جامعة محمد خيضر بسكرة
كلية العلوم والتكنولوجيا
قسم الهندسة الكهربائية

مذكرة ماستر

العلوم والتكنولوجيا
الإتصالات
الشبكات و الإتصالات

رقم: .....

إعداد الطالب(ة) :
بركات إيمان
ويبدن نور الهدى

يوم: 26 جوان 2022

دراسة ومحاكاة شبكة حاسوب آمنة: بإستعمال المحاكي العالمي CISCO PACKET TRACER

لجنة المناقشة:

أ. عميد سفيان	أ. مس أ	جامعة بسكرة	رئيسا
د. بخوش خالد	أ. مح أ	جامعة بسكرة	مشرفا
د. هنداوي منيرة	أ. مح ب	جامعة بسكرة	مناقشا

السنة الجامعية : 2021 – 2022

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research

جامعة محمد خيضر بسكرة
كلية العلوم والتكنولوجيا
قسم الهندسة الكهربائية
شعبة: الإتصالات
التخصص: شبكات واتصالات

أطروحة التخرج

للحصول على درجة الماستر

دراسة ومحاكاة شبكة حاسوب آمنة: بإستعمال المحاكي العالمي CISCO PACKET TRACER

تقديم :

بركات إيمان

ويبدن نور الهدى

رأي المشرف:

د. بخوش خالد

رأي رئيس لجنة المناقشة :

أ.عميد سفيان

ختم و توقيع

شكر

قال تعالى : { وَمَن يَشْكُرْ فَإِنَّمَا يَشْكُرُ لِنَفْسِهِۦ } لقمان:12

و قال رسولنا الكريم صلى الله عليه وسلم : " من لم يشكر الناس ، لم يشكر الله عز وجل "

نحمد الله تعالى حمدا كثيرا طيبا مباركا مليء السموات و الأرض على ما أكرمنا به من اتمام هذه الدراسة التي نرجو ان تنال رضاه.

ثم نتوجه بجزيل الشكر و عظيم الإمتنان إلى كل من :

الدكتور "خالد بخوش" على قبوله الإشراف على مذكرتنا هاته وعلى مساندته لنا خلال إنجاز هذه الدراسة وحرصه على توجيهنا.

استاذ "عميد سفيان" على قبوله مساعدتنا في اتمام هذا العمل و نصائحه لنا .

اعضاء لجنة المناقشة الكرام : الاستاذة "هنداوي منيرة" مناقشا و الأستاذ "عميد سفيان" رئيس اللجنة لقبول مناقشة هذه الدراسة

كما نحي كل الأساتذة الذين تابعونا طيلة مشوارنا الدراسي ابتداء من المستوى الإبتدائي وصولا إلى الجامعة.

اهداء

أهدي ثمرة جهدي و نجاحي الى أعز وأغلى إنسانين في حياتي الى من منحاني القوة و العزيمة "أمي و أبي" فلقد كانوا بمثابة العضد والسند في سبيل استكمال مشواري الدراسي .

الى اخوتي "هارون و محسن " حفظهما الله عز وجل .

الى صديقاتي العزيزات ، بدة رحمة ومان ايثار هدفي فيروز مقران رفيدة

الى كل العائلة الكريمة ، و زملاء الدراسة متمنية لهم التوفيق.

الى كل الأشخاص الذين احمل لهم المحبة و التقدير .

الى كل من نسيه القلم و حفظه القلب.

نور

أشكر الله تعالى على كل نعمه ، ولولا فضل الله لما وصلت إلى المكان الذي أنا فيه والحمد لله والشكر فوق كل شيء.

أشكر عائلتي أمي وأبي وأخوتي والشخص العزيز على قلبي الذي آمن بي وساعدني في مسيرتي الأكاديمية. هم السبب في هذا العمل المتواضع هو هديتي لهم. لولا حبهم ووقوفهم بجانبي لما أنجح، لذا أشكرهم مرة أخرى لأنهم مصدر إلهامي وقوتي وشغفي.

لن أنسى أبدًا أصدقاء الدراسة وتعاوننا مع بعضنا البعض لتحقيق النجاح.واخيرا شكرا لكل من ساندني سواء من قريب او بعيد ولو بكلمة طيبة لان هذا العمل لم يكتمل بدون خير الجميع.

إيمان

جدول المحتويات

قائمة الأشكال:

قائمة الأوامر:

قائمة الجداول :

قائمة الإختصارات :

PAN = Personal Area Network.

LAN = Local Area Network.

WAN = Wide Area Network.

MAN = Metropolitan Area Network.

CSMA / CD = Carrier-Sense Multiple Access with Collision Detection.

IP = Internet Protocol.

OSI = Systems Interconnection Model.

EIGRP = Enhanced-Interior-Gateway-Routing-Protocol.

IGRP = Interior Gateway Routing Protocol.

RIP = Routing Information Protocol.

OSPF = Open Shortest Path First.

IS-IS = Intermediate-System-to-Intermediate-System.

NIC = Network Interface Card.

MAC = Media Access Control.

PSTN = Public Switched Telephone Network**.**

DSL = Digital Subscriber Line**.**

BNC = Bayonet-Neil-Concelman.

RJ-45 = Registered Jack 45.

STP = Spanning Tree Protocol.

STP = Shielded Twisted-Pair.

UTP = Unshielded Twisted-Pair.

ST = Straight Tip.

SC = Subscriber Connector.

FC = Ferrule Connector.

LC = Lucent Connector.

ISO = International Organization for Standardization.

UDP = User Datagram Protocol.
TCP = Transmission Control Protocol.

VLAN = Virtual Local Area Network.
VPN = Virtual Private Network.

SSH = Secure Socket Shell.

IP Sec = IP Security.

VTP = Virtual Trunking Protocol.

ISL = Inter-Switch Link.

DHCP = Dynamic Host Configuration Protocol.

NAT = Network Address Translation.

ISP = Internet Service Provider.

AAA = Authentication / Authorization / Accounting.

HSRP = Hot Standby Router Protocol.

DTP = Dynamic Trunking Protocol.

ملخص :

في ظل الانتشار الواسع والسّريع لتكنولوجيا المعلومات والاتصال و الدّور الذي تلعبه في مختلف المجالات، قمنا ببحث حول إحدى أهم تكنولوجيا الاتصالات و هي شبكات الحاسوب .

اصبحت الشبكات في عصرنا مهمة جدا و اكثر استعمالا في المؤسسات لسهولة نقل و مشاركة المعلومات ، مما دفعنا ذلك للقيام بدراسة شاملة عامة في هذا المجال لكونه يعتبر بحرا بحد ذاته لما يحتويه من معلومات هائلة و اصناف مختلفة . كما نعلم انه كلما تطورت هاته التكنولوجيا اصبحت اكثر عرضة للمخاطر التي تهدد أمن وسلامة المعلومات المتواجدة بها، نتيجة ظهور ما يُعرف بالاعتداءات الإلكترونية كالبرمجيات الخبيثة وبرامج القرصنة ومختلف الأشكال التي تهدف إلى تخريب أو سرقة معلومات المؤسسة وإلحاق الضرر بها.

هدفنا من هذا البحث هو تجسيد كل ما تعلمناه طوال مسيرتنا الدراسية في مجال الشبكات و جمعها في هذه المذكرة ، ابتداءا من اساسيات الشبكات الى دراسة تصميم و اعداد شبكة قرية جامعة ، التي تتكون من مجموعة أجهزة شبكية وبروتوكولات تستعمل لبناء الشبكة. و اختبار اتصال الأجهزة مع بعضها البعض أو خارج الشبكة (كالإتصال بالأنترنت أو بالفرع اخر)، و حمايتها من اي هجومات سواءا من الداخل أو الخارج و ذلك بإستعمال برنامج محاكي الخاص بشركة سيسكو .« Packet Tracer »

Abstract:

In light of the rapid spread of information and communication technology and the growing role it plays in various fields, we have researched one of the most important communications technology which is computer networks.

The networks of our time have become very important and more used in institutions for easy transmission and sharing of information, which prompted us to do a comprehensive study in this field because it is considered a sea itself for its enormous information and different varieties. We also know that as this technology evolves, it becomes more vulnerable to threats to the security and integrity of existing information, as a result of the emergence of so-called cyberattacks such as malware, hacking software, and various forms aimed at sabotaging or stealing and damaging enterprise information.

Our goal in this research is to embody everything we have learned throughout our career in networking and collect it in this thesis, from the basics of networks to study the design and development of a campus network, which consists of a set of network devices and protocols used to build the network. And test the connection of devices with each other or outside the network (such as Internet connection or another branch), and protect them from any attacks either inside or outside using the simulator software of the company "Packet Tracer."

مقدمة عامة

مـقـدمـــة عـامـــة:

تعتبر الشبكة مهمة بالنسبة للمؤسسات و الشركات منذ القدم في عصر تقنية المعلومات ، تحولت شبكة المعلومات القديمة إلى شبكة كمبيوتر سريعة جدًا ويمكن إدارتها بسهولة. على غرار تهديد أمن شبكات الكمبيوتر في العصر القديم تعد دائمًا مشكلة خطيرة ومهمة للغاية.[1]

شبكة قرية جامعية « Campus Network » هي شبكة مستقلة تخضع لإدارة القرية الجامعية و بشكل عام هي جزء من البنية التحتية للشبكة التي توفر الوصول إلى خدمات وموارد اتصالات الشبكة للمستخدمين النهائيين.

اليوم، يحظى أمن معلومات شبكة قرية جامعية باهتمام متزايد هذا ما جعل مسؤولي شبكات الكمبيوتر يواجهون العديد من التحديات في الحفاظ على الأداء الجيد والأمن. مما دفعنا هذا إلى دراسة كيفية تصميم شبكة قرية جامعية وحمايتها.

في هذا العمل ، سنناقش بعض اعتبارات التخطيط والتصميم التي يجب مراعاتها عند تصميم شبكة حرم جامعية قابلة للتطوير. استخدم البرامج التي تحاكي شبكة قرية جامعية والأدوات المحددة الموجودة بالفعل لمساعدة محترفي الشبكات على تطوير مهاراتهم واختبار بعض التصميمات قبل تثبيت الأجهزة المادية فعليًا.

لتقديم عملنا المتواضع بشكل صحيح، نقسمه إلى ثلاثة فصول رئيسية:

الفصل 1: نقدم فيه اساسيات شبكة الحاسوب من انواع الشبكات و البنية المعمارية الخاصة بها والاجهزة المستعملة لتركيب و تثبيت شبكة حاسوبية.

الفصل 2 : قدمنا نظرة عامة على شبكة المنطقة المحلية للقرية الجامعية « Campus LAN » ، بدلا من ذلك لا ننسى أمن المعلومات والتهديدات المعروفة التي يمكن أن تحدث مع مبدلات الشبكة وبعض حلول الأمان وبروتوكولاتها لحماية التصميم.

الفصل 3: تصميم وتكوين شبكة قرية جامعية يمكن استخدامها في الجامعات من خلال تفعيل بروتوكولات معينة و خاصيات لتشغيل الشبكة بنجاح. وذلك عن طريق أدوات برنامج المحاكاة واختبار النتائج من خلال متابعة تدفق حركة المرور من المصدر إلى الوجهة.

الفـصـل الأول: أساسيات شبكات الحاسوب

1.1.المقدمة :

جاءت الشبكات لتلبية الحاجة الى تبادل المعلومات بسرعة و سهولة و التوصيل بين الأجهزة الطرفية البعيدة . في الوقت الحاضر الاتصالات لم تعد تقتصر على نقل بيانات الكمبيوتر فقط , بل يمكن نقل البيانات التي تحتوي على الصوت و الصور و الفيديوهات. يهدف هذا الفصل إلى فهم المفاهيم الأساسية لشبكات الكمبيوتر و التعرف على مختلف الاجهزة و المعدات المستعملة في الشبكة.

2.1. تعريف شبكة الحاسوب :

المصطلح العام « network »: هي عمل اتصال أو ربط بين جهازين أو أكثر ، تسمح هذه الشبكة بتبادل البيانات مثل الملفات و المجلدات و الصور و البرامج بين تلك الأجهزة وفقا لقواعد محددة .

شبكة الحاسوب « computer network » :هي عبارة عن مجموعة من أجهزة الحواسيب و الأجهزة الطرفية (طابعات, كاميرات مراقبة ...) المربوطة مع بعضها عن طريق اسلاك التوصيل" cables " أو لاسلكيا و بالتالي امكانية التواصل و تبادل المعلومات فيما بينهم ، و تتضمن كل شبكة معدات و برامج " software and hardware " التي تقوم بربط أجهزة الكمبيوتر و الأدوات .

3.1.أنواع الشبكات :

اعتمادًا على المسافة بين هذه الأجهزة ، يتم تمييز عدة أنواع من الشبكات ، مصنفة حسب حجمها وسرعتها ومداها.

1.3.1.الشبكات الشخصية(PAN) :[2]

الشبكات الشخصية، هي شبكات ذات مدى قصير جدًا ، تصل إلى عشرة أمتار. يتم استخدامها لتوصيل أجهزة الكمبيوتر ببعضها البعض دون اتصال سلكي.

2.3.1. الشبكات المحلية (LAN):[3]

عبارة عن مجموعة من الاجهزة المربوطة مع بعض عن طريق جهاز مبدل " switch " ليعمل على ربط الاجهزة و امكانية الاتصال ببعضها و يستخدم اسلاك من نوع خاص للربط و لنقل البيانات , يغطي هذا النوع من الشبكات منطقة جغرافية صغيرة تستخدم في المؤسسات الصغيرة او الجامعات .

- و يمكن أن تتراوح سرعة نقل بيانات الشبكة المحلية من 10Mbit/s – 1Gbit/s.
- حجم الشبكة المحلية يمكن أن تصل الى 100 أو 100 مستعمل أو اكثر .

3.3.1.الشبكات المدينية (MAN) :

هي شبكة تربط بين العديد من الشبكات المحلية تقع في نفس المنطقة الجغرافية اي تغطي مدينة بأكملها , و مكونة من موجهات" Routers "و مبادلات " Switches" المربوطة بأسلاك عالية السرعة(عادة ما تكون ألياف بصرية) يتم استعمال هذه الشبكة في المؤسسات او الشركات متعددة الفروع .

4.3.1.الشبكات الواسعة (WAN) :

الشبكة الواسعة تغطي منطقة جغرافية واسعة النطاق , تقوم بتوصيل شبكات أصغر مختلفة بما في ذلك الشبكة المحلية و الاقليمية , يتم استعمال مثل هذه الشبكات في الشركات أو المؤسسات التي تعمل بمواقع مختلفة و منفصلة موزعة على مساحات جغرافية كبيرة .

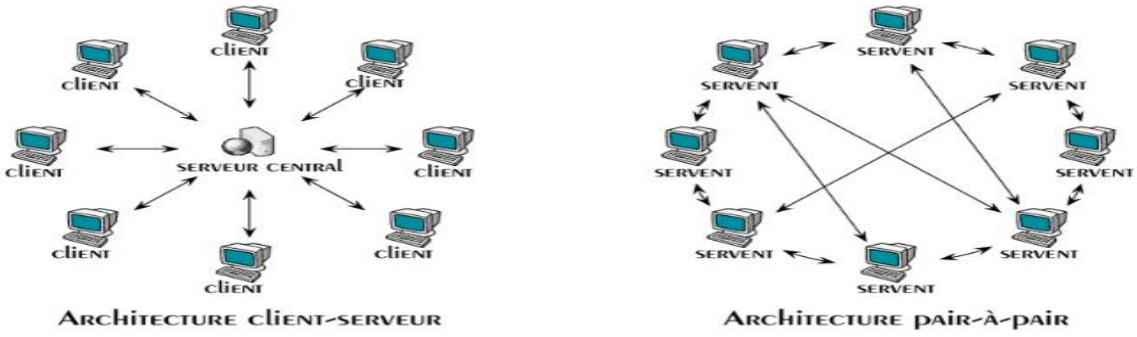
4.1. البنية المعمارية للشبكة(Network Architecture): هناك نوعان من بنية الشبكة [4]

1.4.1. شبكة نظير الى نظير (Peer to Peer) :

في هذه الشبكة كل حاسوب يعتبر عميلا و خادما في نفس الوقت , الحواسيب تكون متصلة مباشرة مع بعضها ولا يوجد حاسوب مركزي أو خادم « server » بينهم (كما هو موضح في الشكل) . من ميزات هذه الشبكة تكلفة تركيب الأجهزة منخفضة ، و اذا تضمنت الشبكة العديد من الحواسيب يصبح من المستحيل ادارتها , اذن هذه البنية مناسبة فقط للشبكات الصغيرة .

2.4.1. شبكة خادم/عميل (Client/Server) :

يتم توصيل جميع اجهزة الحاسوب (العميل) بجهاز حاسوب مركزي (خادم) ذو سعة قوية و يتم استخدامه لمشاركة اتصال الانترنت و البرامج المركزية ، و هذا النوع من البنية يسهل ادارتها و تتطلب برامج متخصصة باهظة التكلفة لتشغيل الشبكة.



شكل 1.1 : شبكة نظير إلى نظير +شبكة خادم / عميل.

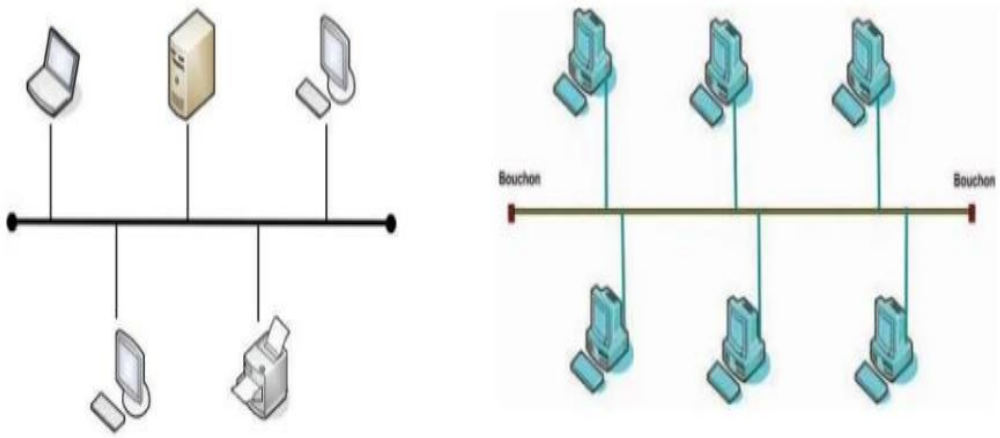
5.1. طوبولوجيا الشبكات (Network Topology) :

هي مخطط الاتصال و الموقع الفعلي لأجهزة الشبكة [6] [5]

1.5.1. طوبولوجيا الخطية (Bus Topology):

هي من ابسط الطوبولوجيات الأساسية ، حيث يتم ترتيب و توصيل الحواسيب على جانبي السلك الرئيسي مع بعض (انظر الشكل) ، سلك التوصيل المستعمل في هذه الشبكة هو سلك احادي المحور (coaxial cable) أو سلك

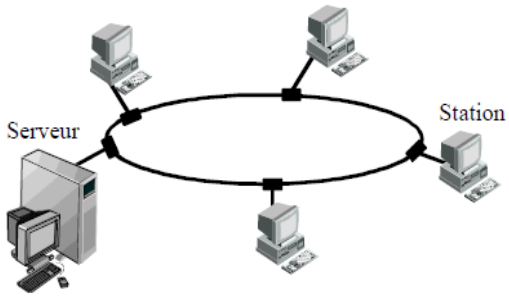
Rj45، عندما يرسل حاسوب المعلومات تتلقى جميع الحواسيب الاخرى في الشبكة المعلومات اي تبث المعلومات عبر الشبكة بأكملها لكن الحاسوب الذي تم توجيه تلك المعلومات له هو من سيستقبلها و يستخدمها .



