**Tugas Pertemuan 6 IoT**

Nama : Tanzil Rahmatul Karim

Prodi : D3 TI PSDKU – Kelas E

NIM : V3920057

**Kuis**

1. IoT menerapkan konsep security by design untuk mengimplementasikan keamanan pada sebuah jaringan atau sistem yang digunakan. Jelaskan apa yang dimaksud dengan security by design !

Jawab:

Security by design adalah pencegahan cybersecurity yang membuat sebuah organisasi mengotomatiskan kontrol keamanan datanya dan memformalisasi desain infrastrukturnya, sehingga dapat membangun keamanan ke dalam proses manajemen IT.

1. Implementasi keamanan pada IoT harus dapat melindungi beberapa faktor. Jelaskan apa saja yang harus dilindungi pada sebuah sistem IoT !

Jawab:

Perangkat terhubung terus berkomunikasi dengan satu sama lain, dan cloud menggunakan berbagai jenis protokol komunikasi nirkabel. Meski komunikasi membuat aplikasi IoT yang responsif, komunikasi ini juga dapat membawa kerentanan keamanan IoT dan membuka saluran ke hacker berbahaya maupun kebocoran data yang tidak disengaja.

Untuk melindungi pengguna, perangkat, dan perusahaan, perangkat IoT harus diamankan dan dilindungi. Landasan keamanan IoT terletak dalam kontrol, manajemen, dan penyiapan koneksi antarperangkat. Perlindungan yang tepat akan memastikan data tetap privat, membatasi akses ke sumber daya perangkat dan cloud, menawarkan cara aman untuk terhubung ke cloud, dan mengaudit penggunaan perangkat. Strategi keamanan IoT akan mengurangi kerentanan menggunakan berbagai kebijakan seperti manajemen identitas perangkat, enkripsi, dan kontrol akses.

**Tugas Individu**

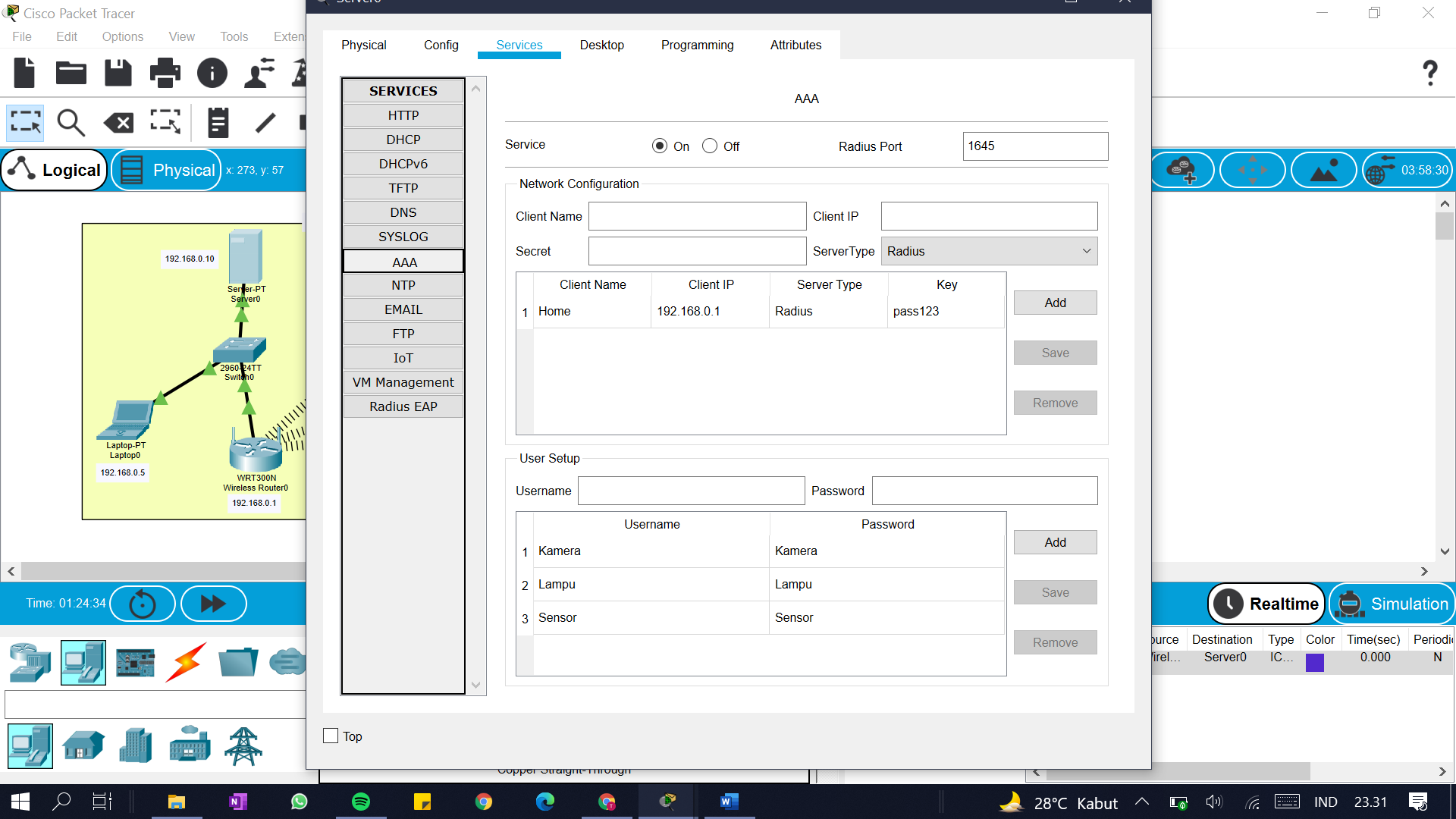
1. Membuat simulasi rangkaian IoT menggunakan wireless router. Tambahkan protokol keamanan dan tipe enkripsi dalam membuat registration server. Protokol dan algoritma enkripsi yang dipakai boleh berbeda dengan contoh yang ada (contoh : WPA2 Enterprise, AES).
2. Device yang digunakan adalah hasil dari tugas pertemuan sebelumnya (membuat registration server). Tambahkan wireless router agar device dapat terkoneksi pada jaringan wifi.

