Task 2(Networking):

First :

This summary related to network types:

Types of Network:

1- LAN:

هي شبكة عبارة عن مجموعة اجهزة متوصلين ببعض في نفس المبني

2-WLAN:

الفرق بينها وبين ال LAN ان ال WLAN هي بشكل Wireless

3-CAN(campus area network):

مثلا عبارة عن شبكة مكونه من شبكتين LAN او اكثر في نطاق جغرافي محدود

ex: الجامعة

4-MAN(Metropolition network):

بتربط اكثر من شبكة LAN في مدينة صغيرة

5-WAN(Wide area network):

دي الشبكة العالمية ال internet يعني مثلا بفتح فيديو يوتيو هنا في مصر وسيرفرات اليوتيوب موجودة في اميركا

6-SAN(Storage area network):

مسئولة عن تحزين الداتا الخاصة بالاشخاص الموجودين علي الانترنت يعني هي الي موصلة الهاردات والسيرفرات ببعض

This is summary related to network tapologies:

1-Bus tapology:

all devices with each other with one cable

لو حصل اي مشكلة ف الكابل دا الشبكة باظت

2-Ring:

كل جهاز يكون متوصل بجهازين الي جنبه ولو حصل اي مشكلة ف اي جهاز تكون الشبكة كلها باظت

3-Mesh:

كل الاجهزة بتكون متوصلة ببعض

hight cost and difficult to install and troubleshot

4-Star(common use):

بتكون كل الاجهزة مرتبطة ببعضها عن طريق *hub or switch*

مشكلته ان لو ال *centrel device* حصل فيه مشكلة بس حلها عن طريق ال *concept redundency* يعني في *centrel device stand by* لو حصل اي مشكلة ف الاساسي

This is summary of network devices:

1-Hub:

ابسطهم وهو اول جيل من اجيال اجهزة الشبكات . يستخدم في توصيل الاجهزة خلال شبكة داخلية واحدة

broadcast device,half duplex,doesnot store any information ,only one device can send data at a time

2-Switch:

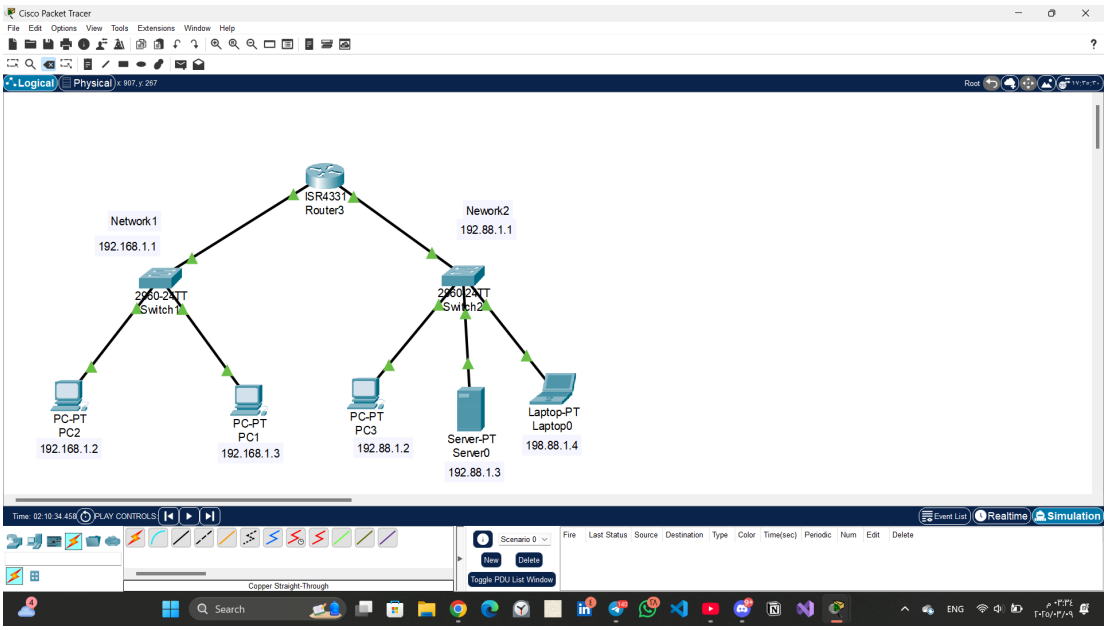
زي الهاب ولكن مش بيرسل الداتا لكل الاجهزة ولكن بيرسل بال *MAC Address*

