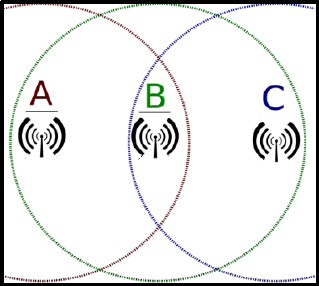
Experiment 3

**AIM:** To Study the hidden node problem in WLAN

# Theory:

Hidden nodes in a wireless network are nodes that are out of range of other nodes or a collection of nodes. In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as **A**, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, **C**. These nodes are known as *hidden*.



The problem is when nodes A and C start to send packets simultaneously to the access point

B. Because the nodes A and C are out of range of each other and so cannot detect a collision while transmitting, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur, which then corrupt the data received by the access point.

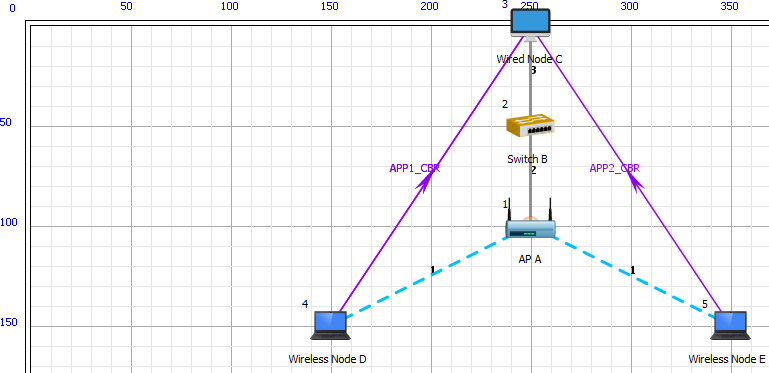
To overcome the hidden node problem, RTS/CTS handshaking (IEEE 802.11 RTS/CTS) is implemented in conjunction with the Carrier sense multiple access with collision avoidance (CSMA/CA) scheme. The same problem exists in a MANET.

# Procedure:

**Sample Inputs:**

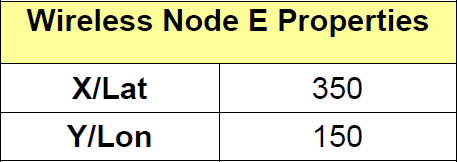
Follow the steps given in the different samples to arrive at the objective. In Sample 1,

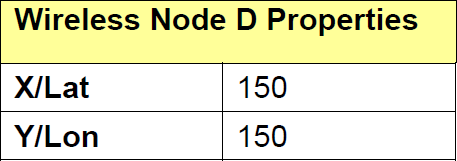
* Total no of APs (Access Points) used: 1
* Total no of Wireless Nodes used: 2
* Total no of Switch used: 1
* Total no of Wired Node used: 1



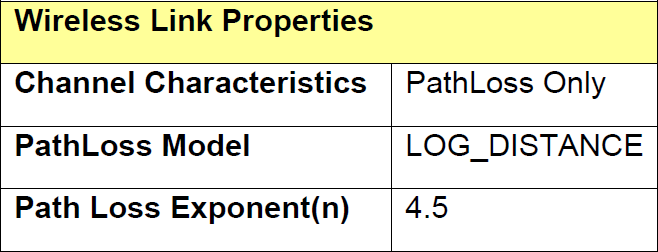
The devices are interconnected as shown:

Also edit the following properties of AP A, Wireless Node D and E:





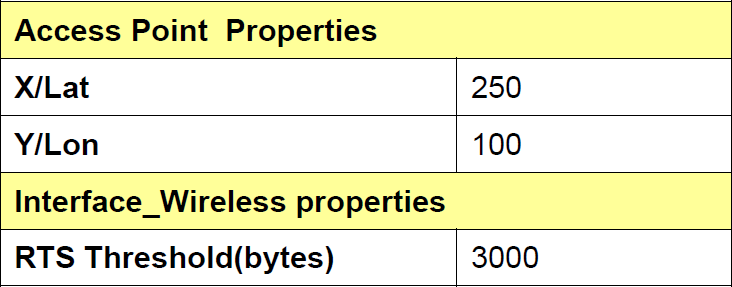
Edit Wireless link properties as shown



Properties of Wired Links are default.