شكل 2.1: طوبولوجيا الخطية.

2.5.1. طوبولوجيا الحلقية(Ring Topology) :

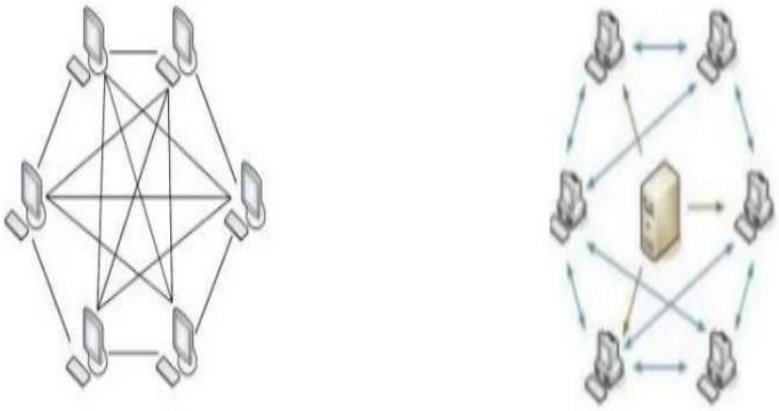
في الشبكة الحلقية يتم ربط اجهزة الحاسوب في شكل حلقة ، تتدفق البيانات في اتجاه واحد من حاسوب الى اخر .هذه الشبكة تستخدم سلك توصيل في كل جهازين لربط مجموعة من الحواسيب معا ،و يعتبر الحاسب المركزي جزء من الحلقة و تتدفق البيانات بشكل دائري مما يتسبب في حدوث بطء في الشبكة .



شكل 3.1 : طوبولوجيا الحلقية .

3.5.1. طوبولوجيا المعقدة (Mesh Topology) :

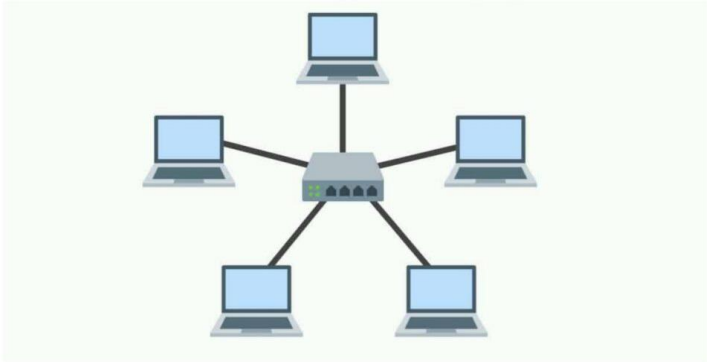
سميت بالشبكة المعقدة لإحتواءها على الكثير من الأسلاك للربط بين الأجهزة و في جميع الأجهزة يخرج ناقل على عدد الأجهزة الموجودة ، و كل عقدة في الشبكة تتصل بالأخرى مباشرة . يتم ارسال البيانات من جهاز الى اخر بشكل مباشر دون المرور بحاسوب مركزي او جهاز محدد .



شكل 4.1 : طوبولوجيا المعقدة.

4.5.1. طوبولوجيا النجمية(Star Topology) :

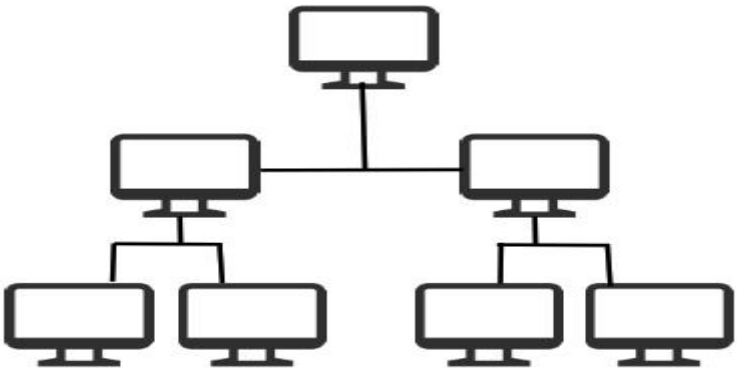
في هذه الشبكة اجهزة الحاسوب تكون متصلة بجهاز مركزي يسمى مبدل " switch" الذي بدوره يضمن الاتصال بين الاجهزة المتصلة بها و مرور البيانات عبره ويفحص كل رسالة يتلقاها و يحولها فقط الى المتلقي المطلوب . هذه البنية النجمية لا يوجد لها سلك توصيل واحد رئيسي بل يوجد فيها اكثر من سلك .في حالة تعطل احد الاسلاك لا تتوقف الشبكة فقط يتم توقف الجهاز الذي تم تعطل السلك الخاص به ، هذه الشبكة الاكثر انتشارا نظرا لسهولة الصيانة و العمل فيها .



شكل5.1: طوبولوجيا النجمية.

5.5.1. طوبولوجيا الشجرة (Tree Topology) :

ويسمى أيضًا الطوبولوجيا الهرمية، كل كمبيوتر لديه روابط إلى كمبيوتر آخر حيث يتم إعطاء عقدة جديدة لكل عقدة. لذلك تنقسم الشبكة إلى مستويات. المستوى الأعلى ، المستوى الأعلى ، متصل بالعديد من عقد المستوى الأدنى في التسلسل الهرمي.



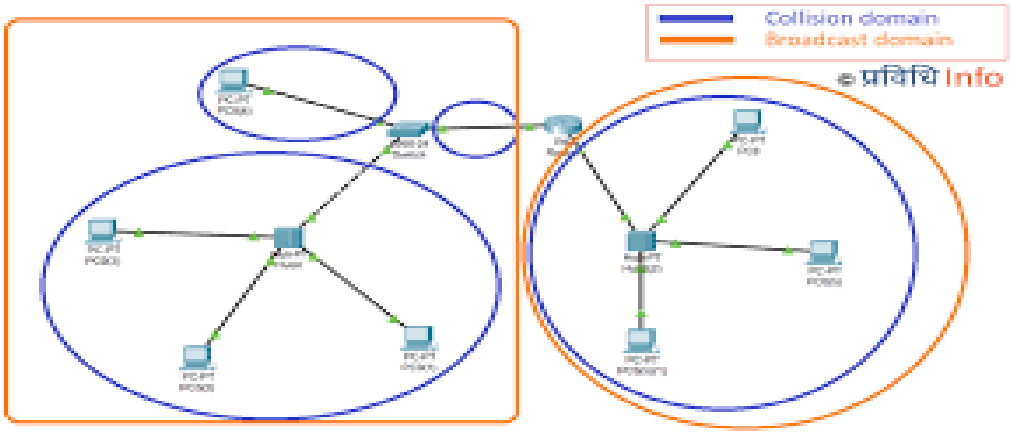
شكل6.1 : طوبولوجيا الشجرة.

6.1. معيار Ethernet/802.3 :

يعد احد المعايير المميزة و الاكثر استعمالا لشبكات الحاسوب، يلعب دورا مهما في تصميم و تنفيذ الشبكات ، حيث يتم تطويره باستمرار لتلبية متطلبات التكنولوجيا المتزايدة . يعتمد هذا المعيار على بروتوكول CSMA/CD و ارسال(broadcast, multicast…) و اعدادات Duplex و غير ذلك …

1.6.1. مجال تصادم البيانات 'Collision Domain' : عبارة عن تصادمات التي تحصل عند التقاء حزم البيانات في مسار واحد .

2.6.1. مجال البث 'Broadcast Domain' : عبارة عن مجموعة من الاجهزة المتصلة في شبكة واحدة تحت نطاق واحد ، حيث يوجد امكانية حدوث تصادم البيانات المرسلة فيما بينهما .



شكل7.1 : تحديد مجال تصادم البيانات و مجال البث.

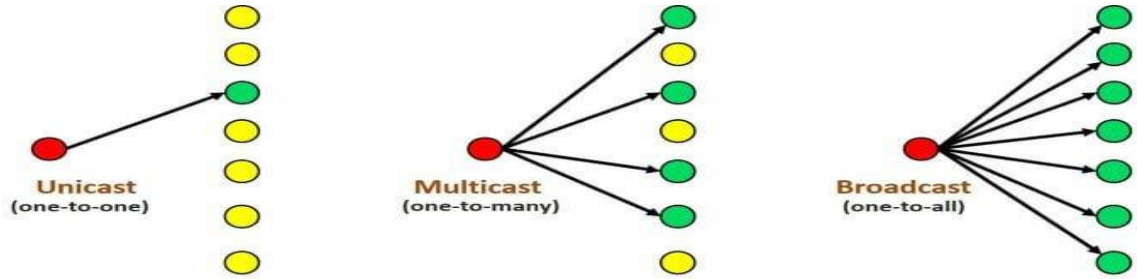
3.6.1. CSMA/CD :

بروتوكول تجنب تصادم البيانات داخل الشبكة يستعمل فقط في الاتصال نصف الاتجاه 'Half Duplex' ، و المنافذ ذات الاتصال كامل الاتجاه 'Full Duplex' لا تستخدم بروتوكول CSMA/CD. عند تفعيل هذا البروتوكول يجعل جميع اجهزة الشبكة التي لديها بيانات للإرسال أن تقوم بعملية الاستماع قبل الارسال بمعنى يجعل

اي جهاز من الشبكة ان يتحقق اولا من محطة الارسال ما اذا كانت القناة مشغولة او متاحة و جاهزة للاستقبال . ففي حالة اذا كانت القناة مشغولة ينتظر الجهاز و يؤجل الارسال حتى تصبح القناة متاحة للاستقبال من ثم يتم الارسال مع مراقبة القناة بإستمرار لإكتشاف التصادم .[7]

4.6.1. طرق ارسال البيانات في داخل الشبكات :

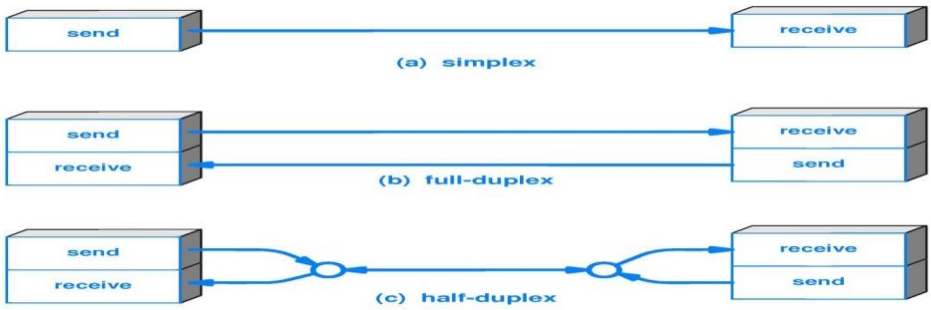
- **إرسال احادي الإتجاه « Unicast »** : هذه الطريقة تقوم بإرسال البيانات من جهاز الى الجهاز المطلوب فقط ، مرسل و مستقبل واحد فقط .
- **إرسال متعدد الاتجاه « Multicast »** : يقوم بإرسال البيانات لمجموعة محددة فقط من الاجهزة .
- **ارسال البث « Broadcast »**: يقوم بإرسال البيانات لكل الشبكة لجميع الأجهزة المتصلة في الشبكة.



شكل8.1 : طرق ارسال البيانات.

5.6.1. طرق ارسال البيانات عبر الوسائط المادية للشبكات : [8]

- **وضع أحادي الاتجاه « Simplex »:** هو الوضع الذي يمكن من خلاله إرسال البيانات في اتجاه واحد فقط، بمعنى الاتصال يكون أحادي الاتجاه يمكنه فقط إرسال البيانات ولا يمكن تلقي أو استقبال أي رد عليها، ومثال على ذلك البث التلفزيوني و الاذاعة
- **وضع نصف الاتجاه « Half duplex »** : هو الوضع الذي يمكن من خلاله نقل البيانات في كلا الاتجاهين على ناقل واحد ولكن ليس في نفس الوقت، ومثال على ذلك جهاز الووكي توكي
- **وضع ثنائي الاتجاه « Full duplex »** : هو الوضع الذي يمكن من خلاله إرسال البيانات في كلا الاتجاهين في وقت واحد ، مثل الهاتف .



شكل9.1: أوضاع الارسال.

7.1. مكونات الشبكات : [10] [9]

1.7.1. أجهزة الشبكات :

- **المبدل(Switch)** : جهاز ربط يعمل في الطبقة الثانية(Data Link) ، يحتوي على ميزات أكثر تقدما من الموزع حيث يقوم بعملية تسمى بـ (Switching Table) .

شكل10.1: المبدل SWITCH.

- **الموجه(Router)**: هو جهاز يعمل في الطبقة الثالثة « Network Layer »من نموذج OSI ، يقوم بربط شبكات مختلفة البعيدة او القريبة . وله وظيفتين أساسيتين هما:

- إعطاء أو تشغيل " Operate " العناوين المنطقية Logical Address وهو IP address .

- يعمل على اختيار أفضل مسار يمكن أن تمر من خلاله البيانات من المرسل إلى المرسل إليه ويستخدم عنوان IP في تكوين Routing table، ويستخدم إحدى أساسيات شبكات الحاسوب بروتوكولات التوجيه المعروفة RIP ، IGRP، EIGRP، OSPF، IS-IS.

شكل11.1: الموجه ROUTER.

- **مبدل متعدد الطبقات(Multilayer Switches) :**هو جهاز شبكة لديه القدرة على العمل في طبقات أعلى من نموذج OSI المرجعي ، على عكس طبقة ارتباط البيانات (DLL) التي تستخدمها المحولات تقليديًا. يمكن لمبادلات متعدد الطبقات "multilayer switches" أداء وظائف المبادلات "switches" بالإضافة إلى وظائف جهاز التوجيه " Router " بسرعات عالية.

شكل12.1: مبدل متعدد الطبقات

- **جدار الحماية (ASA Firewall):** جهاز اساسي و رئيسي خاص ب Cisco في مجال الأمن و الحماية ، حيث تم تصميمه لتمييز حزم البيانات الشرعية تحت انوع اتصال مختلفة . يمكن السماح فقط لحزم البيانات المطابقة للاتصال النشط بالمرور عبر جدار الحماية ، و سيتم رفض حزم البيانات الأخرى .

شكل13.1: جدار الحماية ASA

- **المكرر(Repeater) :**يعد أبسط أجهزة الربط المستخدمة في الشبكات و يعمل في الطبقة الأولى و هي الطبقة الفيزيائية يقتصر عمله على تكرار كل ما يصل إليه من إشارات أي إعادة انتاج الاشارة بالقوة الفعلية دون تقويتها. يستخدم هذا الجهاز في الشبكة لزيادة المسافة التي يمتد إليها السلك المستخدم والتغلب على ضعف الاشارة المرسلة. من المعروف أن الإشارات ينتابها الضعف أثناء انتقالها في الكابل وكلما كان الكابل أطول كلما اصحبت الإشارات ضعيفة نتيجة طول المسافة التي تقطعها للوصول إلى وجهتها لذلك يستخدم هذا الجهاز لضمان وصول الاشارة الى وجهتها .

شكل14.1: المكرر Repeater.

- **بطاقة واجهة الشبكة (Network Interface Card) NIC :** هي من احد المكونات المادية لأجهزة الحاسوب و التي تتصل باللوحة الرئيسية " Motherboard " و التي تسمح للحاسوب الاتصال بالشبكة الغرض

منه نقل و استقبال البيانات وتتم هذه العملية من خلال جهاز إرسال واستقبال الإشارات " transceiver " في ال NIC تحتوي هذه البطاقة على عنوان فيزيائي فريد و كل بطاقة تختلف عن الاخرى و لا يمكن تكرار العنوان على اكثر من بطاقة . وطبعا مثل ما عرفنا ال MAC هو الذي يعرف به جهاز السويتش عنوان الواجهة.

شكل15.1 : كرت الشبكةNIC.

- **المودم (Modem):**

كارت يستخدم في عملية " modulator-demodulator " وهي عملية تحويل البيانات من " Analog to Digital " أو العكس ويستخدم في عملية اتصال الشبكة عن طريق خط الهاتف من شركة الهواتف وتسمى في الشبكات PSTN ويعتبر المودم جهاز قديم وال DSL تكنولوجيا حديثة معتمدة على NIC أفضل وأسرع منه.هناك نوعان من المودم:

- External Modem : ويتم تركيبة خارج جهاز الكمبيوتر.
- Internal Modem : ويتم تركيبة داخل جهاز الكمبيوتر.

شكل16.1: المودم Modem.

2.7.1. أنواع الأسلاك و الموصلات في الشبكات : [11] [9]

- **الاسلاك الثنائية الملفوفة(Twisted Pair Câble):**

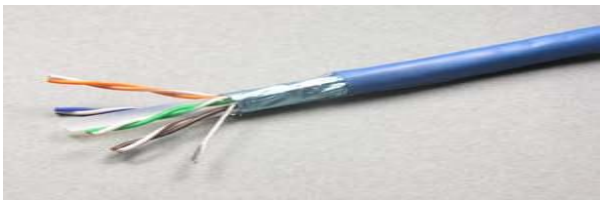
هذا النوع من الاسلاك يتكون من 8 اسلاك كل سلكين ملفوفان على بعضها و هذا الالتفاف يعمل على تقليل التشويش او التداخل الكهرومغناطيسي ، الموصل المستعمل لتركيب اسلاك الثنائية الملفوفة هو موصل Rj45 « Rejected Jack ».

شكل20.1: الاسلاك المزدوجة .

شكل21.1: موصل 45 –RJ.

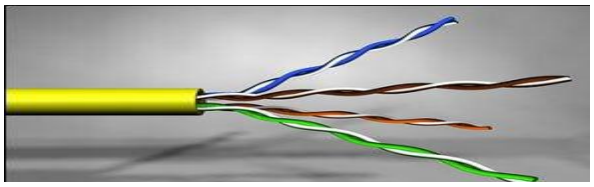
- **انواع الاسلاك الثنائية :**

- **الاسلاك الثنائية الملفوفة المحمية STP :** و هي عبارة عن اسلاك محمية بطبقة من القصدير ثم بغلاف بلاستيكي خارجي



شكل22.1:الاسلاك الثنائية المحمية STP.

- **الاسلاك الثنائية الملفوفة الغير محمية UTP :** هي عبارة عن اسلاك ملتوية داخل غطاء بلاستيكي بسيط .

