 جامعة الاتحاد الخاصة  
كلية الهندسة المعلوماتية  
قسم هندسة الاتصالات

تصميم شبكة خدمية متعددة الأفرع

تقرير مشروع التخرج 1

إعداد الطالب: أيهم جولو

بإشراف الدكتور: ياسر فواز

العام الدراسي: 2022-2023

الفهرس

الخلاصة:

يهدف هذا المشروع إلى تصميم شبكة خدمية لشركة لها عدة أفرع و تنظيم عملية مشاركة البيانات بين المستخدمين حيث سيتم السماح لفئة محددة فقط من الأفراد من الوصول لبيانات محددة ضمن المؤسسة و سيتم ضمان حماية البيانات من خلال تشفير البيانات المتبادلة بين الأفرع بالإضافة لاستخدام تقنية التبديل متعدد الاتفاقيات باستخدام المؤشرات التعريفية (MPLS) التي سيتم من خلالها نقل البيانات بشكل سريع جدا.

Abstract:

This project aims to design a service network for a company with several branches and organize the process of data sharing between users, where only a specific category of individuals will be allowed to access specific data within the organization, and data protection will be ensured through encryption of data exchanged between branches in addition to the use of multi-agreement switching technology Using MPLS through which data will be transmitted very quickly.

**الفصل الأول – منهجية المشروع**

:1-1 أهمية المشروع:

يهدف المشروع الى رفع مستولى حماية الشبكات المحلية أو العامة من الاختراقات أو الدخول غير المصرح به وقد يكون من مستخدمين الشبكة أو مستخدمين خارجيين، حيث أن مستخدمين الشبكة لهم صلاحيات محدودة عليها؛ وأي تعدي للمستخدم خارج نطاق صلاحياته يعتبر اختراق للشبكة، لذلك هناك مجموعة من القوانين والممارسات التي تمنع أي دخول غير قانوني أو غير مصرح به إلى الشبكة، يتضمن حماية الشبكات إذن الوصول إلى البيانات في الشبكة.

1-2: أهداف المشروع:

* 1. بناء شبكة ذات موثوقية عالية.
  2. التعرف على المشاكل الموجودة في الشبكة و محاولة حلها.
  3. توفير الوقت اللازم لإدارة الشبكة.
  4. إدراك أهمية المشروع وتأثيره على الشركات.
  5. بناء شبكة ذات حماية عالية.

**الفصل الثاني – الدراسة النظرية**

:2-1 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:

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

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

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

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

:2-2-1 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 .

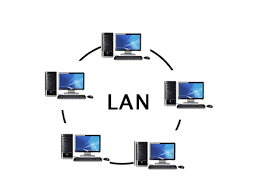
**\*الموارد:** تكون مصادر مادية (الطابعات) أو برامج تطبيقية أو بيانات.

أين تستخدم شبكات الLAN؟

تستخدم شبكات LAN في محيط التجارة والأعمال حيث يكون هناك ارتباط بين عدة أجهزة للعمل بصورة تعاونية مثل شبكة المعلومات داخل ورش العمل داخل مصنع أو بنك حيث يكون هناك جهاز واحد له سعة تخزينية فائقة وسرعة عالية جدا يسمى server ومجموعة من الأجهزة الفرعية تسمى clients .   
عادة لدى الشبكات المحلية LAN معدلات لسرعة البيانات من 4 إلى 16 Mbpsوقد تصل هذه السرعة فيما بعد إلي ما يزيد عن 200 Mbps .

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

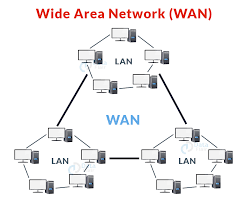
:2-2-3 شبكات بعيدة أو طويلة المدى :(Wide Area Network)

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.

مما تتكون شبكة WAN؟

تتكون شبكة WAN من عدة شبكات MAN أو LAN يتم ربطهم من خلال الأقمار الصناعية المنتشرة عبر العالم كله على عكس الشبكات المحلية LAN والتي تعتمد على معداتها الخاصة في الاتصالات فإن شبكة WAN قد تستخدم أجهزة اتصالات عامة أو مستأجرة أو خاصة حيث يتم تجميعهم وبالتالي يمكن امتداد مساحة تغطية الشبكة عبر مساحات جغرافية شاسعة قد تصل إلي آلاف الأميال.