Disable TCP in both the Wireless Nodes and Wired Node:

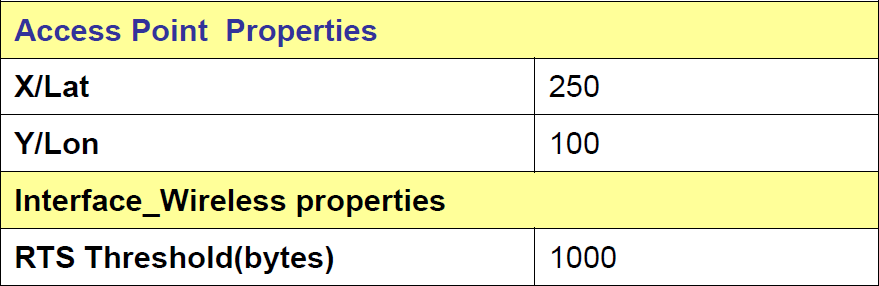
Set the properties of Access Point as follows:



# Click and drop the application and set the properties as per the NetSim manual V10.

**In Sample 2,**

**Set the properties of Access Point as follows:**



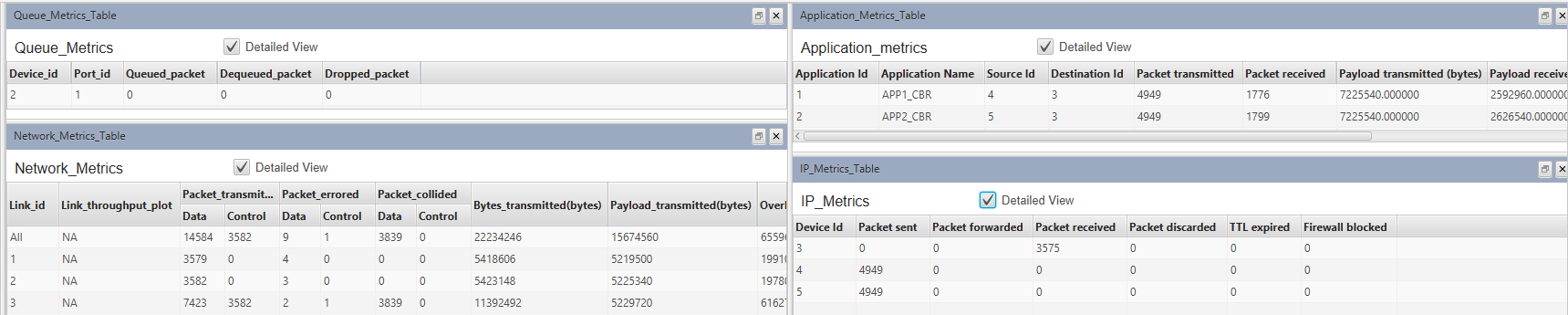
(PART B: TO BE COMPLETED BY STUDENTS)

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

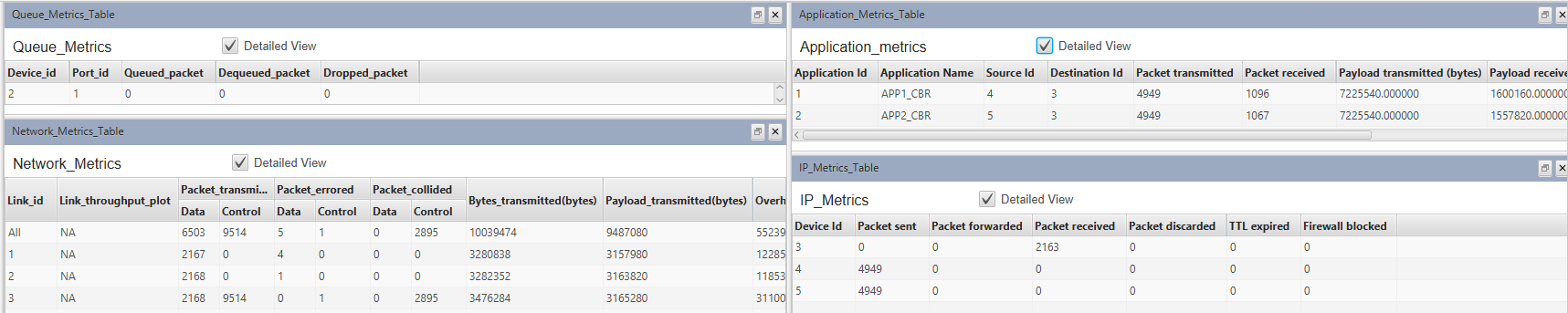
|  |  |
| --- | --- |
| Roll No. C114 | Name: Rishikesh Vadodaria |
| Class: C | Batch: C2 |
| Date of Experiment: 01-02-2025 | Date of Submission: 01-02-2025 |
| Grade : |  |

Output:

