2022-2023العام الدراسي :

مشروع أُعدّ لنيل إجازة في هندسة الاتصالات

اكتشاف و استغلال الثغرات الأمنية في نظام التشغيل ويندوز

إعداد الطالبة : سهى الطحان

بإشراف الدكتور : صبحي شيخة

جامعة الاتحاد الخاصة

كلية الهندسة المعلوماتية

قسم هندسة الاتصالات

إهداء

الى رمز الحكمة والإلهام، للنجم الذي ينير طريقي، أعلم أن كلمات الشكر والامتنان لن تكون كافيةgللتعبير عن مدى امتناني واعترافي بالدعم المستمر الذي قدمته في حياتي. لقد كنت السند الذي لا يضاهى، والمصدر الملهم الذي يشع النور في كل مرحلة من مراحل رحلتي

أبي العزيز

الى من سارت بجانبي طريق النجاح في كل خطوة... الى الروحٌ التي تنبض بالعطاء والدعم اللامحدود. أنتِ الشمعة التي تنير دربي والحنان الذي يشدني ويحملني في أيام الشدة.

أمي الغالية

الى الذين شاركوني خطوات حياتي ...الى الذين يملكون مكانة خاصة في قلبي ... أنتم الروح التي تنير دربي والقوة التي تدفعني للأمام ...

إخوتي

إلى شركاء المغامرات والضحكات، الذين يجعلون كل لحظة معهم ذكرى لا تُنسى ...

إلى رفقاء الطريق ، الذين أرافقهم في رحلة الحياة بكل ما تحمله من تحديات وصعاب ...

أصدقائي

إلى من هم سبب سعادتي الدائمة ومصدر قوتي.... إلى الذين منحوني الحب ودعموني بجميع اللحظات.

عائلتي الكريمة

الى من ساندونا وكان لنا عونا وسندا ... الى من زرعوا في نفوسنا الثقة بالنفس ... الى من بوجودهم يكتمل النجاح وبسواعدهم تنتهض الأمم

إلى الدكاترة الأفاضل

أود أن أهدي هذه الأطروحة إليك تعبيرًا عن امتناني العميق وتقديري الكبير لك. لا يمكنني وصف كم الإلهام والإرشاد القيمين الذين كنت عليهما طوال هذه الرحلة البحثية. بفضلك، استطعت تطوير رؤية عميقة ومفهوم شامل في مجال دراستي.

الدكتور ياسر فواز

الى مدينة الزيتون والسلام ..... الى ارض الحب والعطاء

عفرين

الفهرس

* الاختصارات المستخدمة 10
* الفصل الأول – منهجية المشروع 12
  + :1-1 أهمية المشروع 12
  + 1-2: أهداف المشروع 12
* الفصل الثاني – الدراسة النظرية 31
  + :1-2 تعريف الشبكات 31
  + 2-2: أنواع الشبكات (Type of Networks) 41
    - : 1-2-2الشبكات المحليةLAN 41
    - :2-2-2الشبكات الإقليمية MAN 16
    - :3-2-2الشبكات بعيدة أو طويلة المدى WAN 17
    - :4-2-2الشبكات الشخصية 18
  + :3-2طوبولوجيا الشبكات 19
    - :1-3-2الحلقي (Ring) 19
    - :2-3-2الخطي (Bus) 19
    - :3-3-2نجمية (Star)‏ 20
    - :4-3-2مختلطة Mix)‏( 20
  + : 4-2أصناف عناوين IP 21
    - :1-4-2تعريف الIPv4 21
      * 1-4-2-:1 أنواع ارسال البيانات فيIPv4 23
    - 2-4-2: تعريف الIPv6 26
      * 2-4-2-:1 أنواع ارسال البيانات فيIPv6 26
  + :5-2البروتوكولات المستخدمة في ال Application Layer 27
    - **:**1-5-2بروتوكول (DHCP) 28
    - :2-5-2بروتوكول (DNS) 28
    - :3-5-2بروتوكول (FTP) 28
    - :4-5-2بروتوكول (HTTPS) 30
    - 2-5-:5 بروتوكول(SMTP) 30
    - 2-5-:6 بروتوكول (Telnet) 31
  + :6-2البروتوكولات المستخدمة في ال Transport Layer 32
    - :1-6-2 بروتوكول (TCP) 32
    - :2-6-2 بروتوكول (UDP) 33
  + :7-2البروتوكولات المستخدمة في ال Network Layer 33
    - :1-7-2بروتوكول (OSPF) 33
* الفصل الثالث - الأجهزة المستخدمة 31
  + 3-1: الموجه (Router) 31
  + 3-2: المبدل (Switch) 32
  + 3-3: المبدل متعدد الطبقات ((Multi LayerSwitch 32
  + 3-4: الخادم (Server) 34
  + 3-5: هاتف (Voice over IP) 35
  + 6-3: الجدار الناري(Firewall) 36
  + 3-7: وحدة (WLC) 37
  + 3-8: نقطة الوصول (Access Point) 38
* الفصل الرابع - التقنيات المستخدمة و التصميم العملي 40
  + 1-4: المخطط العملي للمشروع 40
* الفصل الخامس - الاستنتاجات والعمل المستقبلي 41
  + 5-1 النتائج العملية 43
  + 5-2 العمل المستقبلي 43
* المراجع References 44

مقدمة

انتشرت الشبكات في كافة مناحي الحياة فسيطرت على المجالات الاقتصادية والفنية والتعليمية والعسكرية وغيرها؛ هذه السيطرة والأهمية تعود لربطها العالم ببعضه البعض . مما أتاح سرعة وصول المعلومات عبر القارات والبلدان وبالتالي زيادة النشاط الحيوي والفكري وتنشيط الأرباح المادية ولقد تزامن التطور الكبير في أجهزة الحاسب وأنظمة المعلومات مع التطور في شبكات المعلومات والسرعة الكبيرة التي يمكن أن تنتشر بها المعلومات وصاحب التطور في استخدام المعلومات الإلكترونية ازدياد مشاكل أمن الشبكات و المعلومات كالاختراقات بكافة أنواعها. مما شكل خطرا كبيرا على البنيات الأساسية للمنشآت الحكومية والخاصة. وتكمن خطورة مشاكل أمن الشبكات و المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية. أو تخريبها بالكامل مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة . أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع والتنصت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة.

يهدف المشروع إلى رفع المستوى الأمني و زيادة سرعة نقل البيانات بين الفروع عن طريق تطبيق مجموعة من البروتوكولات والتقنيات وإن رفع نسبة الحماية تحمينا بشكل كبير من الاختراقات التي تعطل الشركة و الموظفين عن أداء مهامهم و أداء عملهم. و من هذه التقنيات هي عدم السماح لكافة المستخدمين داخل هذه الشركة بالحصول على الأذونات في التحكم أو تغيير الإعدادات أو الضبط وبالتالي تكون صلاحياتهم محصورة.

الخلاصة:

تهدف هذه الدراسة إلى تصميم شبكة باستخدام المحاكي GNS3 ، تهدف الى تنظيم عملية مشاركة البيانات بين المستخدمين وتحقيق سرعة نقل ممتازة بين الفروع, حيث تم استخدام تقنية MPLS لتحسين سرعة نقل البيانات بين الفروع، و استخدام أجهزة Multilayer Switch لتنفيذ عملية تحويل حزم البيانات. واستخدام بروتوكول OSPF للتوجيه و يمكننا التحكم في جميع نقاط الوصول من خلال مركز تحكم الشبكة اللاسلكي (WLC).

Abstract:

This study aims to design a network using the GNS3 emulator, aiming to organize the process of data sharing between users and to achieve excellent transfer speed between branches, where MPLS technology was used to improve the speed of data transfer between branches, and the use of Multilayer Switch devices to implement the process of switching data packets. And using the OSPF protocol for routing, we can control all access points through a Wireless Network Control Center (WLC).