3-Router:

دي البوابة الي بتخرجني من شبكتي للشبكة العالمية

using IP Address

This is simple simulate network with 2 switches and rourter in Cisco packet tracer :



Explain how ARP, DNS, and NAT play a role in communication:

1-DNS(Domain name system):

الاجهزة طبعا بتكلم بعضها عن طريق ال *IP* . طب ازاي لما اكتب لينك اي موقع ف اي ويب براوسر بيوصلني للموقع دا من غير ما اكتب ال *IP* الخاص به؟؟؟

دا بقا دور ال *DNS* هو المترجم هنا الي بيترجم اي لينك او ال *url* الي دخلته ل *IP*

2-ARP(Address resolution protocol):

نعمل مثال *:*عندنا مثلا جهاز *x* عاوز يبعت داتا لجهاز *y* فلازم ال *source device* يكون عارف ال *MAC AND IP Addresses for targrt device* بس هو مش بيكون عارف غير ال *IP* فقط ودا دور ال *ARP* اول حاجة هيعملها جهاز *x* هيشوف ال *MAC* في ال *ARP Cache* لو كان اول مرة يكون ف النتورك دي وقتها هيبعت *broadcast message* ياجماعة الخير مين الجهاز الي ال *IP* بتاعه كذا؟؟

وبعدين جهاز *y* هيرد عليه بال *MACaddress* الخاص بيه ويخزنه بقا ف ال *ARP cache for future use*

3-NAT:

طبعا علشان اقدر ادخل ع الانترنت لازم ادخل ب *public IP* ف دور ال *NAT* انه يحول ال *private IP* الموجود علي كل اجهزتنا الي *public IP* وله *3* انواع

1-Static(one to one mapping) :

يعني لو عندي *10* اجهزة عاوزة ادخلهم الانترنت هشتريلهم *public IP 10*

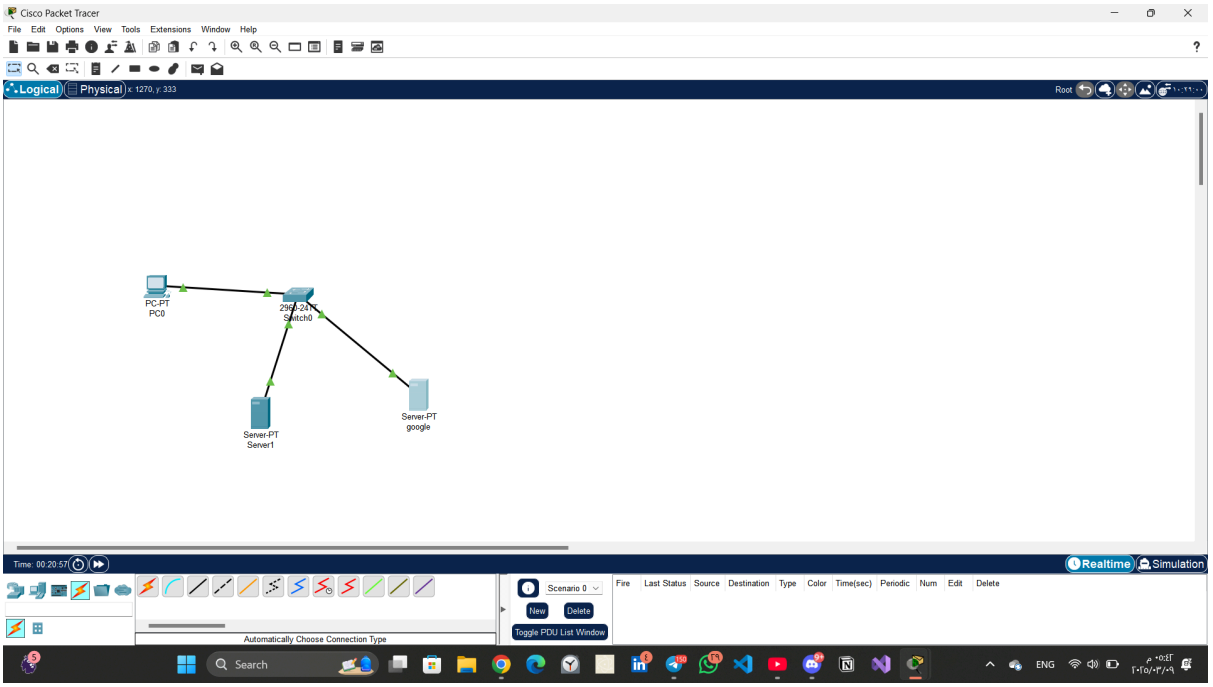
2-Dynamic(many to many mapping):

