# **Experiment No.5**

**Aim:** To Study how channel selection affects packet collisions in WLAN

**Prerequisite:**

1. Understanding of basics of WLAN

**Outcome:**

After successful completion of this experiment students will be able to

1. Understand how channels selection affects packet collisions in WLAN

**Theory:**

The 2.4 GHz band is 100 MHz wide and spans from 2.4 GHz to 2.5 GHz. The IEEE standard

divides the 2.4 GHz band into 14 separate channels. Channels are designated by their

centre frequency and how wide the channel is depends on the technology used by the

802.11 transmitter. Unfortunately, the distance between channel centre frequencies in the

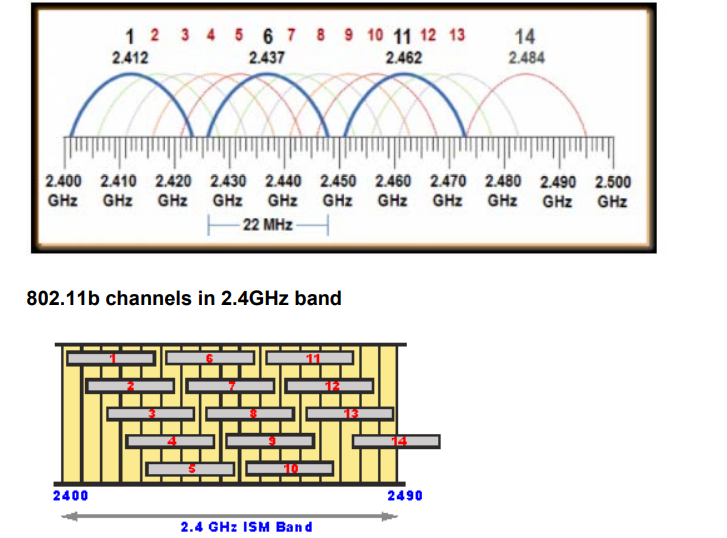
2.4 GHz spectrum is only 5 MHz (and each channel is 22 MHz wide), which means that the

channels have overlapping frequency space.

Only channels 1, 6, and 11 are separated from each other by enough frequencies that they

do not overlap. Enterprise deployments of three or more access points in the 2.4 GHz band

should normally only use channels 1, 6, and 11 which are shown below.



From the diagram above, it can be seen that Wi-Fi channels 1, 6, 11, or 2, 7, 12, or 3, 8, 13 or 4, 9, 14 (if allowed) or 5, 10 (and possibly 14 if allowed) can be used together as sets. Often WiFi routers are set to channel 6 as the default, and therefore the set of channels 1, 6 and 11 is possibly the most widely used.

**Refer NetSim experiment manual experiment no 5 available in portal and follow the steps systematically.**

**Create the scenario for Sample 1 and Sample 2**

**Experiment No.5**

(PART B: TO BE COMPLETED BY STUDENTS)

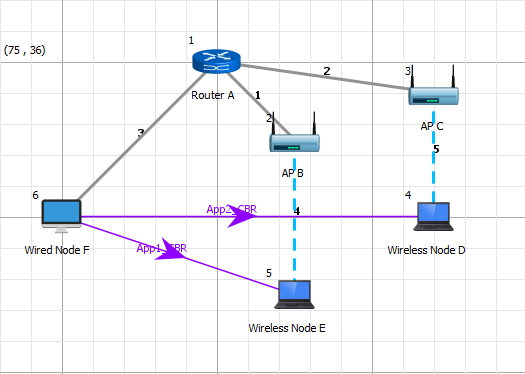
**(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)**