الكلمات المفتاحية (key words)

|  |
| --- |
| * Routers |
| * Switches |
| * Servers |
| * Voice Over IP |
| * Firewall |
| * WLC |
| * Access Points |

الاختصارات المستخدمة (Shortcuts Used)

|  |
| --- |
| * DHCP: Dynamic Host Configuration Protocol |
| * DNS: Domain Name System |
| * FTP: File Transfer Protocol |
| * [HTTPS: Hypertext Transfer Protocol Security](https://www.imperva.com/learn/performance/http2/) |
| * ICMP: Internet Control Message Protocol |
| * IP: Internet Protocol |
| * OSPF: Open Shortest Path First |
| * SMTP: Simple Mail Transfer Protocol |
| * TCP: Transmission Control Protocol |
| * TELNET: Teletype Network |
| * UDP: User Datagram Protocol |
| * VOIP: Voice-Over-IP |
| * VPN: Virtual Private Network |
| * VTP: VLAN Trunking Protocol |

**الفصل الأول – منهجية المشروع**

:1-1 أهمية المشروع:

يهدف المشروع الى رفع مستوى حماية الشبكة و الدخول غير المصرح به سواء كان من قبل مستخدمي الشبكة أو مستخدمين خارجيين، و يهدف ايضا هذا المشروع إلى تحقيق عدة فوائد مهمة للشركة التي تعمل فيها عدة فروع مثل تحسين سرعة نقل البيانات من خلال استخدام تقنية MPLS وأجهزة Multilayer Switch، يتم تحسين سرعة نقل البيانات بين الفروع. هذا يعني أن المستخدمين سيتمكنون من مشاركة البيانات بسرعة عالية وفعالية، مما يؤدي إلى زيادة الإنتاجية وتحسين أداء العمل.

و تحسين تنظيم مشاركة البيانات بفضل شبكة الخدمات المصممة، سيتم تنظيم عملية مشاركة البيانات بين المستخدمين بشكل أفضل. ستكون هناك آليات واضحة للوصول إلى البيانات ومشاركتها بين الفروع، مما يقلل من التكرار والتباين في البيانات ويسهل التعاون بين الفروع. بالإضافة لتحسين إدارة الشبكة باستخدام بروتوكول OSPF للتوجيه والتحكم، يصبح من السهل إدارة ورصد شبكة الفروع. يصبح بامكاننا تكوين نقاط وصول مختلفة وإدارتها بشكل مركزي من خلال مركز تحكم الشبكة اللاسلكي (WLC) هذا يعني أنه يمكن اتخاذ الإجراءات اللازمة للتعامل مع أي مشاكل في الشبكة بشكل فوري وفعال.

باختصار، فإن هذا المشروع يعمل على تحسين أداء الشبكة وتنظيم مشاركة البيانات وتحقيق سرعة نقل ممتازة بين الفروع. وهذا بدوره يؤدي إلى زيادة الإنتاجية وتحسين كفاءة العمل في الشركة.

1-2: أهداف المشروع:

* 1. بناء شبكة ذات موثوقية عالية.
  2. بناء شبكة ذات حماية عالية.
  3. تحسين سرعة نقل البيانات باستخدام تقنية MPLS وأجهزة Multilayer Switch.
  4. تحسين تنظيم مشاركة البيانات
  5. تحسين إدارة الشبكة باستخدام بروتوكول OSPF للتوجيه والتحكم
  6. تكوين نقاط الوصول المختلفة وإدارتها بشكل مركزي من خلال مركز تحكم الشبكة اللاسلكي .(WLC)
  7. توفير استقرار وموثوقية.

**الفصل الثاني – الدراسة النظرية**

:1-2 تعريف الشبكات:

يمكن تعريف الشبكات بانها التواصل بين الأجهزة سواء كانت اجهزة حاسوب أو هواتف أو كاميرات مراقبة أو طابعات، فهي تشمل التواصل بين جهازين أو عدة أجهزة ويكون التواصل من خلال أسلاك أو يوجد تواصل لاسلكي فيما بينهم، فإن تعريف الشبكات ليست مجرد كلمة بل إنها عالم كبير من التواصل.



الشكل (1) الشبكة

2-2: أنواع الشبكات :(Type of Networks)

إن الشبكات هي السبب في تواصل العالم مع بعضه البعض مما جعل العالم قرية صغيرة ويتم استخدامها في كل مكان سواء المنازل أو المصانع أو الشركات أو الجامعات أو المدارس فنجد أن الشبكات تختلف في نوعها وتقسيمها أيضا من حيث الغرض والمساحة وعدد الأجهزة المستخدمة أيضا فإن تقسيم الشبكات يكون كالآتي :

تنقسم الشبكات حسب المساحة التي تغطيها الى 4 أنواع:

: 1-2-2الشبكات المحلية LAN (Local Area Networks)

:2-2-2الشبكات الإقليمية MAN (Metropolitan Area Network)

:3-2-2الشبكات الواسعة WAN (Wide Area Networks)

:4-2-2الشبكات الشخصية :(Personal Area Network)

:1-2-2 شبكات محلية أو منزلية صغيرة :(Local Area Network)

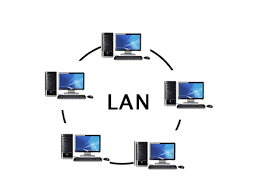
أن الشبكة بعيدة المدى هي التي تغطي مساحة جغرافية صغيرة فهي غالبا التي تستخدم في المنازل من خلال اتصالها على جهاز حاسوب واحد أو هاتف خلوي أو في مكتب ذات مساحة صغيرة فهي تعتبر أبسط أنواع الشبكات.

هي شبكة الاتصال التي تغطي منطقة صغيرة مثل مكتب أو مبني تصمم شبكة LAN لتسمح لأجهزة الحاسب بالمشاركة في استخدام \*الموارد Resources .

**\*الموارد:** تكون مصادر مادية (الطابعات) أو برامج تطبيقية أو بيانات.

من خواص شبكة الحاسب المحلية (LAN) :

تتميز الشبكات المحلية LAN بعدة خصائص من أهمها:

* قصر المسافة بين وحدات الشبكة لوجودها في منطقة جغرافية محدودة.
* سرعة تراسل عالية بين وحدات الشبكة قد تصل إلي 100 Mbps
* إدارة الشبكة وملكيتها لهيئة أو مؤسسة خاصة.

الشكل (2) شبكة LAN

:2-2-2 الشبكات الحضرية أو المدنية :(Metropolitan Area Network)

هي تكون شبكات متوسطة أي بمعنى أدق أنها تقوم بتغطية مناطق متوسطة المساحة مثل تغطية مدنية على سبيل المثال فهي تكون أكبر من الشبكات المحلية وأصغر من الشبكات طويلة المدى.

تم تصميم شبكة MAN للامتداد على مدينة بالكامل وقد تكون شبكة واحدة مثل شبكة التليفزيون الخاصة، أو قد تتكون من توصيل عدد من شبكات محلية LAN في شبكة كبيرة.

شبكة MAN تملك تماما وتشغل بواسطة شركة خاصة، أو قد يكون خدماتها مزودة بشركة خاصة مثل شركات التليفون المحلية والتي يمكن أن تغطي مدينة بأكملها.

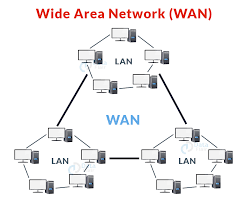


الشكل (3) شبكة MAN

:3-2-2 شبكات بعيدة أو طويلة المدى :(Wide Area Network)

أن الشبكة البعيدة المدى هي التي تغطي مساحات كبيرة جدا و من الأمثلة التي توضح مساحة تغطيتها هي شبكة الإنترنت العالمية فهي مثل التي تغطي قرية بالكامل أو مدينة متكاملة وتشمل عدد لا نهائي من الأجهزة المستخدمة.

هي الشبكات التي تستخدم في الاتصالات الواسعة والتي تمكن من إرسال المعلومات والصور والصوت multimedia عبر مساحات جغرافية واسعة تشمل بلد أو قارة أو قد تصل إلي تغطية العالم بأسره.



الشكل (4) شبكةWAN

:4-2-2الشبكات الشخصية :(Personal Area Network)

الشبكة الشخصية هي شبكة بسيطة حيث أنها تكون لاستخدام شخصي مثل جهاز حاسب آلي واحد أو هاتف خلوي على نطاق صغير لشخص واحد.

