Internet of Things

Nama : Agha Syafrila Myzantina

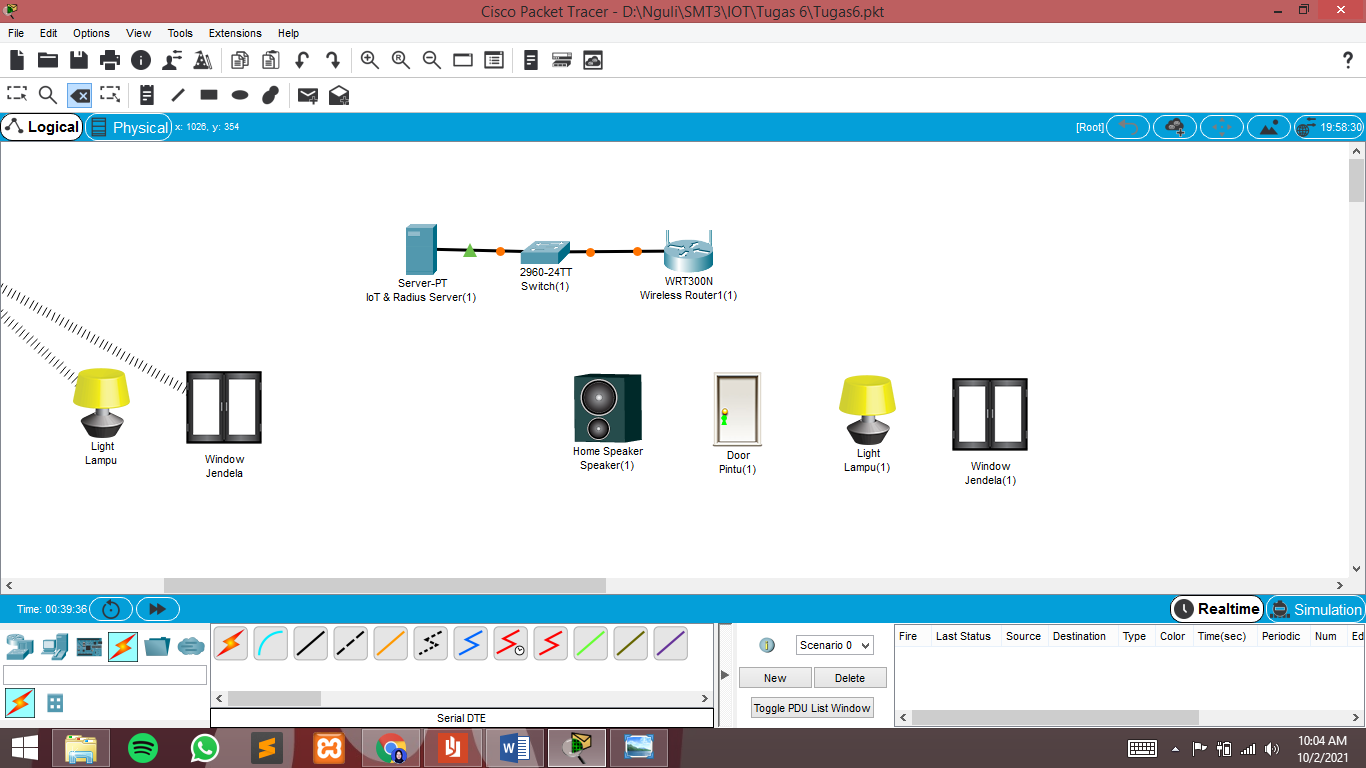
NIM : V3920002

Kelas : TI D

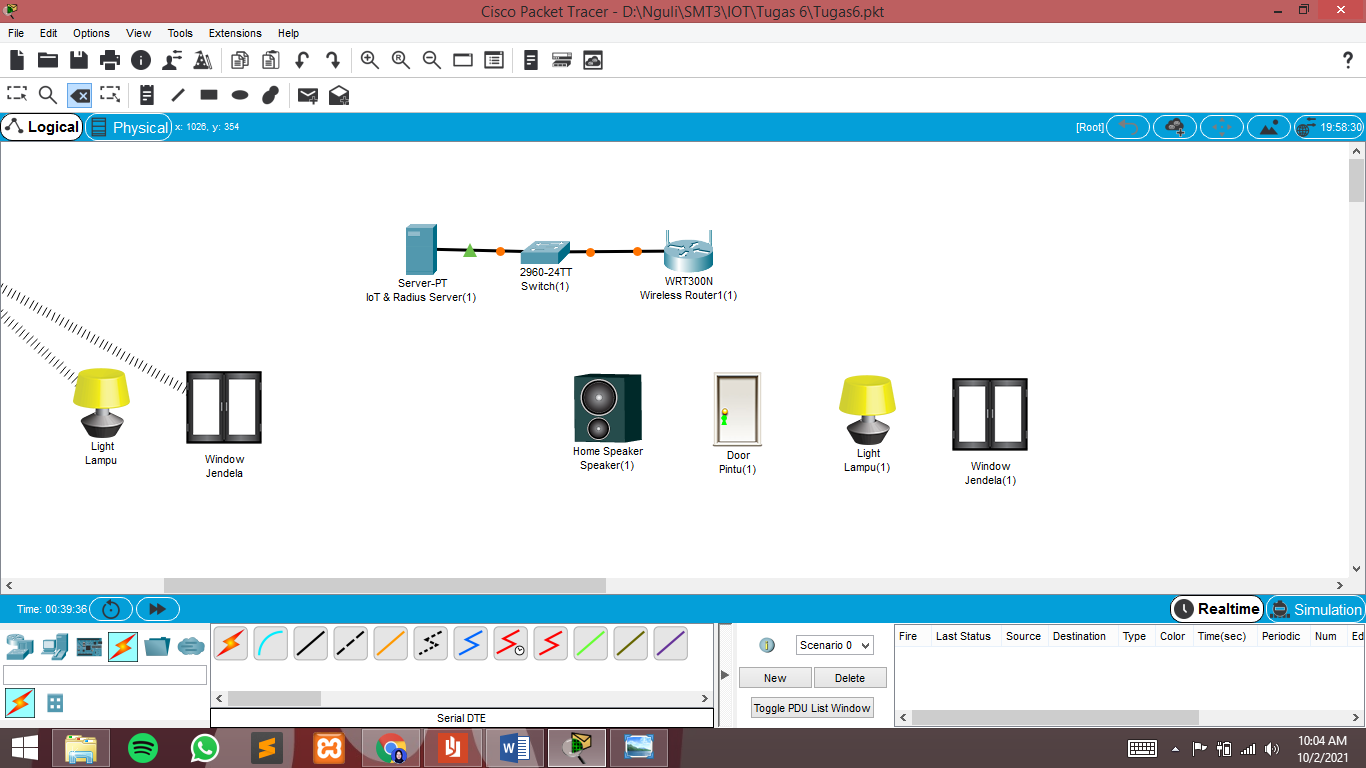
Materi : • Security by Design

• Implementing Security

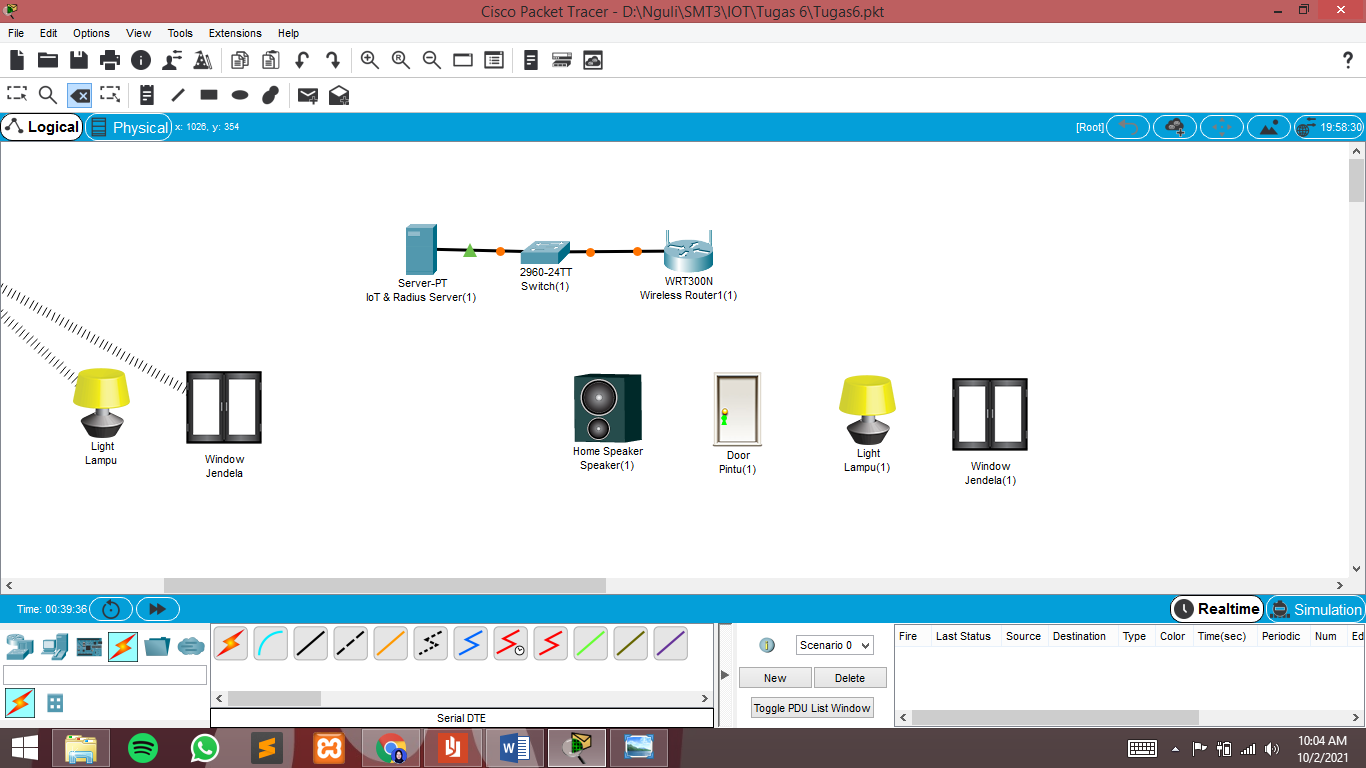
1. **Penjelasan Sistem**
2. Siapkan sebuah server, switch, router dan device yang diperlukan.