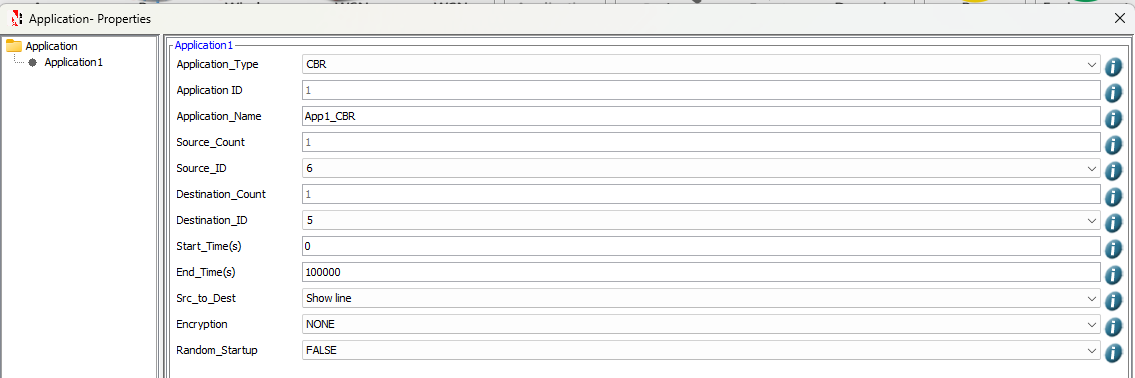
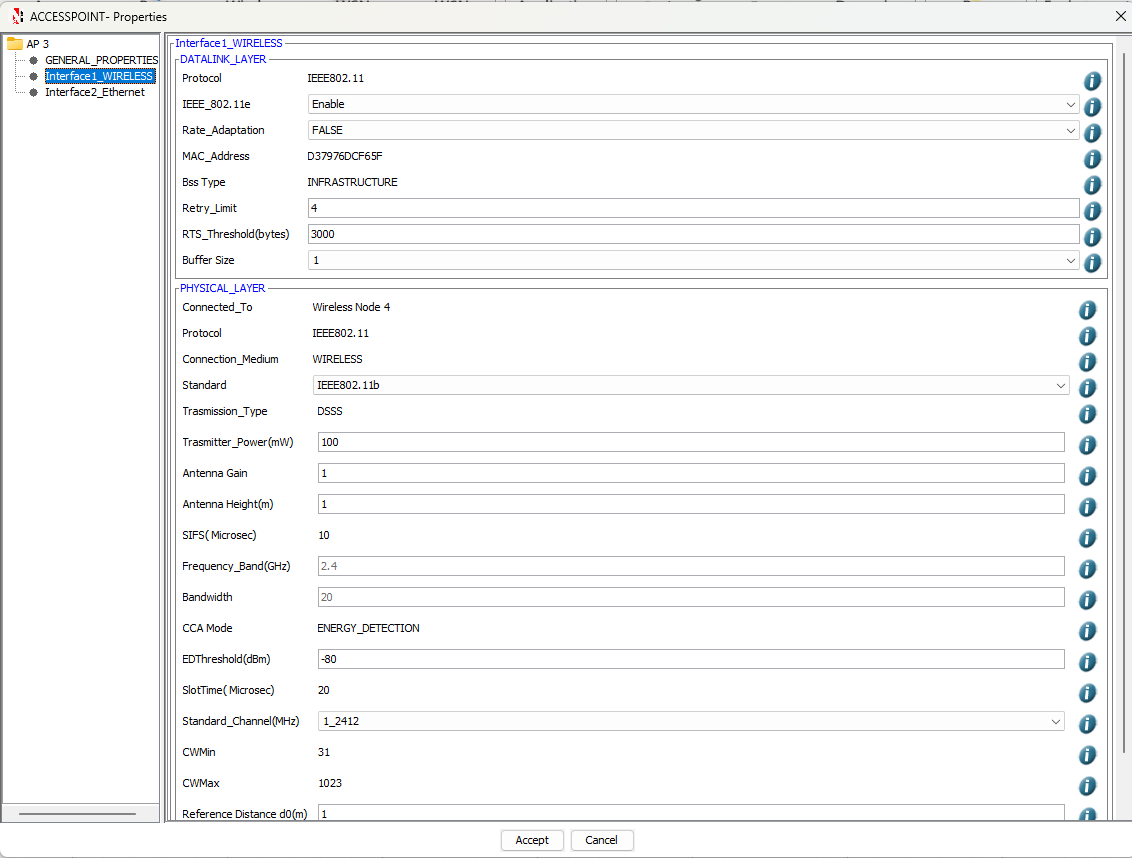
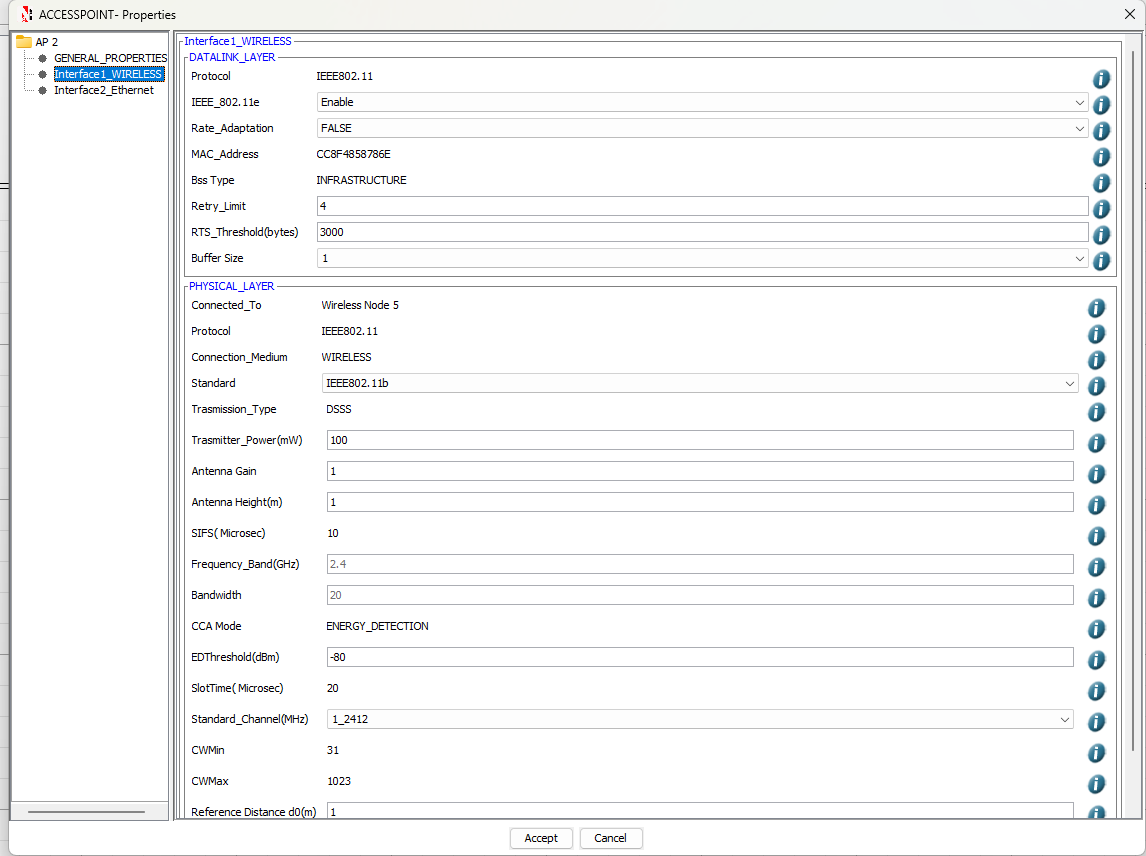
|  |  |
| --- | --- |
| Roll No. C114 | Name: Rishikesh Vadodaria |
| Class: C | Batch: C2 |
| Date of Experiment: 22nd February 2025 | Date of Submission: 22nd February 2025 |
| Grade : |  |