إن الشبكات لها أشكال كثيرة ومتعددة وتختلف أشكالها حسب الهدف من الاستخدام فكل نوع له وظائف ومهام محددة ويختلف أيضا تصميمها من حيث السعر وعدد الأجهزة المستخدمة.

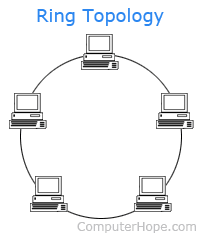


الشكل (5) شبكة شخصية

:3-2طوبولوجيا الشبكات(Network Topology) :

:1-3-2الحلقي(Ring) :

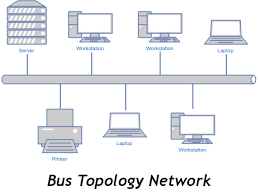
إن هذا النوع هو من الأنواع المعروفة حيث انه يعتمد على اتصال الجهاز أتوماتيكيا بالجهاز الذي قبله والجهاز الذي بعده ويكون هذا الاتصال مباشر حيث انه يكون مشكل في صورة دائرة مغلقة وهذا يكون في اتجاه واحد.



الشكل (6) الحلقي

:2-3-2الخطي (Bus):

  أن هذا النوع هو من أقدم أنواع الشبكات حيث انه يقوم باتصال الشبكات بعضها البعض وذلك عن طريق خط رئيسي ولكن لا يسمح أن يتم تبادل البيانات بين جهازين وان حدث فذلك يؤدي إلى تصادم البيانات واتلافها.

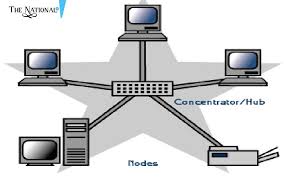


الشكل (7) الخطي

:3-3-2نجمية (Star)‏:

هي إحدى نماذج [الشبكات](https://ar.wikipedia.org/wiki/%D8%B7%D9%88%D8%A8%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7_%D8%B4%D8%A8%D9%83%D8%A9)، ويرتبط فيها كل جهاز بخط إلى خادم مركزي مثل [جهاز توزيع الشبكة](https://ar.wikipedia.org/wiki/%D9%85%D8%A8%D8%AF%D9%84_(%D8%B4%D8%A8%D9%83%D8%A7%D8%AA))، وترسل البيانات إلى الجهاز المحدد. في حالة كان الخادم عبارة عن [موزع مركزي](https://ar.wikipedia.org/wiki/%D9%85%D9%88%D8%B2%D8%B9_(%D8%AD%D8%A7%D8%B3%D9%88%D8%A8)) فإن البيانات ترسل إلى جميع الأجهزة المتصلة بالشبكة.

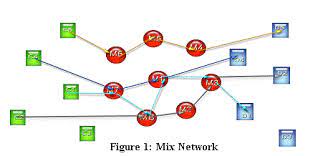
وهي شبكه تستخدم في الشبكة (LAN)



الشكل (8) النجمي

:4-3-2مختلطة Mix)‏( :

وهي بروتوكولات [تسييرية](https://ar.wikipedia.org/wiki/%D8%AA%D9%88%D8%AC%D9%8A%D9%87_(%D8%B4%D8%A8%D9%83%D8%A7%D8%AA)" \o "توجيه (شبكات)) وهي تجعل الاتصالات صعبة التعقب باستخدام سلسلة من خوادم [البروكسي](https://ar.wikipedia.org/wiki/%D9%88%D9%83%D9%8A%D9%84_(%D8%AD%D9%88%D8%B3%D8%A8%D8%A9)) والذي تعرف بالمختلطة، يأخذ الرسائل من عدة مرسلين ويخلطهم، ويرسلهم بترتيب عشوائي إلى الوجهة المخصصة لهم، (في اغلب الأحيان عقدة مختلطة أخرى). هذا يكسر الرابط بين مصدر الطلب والوجهة من ما يجعله صعباً لتقفي الاتصالات.



الشكل (9) المختلطة

**:4-2أصناف عناوين IP:**

:1-4-2تعريف الIPv4:

الـ  IPيوفر عدد هائل من العناوين فالإصدار الرابع من برتوكول الـIP  يكون طول أي عنوان فيه 32  خانة ثنائية هذا يوفر لنا عددا من العناوين قدره 4,294,967,296  = 232

إن عنوان  IPv4 مكون من 32 خانة  مقسمة الى أربع ثُمانيات Octet  و يكتب بالصيغة التالية :

Octet1**.**Octet2**.**Octet3**.**Octet4

يمكننا توضيح كيف يقسم عنوان الـ IP الى معرفين هما معرف الشبكة و معرف المستخدم:

Network ID  Host ID

فاذا استخدمت الثُمانية الأولى فقط لترقيم الشبكات المحلية فأنت تستخدم الصنف A أو ClassA.

Network . Host . Host . Host

أما اذا استخدمت الثُمانية الأولى و الثانية فقط لترقيم الشبكات فأنت تستخدم الصنف B أو ClassB.

Network . Network . Host . Host

أما اذا استخدمت الثُمانية الأولى و الثانية و الثالثة لترقيم فأنت تستخدم الصنف C أو ClassC.

Network . Network . Network . Host

* بالنسبة للصنف A : يجب أن تكون الخانة الأولى 0 دائماً و بهذا تصبح صيغة الثُمانية الأولى كالتالي :

First Octet : 0xxx xxxx

* بالنسبة للصنف B : يجب أن يبدأ العنوان بالخانتين 01 دائماً و بهذا تصبح صيغة الثُمانية الأولى كالتالي :

First Octet : 10xx xxxx

* بالنسبة للصنف C : يجب أن يبدأ بالخانات 011 دائما و بهذا تصبح صيغة الثُمانية الأولى كالتالي :

First Octet : 110x xxxx

مجالات الأصناف Classes:

|  |  |  |
| --- | --- | --- |
| **IP Class** | **From** | **To** |
| **A** | 0 | 127 |
| **B** | 128 | 191 |
| **C** | 192 | 223 |

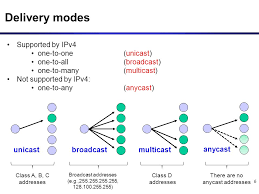
الجدول(1) IPv4

1-4-2-:1 أنواع ارسال البيانات في الشبكة IPv4 :

Broadcast : تكون الرسالة موجهة من جهاز إلى كل الأجهزة.

Multicast : تكون الرسالة موجهة من جهاز إلى مجموعة محددة من الأجهزة.

Unicast : تكون الرسالة موجهة من جهاز إلى جهاز محدد.

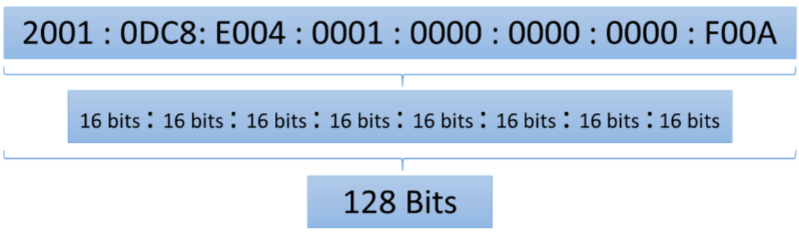


الشكل (10) أنواع ارسال البيانات IPv4

2-4-2: تعريف الIPv6:

هو أحد إصدارات بروتوكول الإنترنت (IP) الذي يوفر مساحة عناوين IP أكبر لمستخدمي الإنترنت. الميزة الأساسية في IPv6 أنه يقوم بزيادة حجم العنوان من ٣٢ بت معيار IPv4 إلى 128 بت. ويسمح هذا بعدد أكبر من العناوين ونقاط التوصيل عما هو متوفر في IPv4 كما يوفر IPv6المزيد من الأساليب لإعداد العنوان وتكوينًا تلقائيًا أكثر سهولة.

يتم تمثيل عناوين IPv6 في شكل ثماني مجموعات من أربعة أرقام سداسية عشرية لكل منها ، مفصولة بنقطتين. قد يتم تقصير التمثيل الكامل.