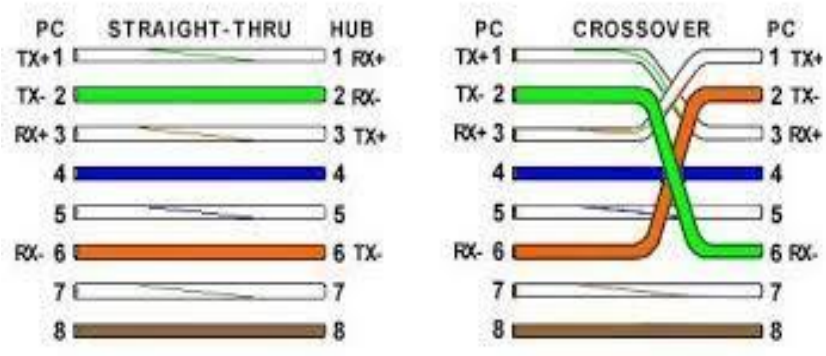


شكل23.1:الأسلاك الثنائية الغير محمية UTP.

- **انواع توصيل اسلاك STP و UTP :**

- **التوصيل المباشر " Straight cable" :** يستخدم لتوصيل أجهزة مختلفة مثل كمبيوتر مع سويتش.

- **والتوصيل التقاطعي "Crossover cable " :** يستخدم لتوصيل أجهزة متشابهة مثل سويتش مع سويتش.



شكل24.1: انواع توصيل STP و UTP.

- **اسلاك الالياف الضوئية « Fiber Optic » :**

تستخدم في نقل البيانات في شكل اشارات ضوئية , وهي مصنوعة من ألياف الزجاج النقي طويلة ورفيعة لا يتعدى سمكها سمك الشعر يجمع العديد من هذه الألياف في حزم داخل الأسلاك البصرية.

- نستعمل هذا النوع من الاسلاك للتوصيل بين الشبكات (بين بلد و بلد) الى عدة كيلومترات .
- و لاستعمال سلك الالياف البصرية في الشبكات المحلية نستعمل نوع « multimode » و هو النوع الذي يستعمل في الشبكات الداخلية حيث ينقل البيانات لمسافة 500 متر .

- **مزايا:**
  - منيعة ضد التداخل الكهرومغناطيسي و التداخل من الأسلاك المجاورة .
  - معدلات التوهين منخفضة جدا .
  - سرعة إرسال بيانات مرتفعة جدا بدأت ب 100 ميجابت في الثانية و قد وصلت حاليا إلى 200000 ميجابت في الثانية.
  - في الألياف البصرية يتم تحويل البيانات الرقمية إلى نبضات من الضوء، و حيث أنه لا يمر بهذه الألياف أي إشارات كهربائية فإن مستوى الأمن الذي تقدمه ضد التنصت يكون مرتفعا .

- **عيوب :**
  - صعوبة في التركيب والصيانة .
- **موصلات الألياف الضوئية:** [12]

يوجد أكثر من مائة نوع من الموصلات ، ولكن يتم استخدام القليل منها بشكل متكرر. يمكن أن تكون الموصلات أحادية الوضع أو متعددة الأوضاع حسب وسيط الإرسال. الأكثر استخدامًا هي : موصلSC ،موصلLC ، موصلFC، موصل ST

شكل25.1: موصلات الالياف الضوئية.

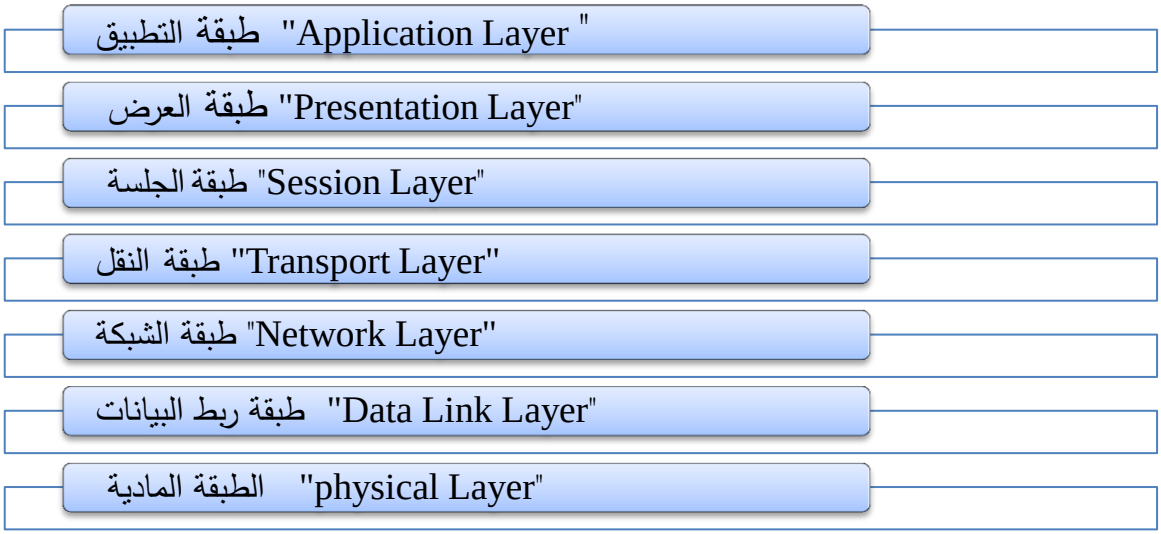
8.1. نماذج الشبكة (Network Models): [13] [6]

هناك نوعان أساسيان من نماذج الشبكة:

النموذج المرجع(Reference Model)ونموذج التطبيق(Application Model)

1.8.1. نموذج المرجعي OSI (OSI Model) :

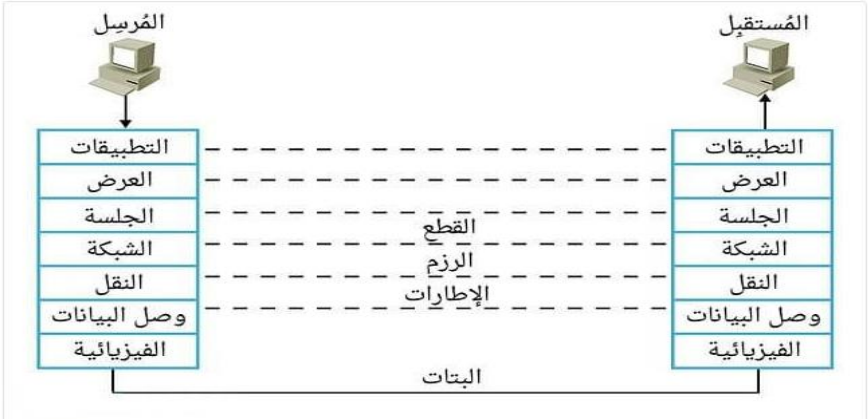
تم تطوير هذا النموذج من قبل(المنظمة الدولية للمعايير ISO) من أجل وضع معيار للاتصالات بين أجهزة الكمبيوتر على الشبكة ، و هو عبارة عن نموذج او طبقات(Layers) يشرح المراحل التي تمر بها البيانات عندما تنتقل من المصدر الى المتلقي "المستقبل" عبر الشبكة ، يتكون من 7 طبقات كل طبقة تقوم بمهمة محددة وسنقدمها واحد تلو الآخر ادناه .



شكل26.1: نموذج المرجعي OSI.

- **الطبقة المادية(Physical Layer)** : هي الطبقة المسؤولة عن الاتصال المادي للجهاز بالشبكة بإستعمال نواقل مختلفة : ألياف ضوئية أو ناقل أحادي الاتجاه أو ناقل من نوع Rj45 . و تقوم بتحويل البيانات الى اشارات كهربائية و تتم هذه العملية بواسطة بطاقة الشبكة .
- **طبقة ربط البيانات(Data Link Layer)** : هي طبقة يتم فيها تجهيز البيانات من أجل تسليمها للشبكة ، حيث تقوم بتغليف الحزم(Packets) في إطار(frames) و برتوكولات هذه الطبقة تساعد في تحديد المرسل و المستقبل "عنونة MAC" و اكتشاف الأخطاء و معالجتها.
- **طبقة الشبكة(Network Layer)** : و هي المسؤولة عن الاتصالات بين الاجهزة الطرفية و التي تكون على شبكة مختلفة ، أي هي المسؤولة عن نقل الكاملة للحزم (Packets)من المرسل الى المستقبل .
- **طبقة النقل(Transport Layer)** : هذه الطبقة مسؤولة عن نقل و ادارة البيانات و تحديد نوع البروتوكول المناسب للبيانات في عملية الارسال و نقل البيانات لأنها تعمل بطريقتين مختلفتين ببروتوكولين مختلفين هما TCP وUDP.
- **طبقة الجلسة (Session Layer)**: المسؤولة عن تنظيم و تبادل الاتصال(dialog control) بين الجهازين ، أي تتحكم في جلسة العمل و ادارتها (فتح و غلق الاتصال) ، تقوم كذلك بتحديد نوع الاتصال المستخدم full duplex او half duplex.
- **طبقة العرض(Presentation Layer)**: و هي المسؤولة عن ترجمة أي عملية على الجهاز بلغة الكمبيوتر ، تقوم بالعمليات الاتية : data coding , data compression , data encryption

- **طبقة التطبيق (Application Layer)** : الطبقة المسؤولة عن التطبيقات مثل البرامج التي يتعامل معها المستخدم مثل تصفح الانترنت و ذلك بفضل بروتوكولات التي يتم استعمالها للوصول الى الشبكة .



شكل1.27 : رسم تخطيطي لطبقات .OSI

2.8.1.نموذج التطبيقي TCP/IP: [14]

النموذج الأكثر استخدامًا المستوحى من نموذج OSI ، تم تطوير هذا النموذج (بروتوكول التحكم في الإرسال / بروتوكول الإنترنت) من قبل وزارة الدفاع الأمريكية (DOD) في أوائل السبعينيات ليكون بمثابة أساس لشبكة ARPANET العسكرية التي تأسست قبل الإنترنت. و يحتوي على أربعة طبقات .

شكل1.28 : رسم تخطيطي لنموذج TCP/IP.

- **طبقة الشبكة:** تتعامل مع الوصول الفيزيائي إلى الأجهزة والوسائط بالإضافة إلى طريقة الوصول إليها وإرسال البيانات مع إضافة العناوين الفيزيائية ، أي تحدد الشكل الذي يجب نقل البيانات به مهما كان نوع الشبكة المستخدمة .
- **طبقة الإنترنت:**وهي مسؤولة عن التوجيه واختيار الطريق وإضافة العناوين (عناوين IP).
- **طبقة النقل** : مشابهة لطبقة النقل في نموذج OSI كما أنها توفر اتصالات ذات موثوقية جيدة، و تضمن توجيه البيانات .
- **طبقة التطبيق:** تدمج الطبقات من 5 إلى 7 في نموذج OSI ضمن هذه الطبقة.

الخاتمة :

قد أثرت شبكات الحاسوب هذه على الحياة تأثيرا كبيرا و جعل العالم يبدو مثل قرية صغيرة كما ألغت مفهوم البعد الجغرافي بين الأشخاص .لقد حددنا في هذا الفصل المفاهيم الأساسية للشبكات الحاسوبية. لقد درسنا كيفية تداول الملفات والبيانات على الشبكات ذات الحجم الصغير (على سبيل المثال LAN)أو ذات الحجم الأكبر (WAN) .الفصل التالي سيخصص لي كيفية تصميم شبكات .

الفصل الثاني: تصميم و طرق حماية الشبكة

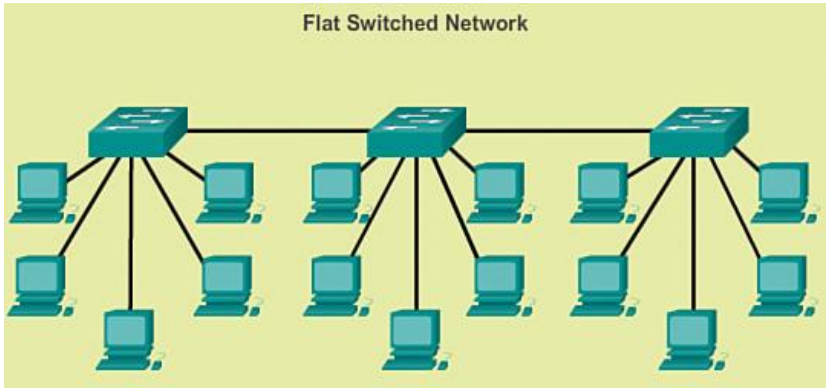
1.2. المقدمة :

في مجال الشبكات نولي اهتماما كبيرا لقواعد اساسيات الشبكة و كيفية حمايتها ، فقد اصبح امن الشبكات مسألة رئيسية نتيجة سرعة التطور التكنولوجي الذي أدى الى زيادة المخاطر و التهديدات التي قد تتعرض لها الشبكة . امن تكنولوجيا المعلومات هو مجموعة من الحلول و التدابير لتجنب تلك المخاطر و الحد منها ، لا بد من توفير تصميم يساعد في تحقيق هذه الحماية . فتركيب المعدات و تكديسها لا يجعلك محترفا في الشبكة .و هذا ما جعل المهندسين يبحثون لإيجاد حل للإنتقال من التقنية القديمة الى احدث تقنيات التصميم لتوفير حماية عالية مثل نموذج الشبكة الهرمية .

2.2. تصاميم الشبكة المحلية LAN : [15]

1.2.2. التصميم المسطح (flat design) :

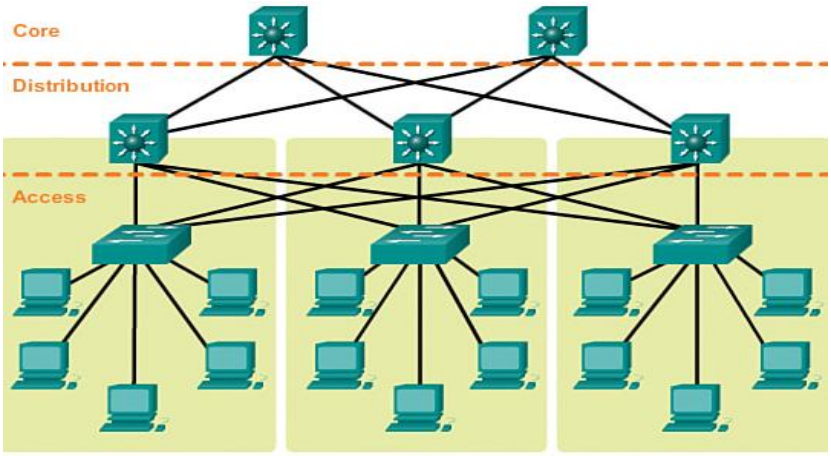
هذا النوع من التصميم خصص للشبكات الصغيرة سهلة التصميم و التنفيذ و الصيانة . كلما كبرت الشبكة يصبح هذا التصميم اكثر تعقيدا و يجعل استكشاف الاخطاء و اصلاحها امرا صعبا ففي حالة حدوث خلل او عطل بجهاز واحد فقط من الشبكة يؤدي الى تعطل الشبكة بأكملها و بالتالي تصبح هذه الشبكة غير مرغوب فيها .



شكل1.2 : شبكة ذو تصميم المسطح[15] .

2.2.2. التصميم الهرمي(Hierarchy Design):

هذا النوع من التصميم يتم فيه تقسيم الشبكة الى ثلاث طبقات هرمية لكل طبقة و ظيفة معينة و أجهزة و بروتوكولات خاصة .



شكل2.2: التصميم الهرمي.

- **طبقة الوصول (Access layer):** [16]

هي الطبقة الخاصة بالأجهزة التي يتعامل معها المستخدمون (حاسوب , طابعة ...) للوصول الى بقية الشبكة . الغرض الرئيسي من طبقة الوصول هو توفير وسيلة لتوصيل الاجهزة بالشبكة .

- **طبقة التوزيع (Distribution layer) :** [16] [17]

تتجمع فيه جميع البيانات الاتية من طبقة الوصول قبل ارسالها للطبقة الاساسية 'core' و توجيهها الى وجهتها النهائية. يتم توصيل أجهزة طبقة التوزيع غالبا بشكل متداخل 'Mesh' لتوفير اسلاك احتياطية 'Redundant Links' لإستخدامها في حالة تعطل احدى الاسلاك المستخدمة . وظيفة هذه الطبقة :

- تمكين أجهزة طبقة الوصول من الاتصال فيما بينهما .
- تتحكم في تدفق حركة مرور الشبكة ، و تحديد مجالات البث 'Broadcast Domain' و يستخدم في هذه الطبقة مبدل خاص يعمل على الطبقة الثانية أو الثالثة من نموذج OSI يطلق عليه 'Switch Multi Layer'.

- **طبقة الاساسية(Core layer):** [17]

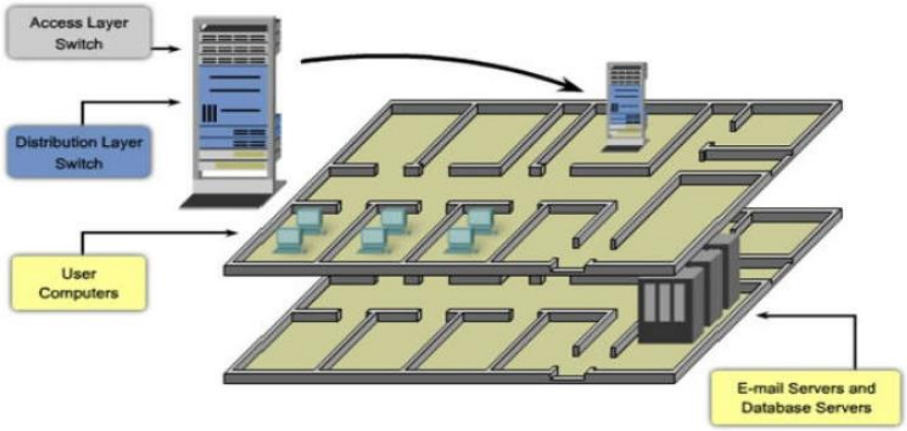
الطبقة الاساسية من التصميم الهرمي هي العمود الفقري للشبكة ذو السرعة العالية في نقل البيانات .يتم توصيل الاجهزة بشكل متداخل لتوفير اسلاك اضافية لإستخدامها في حالة تعطل احدى الاسلاك المستخدمة مما يجعل هذه الطبقة متاحة دائما و خالية من اي عطب 'Highly Available and redundant' من اهم وظائفها:

- تقوم بتجميع حركة المرور من جميع أجهزة طبقة التوزيع
- جعل اجهزة الشبكة قادرة على الاتصال بالطبقة المركزية لتوصيل الاجهزة بجهاز خادم او بشبكة خارجية .

3.2. التصميم الهرمي في مجال الاعمال متوسطة الحجم :

تطبيق هذا التصميم في الواقع مختلف تماما عن التصميم بالمحاكاة فمن الصعب رؤية الطبقات الهرمية عندما يتم تثبيت الشبكة في الشركات او في الجامعات ، كما هو موضح في الشكل اسفله . فبواسطة استعمال برنامج

المحاكاة « Packet Tracer » عند التحويل الى الشكل الواقعي نجد التصميم عبارة عن خزانة بها اجهزة كل طبقة كما موضح في الشكل.



شكل3.2 : التصميم الهرمي في مجال الاعمال متوسطة الحجم [18].

شكل4.2 : التسلسل الهرمي في الواقع.