****

1. Hubungkan server ke switch, switch ke router dan semua device berhasil terhubung ke router.
2. Hubungkan sever ke switch menggunakan Atomatically Chose Connection Type

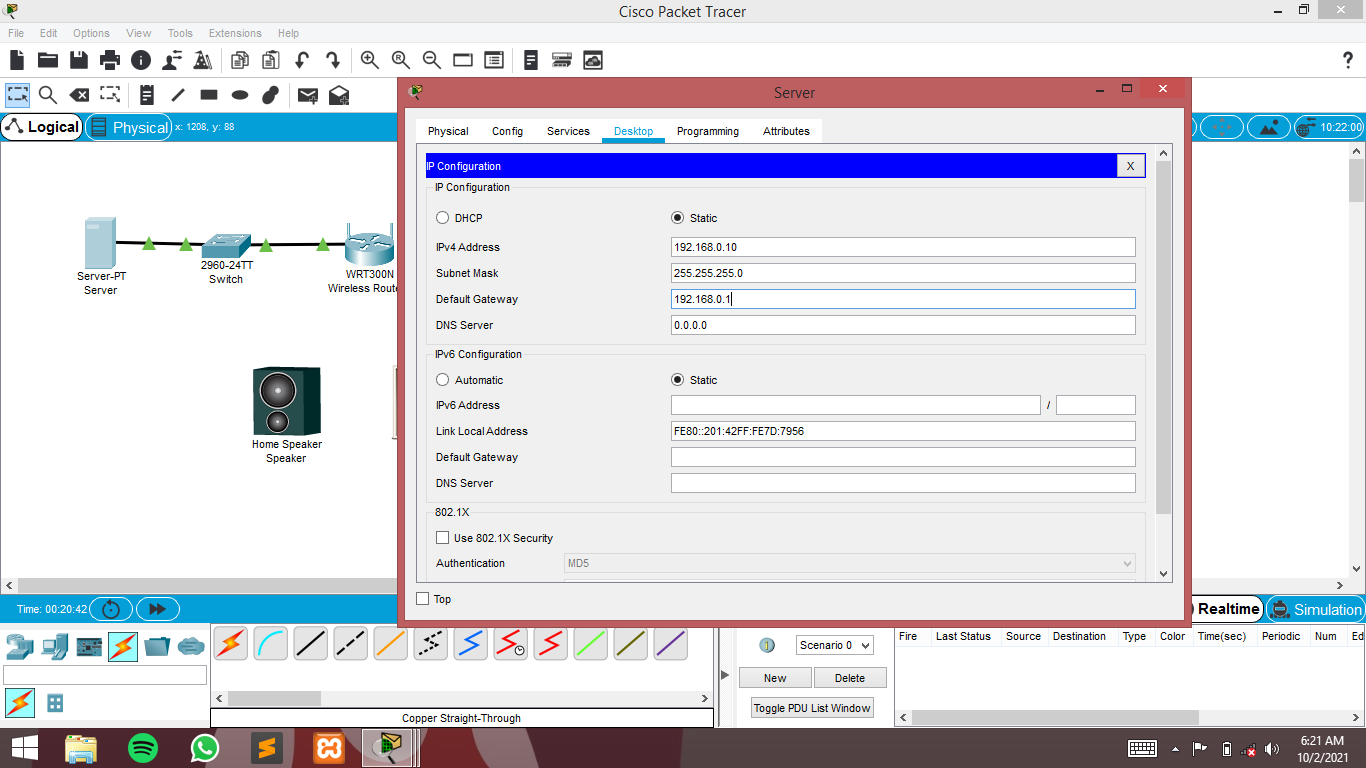
****

1. Hubungkan switch ke router dengan kabel jenis Cooper Straight

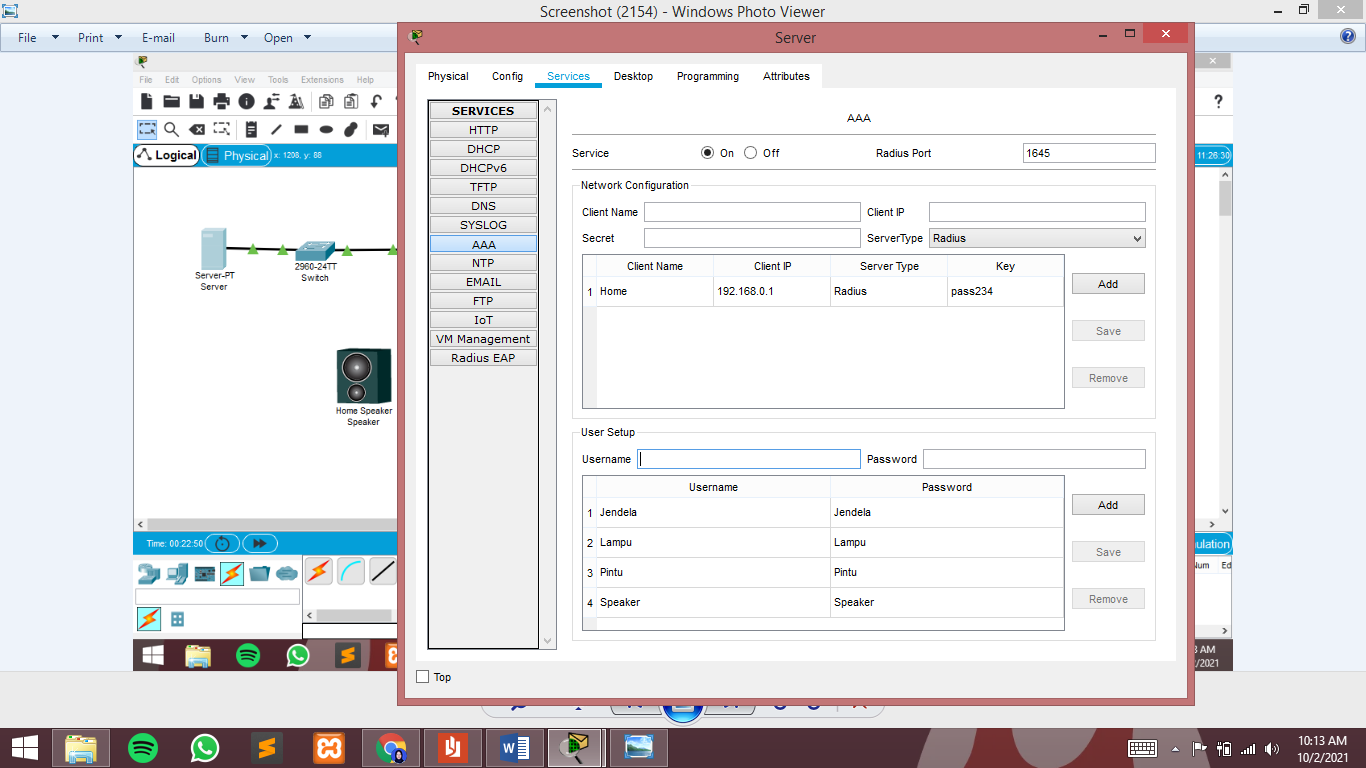
****

1. Hubungkan device ke router dengan setting pada router, IoT & Radius Server dan maisng-masing device.

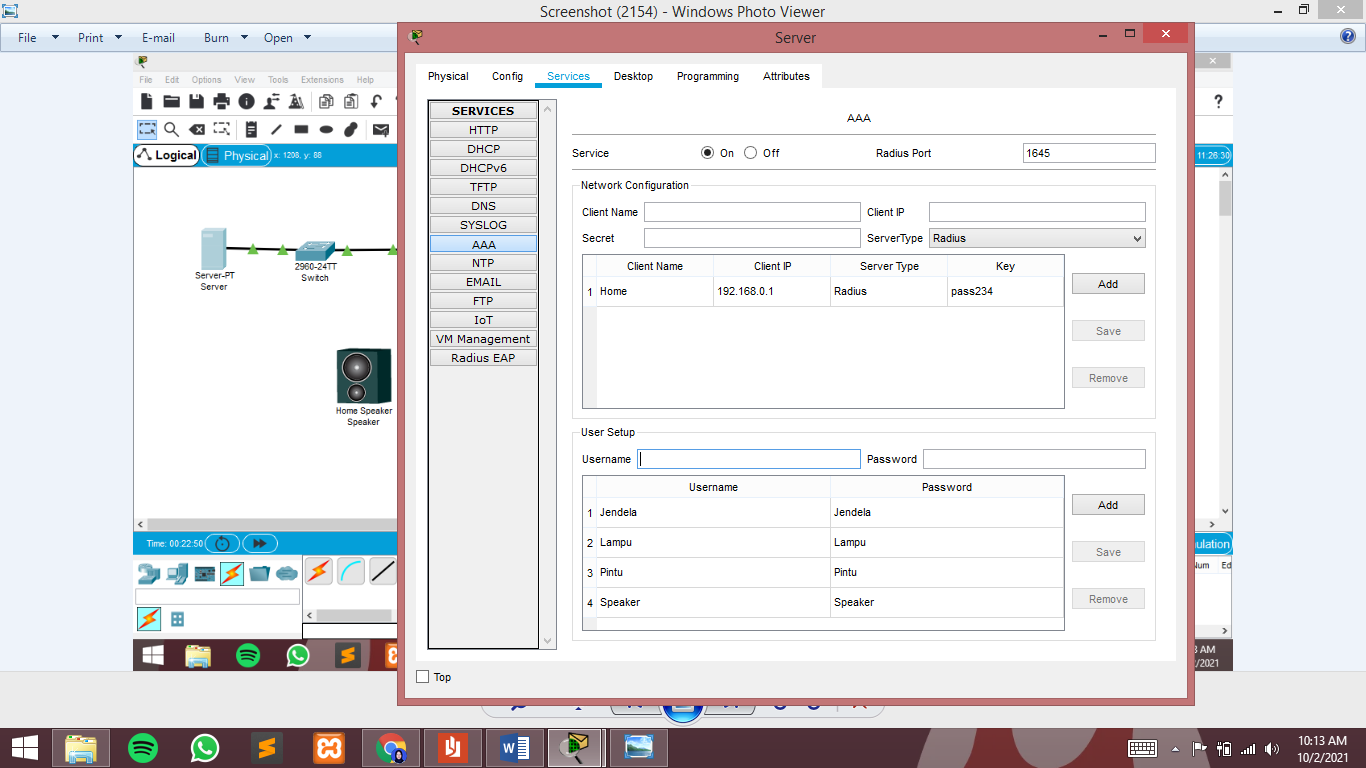
* **Setting konfigurasi IP pada server.**