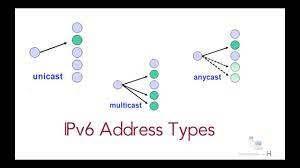
الشكل (11) IPv6

2-4-2-:1 أنواع ارسال البيانات في الشبكة IPv6 :

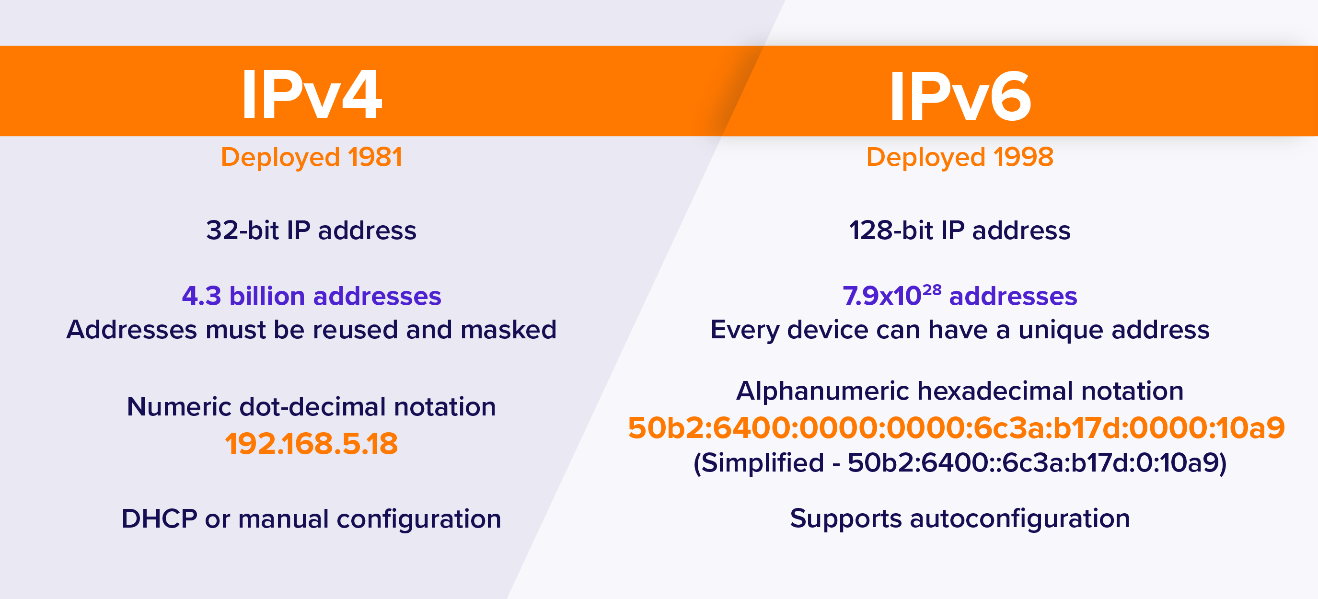
:Unicast هو نوع من الاتصال حيث يتم إرسال البيانات من كمبيوتر إلى كمبيوتر آخر.

:Multicastهو نوع من الاتصالات حيث يتم توجيه حركة مرور البث المتعدد لمجموعة من الأجهزة على الشبكة.

:Anycast هو نوع من الاتصالات حيث يتم فيه توجيه مخططات بيانات IPv6 من مصدر إلى أقرب جهاز (من حيث مسافة التوجيه) من مجموعة خوادم تقدم نفس الخدمة.



الشكل (12) أنواع ارسال البيانات IPv6



الشكل (13) مقارنة IPv6مع IPv4

:5-2البروتوكولات المستخدمة في ال Application Layer:

|  |
| --- |
| * DHCP: Dynamic Host Configuration Protocol . |
| * DNS: Domain Name System. |
| * FTP: File Transfer Protocol. |
| * HTTPS: [Hypertext Transfer Protocol](https://www.imperva.com/learn/performance/http2/) Security. |
| * SMTP: Simple Mail Transfer Protocol. |
| * TELNET: Teletype Network. |

الجدول(2) بروتوكولات ال Application Layer

**:**1-5-2بروتوكول التكوين الديناميكي للمضيف (DHCP):

DHCP هو بروتوكول اتصال يمكّن مسؤولي الشبكة من أتمتة تعيين عناوين IP في الشبكة. في شبكة IP ، يتطلب كل جهاز متصل بالإنترنت عنوان IP فريدًا. يتيح DHCP لمسؤولي الشبكة توزيع عناوين IP من نقطة مركزية وإرسال عنوان IP جديد تلقائيًا عند توصيل جهاز من مكان مختلف في الشبكة. يعمل DHCP على نموذج خادم العميل.

:2-5-2بروتوكول نظام اسم المجال:(DNS)

يساعد بروتوكول DNS في ترجمة أو تعيين أسماء المضيف لعناوين IP يعمل DNS على نموذج خادم العميل ، ويستخدم قاعدة بيانات موزعة عبر تسلسل هرمي لخوادم الأسماء.

يتم تحديد المضيفين بناءً على عناوين IP الخاصة بهم ، ولكن حفظ عنوان IP أمر صعب نظرًا لتعقيده. تعد عناوين IP ديناميكية أيضًا ، مما يجعل من الضروري تعيين أسماء النطاقات لعناوين IP. يساعد DNS في حل هذه المشكلة عن طريق تحويل أسماء مجالات مواقع الويب إلى عناوين IP رقمية.

:3-5-2بروتوكول نقل الملفات: (FTP)

يتيح بروتوكول نقل الملفات مشاركة الملفات بين الأجهزة المضيفة ، سواء المحلية أو البعيدة ، وتعمل فوق TCP. لنقل الملفات ، يقوم FTP بإنشاء اتصالين TCP: التحكم واتصال البيانات. يتم استخدام اتصال التحكم لنقل معلومات التحكم مثل كلمات المرور وأوامر استرداد الملفات وتخزينها وما إلى ذلك ، ويتم استخدام اتصال البيانات لنقل الملف الفعلي. يعمل كلا الاتصالين بالتوازي أثناء عملية نقل الملفات بأكملها.

:6-5-2بروتوكول نقل النص التشعبي الآمن (HTTPS):

بروتوكول نقل النص التشعبي الآمن  ( HTTPS ) هو امتداد [لبروتوكول نقل النص التشعبي](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) (HTTP). يتم استخدامه [للاتصال الآمن](https://en.wikipedia.org/wiki/Secure_communications) عبر [شبكة الكمبيوتر](https://en.wikipedia.org/wiki/Computer_network) ، ويستخدم على نطاق واسع على الإنترنت. في HTTPS ، يتم تشفير [بروتوكول الاتصال باستخدام](https://en.wikipedia.org/wiki/Communication_protocol)[بروتوكول أمان طبقة النقل](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) أو ، سابقًا ، طبقة مآخذ التوصيل الآمنة (SSL). لذلك يشار إلى البروتوكول أيضًا باسم HTTP عبر TLS ،  أو  HTTP عبر .SSL

 الدوافع الرئيسية لبروتوكول HTTPS هي [مصادقة](https://en.wikipedia.org/wiki/Authentication)[موقع الويب](https://en.wikipedia.org/wiki/Website) الذي تم الوصول إليه وحماية [خصوصية](https://en.wikipedia.org/wiki/Information_privacy) وسلامة [البيانات](https://en.wikipedia.org/wiki/Data_integrity) المتبادلة أثناء النقل. إنه يحمي من هجمات [man-in-the-middle ، كما أن](https://en.wikipedia.org/wiki/Man-in-the-middle_attack)[التشفير](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation) ثنائي الاتجاه للاتصالات بين العميل والخادم يحمي الاتصالات [من](https://en.wikipedia.org/wiki/Tamper-evident#Tampering)[التنصت](https://en.wikipedia.org/wiki/Eavesdropping) والعبث. يتطلب جانب المصادقة في HTTPS طرفًا ثالثًا موثوقًا به لتوقيع [الشهادات الرقمية من جانب الخادم](https://en.wikipedia.org/wiki/Public_key_certificate).