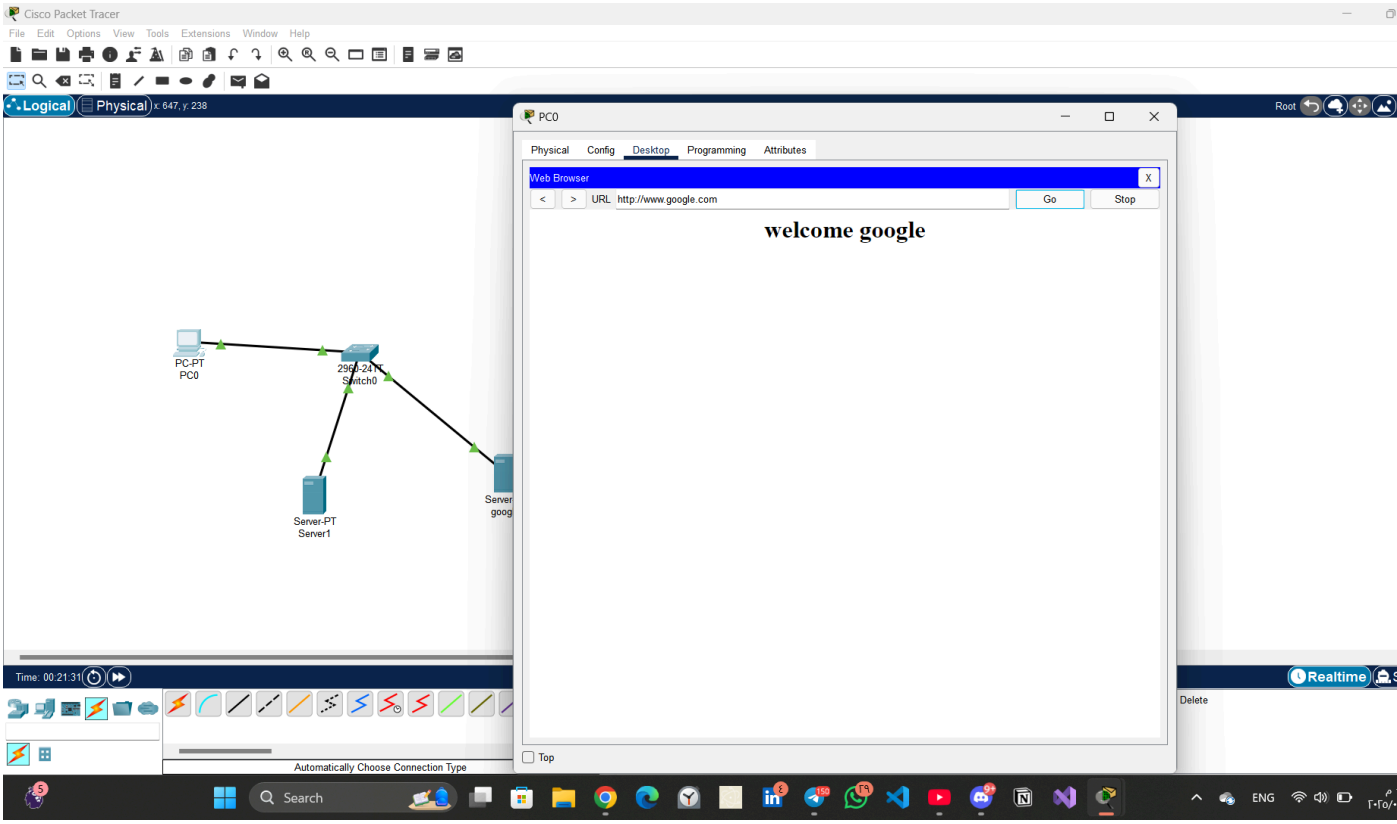
**هشتري *range from public IP*
ع سبيل المثال من *11.0.0.1* الي *11.0.0.4* يعني اي جهاز عندي عاوز يدخل ع الانترنت ياخد اي *IP* من دول بشكل عشوائي**

3-PAT(port address translation)(many to one):

كل الاجهزة الداخلية بتطلع ع الانترنت بنفس ال ***public IP*** ولكن باختلاف ال ***ports***

This is applying DNS packet tracer:





TCP vs. UDP Analysis:

1-TCP:

دا بروتوكول بيضمن لك ان الداتا وصلت سليمة تماما . لازم الجهاز المرسل يتاكد ان الداتا وصلت بشكل سليم لل *receiver* ولازم ال *receiver* يبعت *ACK* الي هو بالظبط ايوا تمام استلمتهممم ولكنه مش اسرع حاجة

2-UDP:

مش بيضمن لي ولا بيتاكد من وصول الداتا ولا وصولها بشكل سليم ولكنه اسرع
كل بروتوكول فيهم وله استخدامه مفيش واحد احسن من التاني

examples for using TCP:

1-Amazon website:

لان لما بنشتري حاجة من امازون بيانات الفيزا والعنوان حساسة جدا يعني اي رقم يضيع من رقم الفيزا الموضوع مش هيكمل

2-Gmail:

مثلا تسجيل الدخول للجيميل لازم كل حرف او رقم ف الباسورد يكونوا بشكل سليم ولو حصل اي خطا بيطلب مني ابعته تاني وكذلك وانا ببعت ايميل اهم حاجة الدقة بنسبة *100%*

examples for using UDP:

1- Whats app calls:

اهم حاجة سرعة البيانات ولو حصل اي خطا ف الارسال ممكن اطلب من الشخص الي بكلمه يعيد الكلام تاني

2-GPS:

لما بتستخدم تطبيق *Google Maps* أو أي نظام *GPS*، الجهاز بيستقبل إشارات من الأقمار الصناعية بشكل لازم مستمر للبيانات بأسرع شكل ممكن عشان يحدد موقعك في الوقت الحقيقي.
لو *GPS* استخدم *TCP*، أي تأخير في استلام البيانات ممكن يخليك تشوف مكانك متأخر على الخريطة حتي لو في جزء ضاع مفيش مشكلة لان النظام بيستقبل تحديثات جديدة كل ثانية

OSI Model & TCP/IP Model

Map out how data travels from a sender to a receiver using the layers of the OSI model.

Explain how TCP/IP differs from OSI :

1-OSI Model:

اي جهاز بيرسل داتا لازم بيمر بال *layers 7* دول وال الجهاز ال *receiver* بالعكس

1-Application layer:

دي بيتحدد فيها انهي بروتوكول انسب للاكشن الي انت هتعمله ك *https,ftp,smtp*

2-Presentation layer:

باخد الداتا ف صورة *human language* و بحولها ل *binaryy* وبعملها *comperssion* علشان تسهل من عملية النقل + بيتعمل لها عملية *encryption* وال *receiver* بيعملها *decryption* للامان طبعا

3-Session layer:

بيحصل فيها اكتر من عمليه اولها بيتحدد ملامح ال *connection* هل هيكون *simple mode* *or half duplex or full duplex*

و بيحصل فيها *authentication and authorization*

session management+* بمعني مثلا لما بندخل ع فيس بوك ومفيش انترنت ع الجهاز الخاص بنا بنلاقي فيه الداتا الي ظهرت لنا اخر مرة لما كنا *connecting

4-Transport layer:

1-*بيتم فيها تقسيم الداتا الي *segments* ولكل *segment port and sequence number* علشان يحافظ علي الداتا لما يحصلها *desegmentation

2-*بيحافظ علي ال *flow control

3-* بيحدد نوع البروتوكول الخاص بنقل البيانات هل *(TCP or UDP)

5-Network layer:

1-*بيستلم ال *data segments* وبيضيف غليها ال *ip for sender and receiver* ويكون ال *packet

2-*بيتم فيها اختيار افضل بروتوكول لل *routing

6-Data link layer:

1-*فيها بتتسلم ال *packet* وبيتضاف عليهم ال *MAC Adress for sender and receiver* وبيتكون ال *frame

***2-error detection and correction* بنتاكد ان الداتا وصلت سليمة ولو في اي ايرور *discard* بيتعملها**

عندنا *3 techniques* لاكتشاف ال ايرور ف ال *frame*

1-parity check and check sum andCRC(cycle redundancy check)

3-*اخر حاجة ف ال *data layer* ان فيها بيتم استخدام *CSMA Protocol (carrier sense multipe access)

يعني لو عندي *3* اجهزة متوصلين ع راوتر و ال *3* لهم نفس ال *transmission media* طب لو الاجهزة دي كلها بعتت داتا في نفس الوقت اكيد هيحصل تصادم*!!!*

البروتوكول دا بيشوف هل الاول ال *media* فاضية ولا لا *(*بينظم ال *traffic* يعني*)*

7-Physical layer:

وصلنا ف الاخر ان الداتا موجوده ف *frame* يعني ع شكل *bits* نبدا نحولها ل *signals* علي حسب ال *transmission media* الي هتتبعت فيه

ثم تنتقل ف الميديا لحد لما توصل لل *physical layer for receiver* وتبدا العمليا الي فاتت دي كلها تحصل بس بالعكس

والحمدلله الذي تتم بنعمته الصالحات

Protocol TCP/IP

How differ it from OSI ?