****

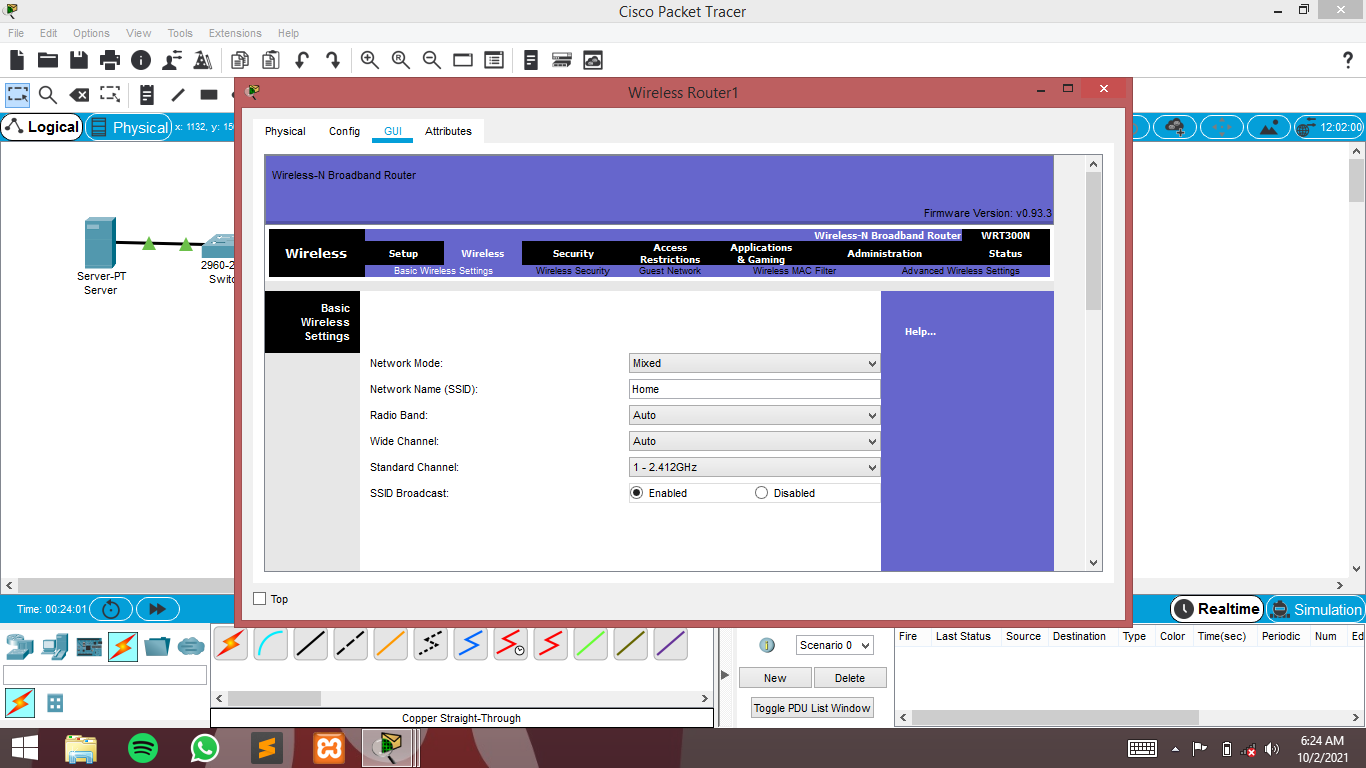
* **On kan setting service pada AAA, ganti Client name, Secret dan Client IP.**

****

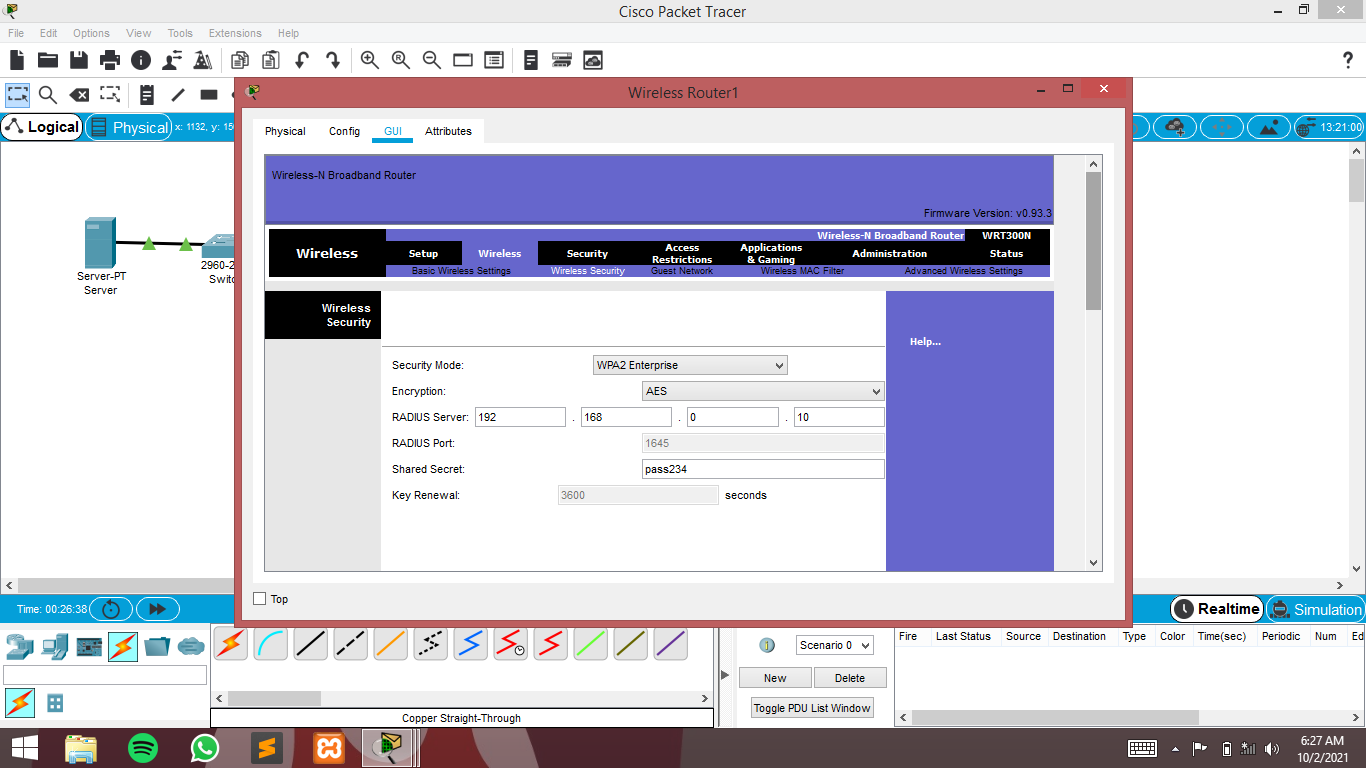
* **Tambahkan Username dan Setup masig-masing device pada User setup.**

****

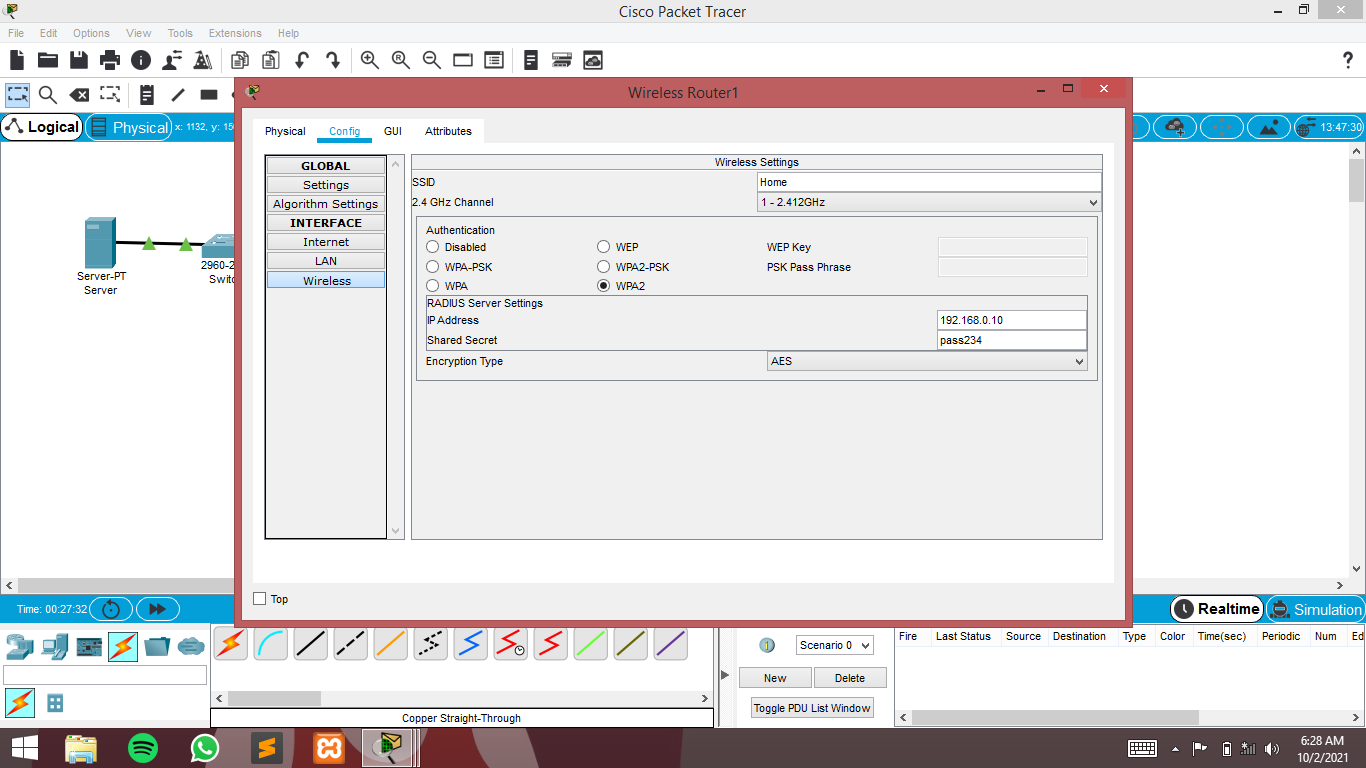
* **Setting nama wireless SSID sebagai nama jaringan**.