2-5-:7 بروتوكول نقل البريد:(SMTP)

SMTP هو بروتوكول مصمم لنقل البريد الإلكتروني بشكل موثوق وفعال. SMTP هو بروتوكول دفع ويستخدم لإرسال البريد الإلكتروني ، بينما يتم استخدام POP و IMAP لاسترداد رسائل البريد الإلكتروني من جانب المستخدم النهائي. ينقل SMTP رسائل البريد الإلكتروني بين الأنظمة ويخطر رسائل البريد الإلكتروني الواردة. باستخدام SMTP ، يمكن للعميل نقل بريد إلكتروني إلى عميل آخر على نفس الشبكة أو شبكة أخرى من خلال مرحل أو بوابة وصول متاحة لكلتا الشبكتين.

2-5-:8 بروتوكول: (Telnet)

Telnet هو بروتوكول طبقة تطبيق يمكّن المستخدم من الاتصال بجهاز بعيد. يتم تثبيت عميل Telnet على جهاز المستخدم ، والذي يصل إلى واجهة سطر الأوامر لجهاز بعيد آخر يقوم بتشغيل برنامج خادم Telnet.

يستخدم Telnet غالبًا بواسطة مسؤولي الشبكة للوصول إلى الأجهزة البعيدة وإدارتها. للوصول إلى جهاز بعيد ، يحتاج مسؤول الشبكة إلى إدخال عنوان IP أو اسم المضيف للجهاز البعيد ، وبعد ذلك سيتم تقديمه مع محطة افتراضية يمكنها التفاعل مع المضيف.

:6-2البروتوكولات المستخدمة في ال Transport Layer:

|  |
| --- |
| * TCP: Transmission Control Protocol. |
| * UDP: User Datagram Protocol. |

الجدول (2) بروتوكولات ال Transport Layer

**:**1-6-2 بروتوكول التحكم في الإرسال (TCP):

يعد بروتوكول التحكم في الإرسال (TCP) أحد البروتوكولات الرئيسية لمجموعة بروتوكولات الإنترنت. نشأ في تنفيذ الشبكة الأولى الذي أكمل فيه بروتوكول الإنترنت (IP). لذلك ، يُشار إلى المجموعة بأكملها عمومًا باسم TCP / IP. يوفر بروتوكول TCP (بروتوكول التحكم في الإرسال) تسليمًا موثوقًا ومرتّبًا ومحققًا من الأخطاء بين التطبيقات التي تعمل على المستخدمين الذين يتواصلون عبر شبكة IP. تعتمد تطبيقات الإنترنت الرئيسية مثل شبكة الويب العالمية والبريد الإلكتروني والإدارة عن بُعد ونقل الملفات على TCP ، وهو جزء من طبقة النقل لمجموعة TCP / IP. غالبًا ما يتم تشغيل SSL / TLS أعلى TCP.

:2-6-2 بروتوكول مخطط بيانات المستخدم (UDP):

يستخدم UDP نموذج اتصال بسيط بدون اتصال مع الحد الأدنى من آليات البروتوكول.

يعد UDP مناسبًا للأغراض التي لا يكون فيها فحص الأخطاء وتصحيحها ضروريًا أو يتم تنفيذهما في التطبيق ؛ يتجنب UDP الحمل الزائد لمثل هذه المعالجة في مكدس البروتوكول. غالبًا ما تستخدم التطبيقات الحساسة للوقت UDP لأن إسقاط الحزم أفضل من انتظار تأخير الحزم بسبب إعادة الإرسال والذي قد لا يكون خيارًا في نظام الوقت الفعلي.

7-2:البروتوكولات المستخدمة في ال Network Layer:

|  |
| --- |
| * OSPF: Open Shortest Path First. |

2-7-1: بروتوكول التوجيه الديناميكي الداخلي(OSPF) :

هو بروتوكول توجيه لحزم بروتوكول الإنترنت (IP) يعمل في الطبقة الثالثة. يستخدم خوارزمية توجيه حالة الارتباط (LSR) ويقع ضمن مجموعة بروتوكولات البوابة الداخلية (IGPs) ، والتي تعمل ضمن نظام مستقل واحد (AS).

يقوم OSPF بجمع معلومات حالة الارتباط من أجهزة التوجيه المتاحة وإنشاء خريطة طوبولوجيا للشبكة. يتم تقديم الهيكل كجدول توجيه إلى طبقة الإنترنت لتوجيه الحزم حسب عنوان IP الخاص بها. يدعم OSPF شبكات بروتوكول الإنترنت الإصدار 4 (IPv4) والإصدار 6 من بروتوكول الإنترنت (IPv6) ويدعم نموذج العنونة للتوجيه بين المجالات دون فئات (CIDR).

يستخدم OSPF على نطاق واسع في شبكات المؤسسات الكبيرة.

**الفصل الثالث - الأجهزة المستخدمة**

3-1: الموجه (Router):

جهاز التوجيه هو جهاز يربط بين شبكتين أو أكثر من شبكات تبديل الحزمة أو الشبكات الفرعية. إنه يخدم وظيفتين أساسيتين: إدارة حركة حزم البيانات بين هذه الشبكات عن طريق إعادة توجيه حزم البيانات إلى عناوين IP المقصودة ، والسماح لأجهزة متعددة باستخدام نفس اتصال الإنترنت.

هناك عدة أنواع من أجهزة التوجيه ، ولكن معظم أجهزة التوجيه تمرر البيانات بين الشبكات المحلية (شبكات المنطقة المحلية) وشبكات WAN (شبكات المنطقة الواسعة).



الشكل (14) Router

يساعد جهاز التوجيه في توجيه حزم البيانات إلى عنوان IP الخاص بها. لتوجيه الحزم بشكل فعال ، يستخدم جهاز التوجيه جدول توجيه داخلي قائمة بالمسارات إلى وجهات الشبكة المختلفة. يقرأ جهاز التوجيه رأس الحزمة لتحديد المكان الذي تتجه إليه ، ثم يستشير جدول التوجيه لمعرفة المسار الأكثر كفاءة إلى تلك الوجهة. ثم يقوم بإعادة توجيه الحزمة إلى الشبكة التالية في المسار.

3-2: المبدل (Switch):



الشكل (15)Switch

هو جهاز شبكة يستخدم في توجيه حركة حزم البيانات على الشبكة المحلية (LAN). يعمل السويتش عند استلام حزمة بيانات من جهاز مرسل (مثل جهاز كمبيوتر) ويقوم بتوجيهها إلى الجهاز المستقبل المناسب.

وظيفة السويتش هي توجيه حركة البيانات على المستوى الثاني (المستوى الرئيسي في نموذج OSI). يستخدم السويتش عنوان الجهاز المستقبل (عن طريق عنوان الوجهة في حزمة البيانات) لتحديد الجهاز الذي يجب إرسال البيانات إليه. وهذا يتم من خلال استخدام جدول MAC (جدول عناوين الوسائط الوصلة) الذي يسجل عناوين الوجهات المعروفة على الشبكة.

عند استلام حزمة بيانات، يتحقق السويتش من جدول MAC الخاص به لمعرفة عنوان الجهاز المستقبل. إذا تم العثور على العنوان في الجدول، يتم إرسال الحزمة عبر الواجهة المناسبة إلى الجهاز المستقبل. وإذا لم يتم العثور على العنوان في الجدول، يتم بث الحزمة إلى جميع الواجهات الأخرى في الشبكة المحلية للبحث عن الجهاز المستقبل وتحديث جدول MAC.

بالإضافة إلى ذلك، يمكن تكوين السويتش لدعم ميزات إضافية مثل الشبكات الافتراضية (VLANs) التي تسمح بتجزئة الشبكة المحلية إلى مجموعات منفصلة لزيادة الأمان وتحسين أداء الشبكة. كما يوفر السويتش أدوات لإدارة حركة البيانات ومراقبة أداء الشبكة.

3-3: المبدل متعدد الطبقات (Multi LayerSwitch):



الشكل (16)MultilayerSwitch

جهاز Multi-Layer Switch هو جهاز شبكات يتم استخدامه للتواصل وتوجيه حركة المرور بين الشبكات المختلفة وتوزيع البيانات على مستويات متعددة. يعمل هذا الجهاز كمفتاح ذكي يجمع بين ميزات أجهزة التوجيه (Routers) والمفاتيح (Switches) في جهاز واحد.