4.2. محاسن التصميم الهرمي : [16]

- قابلية التوسع 'Scalability' : امكانية توسيع الشبكة مستقبلا
- التكرار 'Redundancy' : امكانية ربط أسلاك متعددة عبر الاجهزة في حالة تعطل احد الموجهات فيمكن ايجاد مسار اخر بديل للوصول الى الوجهة
- تحسين الاداء 'Performance': يسمح هذا النموذج بتحسين الاداء عن طريق تجنب نقل البيانات من خلال المبدلات الوسيطة ذات الاداء المنخفض ، حيث يتم ارسال البيانات من طبقة الى طبقة بقدرات تبديل عالية الاداء لتوجيه حركة المرور الى الطبقة الاساسية و من ثم توجيهها الى وجهتها النهائية .
- توفير حماية عالية 'Security'.
- سهولة الصيانة 'Maintainability'.

5.2. أمن الشبكات :

هو حماية أجهزة الكمبيوتر (بما في ذلك مكوناتها الرئيسية والداخلية والبرمجيات والبيانات الإلكترونية) من القرصنة أو الخطر أو التدمير أو الوصول غير القانوني.

1.5.2. وظائف أمن الشبكات : [19]

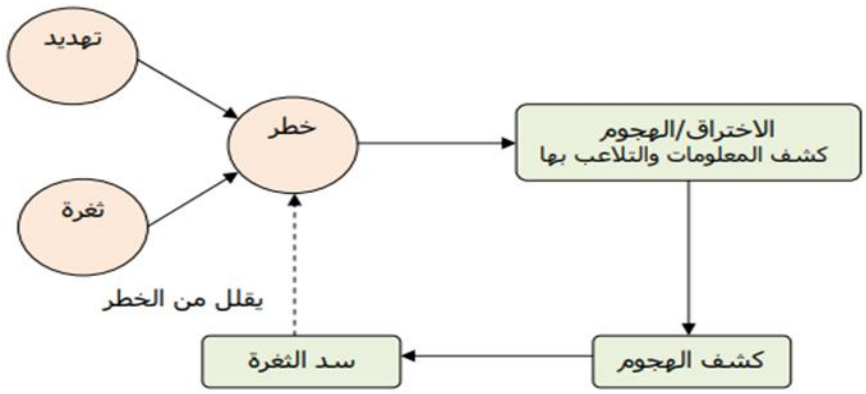
معظم أنظمة الأمن تعتمد على خمس وظائف رئيسية لتحقيق أهداف الامن :

- **المصادقة (Authentication)** :هي عملية التحقق من هوية الاشخاص التي تتواصل عبر الشبكة ، وبدون المصادقة ، يمكن لأي مستخدم لديه وصول إلى الشبكة استخدام الأدوات المتاحة بسهولة لتزوير عناوين بروتوكول الإنترنت (IP) الأصلية وانتحال شخصية الآخرين.
- **الصلاحية (Authorization)**: هي عملية سماح أو رفض الوصول إلى موارد الشبكة او خدماتها .
- **السرية أو الخصوصية(Confidentiality or privacy)**: عملية ضمان على أن المستخدمين المصرح لهم فقط هم من يمكنهم قراءة المعلومات السرية أو استخدامها.
- **الموثوقية(Integrity)** :هي جانب الأمان الذي يؤكد أن المحتويات الأصلية للمعلومات لم يتم تغييرها أو إتلافها (اصلية).
- **عدم النكران (Non-repudiation)**:يضمن لك بأن الشخص الذي يتم التواصل معه هو الشخص المطلوب و ليس وهمي .

2.5.2. مصطلحات أمن تكنولوجيا المعلومات: [20] [19]

هناك مفاهيم مجددة تتكرر في مجالات الأمن المختلفة منها :

- **الخطر « Risk »** : هو احتمالية حدوث مشكلة معينة اي يعتبر مؤشر للتهديدات ، يحدد الخطر باستخدام ثلاث عوامل :
  - احتمال ان يكون هناك تهديدا.
  - احتمال ان يكون هناك ثغرات .
  - التأثير المحتمل للخطر.
- **الثغرات « Vulnerability »** : هو عدم تحصين النظام ، و هذا المصطلح يشير الى اماكن الضعف في هذا النظام و التي تتيح للمهاجم بالاعتداء على سلامة النظام ، و ذلك قد يكون بسبب :
  - وضع كلمة سر غير امنة
  - التصميم الضعيف للشبكة
  - الاستخدام السيء الغير صحيح لبروتوكول الاتصال
  - ادخال المستخدم دون التحقق من الهوية
- **التهديدات « Threats »** : هو حدث من المحتمل ان ينتج انتهاك للسياسات أو الاجراءات الأمنية بدون اذن صاحبها و قسرا و عبر ثغرة محتملة في النظام .



الشكل5.2 :مكونات نظم امن المعلومات والشبكات.

- **أنواع التهديدات** : [21]

➢ **التهديدات غير مقصودة** " **Accidental threats** ": تلك التي توجد دون سبق إصرار ، كفشل الأنظمة ، والأخطاء التشغيلية ، والأخطاء في البرامج.

➢ **التهديدات المتعمدة**" **Intentional threats** ": هو إجراء تقوم به جهة ما لانتهاك أمن المعلومات والاستخدام غير المصرح به للموارد. يمكن أن تكون التهديدات المتعمدة سلبية أو نشطة.

- **التهديدات السلبية** " **passive attack** ": التهديدات السلبية هي تلك التي ، في حالة حدوثها ، لن تؤدي إلى أي تعديل في المعلومات الواردة في النظام (الأنظمة)

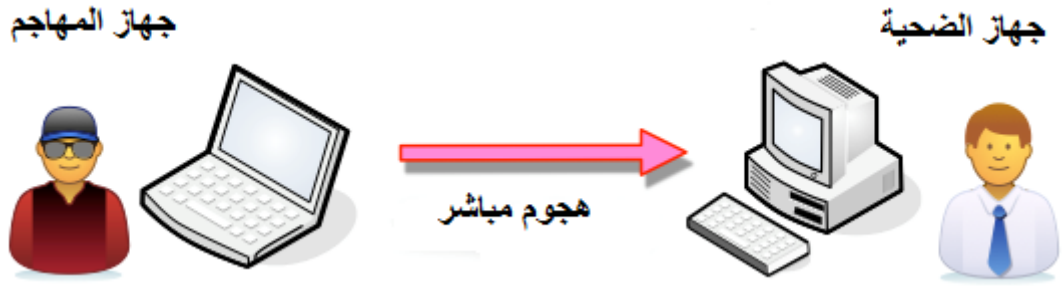
والتي لا ينتج عنها أي تعديل العملية ، ولا تتغير حالة النظام. من الصعب للغاية اكتشاف مثل هذا النوع من التهديدات لأنها غير ضارة بوظائف النظام العادية. استخدام التطفل السلبي لمراقبة المعلومات المنقولة عبر خط اتصال (مراقبة الشبكة) هو تجسيد للتهديد السلبي.

- **التهديدات النشطة** " **active attack** ": تشمل التهديدات أو الهجمات النشطة على النظام تغيير المعلومات الواردة في ذلك النظام ، أو التغييرات في حالة أو تشغيل النظام. تعتبر التهديدات النشطة ، على عكس التهديدات السلبية ، أسهل في اكتشافها إذا تم اتخاذ الاحتياطات المناسبة مسبقًا.

6.2. طرق هجمات الحاسوب **Computer Attacks methods** : [22]

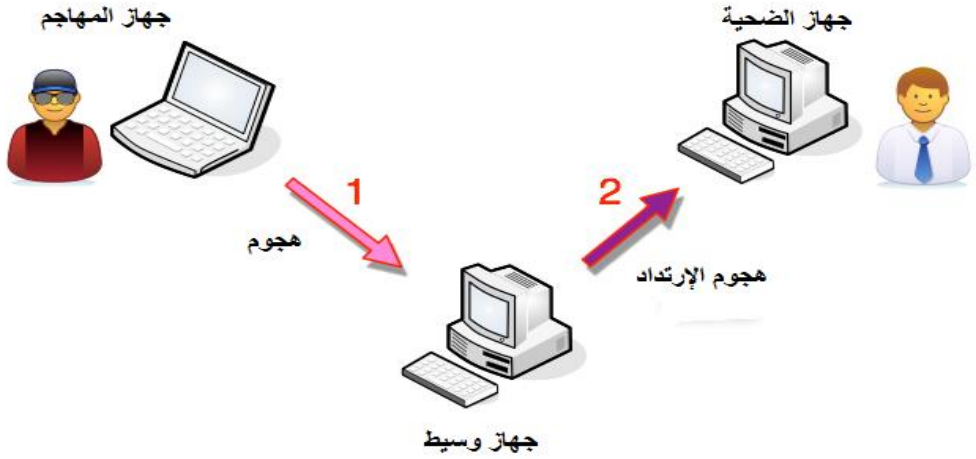
يستخدم الأشخاص المؤذون العديد من تقنيات الهجوم التي يمكن تصنيفها في ثلاث اصناف مختلفة.

- **الهجمات المباشرة** : هذا هو أبسط الهجمات. يهاجم المتسلل ضحيته مباشرة من جهاز الكمبيوتر الخاص به. في الواقع ، فإن برامج القرصنة التي يستخدمونها قابلة للتهيئة بشكل طفيف ، ويقوم عدد كبير من هذه البرامج بإرسال الحزم مباشرة إلى الضحية.



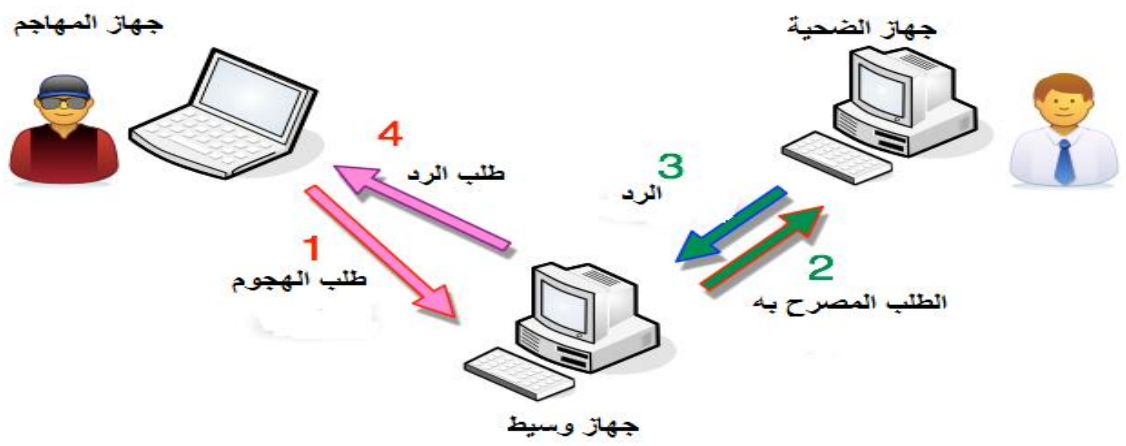
الشكل6.2: هجوم مباشر.

- **هجمات الارتداد غير المباشرة** " **Indirect bounce attacks** " : يحظى هذا الهجوم بشعبية كبيرة بين المتسللين. في الواقع ، لهذا الهجوم ميزتين:
  - إخفاء هوية عنوان (IP)المتسلل
  - من المحتمل استخدام موارد الكمبيوتر الوسيط لأنه أقوى (وحدة المعالجة المركزية ، النطاق الترددي) للهجوم .حيث يتم إرسال حزم الهجوم إلى الكمبيوتر الوسيط الذي ينقل الهجوم إلى الضحية.



الشكل7.2: هجوم الارتداد غير مباشر

- **هجمات الرد غير المباشر**" **Indirect Response Attacks** " : هذا الهجوم مشتق من هجوم الارتداد. من وجهة نظر المخترق إنه يقدم نفس المزايا. ولكن بدلاً من إرسال هجوم إلى الكمبيوتر الوسيط لتمريره ، سيرسل المهاجم طلبًا إليه. وهذا هو الرد على الطلب الذي سيتم إرساله إلى جهاز الكمبيوتر الضحية.



شكل8.2: هجمات الرد غير المباشر.

1.6.2. أنواع الهجمات Type of attacks : [23]

- **هجمات الوصول (Access attacks)**: يتعلق هذا النوع من الهجوم بسرية المعلومات أي عن طريق محاولة الوصول إلى المعلومات من قبل شخص غير مصرح له ، و من بينها :
  - التنصت " Sniffing "
  - أحصنة طروادة " Trojan horses "
  - الباب الخلفي " Backdoor "
  - هندسة اجتماعية " Social engineering "
  - تكسير كلمة المرور" Password cracking "
- **هجمات التعديل (Modification Attacks):** هذا الهجوم موجه ضد سلامة المعلومات يتمثل بالنسبة للمهاجم في محاولة تعديل المعلومات ،و من بينها :
  - الفيروسات "Viruses " والبرامج الضارة " Worms " و فيروس حصان الطروادة " Trojan horses"
- **هجمات التشبع أو رفض الخدمة (Saturation attacks or denial of service)**: هي هجمات على الكمبيوتر تتكون من إرسال آلاف الرسائل من عشرات أجهزة الكمبيوتر ، بهدف إرباك خوادم الشركة وشل موقعها الإلكتروني لعدة ساعات ، وبالتالي منع وصولها إلى مستخدمي الإنترنت. توجد هجمات مختلفة:
  - الفيضانات " Flooding "
  - فيضانTCP-SYN " TCP-SYN flooding "
  - هجومات التطفل " The smurf "
  - تجاوز سعة المخزن المؤقت" buffer overflow "
- **هجمات الإنكار (repudiation attacks):** هو محاولة لتحريف أو إنكار وقوع حدث أو معاملة بالفعل. ومن بينها:
  - انتحال عنوان IP" IP spoofing" .

7.2. الحلول الأمنية:

1.7.2. الحلول الأمنية الأولية:

- توثيق المستخدم عن طريق تسجيل الدخول وكلمة السر.
- إزالة المعلومات السرية من الاجهزة المتصلة بالشبكة إذا لم تكن هناك حاجة إليها.
- الحماية المادية للأجهزة التي تحتوي على معلومات سرية .
- تثبيت برنامج محدث لمكافحة الفيروسات.

2.7.2. جدار الحماية و الوكيل (Firewall and Proxy):[25] [24]

يعد جدار الحماية والخادم الوكيل طريقتين تم تصميمهما لتجنب الهجمات من الإنترنت عبر جهاز التوجيه.

- **الوكيل (Proxy):** هو عبارة عن تطبيق يتم تركيبه على أجهزة خادمة، وتعتمد عليه الشبكات الداخلية ومزودو خدمات الإنترنت والشركات عند تزويدها للخدمة لأي من مشتركيها، بحيث يعمل كوسيط بين مستخدمي الشبكة والإنترنت، كذلك يعمل على عزل الشبكة عن الشبكة الخارجية العالمية (www) ويوفر لها السرعة والأمان . فعلى سبيل المثال عند طلبنا لتصفح موقع معين يعمل الوكيل على البحث باستعمال عنوان IP الخاص به .و يقوم بالوظائف التالية:
  - التخزين (Caching) .
  - الفلترة (filtering) .
  - الأمان (firewall) .
- **جدار الحماية(firewall)** : هو برنامج software يتم تثبيته في جهازك، حيث يقوم بالفصل بين المناطق الموثوق بها في شبكات الحاسوب و مراقبة المعلومات التي تمر عبر الشبكة و منع اي شيء يضر بجهازك خارج الشبكة .

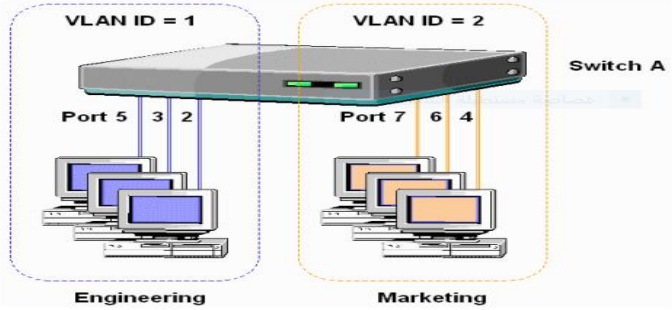
3.7.2. التشفير(Cryptography) : [26]

هو عبارة عن علم في صناعة وتطوير أنظمة التشفير القادرة على حماية المعلومات والتي تستخدم في أمن المعلومات وذلك من خلال تحويل البيانات والنصوص العادية الى بيانات ونصوص مشفرة غير مفهومة. حيث يعتمد على تصميم آليات وخوارزميات رياضية جديدة لتعمل على حفظ المعلومات.يوجد نوعين من التشفير :

- التشفير المتماثل "Symmetric " : يعتمد على مفتاح فريد مشترك بين الطرفين المتصلين. يستخدم لتشفير وفك تشفير الرسائل.
- التشفير الغير متماثل "Asymmetric " : خوارزمية تتطلب مفتاحين منفصلين احدهما سري (خاص) و الاخر عام .

4.7.2. الشبكة المحلية الافتراضية VLAN : [27]

هي شبكة افتراضية تتم عن طريق تقسيم منافذ المبدل الى عدة شبكات محلية وهمية كل منها منفصلة عن الاخرى (كما هو موضح في الشكل) . توفر هده التقنية حلولا جديدة في تجزئة و تأمين الشبكات المحلية اي لو تم تسريب فيروس او حدث هجوم على الشبكة لا يمكن للمهاجم الوصول الى الشبكة الاخرى . بالإضافة الى تقليل من عمليات البث المباشر Broadcasting على الاجهزة الاخرى عن طريق توصيل الاجهزة المتصلة بمبدل في مجال البث Broadcast Domain بحيث يقلل من مجال تصادم البيانات و ضغط المسار مما يؤدي الى تحسين الاداء .



شكل9.2 : طوبولوجيا الشبكة الافتراضية.