****

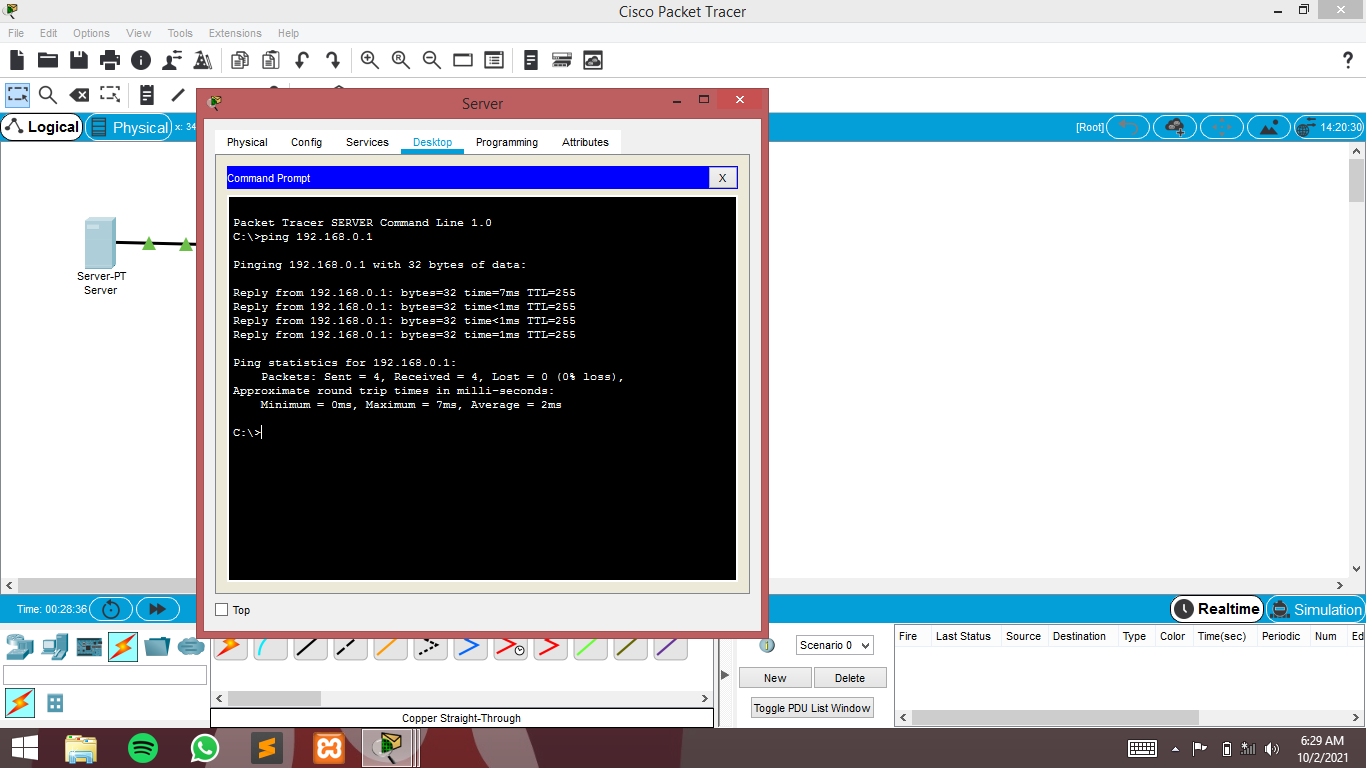
* **Pilih security mode menyesuaikan server tadi agar sama sehingga terhubung**, **tambah password dan pilih jenis enkripsi AES yang berfungsi mempertahankan integritas data pada WSN.**

****

* **Setelah itu cek pada bagian Wireless config untuk memastikan penambahan Mode security sudah berhasil.**