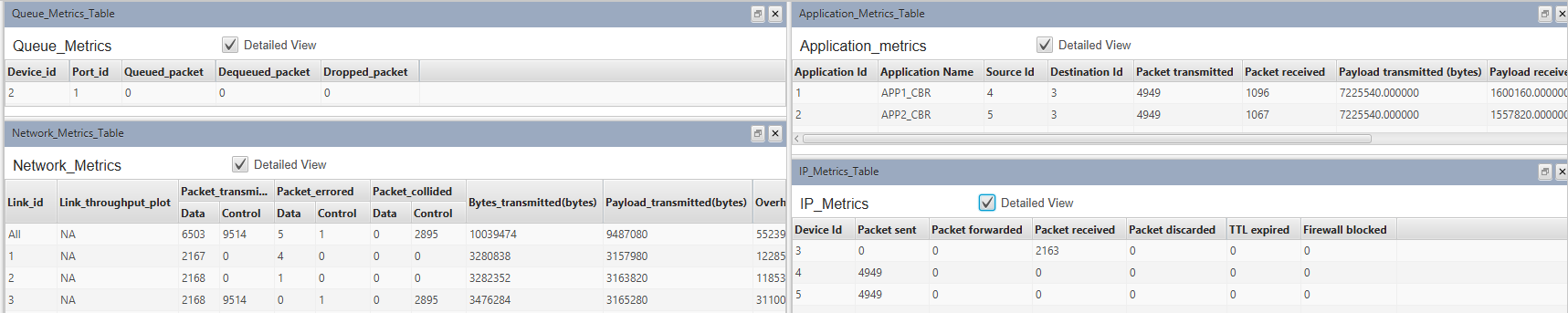
Sample 1 (RTS threshold- 3000):-



Sample 2 (RTS Threshold - 1000):-



Sample 3 (RTS Threshold - 0):-



Comparison Table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Collided Packets** | **Without RTS/CTS** | **With RTS (3000)** | **With RTS (1000)** |
| Control | 2985 | 0 | 2895 |
| Data | 0 | 3839 | 0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Metrics** | | **Without RTS/CTS** | **With RTS (3000)** | **With RTS (1000)** |
| Throughput(Mbps) | Application1 | 0.128013 | 0.207437 | 0.128013 |
|  | Application2 | 0.124626 | 0.210123 | 0.124626 |

**Questions of Curiosity:**

1. What are the ways in which hidden node problems are avoided?

Ans:

**RTS/CTS Mechanism:** The Request To Send/Clear To Send (RTS/CTS) handshaking protocol is widely used to mitigate hidden node issues. Nodes send a short RTS packet to the access point (AP) before transmitting data; the AP responds with a CTS packet, which informs all nodes in range to refrain from transmitting during that time, reducing the chance of collision.

**Increasing Transmission Power:** By increasing the transmission power of hidden nodes, their communication range can be extended, allowing them to detect other nodes and thus avoid becoming hidden. However, this method is effective only if applied to the hidden nodes themselves.

**Using Omnidirectional Antennas:** Employing omnidirectional antennas instead of directional ones helps ensure that all nodes can communicate with each other, thereby reducing the likelihood of hidden nodes.

**Node Relocation:** Physically moving nodes so they can communicate directly with each other can help eliminate hidden node scenarios. This may involve adjusting the layout of a wireless network or adding access points to improve coverage.

**Protocol Enhancements:** Implementing additional protocols that use polling or token-passing strategies can help manage access to the medium more effectively, reducing collisions caused by hidden nodes.

1. What is exposed node problem? How can you avoid this?

Ans: The exposed node problem occurs when a node is unable to send packets because it is within range of another transmitting node, causing interference even though it could successfully transmit to other nodes.

**Avoidance Strategies:**

* Carrier Sense Multiple Access (CSMA): Using CSMA allows nodes to sense the channel before transmitting, helping avoid interference with ongoing transmissions.
* RTS/CTS Mechanism: Similar to its role in mitigating hidden node problems, RTS/CTS can also help manage exposed node situations by coordinating transmissions among nodes.

1. How does the hidden node problem impact different types of network traffic (e.g., real-time video vs file transfer)?

Ans: The hidden node problem affects different types of network traffic in various ways:

* **Real-time Video Traffic:** This type of traffic is highly sensitive to delays and packet loss. Collisions caused by hidden nodes can lead to significant interruptions and degrade video quality due to retransmissions.
* **File Transfer Traffic:** While less sensitive than real-time video, file transfers can still be impacted by hidden node collisions, leading to slower transfer rates as packets are lost and need to be resent.

1. What role does transmission power control play in mitigating hidden node problems?

Ans: Transmission power control plays a critical role in mitigating hidden node problems by enabling nodes to adjust their transmission strength. By increasing power, nodes can extend their communication range and reduce the likelihood of being hidden from each other. However, excessive power increases can lead to interference with other nodes and should be managed carefully.

1. How do different wireless standards (802.11a/b/g/n/ac) handle the hidden node problem differently?

Ans:

| **Standard** | **Handling Method** |
| --- | --- |
| 802.11a | Uses RTS/CTS but has limited effectiveness due to higher frequencies reducing range. |
| 802.11b | Similar RTS/CTS implementation; however, lower frequency allows for better range but still susceptible to hidden nodes. |
| 802.11g | Incorporates RTS/CTS and provides backward compatibility with 802.11b; performance varies based on environment. |
| 802.11n | Enhanced MIMO technology improves range and reduces hidden node issues through better signal processing techniques. |
| 802.11ac | Further improvements in MIMO and beamforming help mitigate both hidden and exposed node problems by optimizing signal paths. |