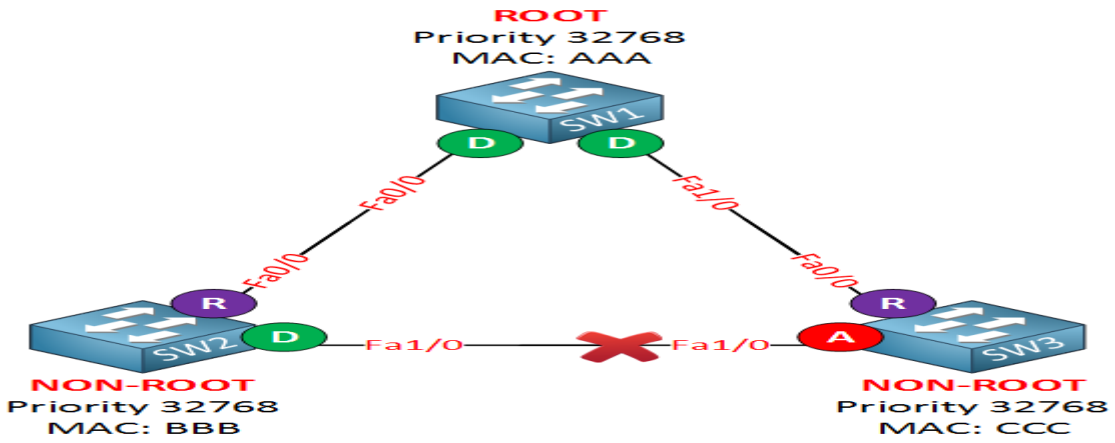
1.4.7.2. بروتوكول الإتصال 'Trunk' : عند تقسيم الشبكة المحلية بإستخدام المبدلات لإنشاء شبكة افتراضية 'VLAN' عبر مبدلين او اكثر يجب تفعيل بروتوكول الاتصال 'Trunk' لإمكانية ارسال البيانات بين المبدلات . [28]

من طرق ربط البروتوكول **'Trunk'** :

- **Inter-Switch Link (ISL)**: بروتوكول تم تأسيسه من قبل شركة cisco يعمل مع اجهزة سيسكو فقط يسمح بتبادل المعلومات بين الشبكات الافتراضية.
- **IEEE802.1Q**: بروتوكول قياسي يسمح بتبادل المعلومات بين الشبكات الافتراضية بإستخدام اجهزة الشركات المصنعة المختلفة سواءا مع اجهزة سيسكو او غيرها 'مصدر مفتوح'. [28]

2.4.7.2. بروتوكول STP: عند تفعيل هذا البروتوكول سيقوم بإنشاء طوبولوجيا خالية من الحلقات و ذلك عن طريق منع تشغيل واجهات معينة في جهاز المبدل ،و تقوم المبدلات بإرسال اطار لبعضها البعض يسمى BPDU ،حيث يحتوي هذا الاطار على عنوان MAC و الاولوية Priority .

- المبدل الذي له الاولوية هو المبدل الذي يملك عنوان MAC اقل.



شكل10.2 : وصف كيفية اختيار Root Bridge. [29]

5.7.2. الشبكة الافتراضية الخاصة (Virtual Private Network): [30]

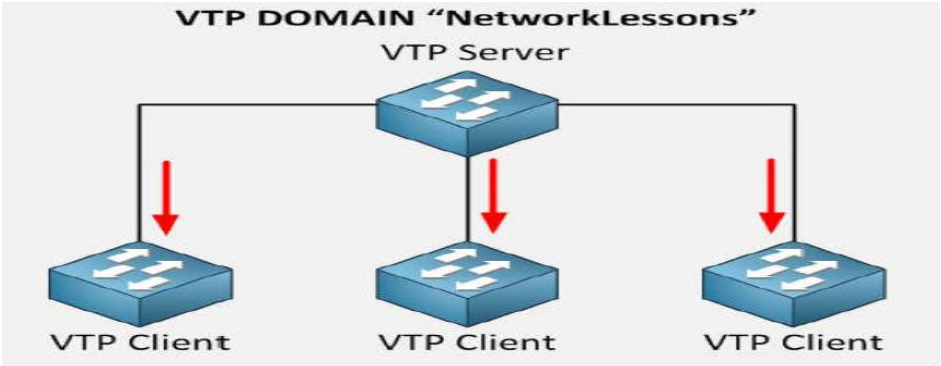
الشبكة الافتراضية الخاصة امتداد لشبكة المحلية هي تقنية تسمح بالاتصال الآمن بالإنترنت عبر نفق مشفر بشبكة أخرى، لضمان خصوصية الإنترنت وحماية سرية بيانات والهوية. تستخدم لحماية نشاطات التصفح من الأشخاص غير المعروفين على الشبكات العامة وشبكات WIFI .

8.2. بروتوكولات حماية الشبكات :

1.8.2. برتوكول VTP "Virtual Trunking Protocol" : [31]

هو بروتوكول نقل خاص بالشبكات الافتراضية VLAN يتيح لأجهزة المبدل تبادل المعلومات عن الشبكات الوهمية VLAN و ذلك عن طريق تحديد جهاز رئيسي يكون مسؤول عن انشاء و تعديل هذه المعلومات و ارسالها للأجهزة الاخرى ، يحتوي المبدل على ثلاث اوضاع لبروتوكول VTP:

- جهاز الخادم VTP Server .
- اجهزة العميل او الزبون VTP Client .
- الجهاز المحايد VTP Transparent .



شكل11.2 : اوضاع بروتوكول VTP.

2.8.2. بروتوكول IP Sec (Internet Protocol Security) : [32]

أمان بروتوكول الإنترنت هو مجموعة من بروتوكولات الشبكة الآمنة التي تصادق وتشفّر حزم البيانات لتوفير اتصال مشفر بين جهازي كمبيوتر على شبكة بروتوكول الإنترنت. يتم استخدامه في الشبكات الخاصة الافتراضية (VPN). يتضمن IP sec بروتوكولات لتأسيس مصادقة متبادلة بين الوكلاء في بداية الجلسة والتفاوض على مفاتيح التشفير لاستخدامها أثناء الجلسة.

3.8.2. بروتوكول SSH(Secure Socket Shell) : [33]

بروتوكول النقل الامن هو بروتوكول شبكي يوفر للمستخدمين مسارا آمن للوصول الأمن للحواسيب عبر الشبكة ، صمم كبديل لبروتوكول (Telnet) ، يهتم بإدارة الحماية للمرسلات عبر الشبكة يشمل التشفير و التوثيق وسلامة البيانات عند تبادلها . استخداماته كالتالي :

- نقل الملفات بسهولة و تلقائية بين الاجهزة .
- إصدار الاوامر عن بعد .
- القيام بإدارة البنية التحتية للشبكة .
- توفير الوصول الامن للمستخدمين .

الخاتمة :

في هذا الفصل ، تحدثنا اولا عن بعض المبادىء التي تستخدم لتصميم شبكة هرمية وكيفية عمل كل طبقة من هذا التصميم بوظائفها المحددة على تسهيل إدارة الشبكة وتوسيعها . كما تحدثنا أيضا عن مباديء الأمن وأهدافه بالإضافة إلى انواع الهجمات المختلفة التي تهدده. مع تقدم بعض الحلول التي تضمن سياسة أمان فعالة مثل جدار الحماية و الوكيل Proxy والتشفير وشبكات VLAN وأخيرًا الشبكات الافتراضية الخاصةVPNs ، وبروتوكولات الحماية المختلفة. الفصل التالي سيخصص لتكوين وتصميم شبكة قرية جامعية أمنة .

الفصل الثالث

محاكاة وتصميم شبكة قرية جامعية أمنة

1.3. مقدمة:

يتضمن هذا الفصل كيفية تصميم وحماية شبكة قرية جامعية « CAMPUS NETWORK » واقعية بإستخدام برنامج محاكي الشبكات « CISCO PACKET TRACER » ، وتوظيف مهاراتنا العملية السابقة لتكوين الشبكة بالكامل على طبقات ووحدات مختلفة في نظام الشبكة الأساسي الخاص بنا.

2.3 . برنامج محاكي الشبكات (Cisco Packet Tracer):

أداة مبتكرة وقوية توفر مزيجًا فريدًا من المحاكاة الواقعية والتجارب المرئية لمحاكاة الشبكة للممارسة واستكشاف الأخطاء وإصلاحها[34]. البرنامج يتوفر تقريبا على جميع الأجهزة التي قد تستعمل في الاتصال مع الشبكة كذلك يوفر جميع أنواع الكابلات الجديدة منها و القديمة لربط بين الأجهزة.

3.3. أجهزة والمعدات الشبكة المستخدمة:

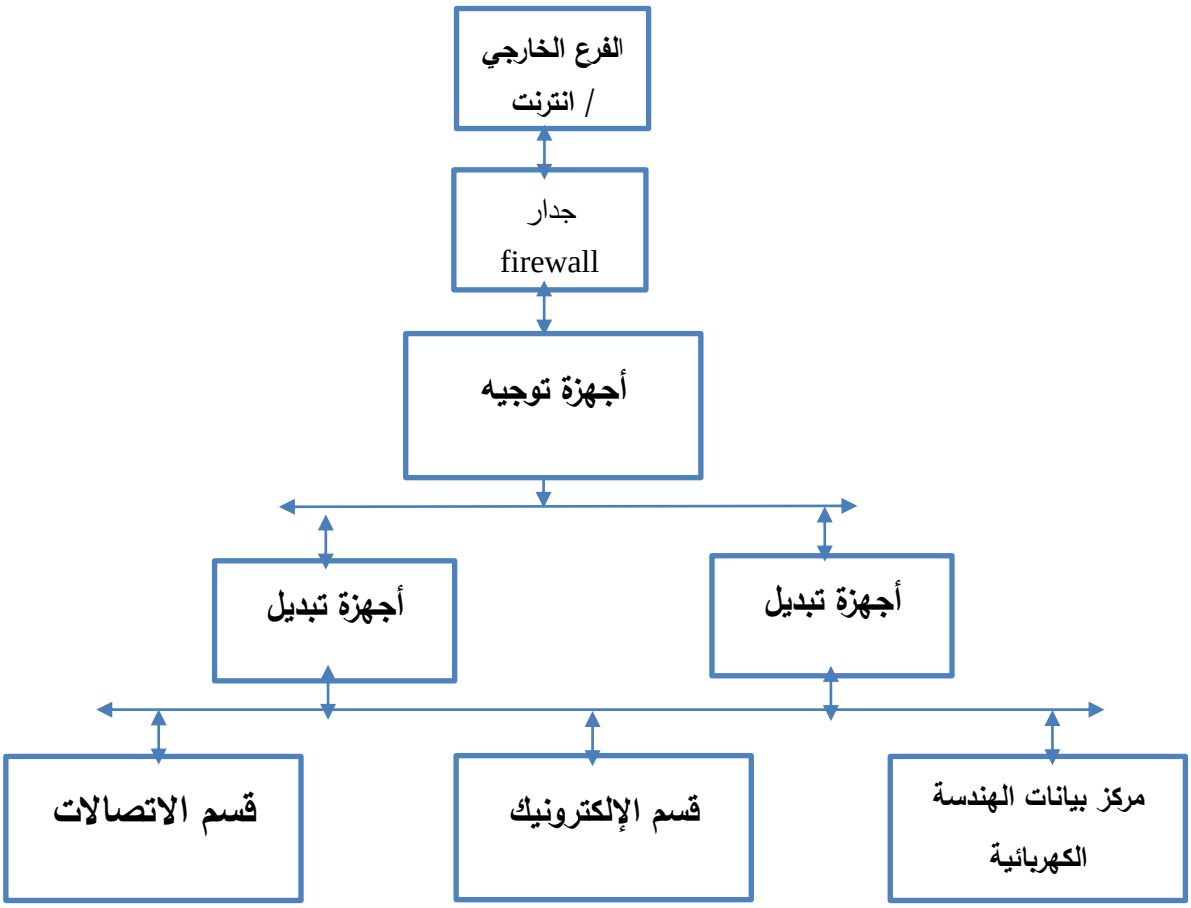
- Router2811
- Multilayer switch-3560
- Switch2960-24TT
- Firewall 5505ASA
- SERVER
- Cable Copper Cross-Over
- Cable Copper Straight-Through
- Serial DTE

4.3 . مشروع حماية شبكة قرية جامعية « Campus Network Security »:

لقد أنشأنا هيكل شبكة بسيطة متواضعة لممارسة مهاراتنا في الشبكات، وسوف يتم تطبيقها على شبكة قرية جامعية التي كانت صعبة في طريقة تكوينها و كيفية حمايتها في المؤسسة.

1.4.3. الهياكل المنطقية :

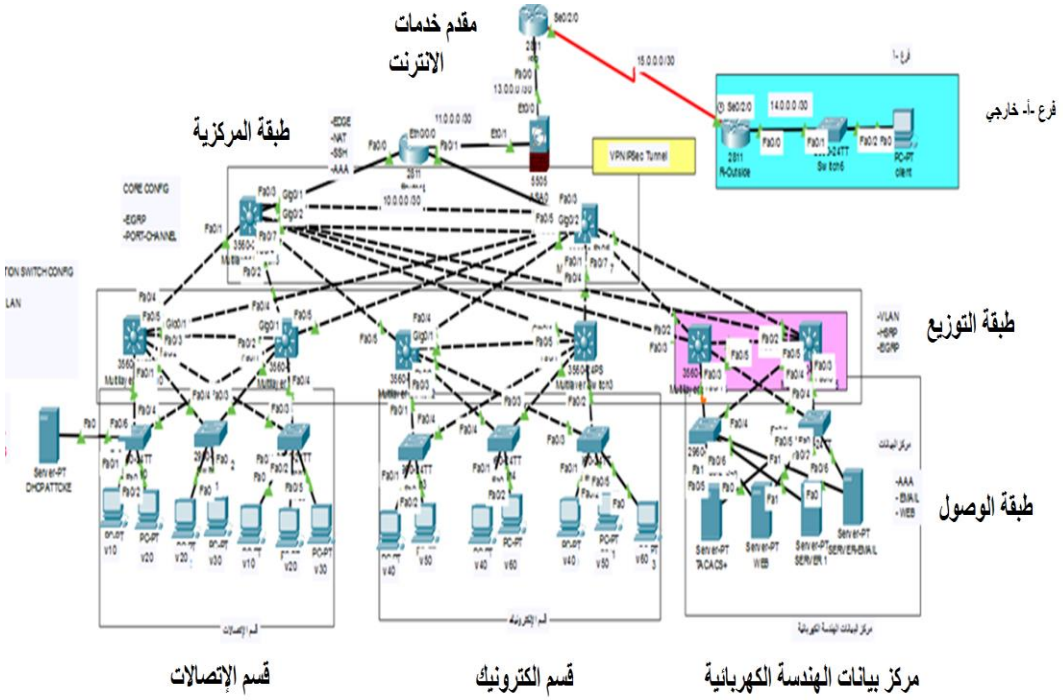
هي ترتيب الأجهزة على شبكة الكمبيوتر وكيفية تواصلها مع بعضها البعض ، والطريقة التي تمر بها البيانات عبر الشبكة من جهاز إلى آخر دون اعتبار إلى الترابط المادي للأجهزة. سوف نقوم بتمثيل الهيكل المنطقي من مشروعنا الخاص بقرية الجامعية" campus network " للمؤسسة كما هو موضح في الشكل:



شكل1.3 : مخطط الهيكل المنطقي للمشروع.

2.4.3. السيناريو:

يتكون مشروع شبكة المؤسسة الخاص بنا من قرية جامعية وطرق حمايته من الهجمات والتهديدات المواجهة للمعلومات الخاصة بالمؤسسة، يوفر تصميم الشبكة هذه الأداء وقابلية التوسع و الوصول إلى خدمات وموارد اتصالات الشبكة للمستخدمين النهائيين والأجهزة المنتشرة في موقع جغرافي واحد مثل مركز البيانات لتزويد المؤسسة بخادم ويب، كما وظفنا بعض الحلول الأمنية من بروتوكولات وأجهزة لحماية الشبكة المؤسسة. لقد أنشأنا أيضًا فرعًا آخر كموقع بعيد للاتصال بالموقع المحلي (الحرم الجامعي) عبر firewall يقوم بالفصل بين المناطق الموثوق بها في شبكات الحاسوب و مراقبة المعلومات التي تمر عبر الشبكة . المعلومات التي ترسل من الشبكة الداخلية الى الشبكة الخارجية تمر عبر نفق سري مشفر و هو vpn ipsec tunnel.



شكل2.3 : الهيكل المنطقي لشبكة الحرم الجامعي.

3.4.3 تسمية شبكات VLAN وتخصيص عناوينIP للأجهزة :

1.3.4.3 جدول شبكات VLAN:

إسم vlan	عناوين الشبكة Network Address	واجهة Interface							
		Sw1	Sw2	Sw3	Sw4	Sw5	Sw6	Sw7	Sw8
Vlan10	192.168.10.0 /24	F0/0		F0/1					
Vlan 20	192.168.20.0 /24	F0/1	F0/1	F0/2					
Vlan 30	192.168.30.0 /24		F0/2	F0/5					
Vlan 40	192.168.40.0 /24				F0/1	F0/1	F0/1		
Vlan 50	192.168.50.0 /24				F0/2		F0/2		
Vlan 60	192.168.60.0 /24					F0/2	F0/5		
Vlan 250	192.168.250.0 /24							F0/1-2 F0/5-6	F0/1-2 F0/5-6

جدول1.3 : شبكات VLAN وعناوين المقترحة في الشبكة.

2.3.4.3 جدول العناوين:

أجهزة	واجهة	عناوين IP	قناع	البوابة
EDGE	F0/0	10.0.0.58	255.255.255.252	F0/3
	F0/1	10.0.0.62	255.255.255.252	F0/3
	ETH0/0/0	11.0.0.1	255.255.255.252	ET0/1
FIREWALL	ET0/1	11.0.0.2	255.255.255.252	ETH0/0/0
	ET0/0	13.0.0.1	255.255.255.252	F0/0
ISP	F0/0	13.0.0.2	255.255.255.252	ET0/0
	S0/2/0	15.0.0.1	255.255.255.252	S0/2/0
R-Outside	S0/2/0	15.0.0.2	255.255.255.252	S0/2/0
	F0/0	14.0.0.1	255.255.255.252	F0/1
C1	F0/1	10.0.0.6	255.255.255.252	F0/4
	F0/2	10.0.0.14	255.255.255.252	F0/4
	F0/3	10.0.0.57	255.255.255.252	F0/0
	F0/4	10.0.0.22	255.255.255.252	F0/5
	F0/5	10.0.0.30	255.255.255.252	F0/5
	F0/6	10.0.0.41	255.255.255.252	F0/1
	F0/7	10.0.0.37	255.255.255.252	F0/3
C2	F0/1	10.0.0.34	255.255.255.252	F0/4
	F0/2	10.0.0.26	255.255.255.252	F0/4
	F0/3	10.0.0.61	255.255.255.252	F0/1
	F0/4	10.0.0.18	255.255.255.252	F0/5
	F0/5	10.0.0.10	255.255.255.252	F0/5
	F0/6	10.0.0.45	255.255.255.252	F0/2
	F0/7	10.0.0.49	255.255.255.252	F0/2
D1	F0/4	10.0.0.5	255.255.255.252	F0/1
	F0/5	10.0.0.9	255.255.255.252	F0/5
D2	F0/4	10.0.0.13	255.255.255.252	F0/2
	F0/5	10.0.0.17	255.255.255.252	F0/4
D3	F0/4	10.0.0.21	255.255.255.252	F0/2
	F0/5	10.0.0.25	255.255.255.252	F0/4
D4	F0/4	10.0.0.33	255.255.255.252	F0/1
	F0/5	10.0.0.29	255.255.255.252	F0/5
DC1	F0/2	10.0.0.50	255.255.255.252	F0/7
	F0/3	10.0.0.38	255.255.255.252	F0/7
	F0/5	10.0.0.69	255.255.255.252	F0/5
DC2	F0/1	10.0.0.42	255.255.255.252	F0/6
	F0/2	10.0.0.46	255.255.255.252	F0/6
	F0/5	10.0.0.70	25.255.255.252	F0/5
SERVER-WEB	F0	192.168.250.103	255.255.255.0	F0/2
SERVER-TACACS+	F0	192.168.250.100	255.255.255.0	F0/1
SERVER-EMAIL	F0	192.168.250.102	255.255.255.0	F0/1

جدول 2.3 : العناوينIP المقترحة في الشبكة.