يتميز الـ Multi-Layer Switch بقدرته على التعامل مع مجموعة متنوعة من بروتوكولات الشبكة وتحليل حركة المرور على مستوى الشبكة والطبقة الثانية والطبقة الثالثة في نموذج .OSI يعتبر هذا الجهاز هجينًا بين جهاز التوجيه والمفتاح، حيث يمكنه التبديل (Switching) بين البيانات على مستوى الطبقة الثانية وتوجيه (Routing) حركة المرور بين الشبكات على مستوى الطبقة الثالثة.

على مستوى الطبقة الثانية، يتم استخدام Multi-Layer Switch لتوجيه حركة المرور بناءً على عناوين MAC (Media Access Control) للأجهزة المتصلة به. يقوم بتعلم عناوين MAC وتخزينها في جدول تبديل (Switching table) الخاص به لتوجيه البيانات إلى العنوان الصحيح في الشبكة المحلية.

على مستوى الطبقة الثالثة، يعمل الـ Multi-Layer Switch كجهاز توجيه بين الشبكات المختلفة. يقوم بتحليل حركة المرور باستخدام عناوين IP (Internet Protocol) ويستخدم جدول التوجيه (Routing table) لاتخاذ قرارات التوجيه الصحيحة. يمكن للجهاز أيضًا تطبيق ميزات الأمان والتحكم في الوصول وإدارة حجم الحركة وتحسين أداء الشبكة بشكل عام. بفضل قدرته على العمل على مستويات متعددة،

3-4: الخادم (Server):



الشكل (71) Servers

هو برنامج أو جهاز كمبيوتر يوفر خدمة لبرنامج كمبيوتر آخر ومستخدمه ، والمعروف أيضًا باسم العميل. في مركز البيانات ، يُشار أيضًا إلى الكمبيوتر الفعلي الذي يعمل عليه برنامج الخادم على أنه خادم. قد يكون هذا الجهاز خادمًا مخصصًا أو يمكن استخدامه لأغراض أخرى.

في نموذج برمجة العميل / الخادم ، ينتظر برنامج الخادم ويلبي الطلبات الواردة من برامج العميل ، والتي قد تعمل في نفس الكمبيوتر أو أجهزة كمبيوتر أخرى. قد يعمل تطبيق معين في الكمبيوتر كعميل لديه طلبات للحصول على خدمات من برامج أخرى وكخادم للطلبات من برامج أخرى.

يمكن أن يشير مصطلح الخادم إلى جهاز فعلي أو جهاز ظاهري أو برنامج يقوم بتنفيذ خدمات الخادم. تختلف الطريقة التي يعمل بها الخادم بشكل كبير اعتمادًا على كيفية استخدام خادم الكلمات.

3-5: هاتف نقل الصوت عبر الإنترنت (Voice over IP):

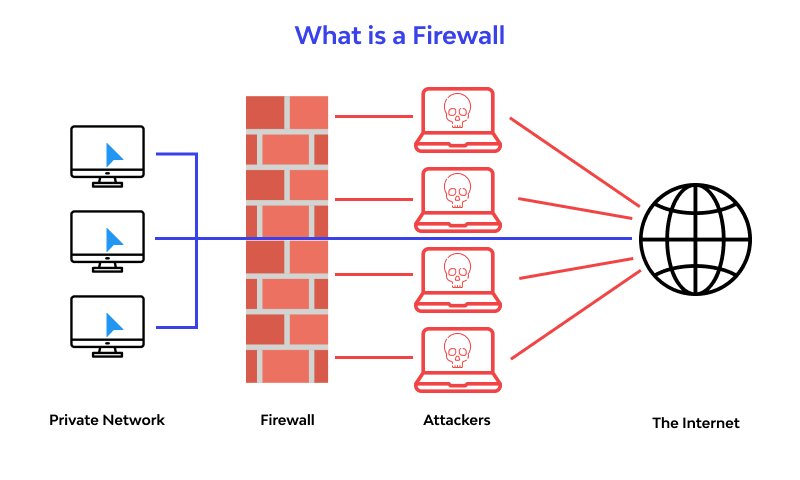


الشكل (81) Voip Phone

يشبه مزود هاتف VoIP إلى حد كبير شركة الهاتف التقليدية الخاصة بك من حيث أنه يدعم خطة الهاتف الخاصة بك ، ولكن مزود الهاتف VoIP (الصوت عبر بروتوكول الإنترنت) يتعامل مع المكالمات الهاتفية التي تحدث عبر اتصال الإنترنت ، بدلاً من خطوط الهاتف التقليدية. يمكنك الحصول على خطة مكالمات هاتفية وجهاز هاتف VoIP وأي معدات VoIP إضافية تحتاجها من مزود خدمة VoIP.

يعد نقل الصوت عبر الإنترنت (VoIP) ، المعروف أيضًا باسم المهاتفة عبر بروتوكول الإنترنت ، طريقة ومجموعة من التقنيات لتقديم الاتصالات الصوتية وجلسات الوسائط المتعددة عبر شبكات بروتوكول الإنترنت (IP) ، مثل الإنترنت. تشير مصطلحات الاتصال الهاتفي عبر الإنترنت والمهاتفة ذات النطاق العريض وخدمة الهاتف ذات النطاق العريض على وجه التحديد إلى توفير خدمات الاتصالات (الصوت والفاكس والرسائل القصيرة والرسائل الصوتية) عبر الإنترنت.

6-3: الجدار الناري(Firewall) :



الشكل (91) Firewall

جدار الحماية هو جهاز أمان للشبكة يراقب حركة مرور الشبكة الواردة والصادرة ويسمح بحزم البيانات أو يحظرها بناءً على مجموعة من قواعد الأمان. والغرض منه هو إنشاء حاجز بين شبكتك الداخلية وحركة المرور الواردة من مصادر خارجية (مثل الإنترنت) من أجل منع حركة المرور الضارة مثل الفيروسات والمتسللين.

3-7: وحدة تحكم الشبكة المحلية اللاسلكية(WLC) :



الشكل (20)WLC

شبكة WLAN هي بنية لاسلكية تهدف إلى تلبية متطلبات الشبكة المتغيرة. تدير وحدة تحكم WLAN نقاط وصول الشبكة اللاسلكية التي تسمح للأجهزة اللاسلكية بالاتصال بالشبكة.

يتم نشره تقليديًا في الحرم الجامعي حيث توجد المباني والشبكات على مسافة قريبة. يعمل هذا النشر على دمج الشبكة اللاسلكية ، مما يسمح بإجراء ترقيات أسهل وتمكين وظائف لاسلكية متقدمة. تعتمد وحدات التحكم على أماكن العمل ويتم تثبيتها في موقع مركزي.

تم تصميم هذا الحل للجامعات الصغيرة أو المكاتب الفرعية. يتيح للعملاء الاتساق في اتصالاتهم اللاسلكية والسلكية. يجمع هذا النشر سلكيًا ولاسلكيًا على جهاز شبكة واحد - مفتاح وصول - ويؤدي الدور المزدوج لكل من المحول ووحدة التحكم اللاسلكية.