الشكل (4) شبكةWAN

:2-2-4الشبكات 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.

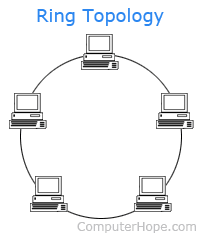


الشكل (5) شبكة شخصية

:2-3طوبولوجيا الشبكات(Network Topology) :

:2-3-1الحلقي(Ring) :

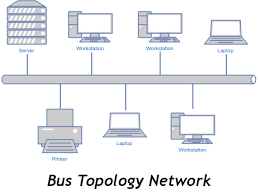
إن هذا النوع هو من الأنواع المعروفة حيث انه يعتمد على اتصال الجهاز أتوماتيكيا بالجهاز الذي قبله والجهاز الذي بعده ويكون هذا الاتصال مباشر حيث انه يكون مشكل في صورة دائرة مغلقة وهذا يكون في اتجاه واحد.



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.

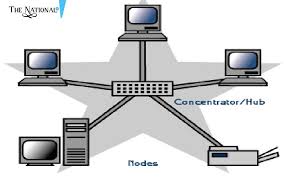


الشكل (7) الخطي

:2-3-3نجمية (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.

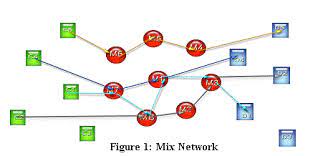
وهي شبكه تستخدم في الشبكة (LAN)



الشكل (8) النجمي

:2-3-4مختلطة 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

**:2-4فوائد الشبكات:**

* تستطيع نقل الملفات من وإلى الشركاء في مواقع مختلفة، أو الدخول إلى شبكة الشركة من المنزل أو من أي مكان في العالم.
* تستطيع إجراء عملية النسخ الاحتياطي بشكل تلقائي وكامل وبذلك توفر الوقت وتضمن بأن كل عملك آمن.
* تخفيض تكلفة الموارد؛ فعند ارتباط أجهزة الحاسوب من خلال الشبكة فإنه يمكنها مشاركة الموارد المختلفة مثل الطابعات، وأنظمة التشغيل والبرامج، وغيرها.
* زيادة مساحة التخزين؛ حيث يتم تخزين البيانات في مساحة ضخمة مُشتركة، مثل خادم مركزي (central server).

**:2-5أصناف عناوين IP:**

:2-5-1تعريف 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 IP  مكون من 4 ثمانيات Octet  كما نعلم، و هذا العنوان بعض خاناته تستخدم كمعرف للشبكة المحلية بينما الخانات الأخرى تستخدم كمعرف للمستخدم داخل الشبكة.  
يتألف ال IP من عنوان الشبكة المحلية و عنوان الجهاز داخل الشبكة ذاتها ( لأنه قد لا يكون الوحيد على الشبكة فمن الممكن أن يكون هناك أشخاص آخرين متواجدين معه )

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

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

إن كل ثُمانية مكونة من 8 خانات ثنائية ( 0 أو 1 ) و أن كل ثُمانية يمكنها العد من 0 الى 255 أي 256 احتمال أو تشكيل.

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

Network ID  Host ID

معرف الشبكة يأتي أولا ( على اليسار ) و بعده يأتي معرف المستخدم ( على اليمين ).

الآن يمكن لأي شخص أن يستخدم الثُمانية الأولى Octet1 فقط كي يرقم الشبكات المحلية في المؤسسة أو الشركة بينما يستخدم باقي الثُمانيات ( الثانية و الثالثة و الرابعة ) لترقيم الأجهزة أو المستخدمين داخل كل شبكة و بهذا سيكون لديه عدد كبير من المستخدمين مقابل عدد قليل من الشبكات المحلية.

