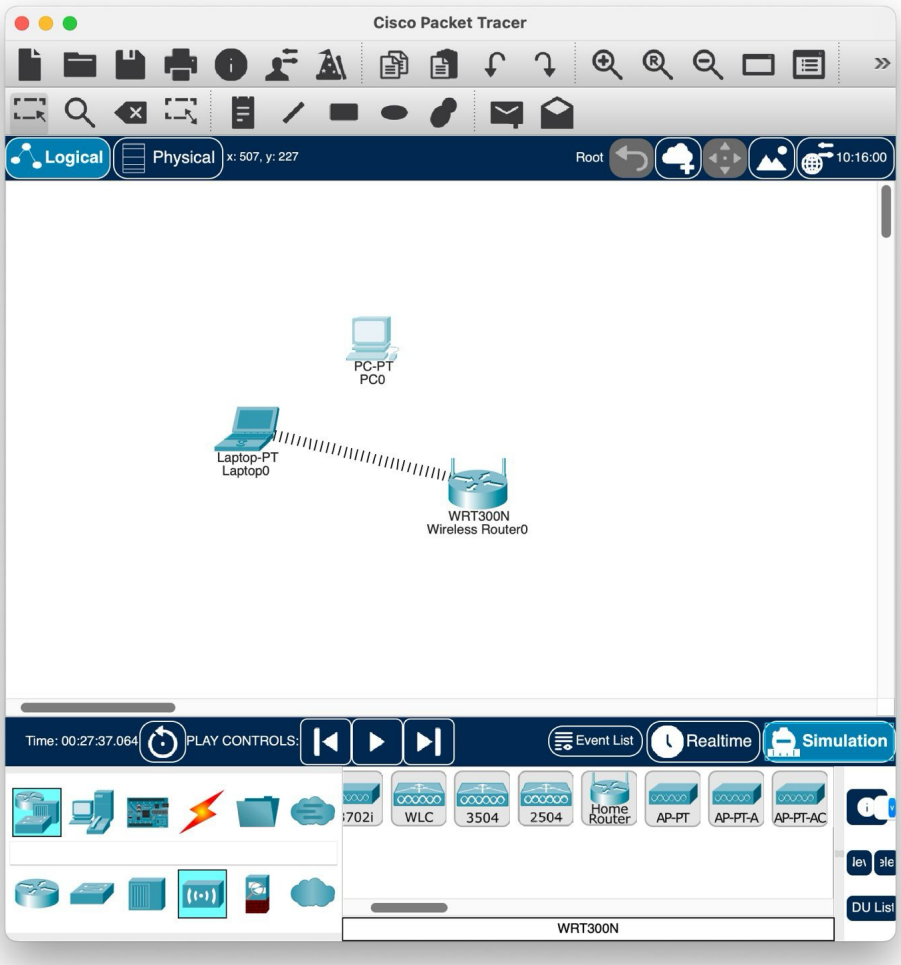
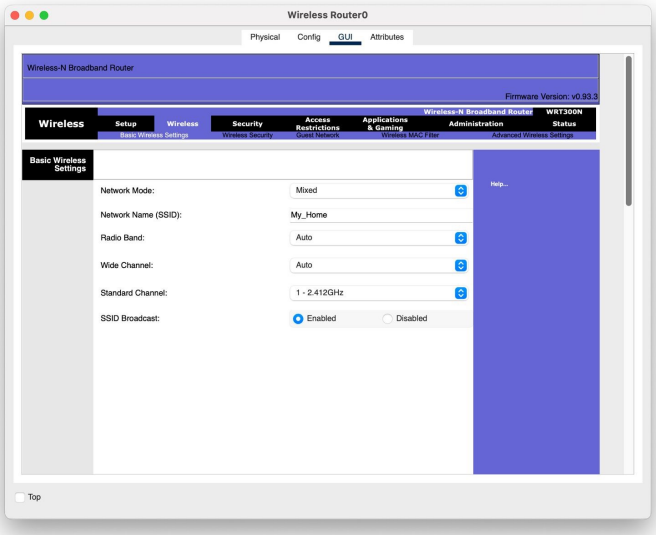
L6 - Old Device Wi-Fi Encryption Incompatibility

