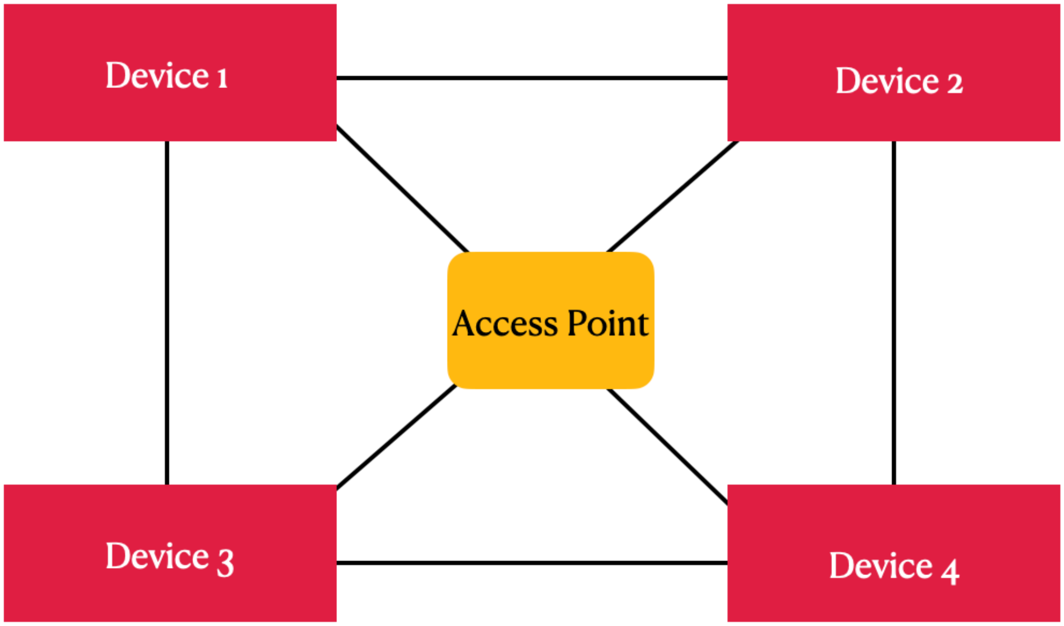

Fig. IBSS Diagram

III.Extended Service Set (ESS)

When two or more Basic Service Sets (BSS) are connected, a new service set is introduced. This is known as Extended Service Set. Unlike BSS or IBSS, the ESS comprise of two or more than two APs, which helps in long range communication facilities. Despite its high usability, this service set is also known for complexity during its usage.

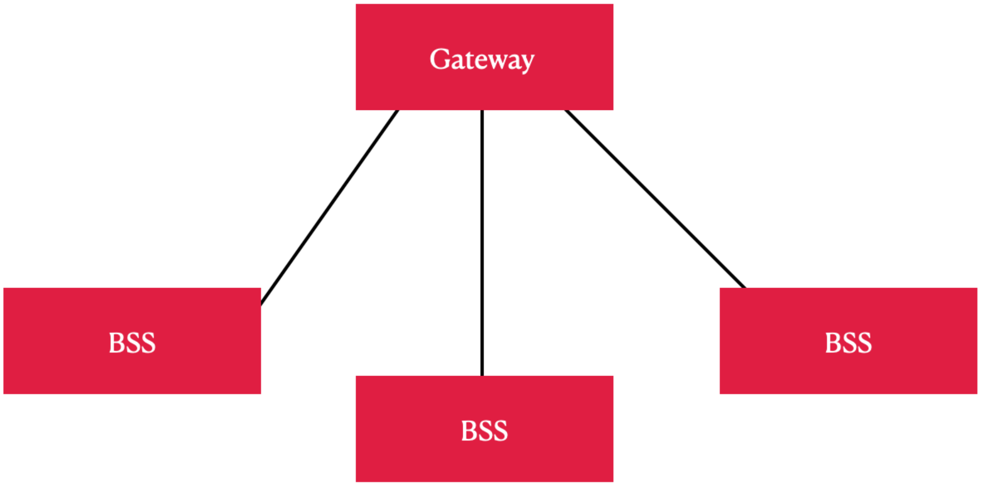

Fig. ESS Diagram

Question no. 3)

b)

Ans

The two Wi-Fi authentication modes are :

I. Open Authentication Method :

This is considered to be the simplest method of authentication in Wireless Fidelity. During this process, end device and access points are communicated for which both of these needs to be aware of each other. An authentication request is sent to SSID, which is approved without any more information.

II. Shared Authentication Method :

This method of Wi-Fi authentication is a bit complex in comparison to that of Open Authentication Method. This is usually used in small scale or in SOHOs. Like the name suggests, this method uses a shared key. The shared key is accessible to both sides during the linkage and the process succeed when the provided key matched in both sides.

Question no. 4)

a)

Ans.