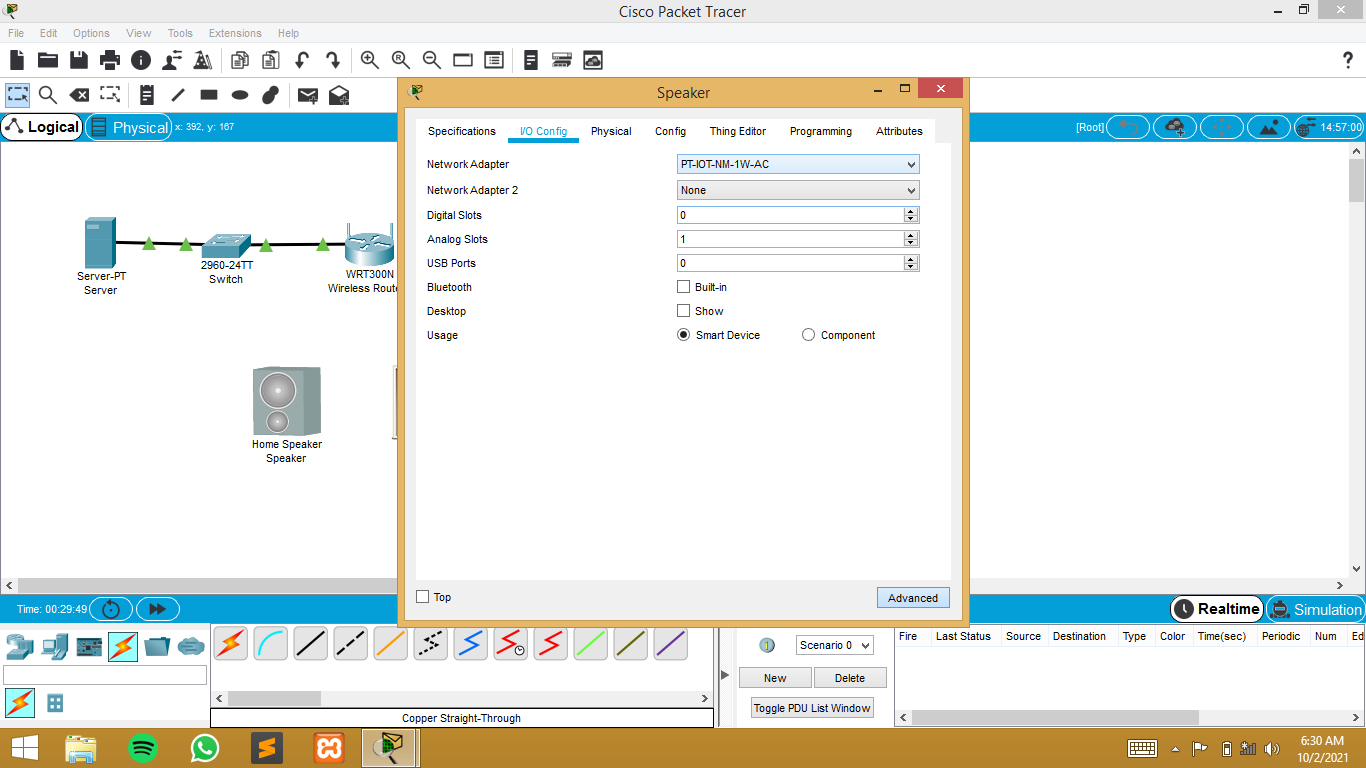
****

* **Cek koneksi pada server.**

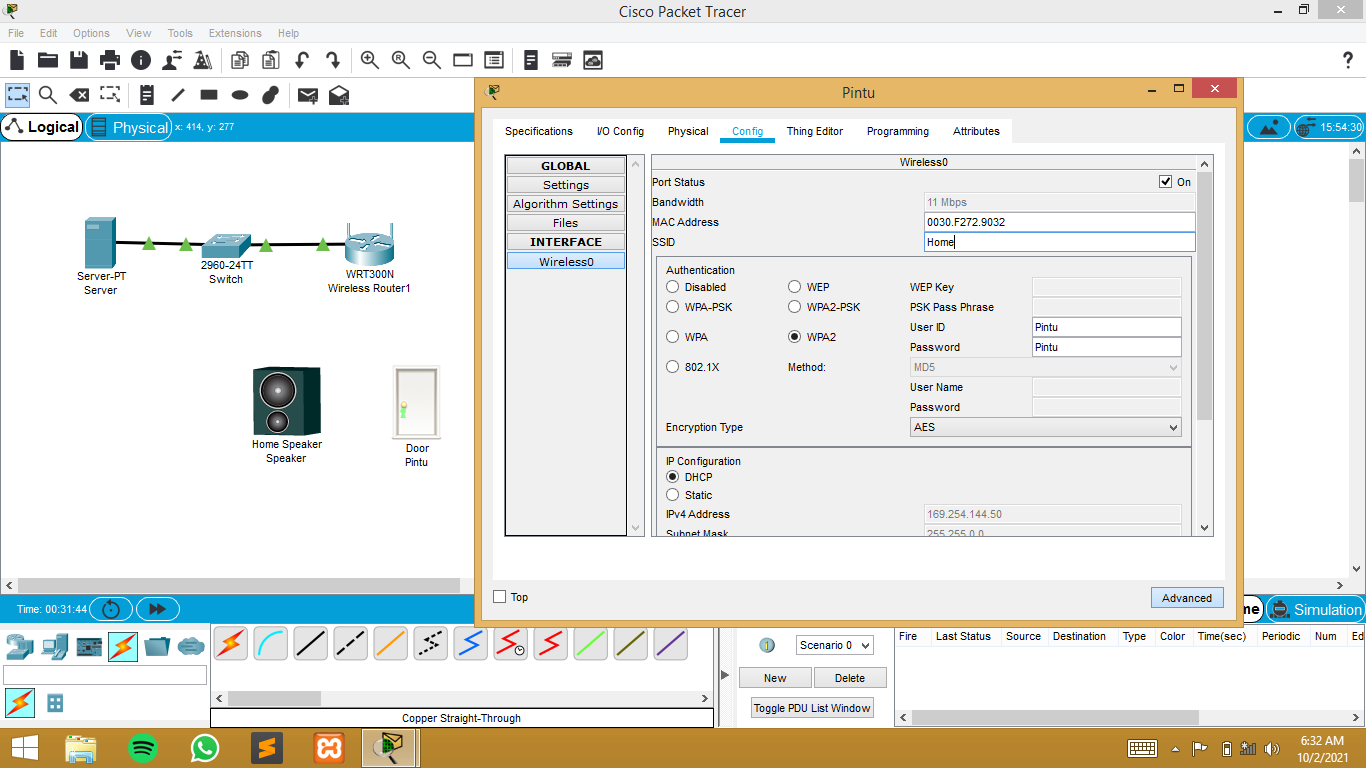
****

* **Atur Network adapter pada masing-masing device dan pastikan SSID sudah sesuai dengan SSID pada server, ubah authentication menjadi WPA2, tambahkan jug auser ID dan Password sesuai yang sudah ditambhakan pada server agar device dapat terhubung.**

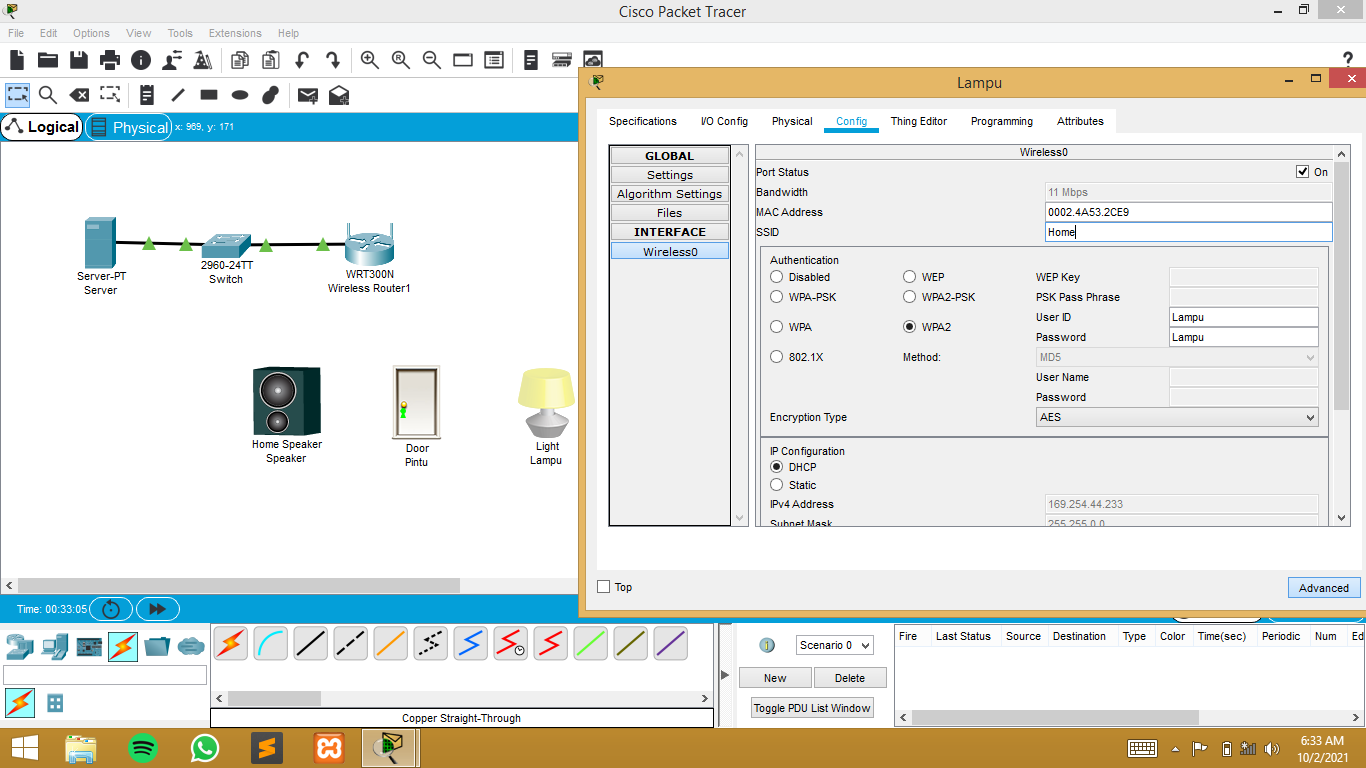
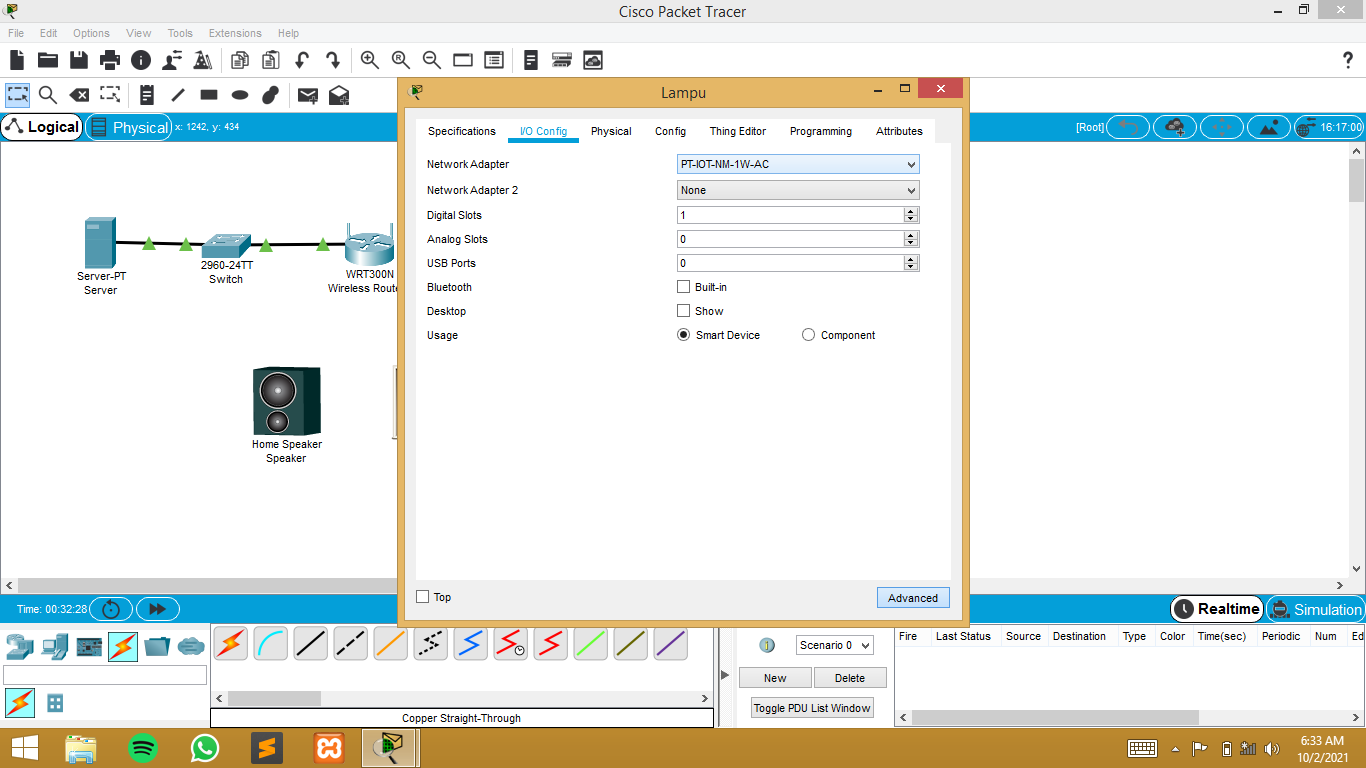
**Spreaker**