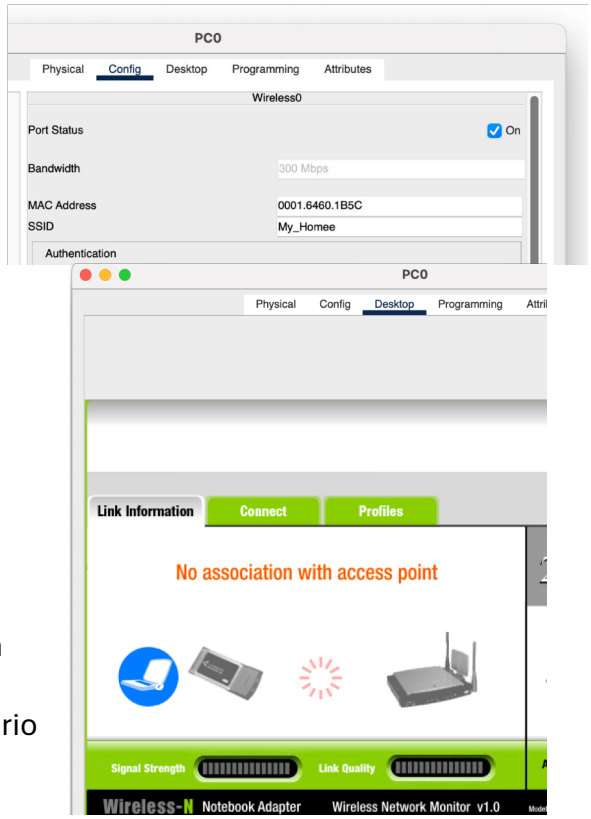
Initial Focus: Encryption Incompatibility of Old Device (Theoretical Problem)

My first goal was to simulate the encryption incompatibility that occurs when my friend has an old computer. In real life, old devices usually support older or diEerent encryption standards such as WPA-PSK (TKIP), while modern networks use stronger and newer standards such as WPA2-PSK (AES).

In this case, the device would not be able to establish a successful connection because it could not correctly decrypt the AES encrypted data coming from the router (the Presentation Layer's decryption task failed). This is the problem of the network data (in encrypted form) not being correctly represented or understood in the Presentation Layer.
Implementation and Change: Incorrect SSID Entry (Successful Simulation Method)

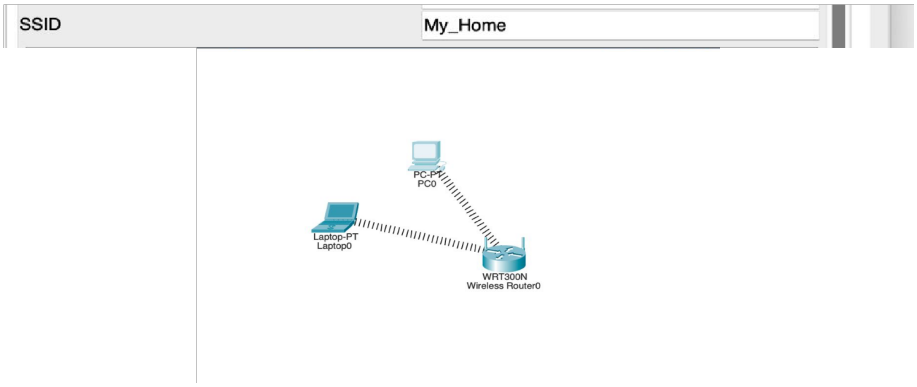






In the Cisco Packet Tracer environment, since default device adapters and router models usually support both old and new encryption standards, it became diEicult to directly simulate the “old device cannot connect” scenario through encryption mismatch alone. Devices could connect even with WPA2-PSK (AES).

In response to this situation, I turned to another real-world problem with OSI Layer 6 that would definitely prevent connectivity in Packet Tracer: Entering the wrong Network Name (SSID). An SSID is the name of a wireless network and is a data format that must be entered correctly and exactly matched in order for a device to “identify” itself to the network.



This approach again falls under the responsibility of the Presentation Layer. Because the Presentation Layer is responsible for correctly formatting and presenting the device’s request to connect to the network. If the network name is entered incorrectly, the device will not be able to find the correct network and present itself correctly, making the connection impossible.