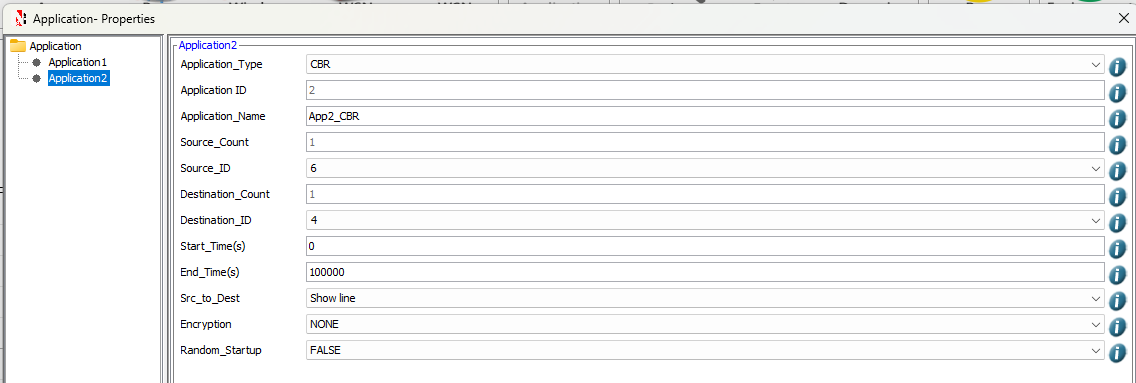
## **B.1 Input**

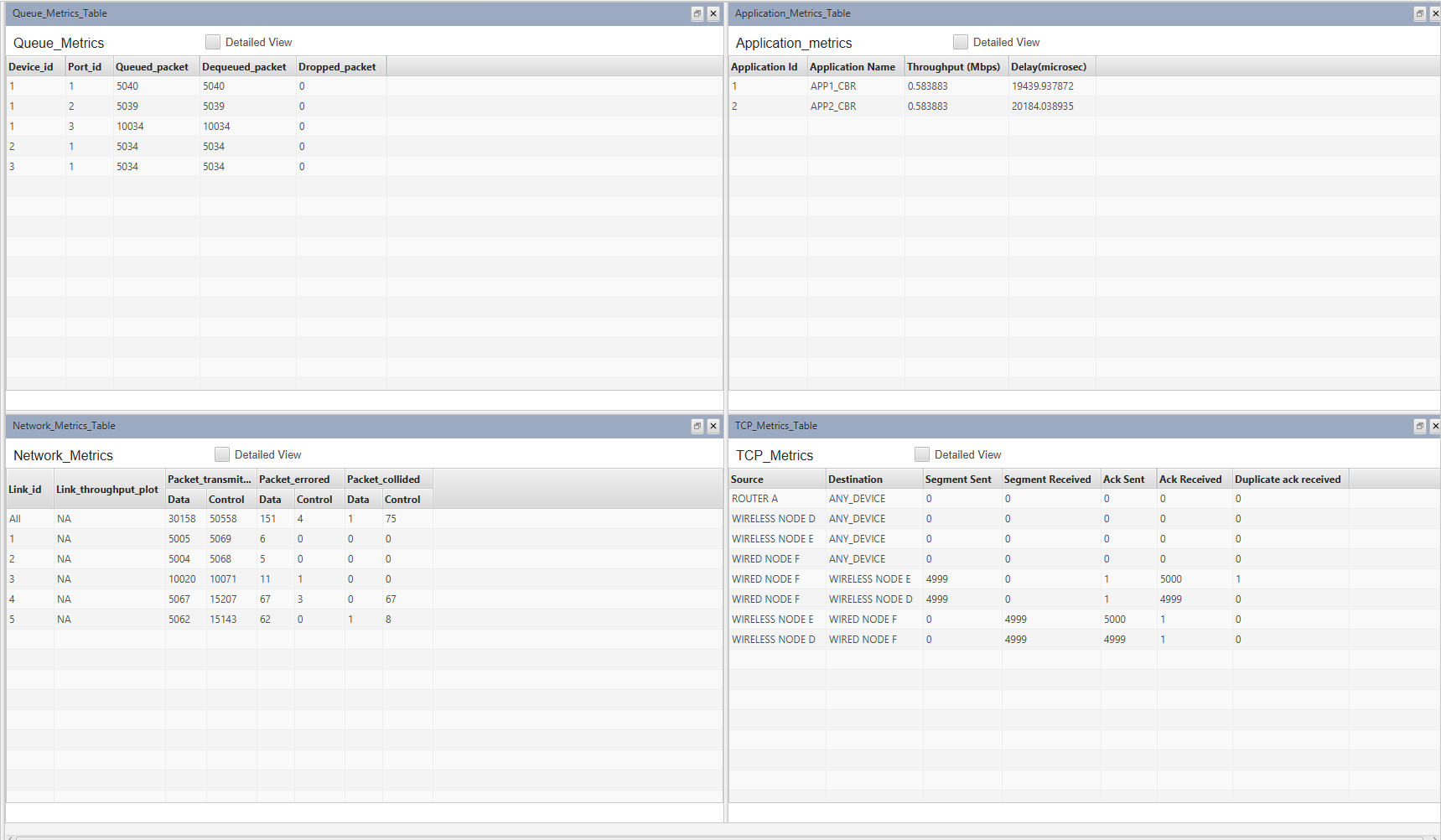
**Include screenshots of the topology for every increase in the number of nodes ( atleast 3-4), parameter metrics of application created.**