شبهه بالظبط ولكن اقل ف عدد ال layers

layers in TCP/IP:
1-application(application,presentation and session in OSI)
2-transport(transport in OSI)
3-internet (network in OSI)
4-link(data link and physical layer in OSI)
and updated to…
1-application
2-transport
3-network
4-data link
5-physical

الحمدلله

Attacks

1-DNS Poisoning:

باختصار لما تكتب موقع زي *facebook.com*، جهازك بيروح ل *DNS* علشان يعرف الـ *IP* الخاص بالموقع دا ف ال *attacker* بيتلاعب في الرد اللي يرجعلك، بحيث بدل ما يوصلك للموقع الحقيقي، يوديك على موقع مزيف فيسرق كل بيانات دخولك و ال *attack* يحصل بسهولة
ممكن نستخدم ال *VPN* لانه بيشفر طلبات ال *DNS* الخاصة بك

2-Homograph Attack(اتاك الحروف المتشابهة):

يعني ال *attacker* بينشئ موقع مزيف بنفس شكل الموقع الأصلي باستخدام حروف مشابهة
مثال: بدل من *facebook.com*، يستخدم *fácebook.com* (بحرف غريب يشبه الأصلي بالظبط ممكن متاخدش بالك منه) ويشرق بياناتك بكل سهولة

security risks in the network &mitigation strategies

1-DHCP Starvation Attack:

يعني ال *attacker* بيرسل آلاف الطلبات ل *DHCP* في الشبكة ف ال *DHCP* يوزع كل عناوين الـ *IP* المتاحة على ال *attacker* وما يبقاش فيه *IP* متاح للأجهزة الحقيقية وبالتالي الشبكة كلها تتعطل
الحل:
1-*تتفعيل *DHCP Snooping* لمنع الأجهزة الغير الموثوقة من طلب عناوين *IP
***2-* تفغيل حد معين لعدد الطلبات اللي ممكن يرسلها كل جهاز**

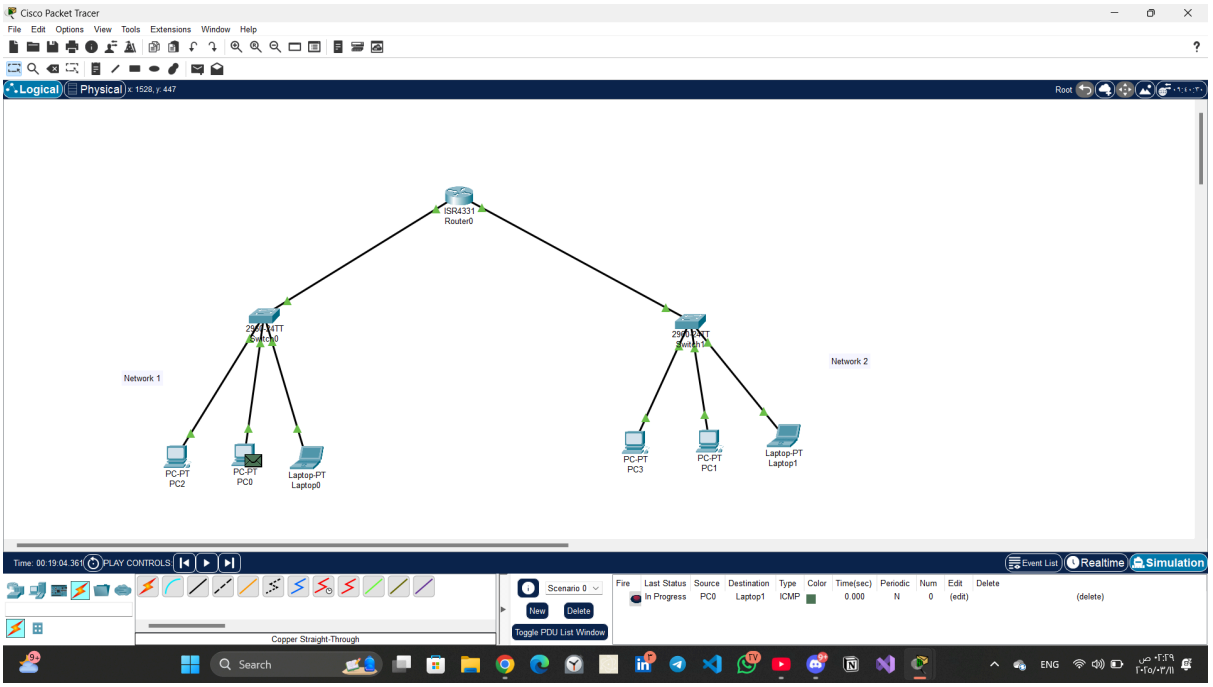
2-MAC Flooding Attack (إغراق جدول *MAC*):