****

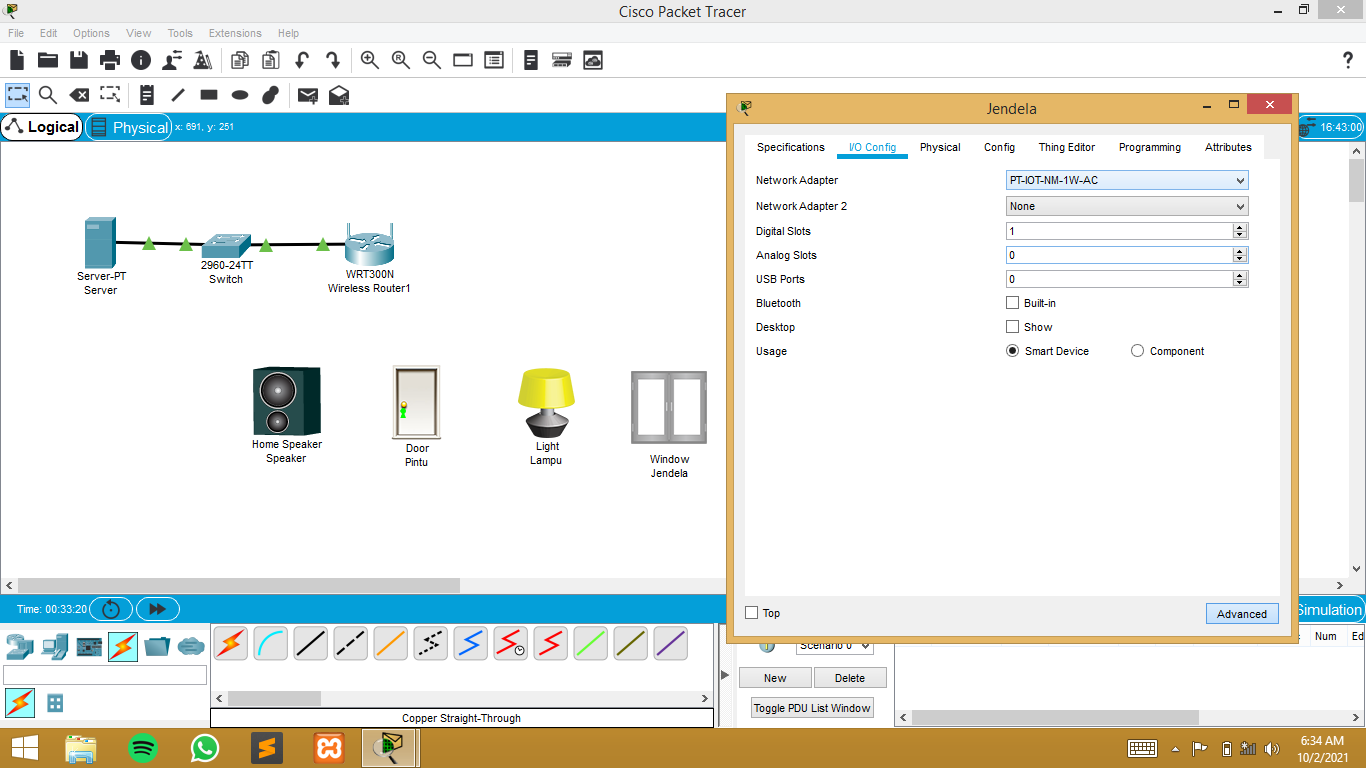
**Pintu**

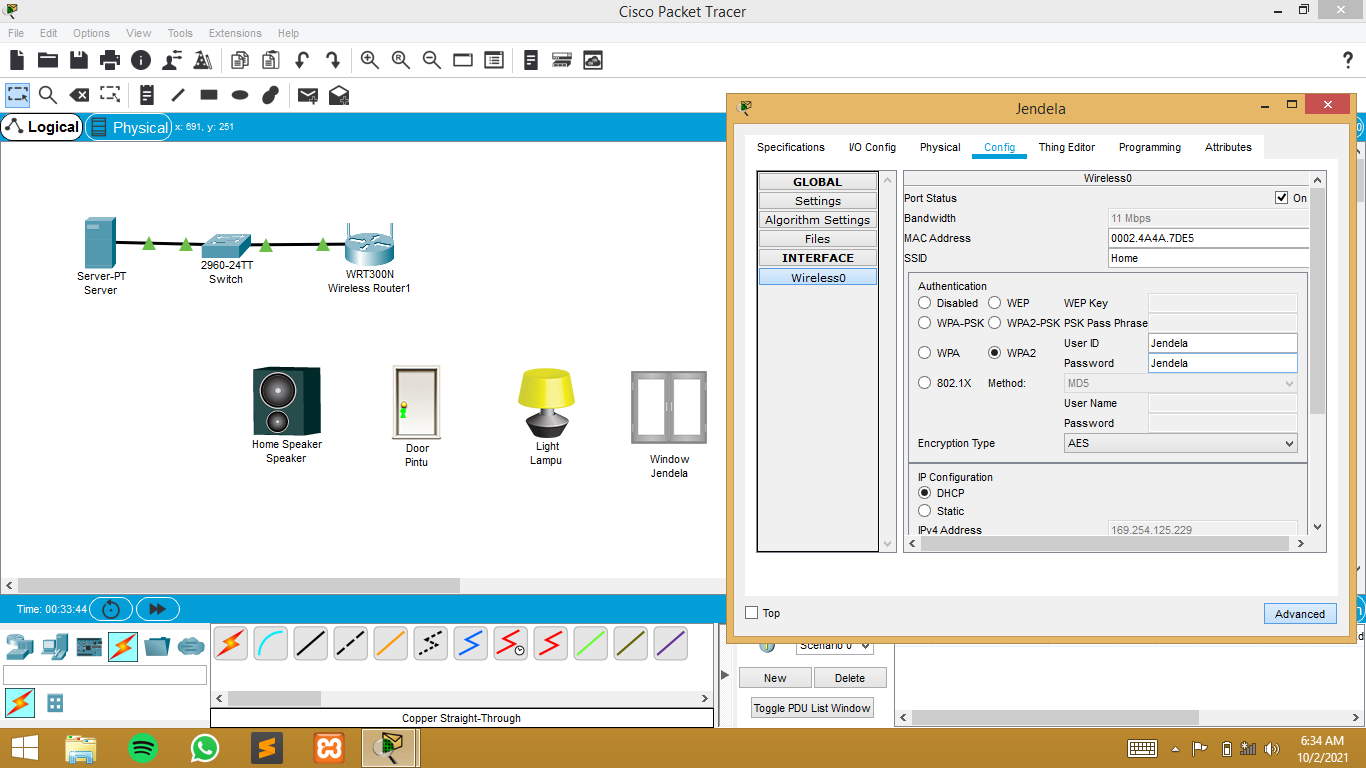
****

**Lampu**

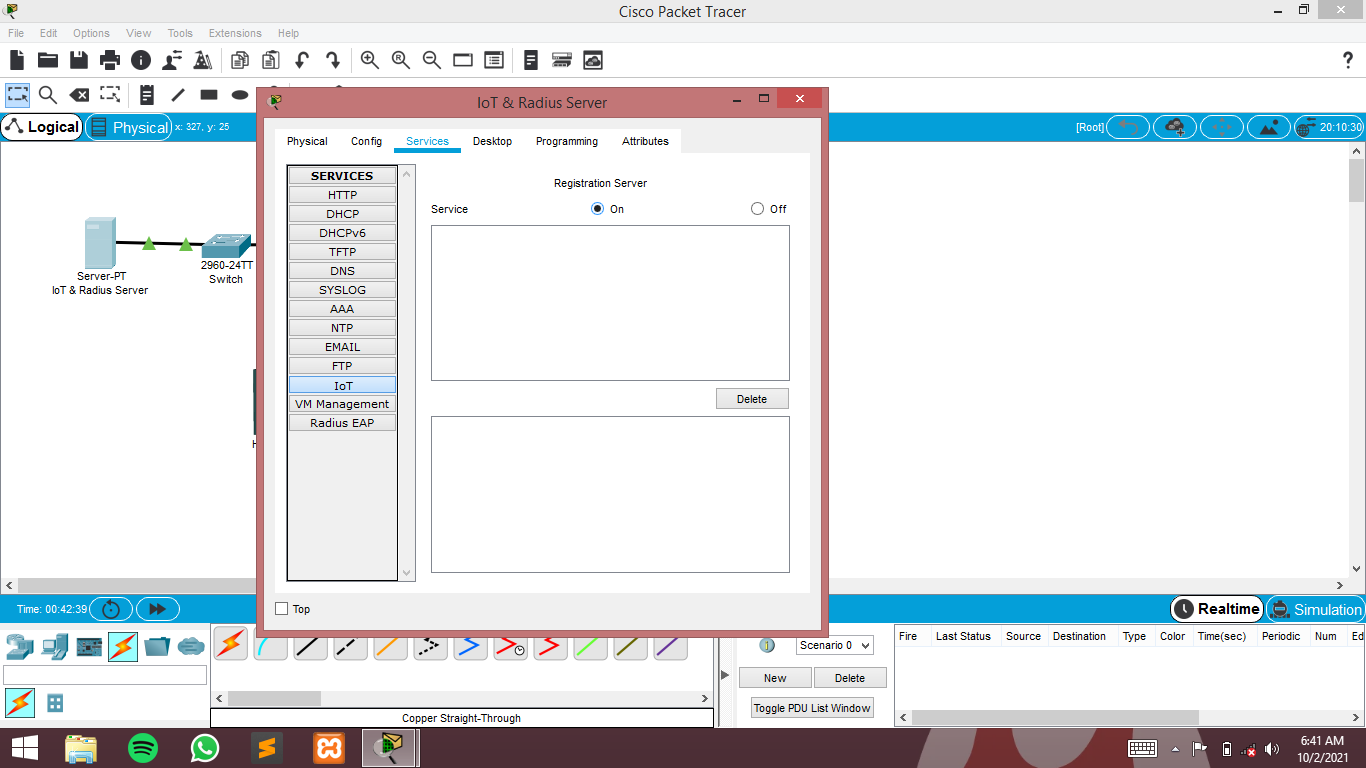
****

**Jendela**

****

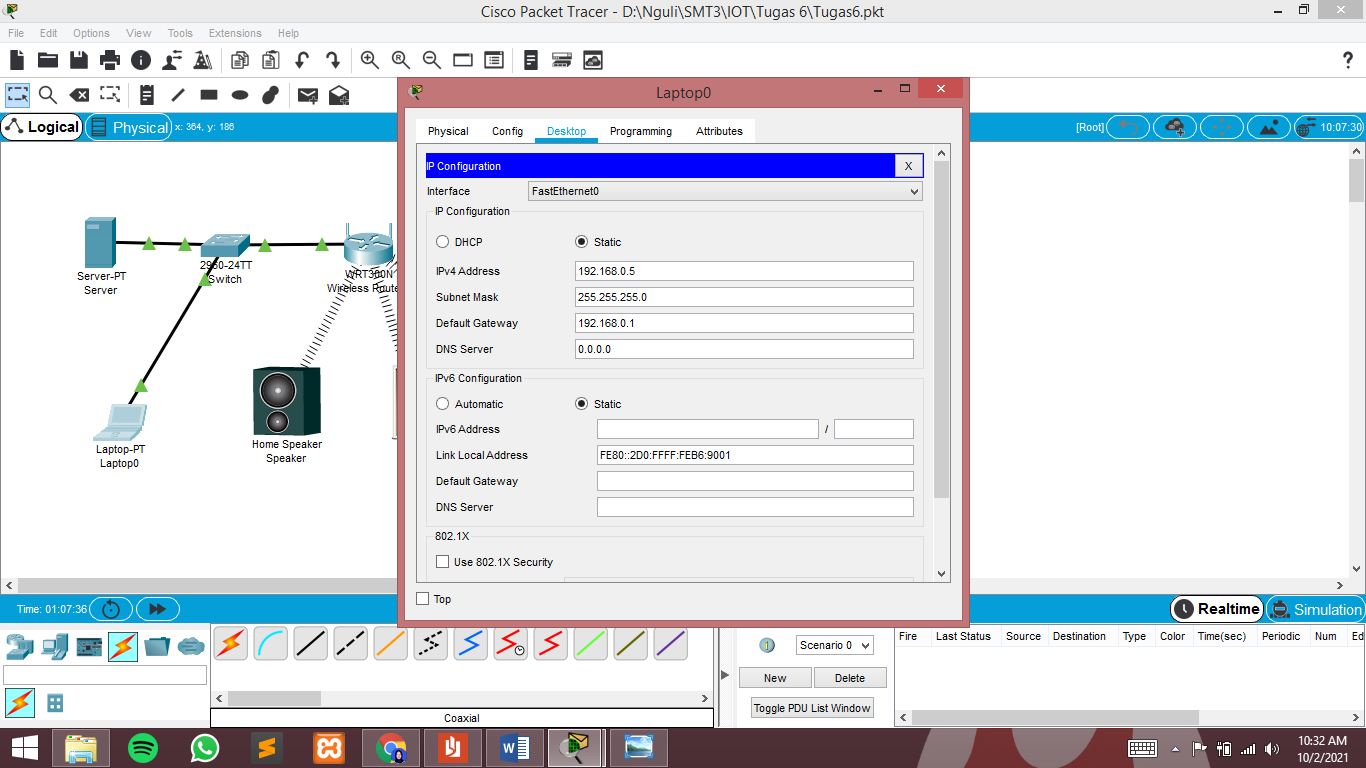
****

* **Setting IoT Server bagian registration menjadi on yang berarti server aktif.**