**Simulation 1:**

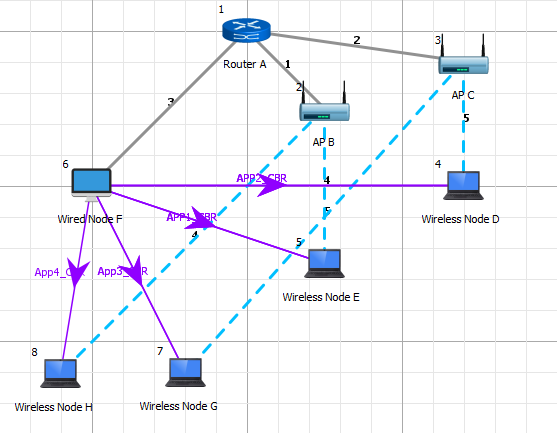


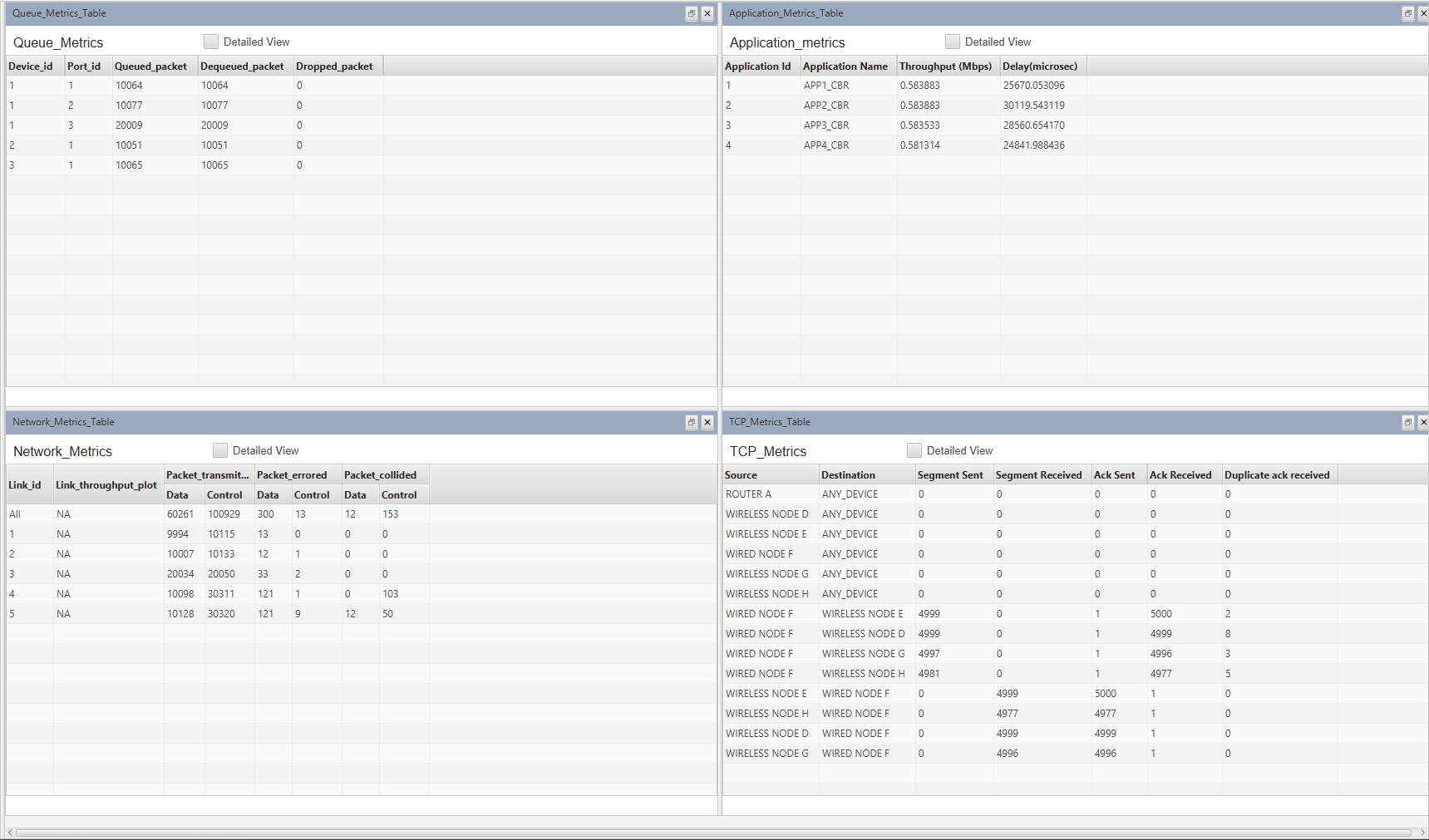






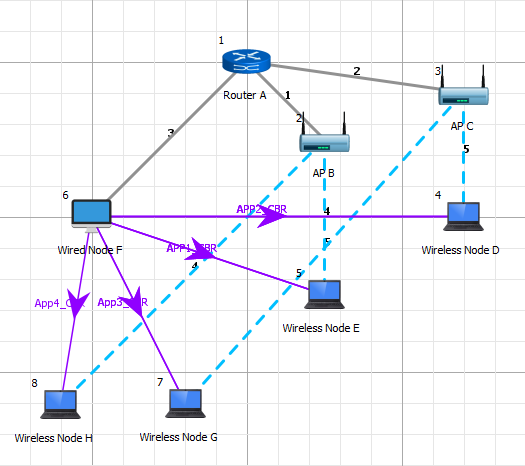
No of Packets collided: 1

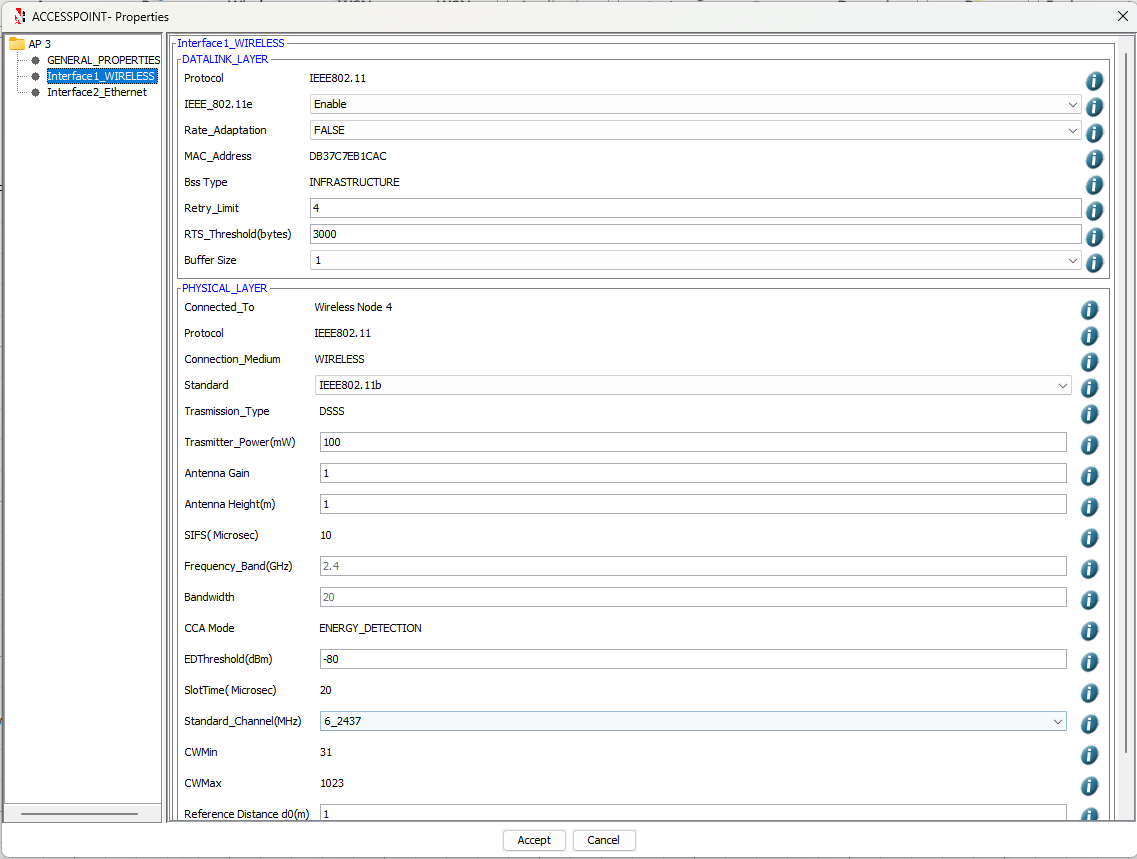


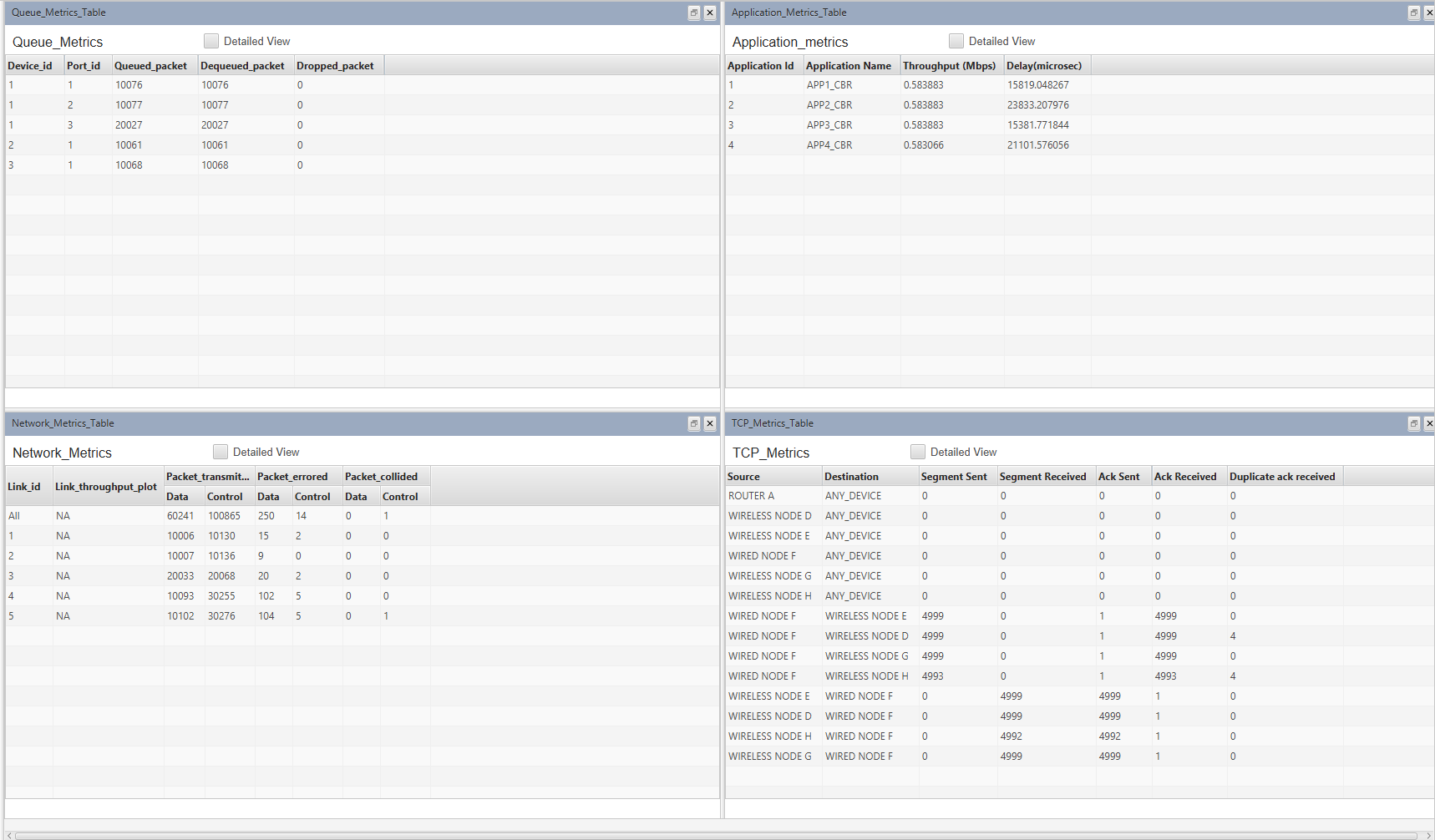


No of Packets collided: 12

**Simulation 2:**

****

****

****

Number of Packets collided: 0

## **B.2 Simulation results**

|  |  |
| --- | --- |
| **Sample** | **Collided Packets** |
| **Sample 1** | **2 Nodes: 1, 4 Nodes: 12** |
| **Sample 2** | **4 Nodes: 0** |

## **B.3 Conclusion and Inferences**

After successful completion of this experiment, I was able to understand how channels selection affects packet collisions in WLAN.