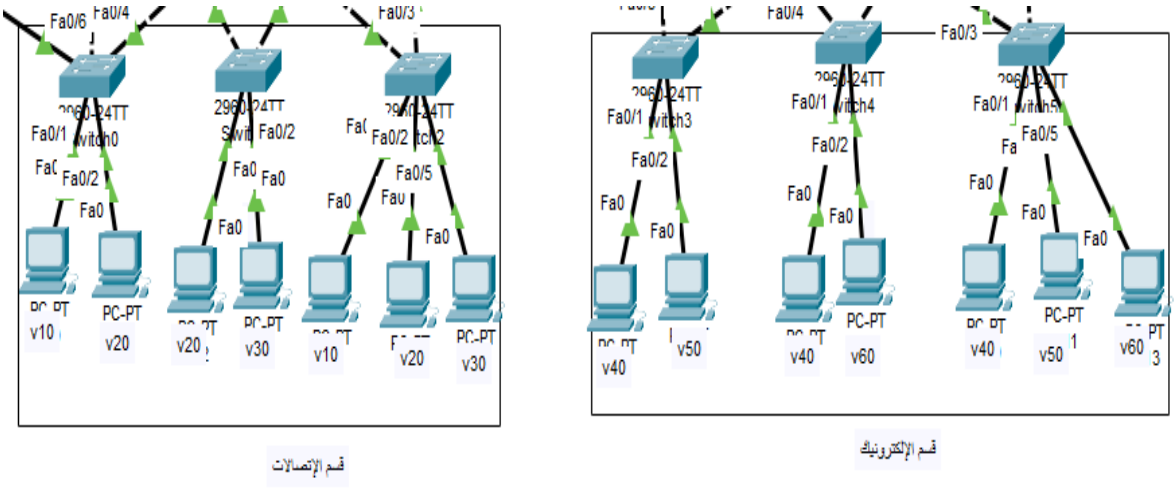
4.4.3 تكوين « configurations » :

سنقوم الآن بتكوين التصميم الخاص بنا حسب الأجزاء مع مراعاة الاعتبارات تصميم الشبكة المعياري.

❖ باستخدام الأمر Show Run في privilege mode ، نستطيع معرفة الاعدادات التي قمنا بها على كل جهاز

1.4.4.3 جزء 1: طبقة الوصول (Access layer)

توفر طبقة الوصول وصول المستخدمين النهائيين إلى الشبكة.



شكل3.3 : أجهزة الحاسوب متصلة بمبادلات الوصول.

أجهزة الحاسوب متصلة بمبادلات الوصول عبر منافذ fast Ethernet تم تكوينها على أنها منافذ نقل اتصال بين طرفين لنقل حركة مرور شبكات vlans المتعددة الموجودة في مبدلات الوصول ، كما هو موضح في قائمة الاوامر ادناه :

```
interface FastEthernet0/1
description to vlan 10 host
switchport access vlan 10
switchport mode access
switchport nonegotiate
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky
0040.0B2C.32C9
spanning-tree portfast
spanning-tree bpduguard enable
storm-control broadcast level 40
! interface FastEthernet0/2
description to vlan 20 host
switchport access vlan 20
switchport mode access
switchport nonegotiate
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky
00D0.9726.336E
spanning-tree portfast
spanning-tree bpduguard enable
storm-control broadcast level 40
!
```

```
!
interface FastEthernet0/3
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/4
ip dhcp snooping trust
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/5
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/6
switchport access vlan 10
!
```

قائمة أمر 1.3 : واجهةf0/1، f0/2، f0/3، f0/4، f0/5 ، f0/6.

- بفضل تقنية الشبكة المحلية الافتراضية VLAN تم تقسيم الشبكة إلى عدة vlans حيث تم تفعيل vlan 10 و vlan 20 في وضع الوصول(Access) في كل واجهة متصلة بجهاز حاسوب المستخدم النهائي لشبكات كما هو موضح في(قائمة أمر1.3) اسم ورقم و واجهة لكل vlan.

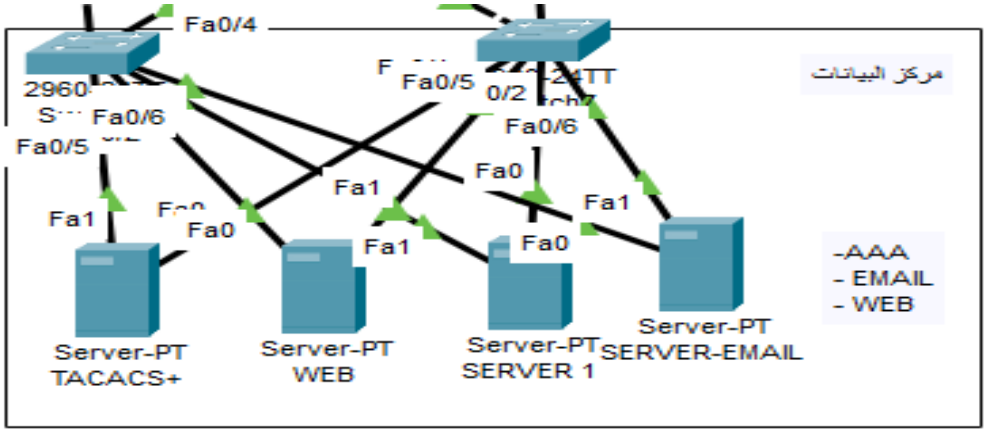
- حماية هذه المنافذ عن طريق port security عبارة عن اعدادات يتم تطبيقها على واجهة الخاصة بالمبادلات للمنع أو السماح في الدخول الى الشبكة عن طريق الـ MAC Address بحيث في حال كان هنالك أحد الأجهزة غير مصرح لها بالدخول وقام الشخص بربط جهازه عبر أحد منافذ switch port التي تم تفعيل عليها هذه التقنية فلن يتمكن من الدخول الى الشبكة ابدا بالطريق المعتاد.
- للحماية ضد هجومات STP :
  - قمنا بتفعيل Port Fast لتغير حالة المنافذ إلى حالة التمرير المباشر دون أن ينتظر فترة(Convergence Time) .
  - وتفعيل BPDU guard لحماية المنافذ و عدم استقبال رسائل الـ BPDU

- storm Controlخاصية مفيدة لحماية الشبكات من هجمات الFlood التي من الممكن أن تتعرض لها الشبكة وفكرته هي مراقبة حركة البيانات دخل كل منفذ موجود عندنا على المبدل.

- تفعيل وضع Trunk في المنافذ المتصلة بطبقة التوزيع لإستقبال وإرسال البيانات إلى جميع الشبكات الوهمية VLANs .

- switchport nonegotiate يقوم بتعطيل تفاوض DTP على واجهة الطبقة الثانية.

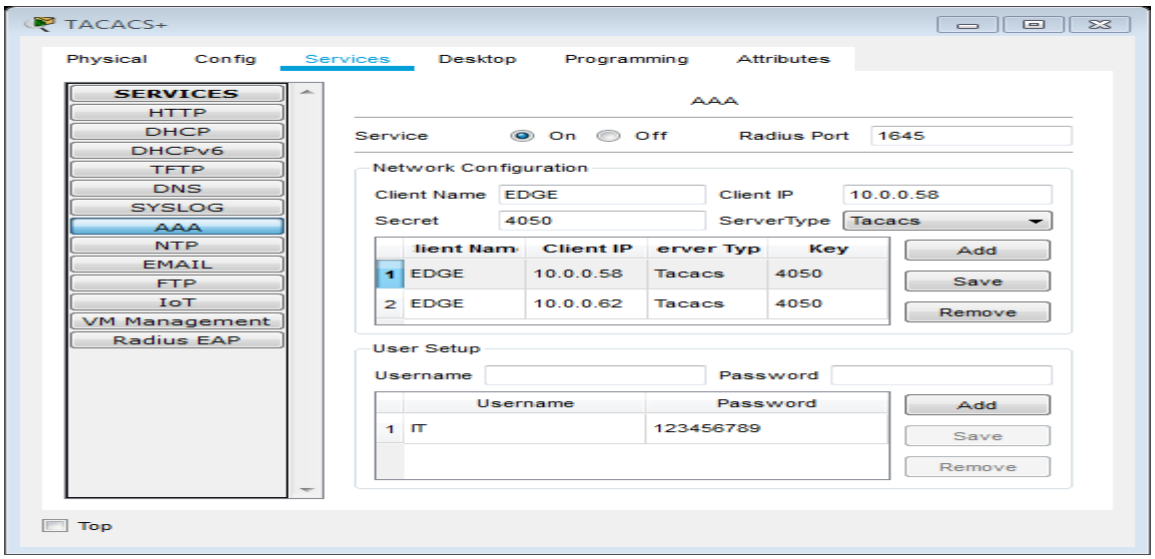
2.4.4.3 جزء 2 : مركز البيانات (Data Center)



شكل4.3 : مركز البيانات.

يوفر مركز البيانات البيئة المُلائمة لعمل الخوادم لتحفظ فيها بيانات العملاء وجميع المواقع الإلكترونية التابعة لها. في مشروعنا إستعمالنا الخوادم التالية :

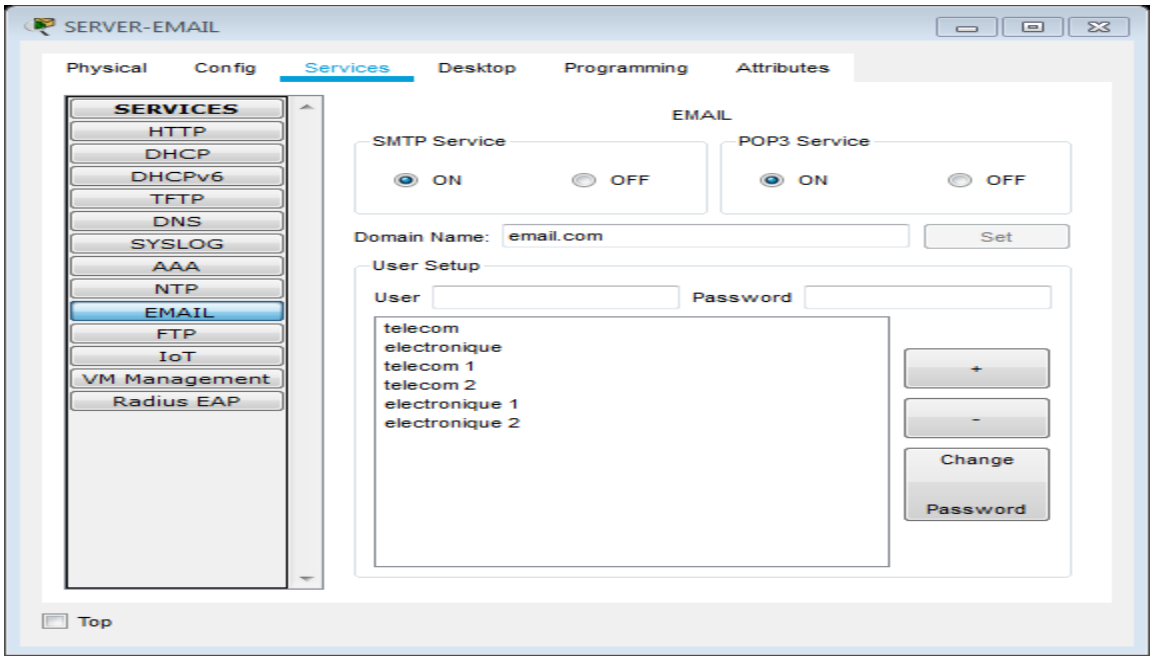
- **تكوين خادم +Tacacs:**



شكل 5.3 : خادم +Tacacs .

- يقوم بالتحقق ، وتحديد الصلاحيات للدخول إلى الشبكة.

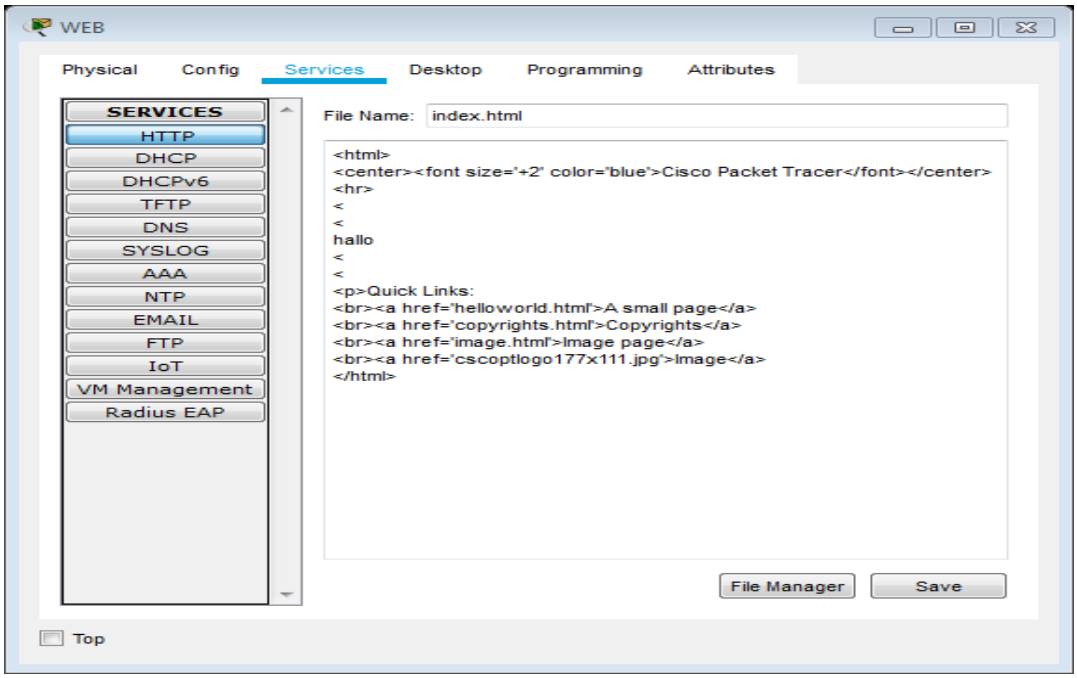
- **تكوين خادم Email :**



شكل 6.3 : خادم Email .

- يستخدم لإرسال الرسائل وتوجيهها إلى المستقبل المحدد.

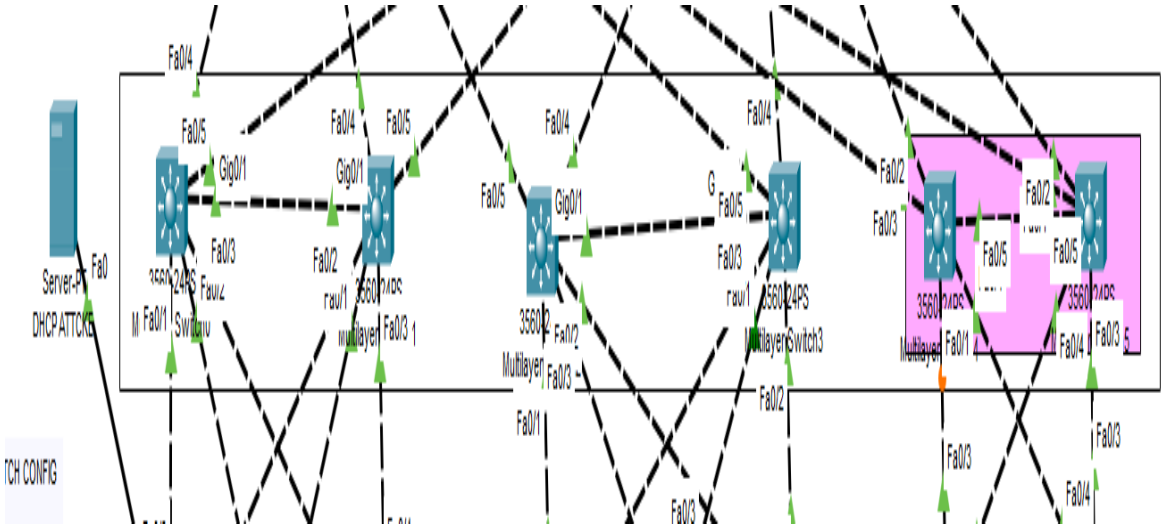
- **تكوين خادم WEB:**



شكل 7.3 : تكوين خادم WEB.

- يقدّم خدمات الإنترنت للمستخدمين.

3.4.4.3 جزء 3 : طبقة التوزيع (Distribution layer)



شكل8.3: بطبقة التوزيع .

تتكون طبقة التوزيع من مبدل متعدد الطبقات « MultiLayer Switch »حيث تقوم هاته الطبقة بتبديل حركة المرور بين شبكات VLAN الخاصة بالمستخدم النهائي وتقوم بتوصيل شبكة طبقة الوصول بطبقة الأساسية .

قمنا بتكوين طبقة التوزيع كما هو موضح في قائمة الاوامر ادناه:

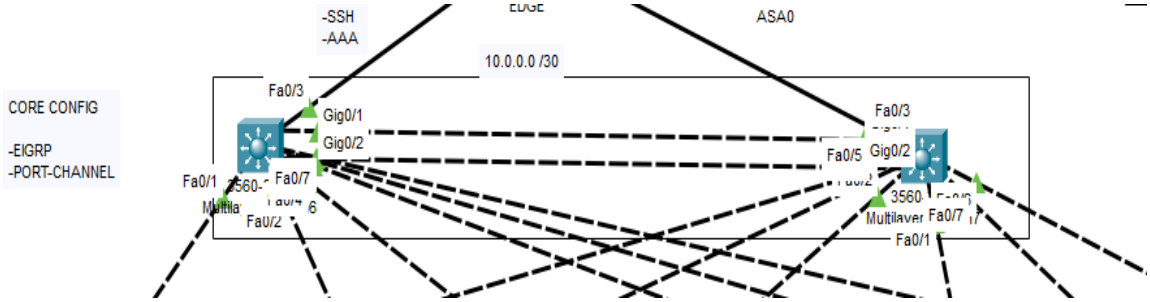
```
!
enable password cisco
!
ip dhcp excluded-address 192.168.10.1
192.168.10.3
ip dhcp excluded-address 192.168.20.1
192.168.20.3
ip dhcp excluded-address 192.168.30.1
192.168.30.3
!
ip dhcp pool vlan10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
domain-name cisco.com
ip dhcp pool vlan20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8
domain-name cisco.com
ip dhcp pool vlan30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
domain-name cisco.com
!
ip routing
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 0001.9713.1601
ip address 192.168.10.2 255.255.255.0
standby 10 ip 192.168.10.1
!
interface Vlan20
mac-address 0001.9713.1602
ip address 192.168.20.2 255.255.255.0
standby 20 ip 192.168.20.1
standby 20 priority 120
standby 20 preempt
```

```
spanning-tree vlan 10 priority 28672
!
interface FastEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/4
no switchport
ip address 10.0.0.5 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/5
no switchport
ip address 10.0.0.9 255.255.255.252
duplex auto
speed auto
!
interface Vlan30
mac-address 0001.9713.1603
ip address 192.168.30.2 255.255.255.0
standby 30 ip 192.168.30.1
standby 30 priority 120
standby 30 preempt
!
router eigrp 1
network 10.0.0.4 0.0.0.3
network 10.0.0.8 0.0.0.3
network 192.168.10.0
network 192.168.20.0
network 192.168.30.0
no auto-summary
!
```

قائمة أمر 2.3 : مبدل متعدد الطبقات الخاص بطبقة التوزيع.