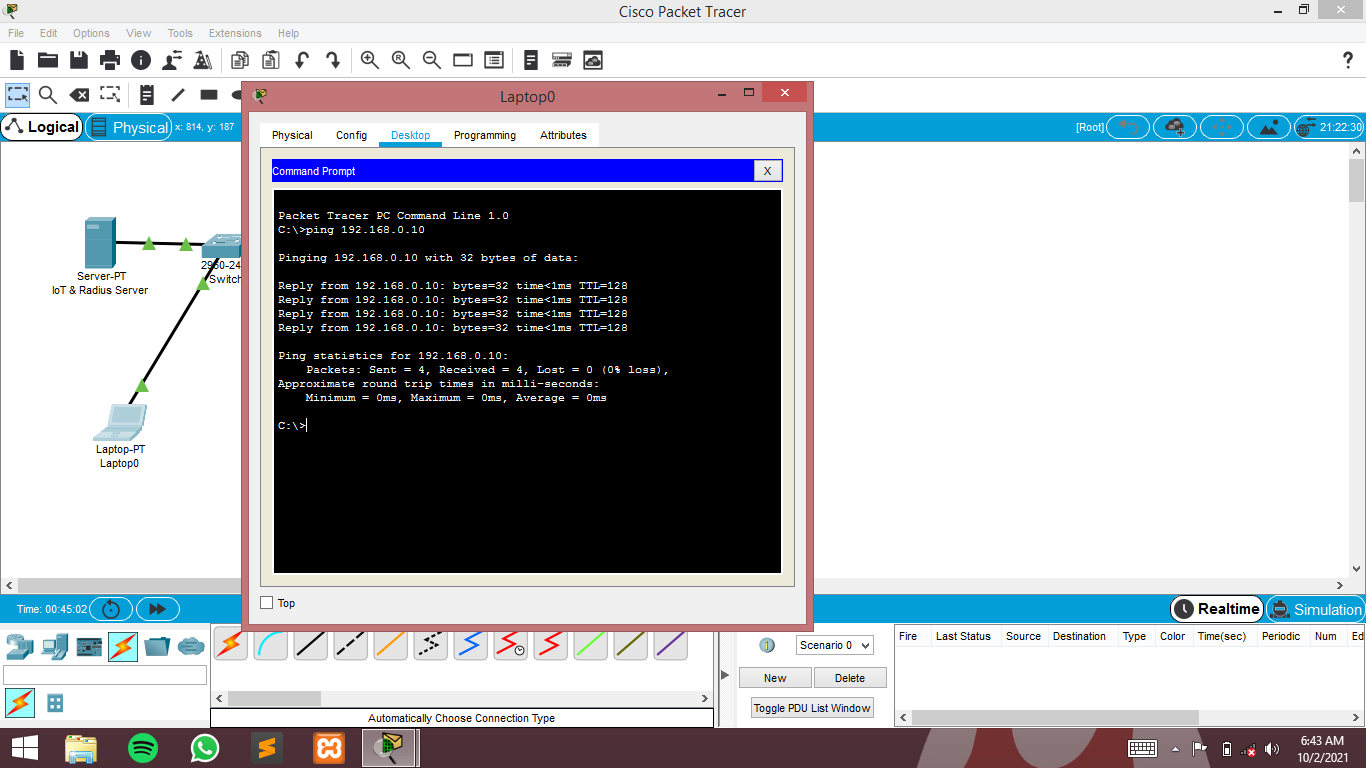
****

1. **Tambahkan Device Laptop dan hubungkan device dengan router menggunakan Atomatically Chose Connection Type.**

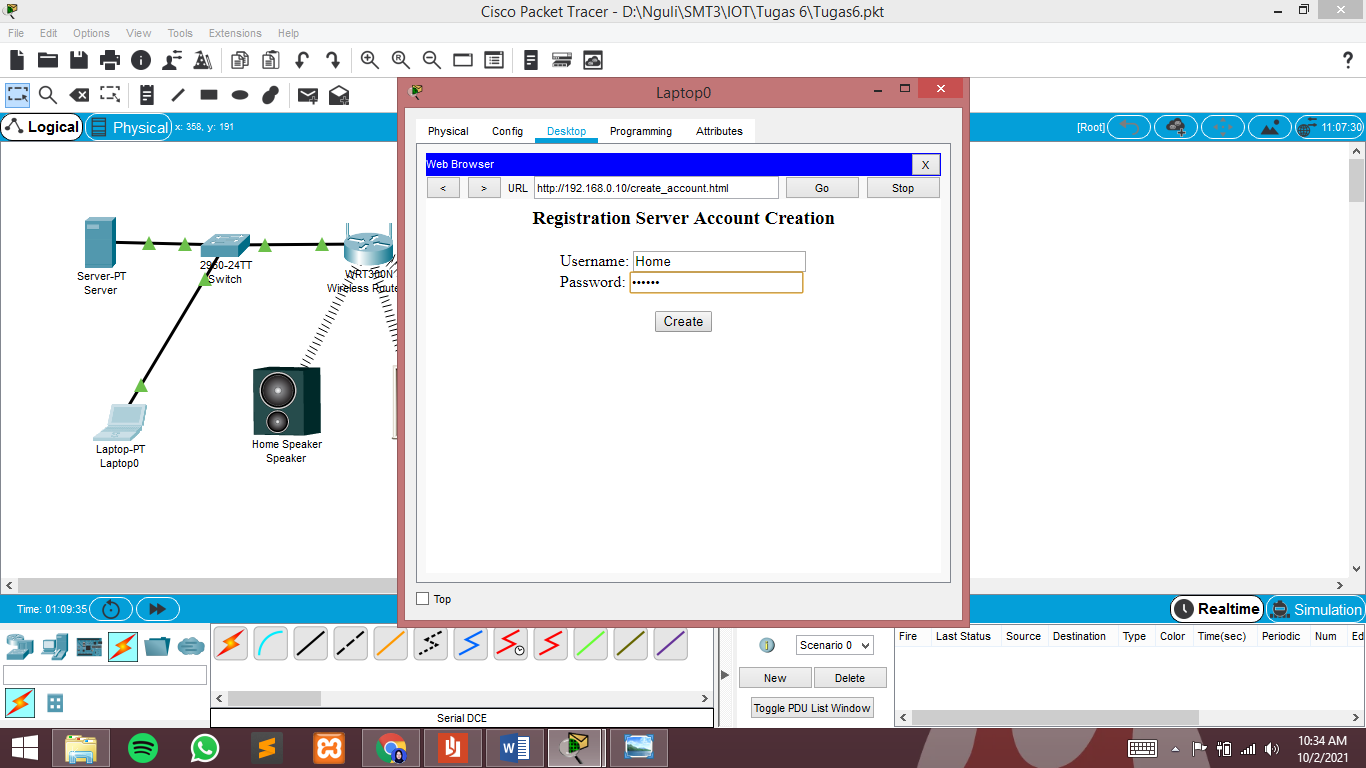
* **Atur IP addres dan default gateway laptop.**