**B4. Questions of curiosity**

Q1. WLANs usually form the end point that connect users to data resources on the internet. What are the highest data speeds presently available in WLANs?

**Answer:**

The highest data speeds available in WLANs depend on the Wi-Fi standards being used:

* **Wi-Fi 6 (802.11ax):** The maximum theoretical data speed of Wi-Fi 6 can reach up to **9.6 Gbps** (gigabits per second), which is significantly faster than previous standards. Wi-Fi 6 offers improvements in efficiency, range, and speed compared to its predecessors.
* **Wi-Fi 6E:** This is an extension of Wi-Fi 6 that operates in the 6 GHz band, offering higher speeds and less interference. It can also support data rates up to **9.6 Gbps** with better performance in crowded environments.
* **Wi-Fi 7 (802.11be) (upcoming):** Expected to be the next major Wi-Fi standard, Wi-Fi 7 promises even higher speeds, potentially reaching **30 Gbps** or more.

So, the highest speeds currently available in WLANs (as of Wi-Fi 6 and Wi-Fi 6E) are around **9.6 Gbps**, with Wi-Fi 7 set to go beyond that.

Q2. Write any two techniques to improve security of Access Point.

**Answer:**

1. **Enable WPA3 Encryption:**
   * WPA3 (Wi-Fi Protected Access 3) is the latest encryption protocol, providing enhanced security over WPA2. It includes features like **individualized encryption** for each device on the network and protection against brute-force attacks, ensuring that data traffic is secured and more difficult to intercept.
2. **Disable WPS (Wi-Fi Protected Setup):**
   * WPS is a feature that makes it easier to connect devices to a Wi-Fi network by pushing a button or entering a PIN. However, WPS is vulnerable to attacks like brute-force cracking. Disabling it helps prevent unauthorized access to the network, improving the overall security of the access point.

By combining WPA3 and disabling WPS, you can significantly enhance the security of an Access Point.