- بروتوكولDHCP هو المسؤول عن تعيين عنوان (IP Address) لكل جهاز يتم توصيله على الشبكة بشكل تلقائي دون أيِّ تدخل ،حيث بتفعيل هذا بروتوكول يتم إعطاءIP Address لكل VLAN موجودة على المبدل متعدد الطبقات ومن ثم توزيعها على المستخدم النهائي.
- يقوم تكوين inter-vlan بعملية التمرير البيانات بين الشبكات الوهمية VLANs المختلفة الموجودة في الشبكة .
- بروتوكول STP عند تفعيل هذا البروتوكول سيقوم بإنشاء طوبولوجيا خالية من الحلقات عن طريق منع تشغيل واجهات معينة في جهاز المبدل ،و تقوم المبدلات بإرسال اطار لبعضها البعض يسمى BPDU يحتوي على عنوان MAC و الاولوية Priority .
- تم تفعيله وضع Trunk في المنافذ المتصلة بطبقة الوصول لإستقبال وإرسال البيانات إلى جميع الشبكات الوهمية VLANs .
- عنوانة المنافذ المتصلة بالطبقة المركزية .
- إستخدام عناوين IP لكل واجهة vlan، وتكوين بروتوكول (HSRP) الذي يستخدم بشكل أساسي لضمان توفر البوابة الافتراضية في شبكة فرعية على الرغم من فشل جهاز مبدل متعدد الطبقات أو التوجيه.
- تم إستخدام بروتوكول توجيه ديناميكي (EIGRP) للعثور على أفضل مسار بين الأجهزة لتسليم الحزمة.

4.4.4.3 جزء4: الطبقة الأساسية (Core Layer)



شكل13.3: الطبقة الأساسية.

تقوم الطبقة المركزية بتبادل الحركة بين جميع الطبقات الأخر وبربط كل الفروع الموجودة على شبكة ومشاركة المعلومات تلك الفروع . مثال من تشغيل ملف التكوين تظهر قائمة الأوامر التالية:

```
!
ip routing
!
port-channel load-balance src-dst-ip
spanning-tree mode pvst
!
interface Port-channel1
no switchport
ip address 10.0.0.1 255.255.255.252
!
interface FastEthernet0/1
no switchport
ip address 10.0.0.6 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/2
no switchport
ip address 10.0.0.14 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/3
no switchport
ip address 10.0.0.57 255.255.255.252
duplex auto
speed auto
```

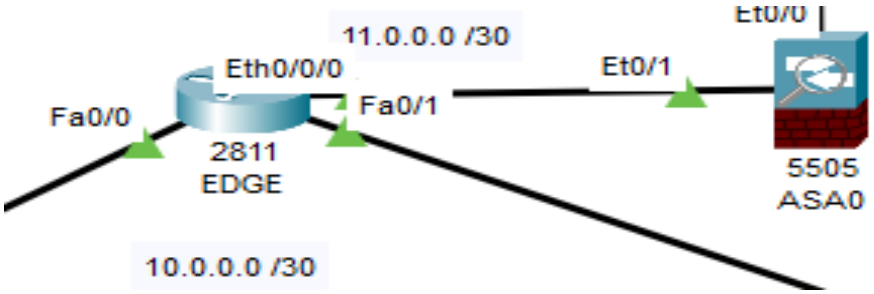
```
interface FastEthernet0/4
no switchport
ip address 10.0.0.22 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/5
no switchport
ip address 10.0.0.30 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/6
no switchport
ip address 10.0.0.41 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/7
no switchport
ip address 10.0.0.37 255.255.255.252
duplex auto
speed auto
!
```

```
router eigrp 1
network 10.0.0.0 0.0.0.3
network 10.0.0.4 0.0.0.3
network 10.0.0.12 0.0.0.3
network 10.0.0.20 0.0.0.3
network 10.0.0.28 0.0.0.3
network 10.0.0.36 0.0.0.3
network 10.0.0.40 0.0.0.3
network 10.0.0.56 0.0.0.3
no auto-summary
```

قائمة أمر 4.3 : مبدل متعدد الطبقات الخاص بطبقة الأساسية .

- Inter-vlan لتمرير البيانات في الشبكة.
- إستخدام port–channel في منفذين المربوطين بين جهازين مبدل متعدد الطبقات للقيام بعملية تسمى بـ Load balancingحيث تجمع الروابط و جعلها كرابط واحد فقط يسمى بالمجموعةEtherchannel Group .
- عنوانة المنافذ المتصلة بالطبقة التوزيع و EDGE.
- إستخدام (EIGRP) للعثور على أفضل مسار بين جهازين لتسليم الحزمة.

5.4.4.3 جزء5 : موجه EDGE و firewall



شكل 14.3: موجه EDGE و firewall.

- **تكوين موجه EDGE:**

جهاز توجيه موجود على حافة الشبكة. يضمن الإتصال شبكته بشبكات خارجية أو شبكة واسعة النطاق أو الإنترنت. البروتوكولات المفعلة عليه في مشروعنا كالتالي:

```
enable secret 5
$1$mERr$sLrKBRiLmgCUQXa52UQTg/
!
!
aaa new-model
!
aaa authentication login default group
tacacs+ local
!
ip domain-name ccna.com
!
!
interface FastEthernet0/0
ip address 10.0.0.58 255.255.255.252
ip nat inside
duplex auto
speed auto
!
```

```
interface FastEthernet0/1
ip address 10.0.0.62 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface Ethernet0/0/0
ip address 11.0.0.1 255.255.255.252
ip nat outside
duplex auto
speed auto
```

```
router eigrp 1
redistribute static
network 10.0.0.56 0.0.0.3
network 10.0.0.60 0.0.0.3
no auto-summary
!
ip nat inside source list nat interface
Ethernet0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0/0
!
ip flow-export version 9
```

```
ip access-list standard nat
permit any
!
tacacs-server host 192.168.250.100
key 4050
!
line con 0
!
line aux 0
!
line vty 0 4
login authentication default
transport input ssh
```

قائمة أمر5.3: موجه EDGE.

- إستخدام SSH حيث انه يهتم بإدارة الحماية للمرسلات عبر الشبكة و يشمل التشفير و التوثيق وسلامة البيانات عند تبادلها و إصدار الاوامر عن بعد .
- تفعيل AAA بإستخدام خادم +TACACS لإعطاء التصاريح للدخول إلى الشبكة بالإضافة إلى تحديد الصلاحيات لكل شخص يدخل الى الراوتر.
- NATهي تقنية تستخدم لاستخدام العناوين الخاصة في الشبكات المحلية والتبديل إلى عناوين IP العالمية عند الاتصال بالإنترنت.

o تكوين جهاز ASA 5505 (Firewall)

يقوم بالفصل بين المناطق الموثوق بها في شبكات الحاسوب و مراقبة المعلومات التي تمر عبر الشبكة و منع اي شيء يضر بجهازك خارج الشبكة . من تشغيل ملف التكوين تظهر قائمة الأوامر التالية:

```
!
hostname FIREWALL
domain-name cisco.com
enable password 4IncP7vTjpaba2aF
encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Vlan1
nameif inside
security-level 100
ip address 11.0.0.2 255.255.255.252
!
interface Vlan2
nameif outside
security-level 0
ip address 13.0.0.1 255.255.255.252
!
object network inside-nat
subnet 192.168.0.0 255.255.0.0
nat (inside,outside) dynamic interface
object network outside-nat
subnet 14.0.0.0 255.0.0.0
!
route outside 0.0.0.0 0.0.0.0 13.0.0.2 1
route inside 192.168.0.0 255.255.0.0 11.0.0.1
1
!
access-list vpn_acl extended permit ip object
inside-nat object outside-nat
```

```
!
class-map inspection_default
match default-inspection-traffic
!
policy-map global-policy
class inspection_default
inspect icmp
!
service-policy global-policy global
!
crypto ipsec ikev1 transform-set vpn_set
esp-aes esp-sha-hmac
!
crypto map vpn_map 10 match address
vpn_acl
crypto map vpn_map 10 set peer 15.0.0.2
crypto map vpn_map 10 set ikev1
transform-set vpn_set
crypto map vpn_map interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
encr aes
authentication pre-share
group 2
!
tunnel-group 15.0.0.2 type ipsec-l2l
tunnel-group 15.0.0.2 ipsec-attributes
ikev1 pre-shared-key ciscocisco
!
```

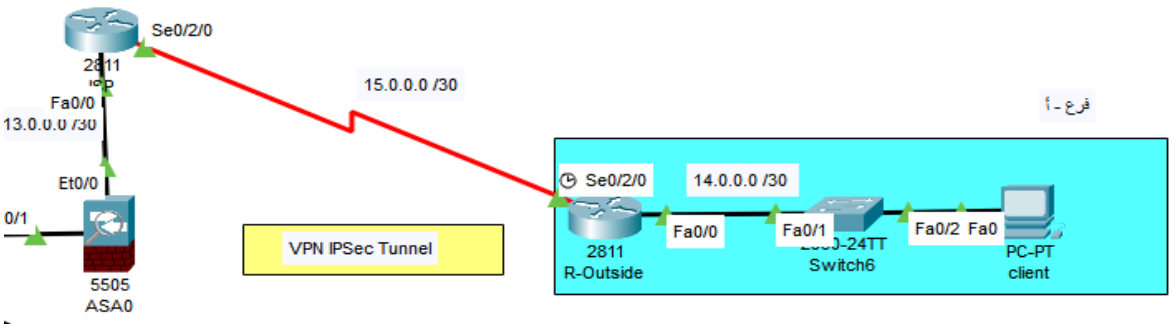
قائمة أمر6.3 : جهاز ASA 5505 (Firewall) .

- تكوين اسم المضيف واسم المجال لجدار الحماية وتمكين كلمة المرور.
- تكوين Vlan 2 على واجهة E0/0 وضع Access .
- تفعيل واجهات vlan 1 ، vlan 2 بإعطاء عنوان IP وتحديد إسم واجهات بإستخدام nameif حيث vlan 1 تأخذ إسم inside و vlan 2 تأخذ إسم outside من أهم الاوامر التي يجب القيام بها من أجل تحديد security-level حيث outside يحصل على leve-0 أي لا يوجد أمان ،بينما inside يحصل leve-100 أي يوجد أمان.
- تفعيل object network NATعندما تدخل الحزمة ASA ، يتم التحقق من عناوين IP للمصدر والوجهة مقابل قواعد Object network NAT.
- تكوين مسار افتراضي ثابت يشير إلى جهاز التوجيه ISP (13.0.0.2)، وقيام بتكوين مسار ثابت يشير إلى الأجهزة داخل الشبكة بإتجاه حافة جهاز التوجيه (EDGE).
- تفعيل calss-map لإنشاء تصنيف حركة مرور و policy-map لإجراءات المعينة على حركة المرور .
- تكوين VPN IP Sec لتشفير جميع حركة المرور والمصادقة عليها وستكون سلامة البيانات.

6.4.4.3 جزء 6 : VPN IP Sec

هي مجموعة من البروتوكولات التي توفر إتصالات أمنة عبر مسارات غير آمنة ،هو مثالي لربط موقعين بعيدين مع بعض. هناك مرحلتان لتكوين VPN IP Sec:

1. نقوم بتكوين ISAKMP Policy في R-Outside و IKEVL Policy فيFIREWALL حيث يحدد الـ Policy قناة أمنة و كيفية المصادقة أقرانIP Sec لبعضهم البعض وبروتوكولات أمان التي سيتم إستخدامها.
2. نقوم بتكوين خريطة التشفير وتتعامل مع إدارة حركة المرور لإتصال البيانات الفعلي بين المواقع وتحدد بروتوكولات المصادقة والتشفير التي سيتم إستخدامها في حركة مرور البيانات .[35]



شكل 15.3: VPN IPSEC لربط موقعين بعيدين مع بعض.

o تكوين موجه ISP

يوفر مزود خدمة الإنترنت الوصول إلى الشبكة الإنترنت حيث في كل مرة تتصل بالأنترنت يتم توجيه الإتصال عبر ISP .

```
interface FastEthernet0/0
ip address 13.0.0.2 255.255.255.252
duplex auto
speed auto
!
interface Serial0/2/0
ip address 15.0.0.1 255.255.255.252
                                    !
ip route 14.0.0.0 255.255.255.0 15.0.0.2
ip route 192.168.0.0 255.255.0.0 13.0.0.1
!
```

قائمة أمر 7.3 : موجه ISP.

- تعين عنوان IP للمنافذ ب f0/0، s0/2/0.
- تكوين مسارين ثابتين الأول يشير إلى الأجهزة داخل الشبكة بإتجاه Firewall ، والثاني يشير إلى أجهزة فرع–أ بإتجاه R-Outside.

o تكوين موجه R-Outside

جهاز توجيه موجود على حافة شبكة الفرع–أ ، يضمن الإتصال شبكة الفرع–أ بشبكات واسعة النطاق أو الإنترنت. تم تكوين فيه VPN IP Sec من ملف التكوين تظهر قائمة الأمر التالية:

```
interface FastEthernet0/0
ip address 14.0.0.1 255.255.255.252
duplex auto
speed auto
!
interface Serial0/2/0
ip address 15.0.0.2 255.255.255.252
clock rate 2000000
crypto map vpn_map
!
ip route 0.0.0.0 0.0.0.0 15.0.0.1
!
ip access-list extended vpn_acl
permit ip 14.0.0.0 0.0.0.255 192.168.0.0
0.0.255.255
!
```

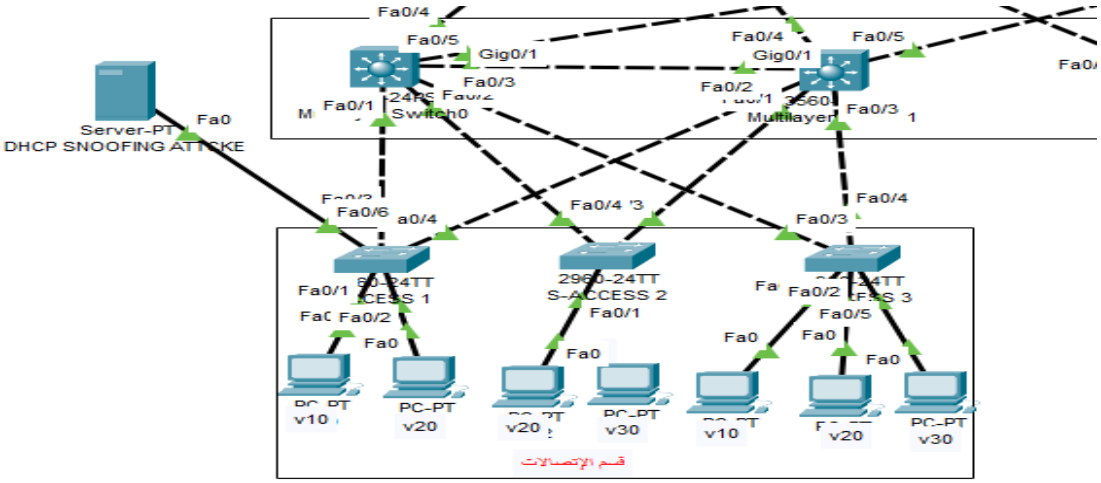
```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
crypto isakmp key ciscocisco address 13.0.0.1
!
crypto ipsec transform-set vpn_set esp-aes
esp-sha-hmac
!
crypto map vpn_map 10 ipsec-isakmp
set peer 13.0.0.1
set transform-set vpn_set
match address vpn_acl
!
```

قائمة أمر8.3 : تكوين موجه R-Outside.

- تعين عنوان IP للمنافذ f0/0،s0/2/0 .

- تكوين مسار افتراضي ثابت يشير إلى جهاز التوجيه ISP (15.0.0.1).
- قيام بتكوين VPN IP Sec لتشفير جميع حركة المرور والمصادقة عليها وتكوين سلامة البيانات.

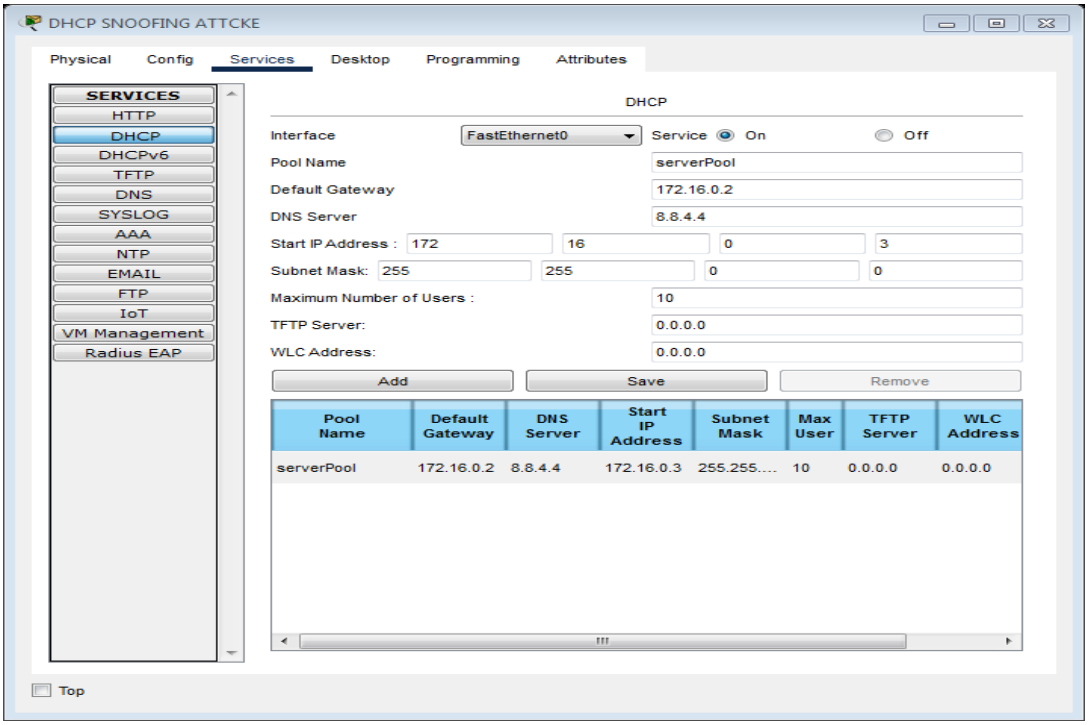
7.4.4.3 جزء 7 : هجمات DHCP Spoofing



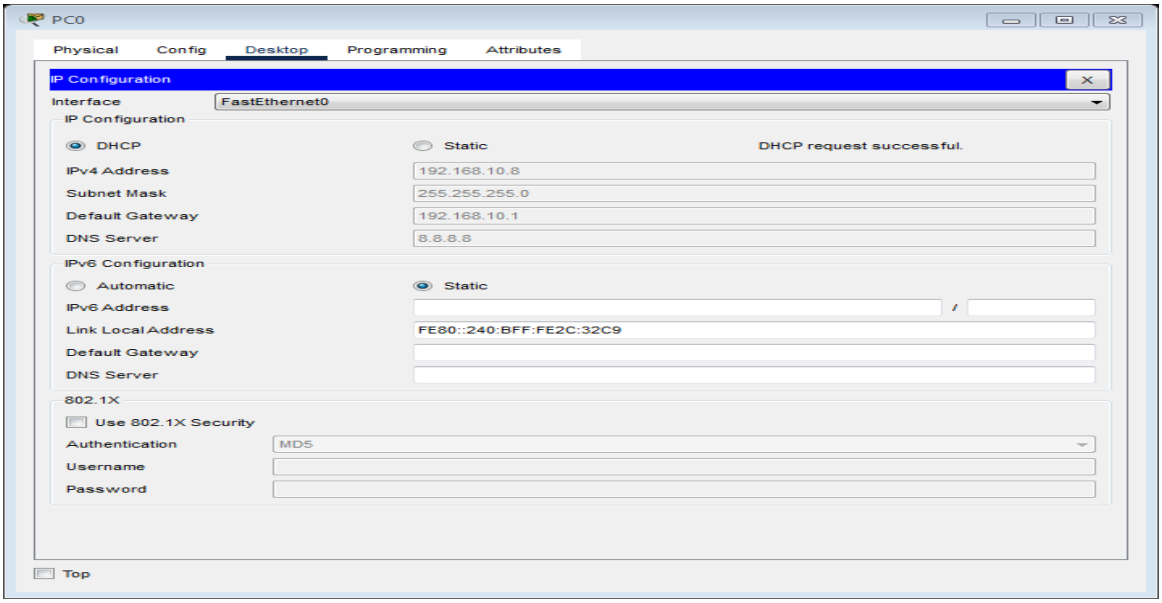
شكل9.3 : هجوم DHCP Spoofing على طبقة الوصول .