****

* **Cek koneksi laptop.**

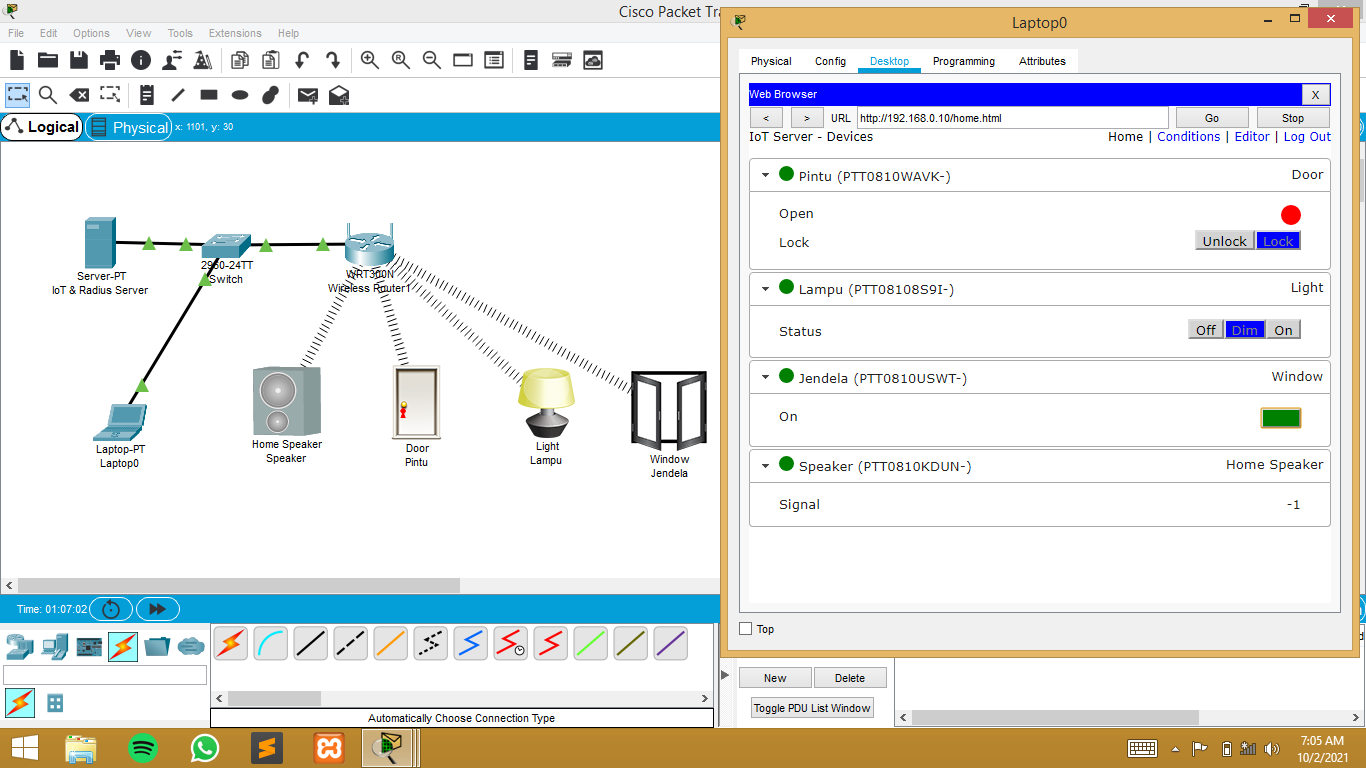
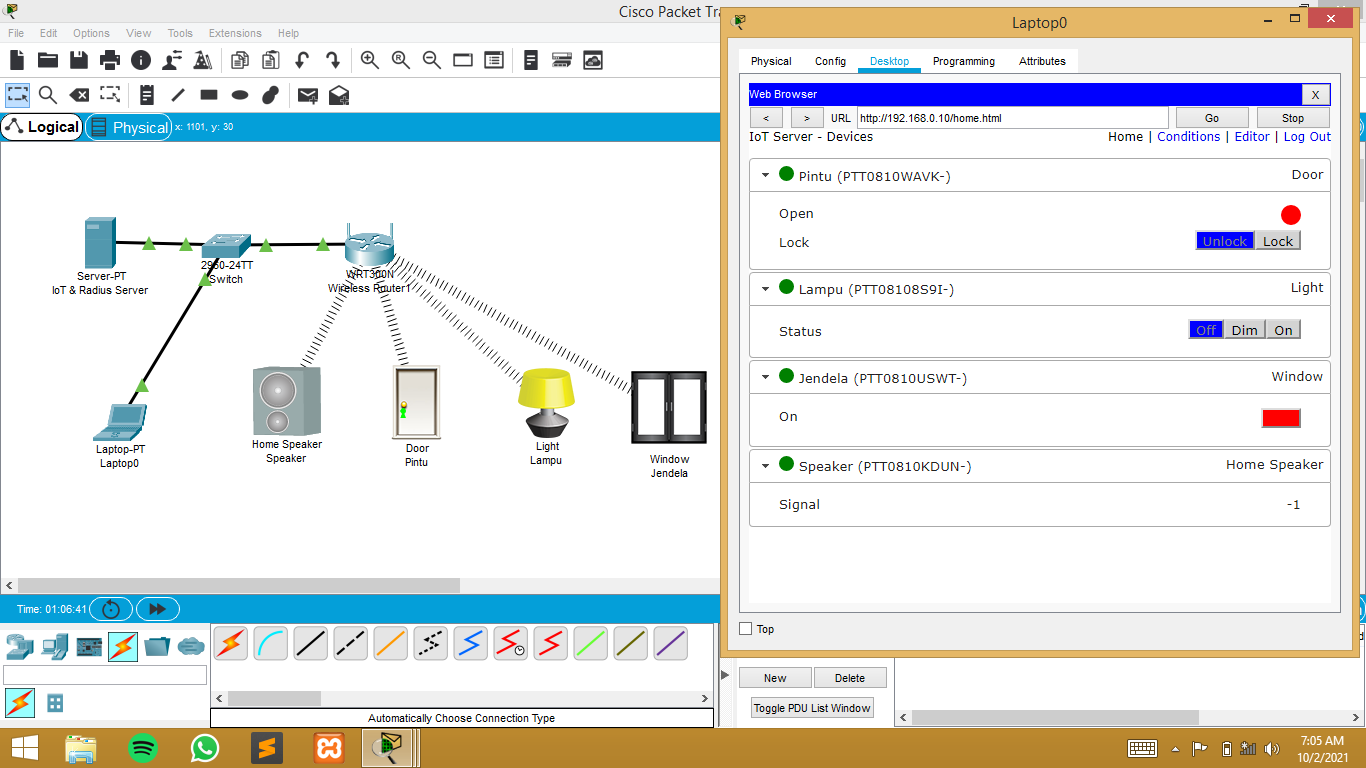
****

* **Buat akun IoE agar dapat login ke system.**

****

1. **Koneksikan masing-masing device dengan setting IoT Server menjadi Remote Server dengan server addres, username dan password sesuai dengan server agar device dapat terdeteksi pada server dan laptop.**

* **Dapat dilihat bahwa semua device dapat terhubung.**

****

1. **KUIS**
2. Security by design adalah suatu keamanan yang dibuat untuk mengamankan suatu desain arsitektur dalam IoT/keamanan dalam desain IoT yang digunakan untuk melindungi dari berbagai ancaman termasuk kebocoran data, penyalahgunaan hak akses ataupun perusakan sistem.
3. Yang dilindungi dalam IoT :
4. Label RFID.

Secara alami, RFID rentan terhadap ancaman keamanan dan privasi. Sifatnya yang tidak memerlukan kontak langsung dan berkomunikasi secara nirkabel dengan memanfaatkan gelombang elektromagnetik. Label RFID sebagai sarana pengenal objek, dibuat dengan biaya yang rendah. Mengingat harganya yang murah, sulit melengkapi label RFID dengan mekanisme enkripsi dan pemrograman yang kuat. Akibatnya label RFID rentan terhadap serangan seperti pencurian, penggandaan maupun pemodifikasian data. Pada sisi kanal komunikasi, RFID yang berkomunikasi dengan memanfaatkan gelombang elektromagnetik, rentan terhadap interferensi. Interferensi akan mengakibatkan kesalahan data dalam proses komunikasi antara label dan pembaca. Dengan mengirimkan sinyal penginterferensi, penyerang dapat menghambat link komunikasi, sehingga pembaca tidak dapat membaca data yang benar, dan menyebabkan serangan denial of service dan data tampering. Selain itu, pembaca RFID juga dapat dipalsukan sehingga komunikasi antara pembaca dan host dapat diserang dengan mudah. Penyerang dapat melakukan serangan middleman (pembaca lain yang diletakkan di tengah jalur komunikasi dan berperan seolah-olah sebagai pembaca yang sesungguhnya), eavesdropping maupun menginterferensi pertukaran data secara langsung maupun tidak langsung antara pembaca dengan host. Akibatnya, label tidak dapat diidentifikasi dengan benar.

1. WSN

WSN merupakan teknologi kunci yang memungkinkan terwujudnya IoT. Dengan WSN jaringan dan layanan dapat diintegrasikan menjadi infrastruktur IoT. WSN dan jaringan komunikasi yang dimanfaatkan pada IoT bekerja secara nirkabel, sehingga mudah diserang dan diinterferensi. Prinsip pengamanan informasi pada WSN dan jaringan komunikasi mengikuti prinsip confidentiality, integrity dan availability, berdasarkan prinsip ini, serangan yang dapat mengancam WSN, dapat dikategorikan dalam 3 kategori: serangan terhadapat kerahasian dan otentikasi, serangan terhadap integritas layanan, dan serangan terhadap ketersediaan jaringan. Jenis serangan yang masuk dalam ketiga kategori ini adalah denial of service (DoS), yaitu serangan yang menyebabkan pengguna yang sah tidak dapat mengakses informasi.