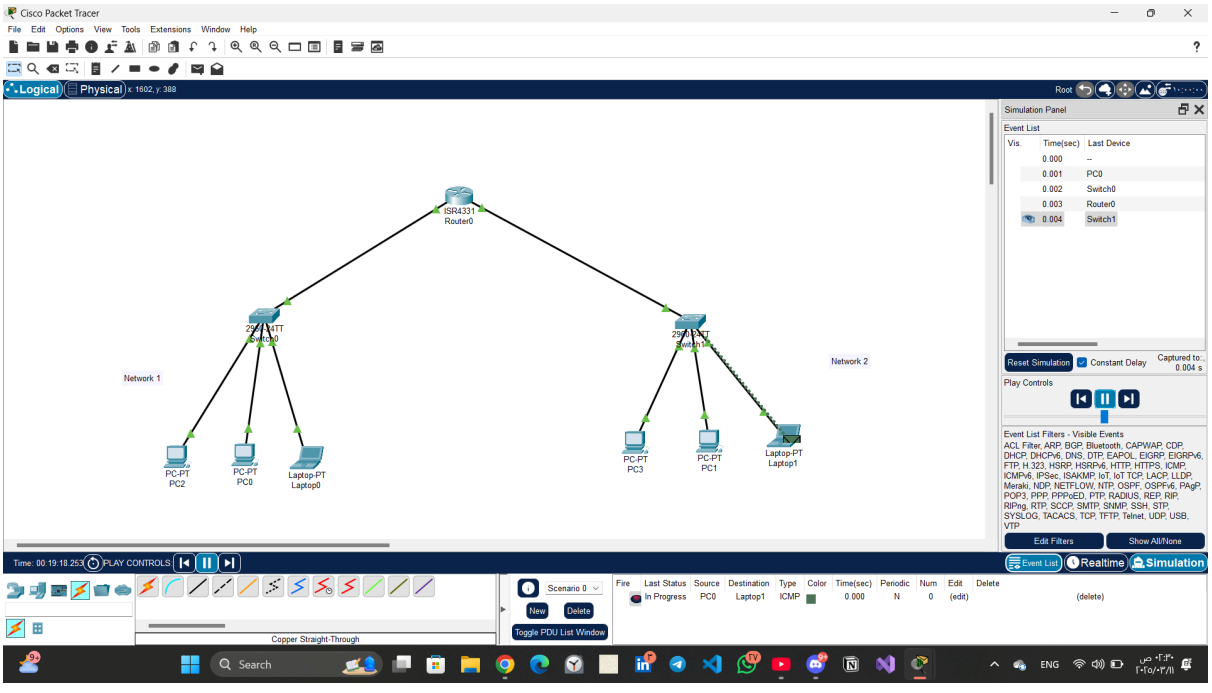
يعني ان ال *switch* بيحتفظ بجدول يربط بين عناوين *MAC* والأجهزة المتصلة فيقوم ال *attacker* يرسل آلاف العناوين العشوائية للسويتش لحد ما الجدول يتملي بالكامل ف النتيجة ان السويتش يتحول لوضع ال *hub* ويرسل كل البيانات لكل الأجهزة، ووقتها ال *attacker* يقدر يتجسس على كل شيء
الحل :

تفعيل ***Port Security*** في السويتش لتحديد عدد العناوين المسموح بها لكل منفذ ولو حد حاول يضيف اكتر بيمنعه

A basic network diagram

I made it with Cisco Packet Tracer:





وصلت الماسدج الحمدلله

وتم الانتهاء و طمعانة ف ال ***Bonusss***