3-8: نقطة الوصول(Access Point) :

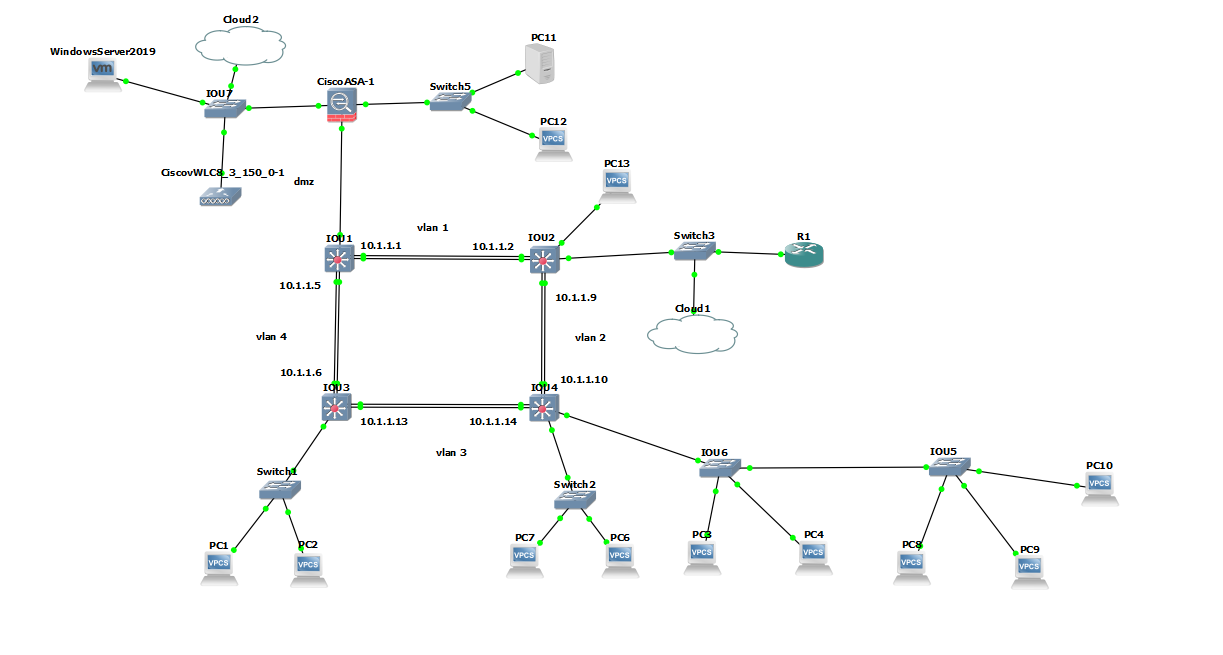


الشكل (21)Access Point

نقطة الوصول هي جهاز يقوم بإنشاء شبكة محلية لاسلكية ، أو WLAN ، عادة في مكتب أو مبنى كبير. تتصل نقطة الوصول بجهاز توجيه أو مفتاح أو محور سلكي عبر كابل Ethernet ، وتعرض إشارة WiFi إلى منطقة معينة. على سبيل المثال ، إذا كنت ترغب في تمكين وصول WiFi في منطقة الاستقبال الخاصة بشركتك ولكن ليس لديك جهاز توجيه داخل النطاق ، فيمكنك تثبيت نقطة وصول بالقرب من مكتب الاستقبال وتشغيل كبل Ethernet عبر السقف إلى غرفة الخادم.

**الفصل الرابع - التقنيات المستخدمة و التصميم العملي**

1-4: المخطط العملي للمشروع :



الشكل (22) المخطط العملي للشبكة

2-4: شرح مبسط للمخطط العملي:

تم استخدام تقنية MPLS (Multi-Protocol Label Switching) في الشبكة لتحقيق توجيه الحزم وتوفير الخدمات بشكل فعال. تعتمد تقنية MPLS على وضع علامات (Labels) على الحزم (Packets) في الطبقة الثانية من الشبكة، وهذه العلامات تستخدم لتوجيه الحزم بشكل سريع وفعال.

عندما يدخل حزمة إلى الشبكة، يتم وضع علامة MPLS عليها وتستخدم هذه العلامة لتحديد المسار المثلى للحزمة عبر الشبكة. يتم تبادل المعلومات حول العلامات بين الـ Multi-Layer Switches والـ Routers الأخرى في الشبكة باستخدام بروتوكولات تبادل المعلومات مثل

.LDP (Label Distribution Protocol)

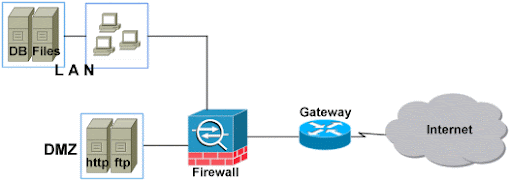
عندما تصل الحزمة إلى جهاز Multi-Layer Switch الوجهة، يتم إزالة العلامة وتوجيه الحزمة بناءً على معلومات الطبقة الثالثة مثل عنوان IP. هذا يسمح بتحقيق توجيه سريع وفعال للحزم في الشبكة.

تم توظيف أجهزة Multi-Layer Switches وتقنية MPLS لتحقيق توجيه فعال وتوزيع البيانات عبر شبكة الشركة. يساعد هذا التصميم في توفير أداء عالي، وفصل الأقسام المختلفة، وتحسين الأمان والحماية.

ومن المتعارف بأن الشبكة بالنسبة لأي مؤسسة تقسم إلى نوعين:  
الشبكة الداخلية LAN: وأهم ما تتضمنه الأجهزة المركزية (السيرفرات) بالإضافة إلى أجهزة المستخدمين. ومن المفروض أن تكون محمية ومؤمنة من أي تداخل مع أي شبكة خارجية أخرى.

الشبكة الخارجية Internet: بصفتها العامة لا يتوفر فيها مستوى عالٍ من الحماية. وهي بالنسبة للشبكة الداخلية تشكل مصدراً رئيسياً لخطر الاختراق والتهديدات.   
عادة يُفصل بين هاتين الشبكتين بوسيلة حماية قد يكون أبسط صورة لها جهاز الراوتر.

DMZ هي نوع ثالث، وتقع في مستوى وسط بين النوعين السابقين… هي شبكة محايدة، فلا هي محمية ومؤمنة بشكل كلّي كما هي الشبكة الداخلية. ولا هي مكشوفة بشكل صريح كما هي شبكة الإنترنت.  
يتم اللجوء لحل DMZ عند الحاجة لتمكين المستخدمين في الشبكة الخارجية من الوصول إلى بعض الخدمات المحلية مثل Web Server أو FTP أو Mail Server فبدلاً من توفيرها ضمن مجال الشبكة الداخلية بما يشكّله هذا من تعريض كامل الشبكة لخطر الاختراق أو الهجمات، يتم وضع هذه الخدمات ضمن شبكة ثالثة منفصلة عن الشبكة الداخلية. وبذلك تتحقق إمكانية العزل عن الأخطار التي يمكن أن تشكّلها الإنترنت، مع إمكانية توفير الخدمات اللازمة للخارج.

[](http://nettales.files.wordpress.com/2009/04/dmz.gif)  
الشكل(23) يوضح مفهوم DMZ

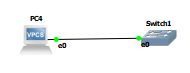
يشكّل جهازي الراوتر وجدار النار firewall مستويين من الحماية هنا…وعملياً، تم التصميم بحيث وضعت كل شبكة من الشبكات الثلاث على أحد منافذ الجدار الناريfirewall interface . بالطبع خصص لكل منها عنوان شبكة network address ومجموعة عناوين IP خاصة بها، ويقوم الجدار الناري بتوجيه البيانات فيما بين المنافذ مثل الراوتر.  
  
  
توضع السياسات المناسبة لكل منفذ، بحيث تمكّن كل طرف من الوصول فقط إلى ما هو مسموح له. مثلاً يستطيع المستخدمون المحليون (الشبكة LAN) الوصول إلى الإنترنت للتصفّح، والوصول إلى DMZ لاستعراض أو إضافة أو تعديل محتويات السيرفرات. بينما يمنع جدار النار المستخدمين الخارجيين من الوصول إلى LAN بل الوصول إلى DMZ فقط.

تم استخدام بروتوكول ال OSPF الذي يستخدم خوارزمية Dijkstra لحساب أقصر طريق بحيث تم تعريف الشبكات المتصلة مباشرة مع كل Multilayer Switch و يقوم كل Multilayer Switch بتعريف الشبكات المتصلة معه و بعد مدة زمنية معينة يصبح جميع الMultilayer Switches تحتوي على جميع الشبكات الموجودة في الشبكة.