Jawab:

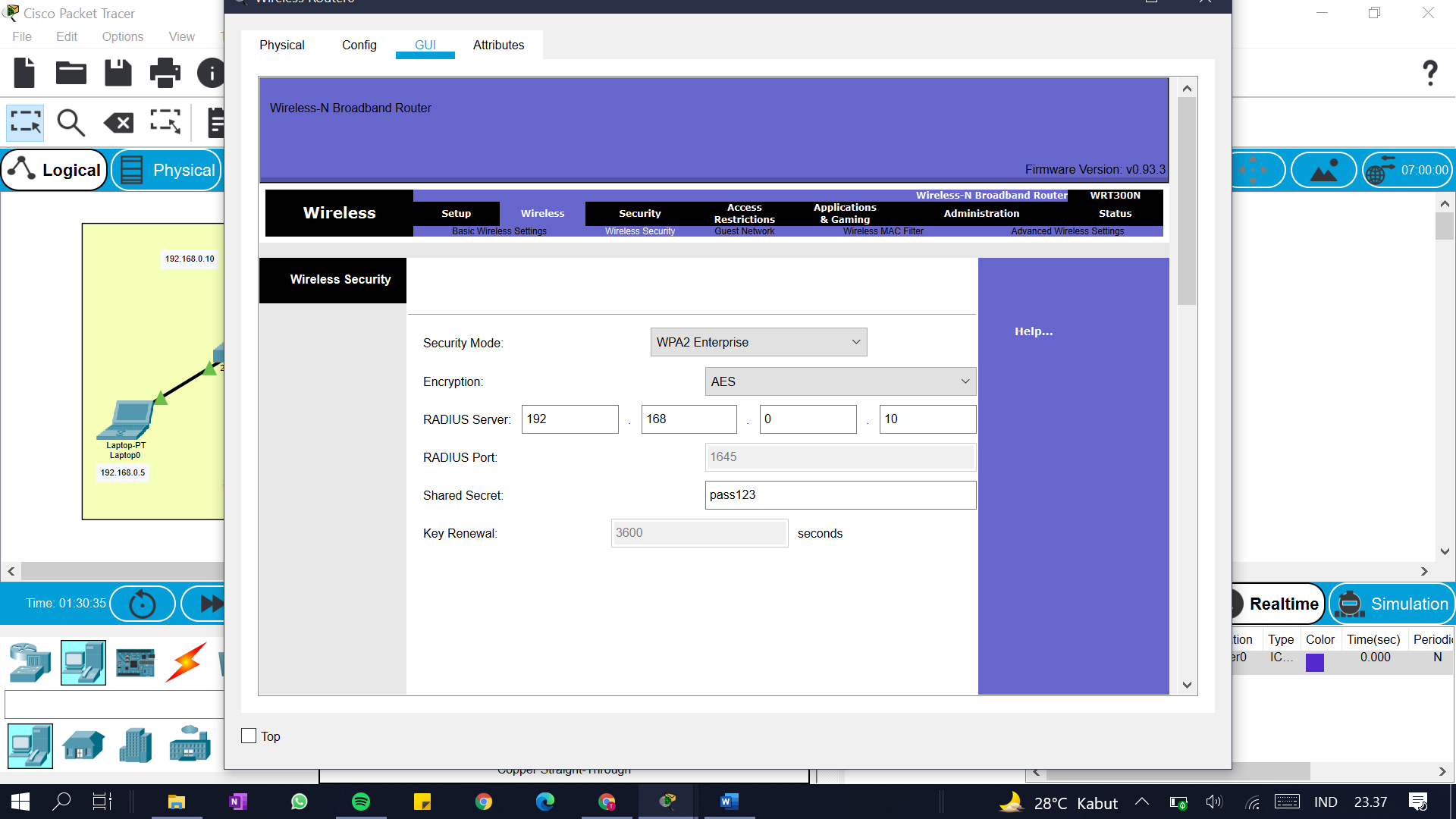
1. Siapkan device dan alat protokol yang digunakan dan hubungkan semua dengan kabel copper-straight:

* Motion Detector [Sensor]
* Lampu dan Kamera
* Wireless Router (WRT300N)
* Switch (2960)
* Server
* Laptop

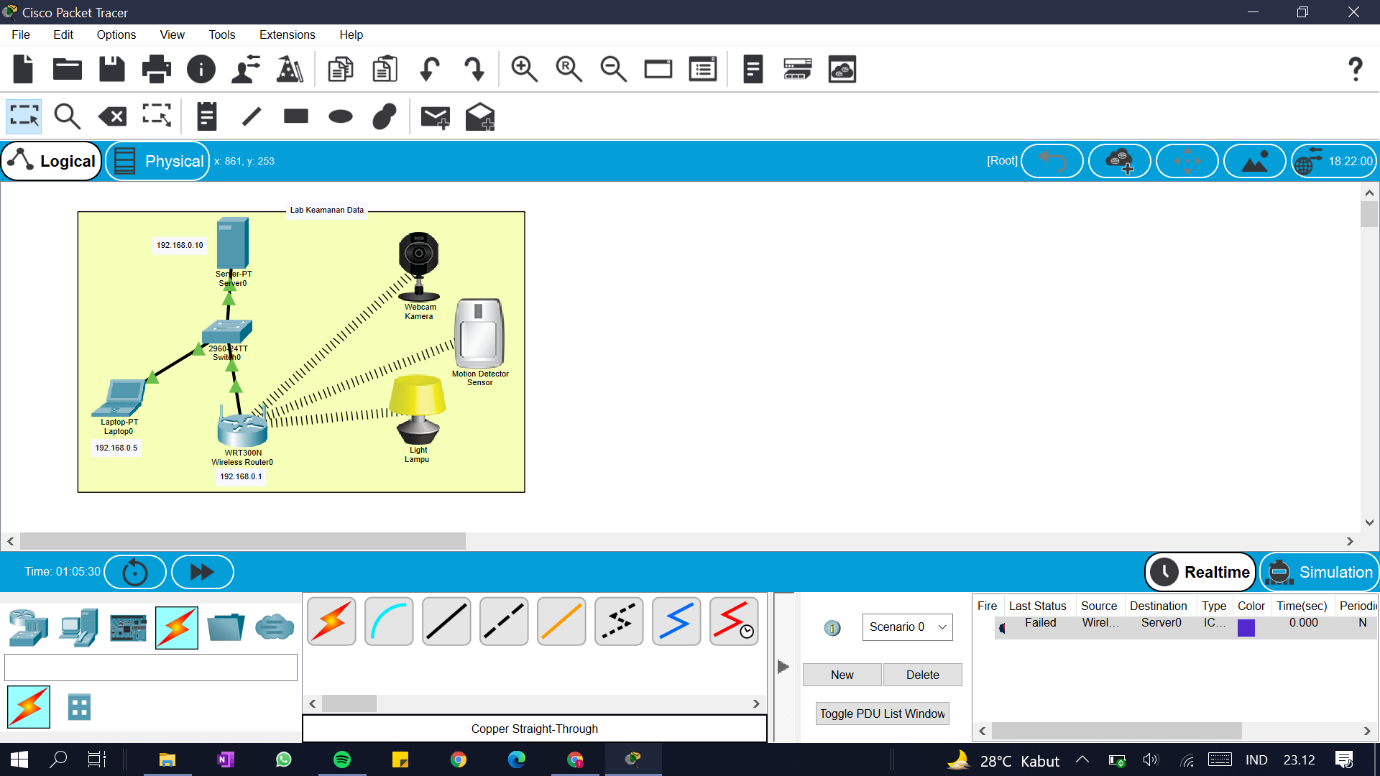
1. Cek ip address dari wireless router terlebih dahulu, ip-nya adalah 192.168.0.1 → Konfigurasi ip address di server (192.168.0.10) dan masukan ip wireless router di default gateaway → Masih di bagian server, buka AAA → buat client name dan key, lalu buat nama device dan password device pada user setup