Any three common early WLAN security mechanisms are :

- **Service Set Identifiers (SSIDs)**

The Service Set Identifier is the mechanism that uses a sequence of characters as a mode of security. Those characters are 32 digits, unique and linked with packet headers. The SSID functions as a security code, when any device such as mobile or laptops tries to authorize the network. With SSID, only devices that use same 32 digit code can access to the network while others are denied.

- **Media Access Control (MAC)**

Similar to other security mechanisms, the Media Access Control (MAC) is unique address of an hardware. This is a inbuilt number that every device user owns when they purchase the gadget. Previously, the MAC address used to have 48 bits within it. However, several changes were made from IEEE and the 64 bit MAC address is there with EUI-64. I charge of transmission of data packets, MAC address also supplies address appliances.

- **Wired Equivalent Privacy (WEP)**

Constructed in 1990s, Wired Equivalent Privacy (WEP) is the first security mechanism for WLAN security. The Wired Equivalent Privacy uses encryption of information with the key values from system as well as users. With this method of key, only with accurate key can authorize the WLAN network in order to communicate, while the wrong key are instantly denied from access. However, with development of technology and increase in number of crackers, this method is being volatile. Hackers can now use several tricks to break the key and enter the secured network as well.

Question no. 5)

b)

Ans.

Any four security threats faced by wireless networks are :

i. Denial of Service :

Denial of Service is a type of cyber attack where the hacker or unauthorized user tries shutting down the network or even the device entirely. The main purpose for these kind go hacks is to block the real users get access to their own information. This is done by creating a huge traffic within a network, which eventually creates complications to users in using their information or credentials. The major victims of DoS are found to me high level institutions and their employees, who are supposed to own important details with them.

ii. Evil Twin Attacks :

The evil twin is a cyber hacking where users are fooled with a fake network. As the name suggests, hackers and crackers construct a duplicate network ID (Twin) which is easy to confuse someone who has not much knowledge about networks. When the user logs in the duplicate network, credentials are stolen and might be used for any purposes. This method of hacking is being used for phishing and stealing the data from users in illegal way.

iii. Configuration Problems :

While configuring a WLAN network, a lot of complications might arise within it. Among all these issues, most of them can be solved in a ease. However, in some cases, the unsuccessful configuration results in weaknesses and loopholes, which eventually posses a lot of threats from the network. This is usually created through some problems in access points, which is later used without solving it. These sort of activities can create threats to WLAN networks and should be prevented as soon as possible.

iv. Rogue Access Points :

Rouge Access Point is one of the most ordinary type of security warn in contemporary period. This type of hack is usually done for phishing and stealing the credentials from users. When a Rogue AP is constructed, the hacker is accessible to act as a access point and create a phishing site on their own. In this way, users somehow enter their important data within that platform, which will eventually get stolen.

Question no. 3)

a)

Ans.

Two major parts of discovery phases in IEEE 802.11 wireless networking are given below:

i) Passive Scanning :

Passive scanning can be defined as a analyzing process that monitors traffic within the network. Considered to be less sensitive, the passive scanning offers precise information to the users despite consuming less power. During this type of scanning, Wireless Local Area Network stations travels to a unique channel and interrelate with the endpoints. This way of scanning requires more time period and remains cases which cannot be noticed with passive scanning. Since this process does not usually create traffics, there is a low risk with this scanning process. The passive scanning process does not require transference as it stays waiting for the frames, which are further deciphered and used to withdraw data.

ii) Active Scanning :

Active scanning is a testing process that checks the condition of system and to extract information within it. During active scanning, the test traffic is transmitted to endpoints in order to supervise the system. This allows the scanning process to gather the information. Unlike passive scanning, the active scanning searches frame instead of waiting for it. This method can be pretty effective if it is used in an appropriate way. However, if it is not handle correctly, it can backfire, creating a lot of complications (including network and cost issues). The overload of signals can distract the scanning process from its actual task and can cause a huge mishap during the process as well.

Question no. 5)

a)

Ans.

The two types of Radio Frequency (RF) Line of Sight are :

- **Visual Line of Sight :**

In visual line of sight, a transmitter should always visualize the receiver in order to maintain ideal and complete transmission. A connection between two points is required where the signal is supposed to transmit in a straight line without any physical obstructions. However, the visual line of sight seems to be impractical in real world as there are several factors (such as environmental factors like diffraction and reflections for example) that disrupts the linear connection between two connection points.

- **RF Line of Sight**

The Radio Frequency (RF) Line of Sight refers to the transmission of radio signals from one station to another station in order to maintain the communication in between them. Unlike Visual LoS, the transmission of signal should not necessarily be in linear path and even with some obstructions which are usually present in a site.

Question no. 4 b)

Ans.

They factors of influence are:

- WLAN Coverage (Area to be covered)
- Applications to be used
- Obstacles within the site
- Line of Sight
- Environmental Interferences (Reflection, Diffraction and Absorption)
- Radio Frequency (RF) range of the network
- Intended users or Number of users
- WLAN Hardware and Output Power
- Power Transmitters and Propagations