التكلم عن البيئة المستخدمة في المشروع GNS3 & VMWare مع الصور المعبرةو شرح طريقة تنصيب البيئة

3-4: Command Line Interface (CLI) :

Telnet:



switch> enable

switch# configure terminal

switch(config)# interface vlan 1

switch(config-if)# ip address 192.168.1.1 255.255.255.0

switch(config-if)#no shutdown

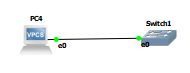
switch(config)# line vty 0 15

switch(config-line)# password telnet

switch(config-line)# login

switch(config-line)# exit

SSH:



switch> enable

Switch# configure terminal

Switch(config)# hostname SW

SW1(config)# ip domain-name tech.com

SW1(config)# crypto key generate rsa

SW1(config)# ip ssh version 2

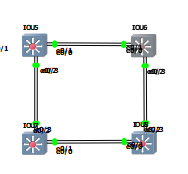
SW1(config)# username admin secret PASSWORD

SW1(config)# line vty 0 15

SW1(config-line)# login local

SW1(config-line)# exit

MPLS and OSPF and Ether channel:



Switch# enable

Switch# configure terminal

Switch(config)# interface fa0/1-2

Switch(config-if-range)# channel-group 1 mode on

Switch(config)#Inter vlan 1

Switch(config-if)#mpls ip

Switch(config-if)#mpls ldp

Switch(config-if)#exit

Switch> enable

Switch# configure terminal

Switch(config)# router ospf 1

Switch(config-router)# network <my networks>

Switch(config-router)# exit

DHCP:

ip dhcp pool Floor1DHCP

network 192.168.0.0 255.255.255.0

default-router 192.168.0.1

dns-server 192.168.0.1

DHCPv6:

router(config)# ipv6 dhcp pool pool-name

router(config-dhcpv6)# dns-server "dns ip"

router(config-dhcpv6)# domain-name "domain name" router(config)# interface type number

router(config-if)# ipv6 dhcp server pool\_name

DHCP Relay Agent:

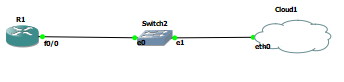
Router1(config)#dhcp pool lan2

Router1(config)#network 10.0.0.0 255.0.0.0

Router2(config)#inter fas 0/0

Router2(config)#ip helper-address the dhcp router ip

VOIP:



RouterA(config)#interface FastEthernet0/0

RouterA(config-if)#ip address 192.168.10.1 255.255.255.0

RouterA(config-if)#no shutdown

RouterA(config)#ip dhcp pool VOICE

RouterA(dhcp-config)#network 192.168.10.0 255.255.255.0

RouterA(dhcp-config)#option 150 ip 192.168.10.1

RouterA(config)#telephony-service

RouterA(config-telephony)#max-dn 5

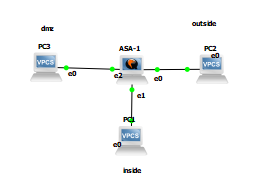
RouterA(config-telephony)#max-ephones 5

RouterA(config-telephony)#ip source-address 192.168.10.1 port 2000

RouterA(config)#ephone-dn 1

RouterA(config-ephone-dn)#number 54001

Firewall:



firewall(config)# switchport access vlan 2

firewall(config)# interface Ethernet0/1

firewall(config-if)# switchport access vlan 1

firewall(config)# interface Ethernet0/2

firewall(config-if)# switchport access vlan 3

firewall(config)# interface Vlan1

firewall(config-if)# nameif inside

firewall(config-if)# security-level 100

firewall(config-if)# ip address 192.168.1.1 255.255.255.0

firewall(config)# interface Vlan2

firewall(config-if)# nameif outside

firewall(config-if)# security-level 0

firewall(config-if)# ip address 198.51.100.1 255.255.255.0

firewall(config)# interface Vlan3

firewall(config-if)# nameif dmz

firewall(config-if)# security-level 50

firewall(config-if)# ip address 192.168.2.1 255.255.255.0

firewall(config)# object network DMZ

firewall(config-network-object)# subnet 192.168.2.0 255.255.255.0

firewall(config)# nat (dmz,outside) dynamic interface

firewall(config)# object network HTTP

firewall(config-network-object)# nat (dmz,outside) static 198.51.100.101

firewall(config)# object network LAN

firewall(config-network-object)# nat (inside,outside) dynamic interface

firewall(config)# class-map INSIDE-DMZ

firewall(config-cmap)# match any

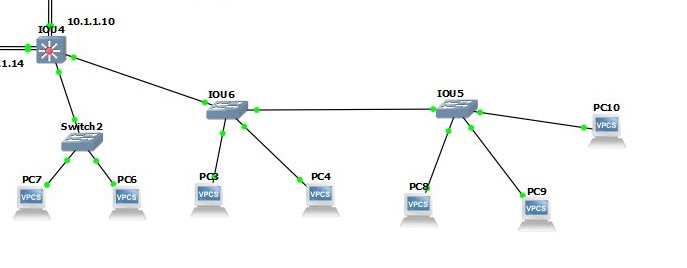
firewall(config)# policy-map POLITICA-INSIDE-DMZ

firewall(config-pmap)# class INSIDE-DMZ

firewall(config-pmap-c)# inspect icmp

firewall(config)# service-policy POLITICA-INSIDE-DMZ interface inside

VLANs and VTP:



Switch(config)#vtp mode server

Switch(config)#vtp domain tech.com

vtp password Switch(config)#password

Switch(config)#vlan10

Switch(config-vlan)#nameMarketing

Switch(config-vlan)#exit

Switch(config)#interface vlan10

Switch(config-if)#ipaddress192.168.10.1 255.255.255.0

Switch(config-if)#exit

**الفصل الخامس - الاستنتاجات والعمل المستقبلي**

5-1 النتائج العملية:

من خلال تنفيذنا لهذا المشروع و دراستنا لبيئة الشركة تبين أنه من الممكن تطبيق هذا المشروع على شركة واقعية لتأمين حماية للبيانات المرسلة بين المستخدمين من خلال استخدام خوارزميات التشفير و انشاء قناة تشفير VPN لمنع أي عملية اختراق من خارج الشركة بالإضافة لبعض التقنيات و الأجهزة الأخرى مثل الFirewall وربط هذه المباني معا تؤمن سهولة و سرعة نقل البيانات المتبادلة. من خلال التنفيذ العملي للشبكة والمشاكل التي تمت مواجهتها وإيجاد الحلول لها وجدنا أنه ليس من الصعب بناء نظام بأسهل وأرخص الطرق المتاحة.

5-2 العمل المستقبلي:

نتوقع تنفيذ هذا المشروع عمليا من قبل الشركات لمواكبته لأحدث تقنيات الحماية وأحدث طرق تشفير ذلك نتيجة للأجهزة و التقنيات الحديثة المستخدمة ونأمل بتنفيذه لأن هذا النوع من المشاريع التي تتطلب حماية و تشفير تحتاج أفكار و تقنيات حديثة مواكبة للتطور الذي يحدث بمجال الاختراق ، لذا يجب الاستفادة من المشروع بكافة الطرق الممكنة.

**References المراجع**

1. https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
2. <https://www.gns3.com/software/download>
3. <https://gns3vault.com/>
4. <https://gns3.com/community>
5. <https://www.udemy.com/course/gns3-certification-training/>
6. https://www.vmware.com/products/hands-on-labs.html
7. [https://www.almrsal.com/](C:\\Users\\E\\AppData\\Roaming\\Microsoft\\Word\\ip address شرح | المرسال (almrsal.com)" \o "https://www.almrsal.com/)
8. <https://wikiarab.com/>
9. [Application layer protocols | Various Protocols of Applications layers (educba.com)](https://www.educba.com/application-layer-protocols/)
10. <https://www.cisco.com/>
11. <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-network-controller.html#~faqs>
12. <https://www.techtarget.com/whatis/definition/server>
13. <https://www.forcepoint.com/cyber-edu/firewall>
14. <https://www.ip-insider.de/was-ist-ospf-open-shortest-path-first-a-905626/>
15. <https://ar.wikipedia.org/wiki/>
16. <https://www.lifesize.com/blog/tcp-vs-udp/#:~:text=TCP%20is%20a%20connection%2Doriented,is%20only%20possible%20with%20TCP>.
17. <https://www.geeksforgeeks.org/differences-between-tcp-and-udp/>
18. <https://www.cisco.com/c/en/us/products/routers/product-listing.html>
19. <https://de.wikipedia.org/wiki/Switch_(Netzwerktechnik)>