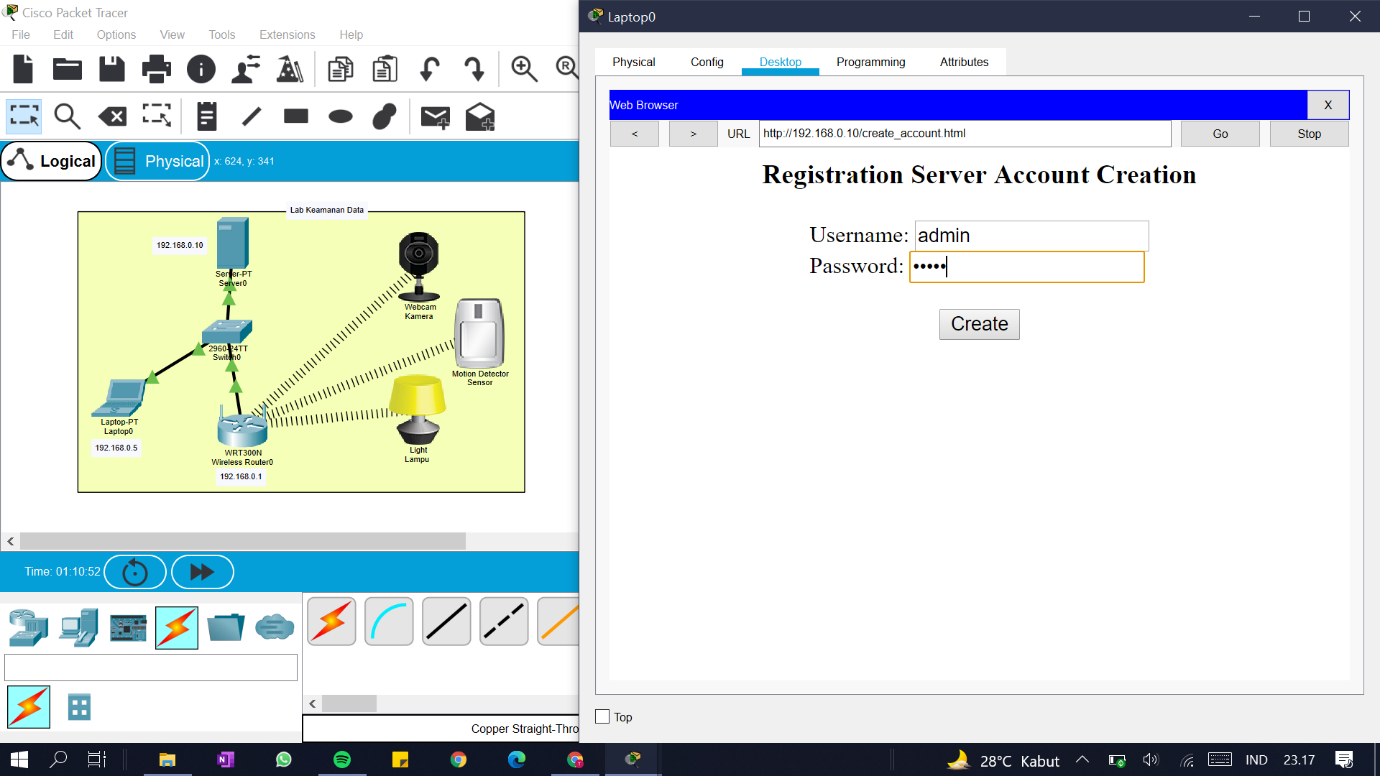
1. Setup nama wireless (SSID) dan wireless security menggunakan WPA2 Enterprise dan AES → Coba cek koneksi melalui server dengan ping ip address dari router (ping 192.168.0.1)