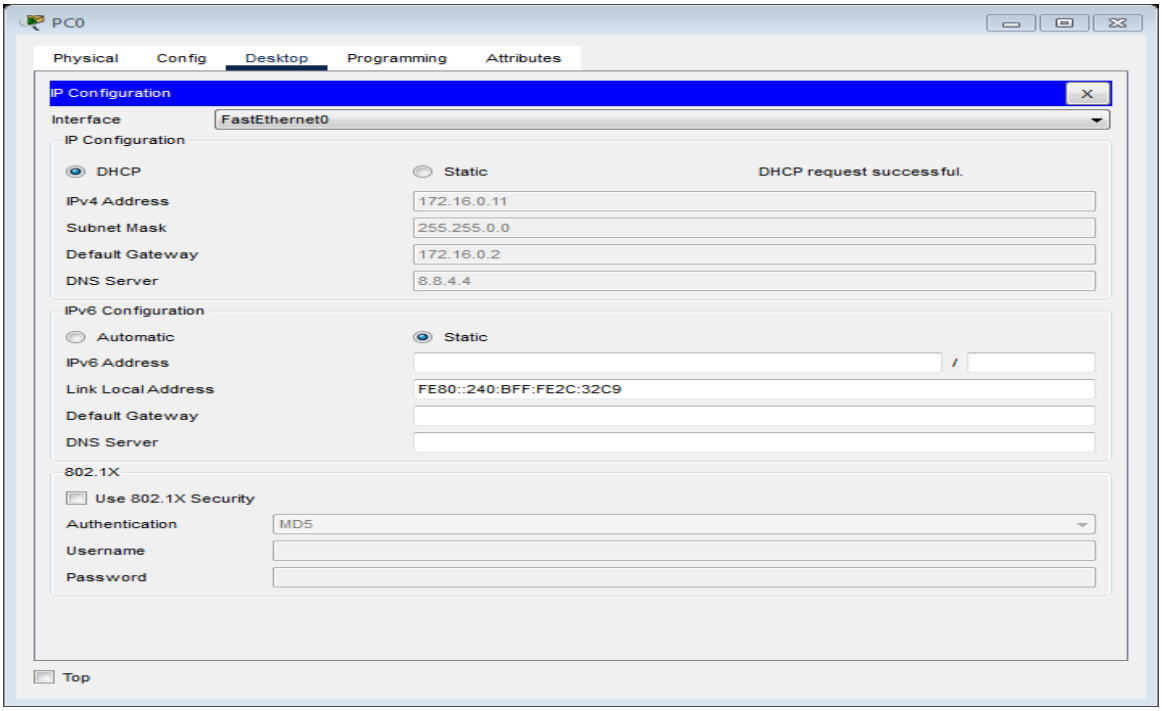
- هجوم DHCP هو هجوم رقمي خبيث يستهدف خوادم DHCP ،أثناء هجوم DHCP يقوم ممثل بإغراق خادم DHCP بحزم DISCOVER الزائفة حتى يستنفد خادم DHCP إمداداته من عناوين IP.

مثال: إستخدام عنوان IP لـvlan10 عن طريق خادم DHCP مزيف كما هو موضح في **شكل9.3** :



شكل 10.3 : خادمDHCP مزيف.



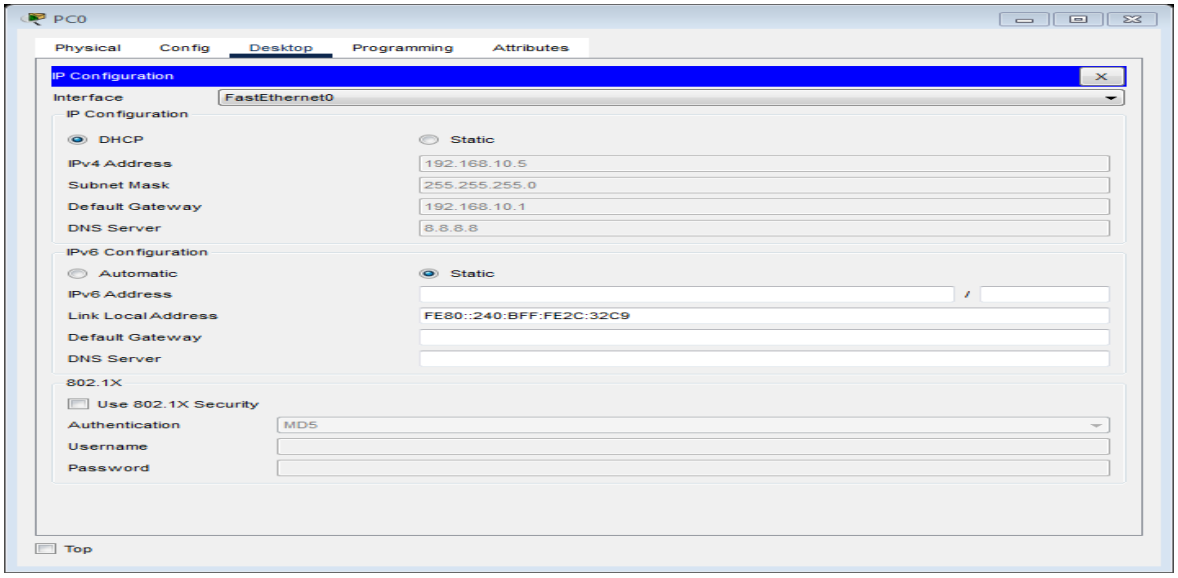


شكل11.3 : عنوان IP من خادم DHCP الحقيقي والخادم DHCP المزيف.

لحماية من هذا الهجوم إستخدامنا خاصية DHCP Snooping تقوم بجعل منفذ السويتش الموصل الـ DHCP الرئيسي هو المنفذ الموثوق trusted ports .كما هو موضح في قائمة أمر :

```
ip dhcp snooping vlan 10,20
no ip dhcp snooping information option
ip dhcp snooping
!
interface FastEthernet0/3
ip dhcp snooping trust
interface FastEthernet0/4
ip dhcp snooping trust
```

قائمة أمر 3.3: تكوين DHCP Snooping.

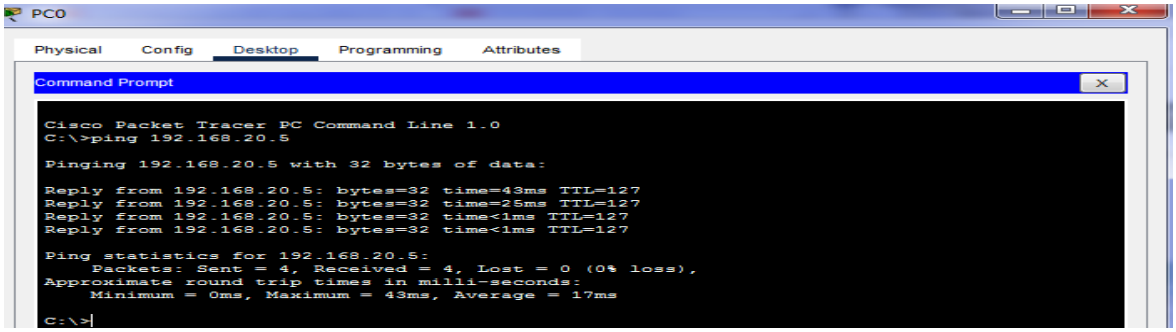


شكل12.3 : عنوان IP من خادم DHCP الحقيقي .

5.4.3 النتائج:

سوف نقوم بالتأكد من صحة التكوين مشروعنا عن طريق الـ Ping بين الأجهزة .

1) قيام بـ Ping بينVlan10 وVlan20 في نفس القسم.



شكل 16.3 : Ping بينVlan10 و Vlan20.

2) قيام بـ Ping بين Vlans مختلفان في قسمين مختلفين Vlan10وVlan40 .

```
C:\>ping 192.168.40.6

Pinging 192.168.40.6 with 32 bytes of data:

Reply from 192.168.40.6: bytes=32 time=22ms TTL=124
Reply from 192.168.40.6: bytes=32 time=12ms TTL=124
Reply from 192.168.40.6: bytes=32 time=11ms TTL=124
Reply from 192.168.40.6: bytes=32 time=1ms TTL=124

Ping statistics for 192.168.40.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 22ms, Average = 11ms

C:\>
```

شكل 17.3 : Ping بينVlan10 و Vlan40.

3) قيام بـ Ping بين Vlan10 وEDGE.

```
C:\>ping 10.0.0.58

Pinging 10.0.0.58 with 32 bytes of data:

Reply from 10.0.0.58: bytes=32 time=11ms TTL=253
Reply from 10.0.0.58: bytes=32 time<1ms TTL=253
Reply from 10.0.0.58: bytes=32 time<1ms TTL=253
Reply from 10.0.0.58: bytes=32 time<1ms TTL=253

Ping statistics for 10.0.0.58:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>
```

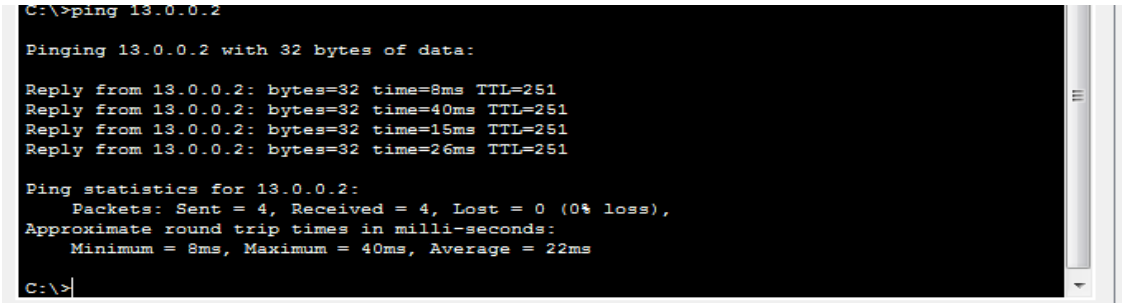
شكل 18.3 : Ping بينVlan10 وEDGE.

4) قيام بـ Ping بين Vlan10 و Firewall.

```
C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Reply from 11.0.0.2: bytes=32 time=24ms TTL=252
Reply from 11.0.0.2: bytes=32 time=22ms TTL=252
Reply from 11.0.0.2: bytes=32 time=13ms TTL=252
Reply from 11.0.0.2: bytes=32 time=21ms TTL=252

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 24ms, Average = 20ms

C:\>
```

شكل 19.3 : Ping بين Vlan10 وFirewall .

5) قيام بـ Ping بين Vlan10 وISP.



شكل20.3 : Ping بين Vlan10 وISP.

6) قيام بـ Ping بين Firewall و R-Outside.

```
FIREWALL#ping 15.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 15.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/14 ms

FIREWALL#
```

شكل21.3: Ping بين Firewall و R-Outside.

7) قيام بـ Ping بين Firewall وISP .

```
FIREWALL#ping 13.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

FIREWALL#
```

شكل22.3: Ping بين Firewall وISP .

8) قيام بـ Ping بين R-Outside وISP .

```
R-Outside#ping 15.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 15.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/23 ms
```

شكل23.3: Ping بينR-Outside وISP .

9) قيام بـ Ping بين R-Outside و Firewall .

```
R-Outside#ping 11.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

شكل24.3: Ping بين R-Outside و Firewall .

6.4.3 الخلاصة :

يعمل الـ Ping بنجاح بين الأجهزة الداخلية لشبكة وحتى الأجهزة الخارجية هذا ما يعني أن الإتصال موجود حيث أن نفق VPN IP Sec بين firewall و R-Outside يعمل بشكل صحيح ومحمي بشكل جيد ، في حين أن الـ Ping بين الأجهزة الخارجية لشبكة لا يمكنها الإتصال بالأجهزة الداخلية لأن جهاز الـ firewall يعمل لحماية الشبكة من الأخطار الخارجية وأيضاً لتصفية التبادلات بين الشبكة المحلية أو الخاصة .

5.3 الخاتمة :

قدم لنا هذا الفصل فكرة عن كيفية الممارسة في العمل الحقيقي، و من بين صعوبات التي يمكن أن نواجهها في هذا العمل هي تكوين وتكيف بين الأجهزة المختلفة أي أنه عمل شاق .ولكن مع المعرفة الأساسية للشبكات وتوظيف مهاراتنا العملية السابقة تمكنا من التعامل مع المشكلات التي قد تحدث .أخيرا تمكنا من تصميم شبكة قرية جامعية التي كانت صعبة في طريقة تكوينها مع توفير أمن و السرية اللازمة لها.

الخاتمة العامة

الخاتمة العامة :

تتطور تكنولوجيا الشبكات يوما بعد يوم ، حيث ان شهرا من التطوير يجعل التكنولوجيا السابقة قديمة . المنظمات الكبيرة المسؤولة عن اختراع أو إطلاق أجهزة جديدة لتقنيات جديدة لها تأثير مباشر على التصميم المستقبلي لشبكات المؤسسات أو الشركات ، مما يعني أننا كطلاب يجب أن نتبع هذا النمو و التطور المذهل على أمل إنشاء تقنيات جديدة.

كنا حريصين على منهجية أطروحتنا ومحتواها ، حيث أولينا أهمية كبيرة لمجال الشبكات، لأنه لا توجد شركة أو أي مؤسسة ليس لديها شبكة، في حين لا تخلو أي مؤسسة أو شركة من التهديدات و الهجمات لغرض الإستلاء على المعلومات والبيانات تلك المؤسسة أو الشركة حيث قدمنا بعض الحلول لتلك التهديدات والهجمات في أطروحتنا .

وأخيرا ، هذي هي الحلول التي قمنا بدراستها و التي من الضروري ان يتم تطبيقها في اي شبكة لحماية معلومات الخاصة بالمؤسسة و موظفيها . فلكل طالب علم لديه شغف للاستعداد لمجال الأعمال أو حتى لتوسيع معلوماته للإعداد الأكاديمي ، فإن هذه الرسالة تعد فرصة لتطوير الطلاب أو أي مرشح للتخرج لتحسين مهاراته في مجال الشبكات .

المراجع :

[1]January2011, Security Problems in Campus Network and Its Solutions Available="https://www.researchgate.net/publication/224771078."

[2] 06.09.19,"Un aperçu des différents réseaux informatiques " Available : "https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/".

[3] LEMAINQUE Fabrice PILLOU Jean-François. Tout sur les Réseaux et Internet, 3e édition. Dunod, 2012 .

[4] https://mtyas.com/2009/05/11/pourquoi-le-web-30-sera-p2p-ou-ne-sera-pas%E2%80%A6
Mtyas.com, Pourquoi le web 3.0 sera P2P ou ne sera pas, May 11, 2009,

[5] M. LIHAN LI NDJOM Hans. Cours sur Les Topologies Physiques des réseaux informatiques, école normale supérieur du Cameroun.

[6] CCNA R&S / Arabic by .Eng. Ahmed H Mashaikh.

[7] Wayne Lewis, 'LAN switching and wireless: CCNA exploration companion guide'Cisco Press, April 2008.

[8] Https/ :/e3arabi.com/تقنية، اساسيات شبكة الحاسوب

[9]Noor-Book.com CCNA R S Arabic.

[10] https://bplpadrar.dz/frm/threads/63/.

[11] https://www.dlylok.com/2021/05/network-cables-types.html.

[12] https://www.telenco-distribution.com/pa10757/les-connecteurs-fibre-optique.

[13] Philippe Adelina. Réseaux informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi...). Editions ENI, 2009.

[14] academy.hsoub.com/certificates/comptia/-مدخل-إلى-شبكات-الحواسيب-مصطلحات-وفهم-طبقات-الشبكة-r65/، 31اغسطس2017.

[15]09/05/2014 ,http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4.

[16] Wayne Lewis, 'LAN switching and wireless:CCNA exploration companion guide'Cisco Press, April 2008.

[17] https://www.ehabbooks.com/?p=5800
الدرس85: تصميم الشبكة

[18] 2018/06/17 http://slideplayer.com/slide/10957395/

[19] https://www.noor-book.com/كتاب الشبكات (م.ياسر ثلجي) امن

[20] https://www.zaadbooks.com/كتاب (سامي شريف) أمن الشبكات

[21] Jöelle MUSSET. Sécurité informatique : Ethical hacking : Apprendre l'attaque pour mieux se défendre, 2009.

[22] https://www.securiteinfo.com/attaques/hacking/typesattaques.shtml

[23]stéphanegill2003,typed'attaques,https://www.academia.edu/15633432/Type_dattaques.

[24] https://ar.wikipedia.org/wiki/وكيل (حوسبة) .

[25] Steven Andrés, Brian Kenyon, and Erik Pack Birkholz. Security Sage's guide to hardening the network infrastructure. Syngress, 2004.

[26] https://www.technawi.net
مدخل إلى علم التشفير التشفير وأمن المعلومات

[27] François Santy. La virtualisation, 2013.

[28] Ron Gilster, 'CCNA for Dummies', IDG Books Worldwide-Inc , June 2009.

[29] 2018/03/11 https://networklessons.com/spanning-tree/introduction-to-spanning-tree/.
[30] 21 April 2022, https://www.alrab7on.com/
ما هي الشبكة الافتراضية الخاصة وما فوائدها.
[31] August 15, 2019, Ahmed Radwan , https://www.linkedin.com/ | أساسيات هندسة الشبكات
VLAN (2 جزء) .
[32] https://fr.isecosmetic.com/wiki/IPsec.
[33]28 أكتوبر 2019,حنان مشقوق , https://www.arageek.com/l/-ssh.
[34].https://arabicprogrammer.com/article/4360877533/
[35]2022 ابريل 25,أحمد حسين, https://www.connect4techs.com/ .