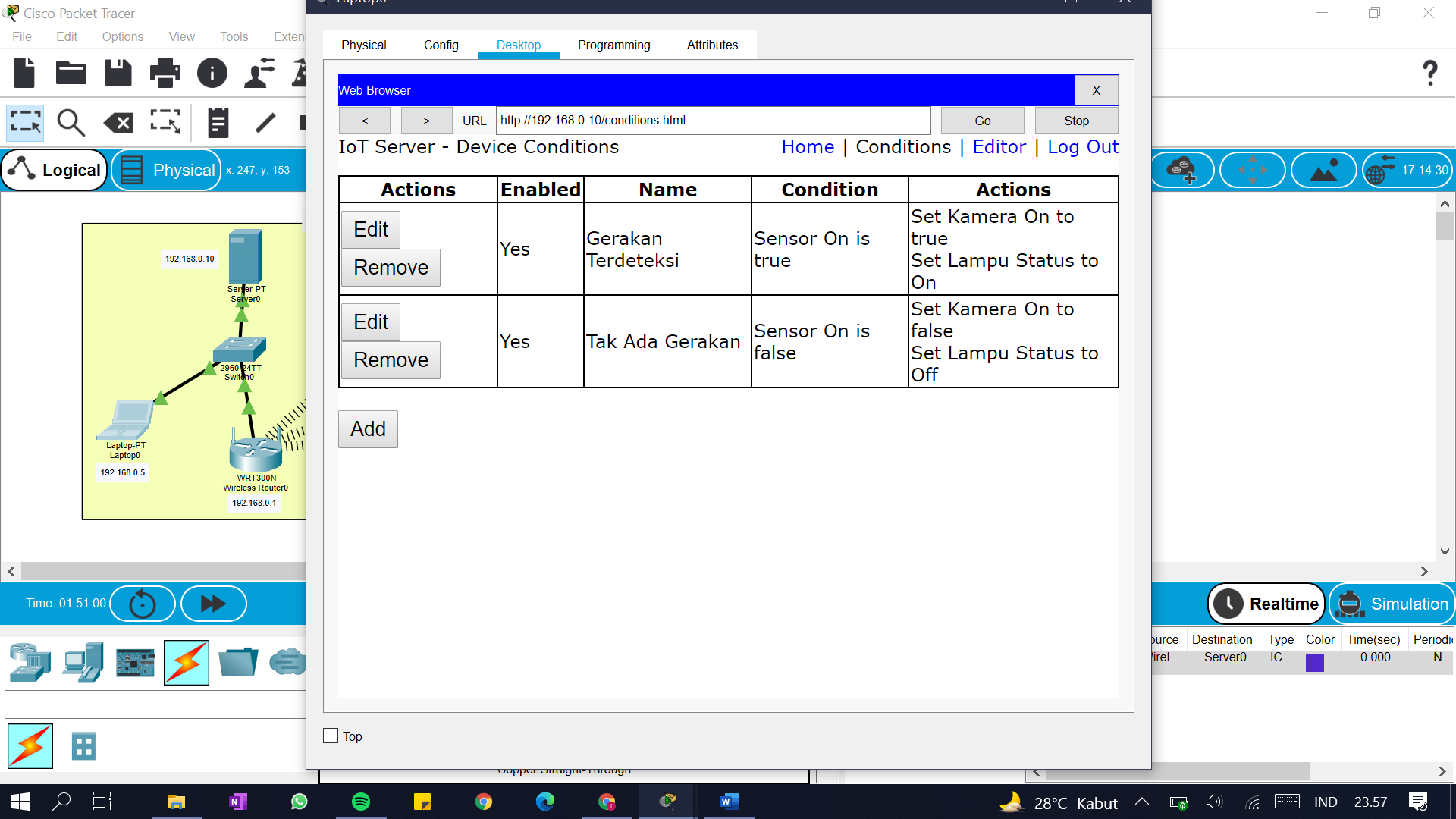
1. Hubungkan device ke wireless router → Pastikan SSID router sudah bener yaitu “Home” → Pada bagian authentication, pilih WPA2 dan isi userID dan password yang sudah dibuat pada cara ke-2



1. Sekarang kita akan membuat sistem keamanan dengan menyalakan registration server pada server → Konfigurasi ip address laptop yaitu 192.168.0.5 → Tes koneksi laptop ke server → Buka web browser di laptop, masukan alamat server 192.168.0.10 → Sign up akun untuk login ke sistem → Pastikan username dan password sudah tersimpan di server



1. Kemudian atur server address di semua device dengan memasukkan server address (192.168.0.10), username (admin), dan password (admin) → Connect → Device berhasil terhubung ke server
2. Simulasi yang saya buat adalah saat terdapat gerakan, motion detector akan merespon (status: true), maka lampu dan kamera pun langsung menyala. Disini saya akan menambahkan kondisi pada motion detector



1. Maka berikut hasil outputnya, saat ada pergerakan dan yang tidak ada pergerakan.