أو يمكنه فعل العكس فقد يستخدم الثمانية الأولى و الثانية و الثالثة لترقيم الشبكات المحلية في المنشأة بينما يستخدم الثمانية الأخيرة الرابعة Octet4 فقط لترقيم المستخدمين داخل كل شبكة و هذه الطريقة توفر عدد كبير من الشبكات المحلية مقابل عدد أصغر للمستخدمين في كل شبكة.  
يمكن ان نستخدم الثمانية الأولى و الثانية Octet1 , Octet2 كي يرقم الشبكات Octet3 , Octet4 كي يرقم المستخدمين داخل كل شبكة و بهذا سيحصل على عدد متساوي من الشبكات المحلية و المستخدمين لأن طول الجزء المخصص لكل منهما متساوٍ.

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 |

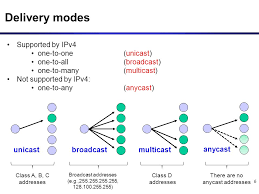
الجدول(1) IPv4

5-2-:2 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

3-5-2: تعريف الIPv6:

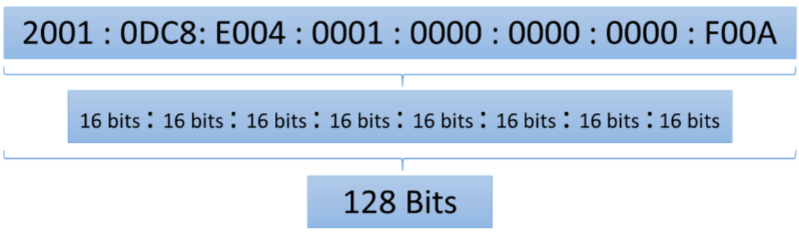
هو أحد إصدارات بروتوكول الإنترنت (IP) الذي يوفر مساحة عناوين IP أكبر لمستخدمي الإنترنت. الميزة الأساسية في IPv6 أنه يقوم بزيادة حجم العنوان من ٣٢ بت معيار IPv4 إلى ١٢٨ بت. من الممكن أن يدعم عنوان IP الذي يبلغ حجمه 128 بت عددًا كبيرًا من العناوين حتى في حالة تعيين العنوان بشكل غير فعال. ويسمح هذا بعدد أكبر من العناوين ونقاط التوصيل عما هو متوفر في IPv4 كما يوفر IPv6 المزيد من الأساليب لإعداد العنوان وتكوينًا تلقائيًا أكثر سهولة.

بشكل افتراضي، يتم تكوين IPv6 تلقائيًا، وتكون الإعدادات الافتراضية كافية للغالبية العظمى من أجهزة الكمبيوتر التي تحتاج إلى استخدام .

الإصدار 6 من بروتوكول الإنترنت (IPv6) هو أحدث إصدار من بروتوكول الإنترنت (IP) ، وهو بروتوكول الاتصالات الذي يوفر نظام تحديد الهوية والموقع لأجهزة الكمبيوتر الموجودة على الشبكات وتوجيه حركة المرور عبر الإنترنت.

يتم تخصيص عنوان IP فريد للأجهزة الموجودة على الإنترنت لتحديد الهوية وتحديد الموقع. مع النمو السريع للإنترنت بعد التسويق التجاري في التسعينيات ، أصبح من الواضح أنه ستكون هناك حاجة إلى عدد أكبر بكثير من العناوين لتوصيل الأجهزة أكثر من مساحة عنوان IPv4 المتاحة. يستخدم IPv6 عناوين 128 بت ، ما يقرب من 3.4 × 1038 عناوين إجمالية. الرقم الفعلي أصغر قليلاً ، حيث يتم حجز نطاقات متعددة للاستخدام الخاص أو مستبعدة تمامًا من الاستخدام. لم يتم تصميم البروتوكولين ليكونا قابلين للتشغيل البيني ، وبالتالي فإن الاتصال المباشر بينهما مستحيل ، مما يعقد الانتقال إلى IPv6. ومع ذلك ، فقد تم وضع العديد من آليات الانتقال لتصحيح ذلك.

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



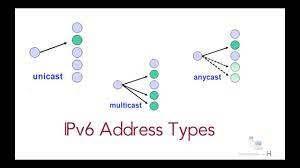
الشكل (11) IPv6

تم تعريف بنية العنونة الخاصة بـ IPv6 في RFC 4291 وتسمح بثلاثة أنواع مختلفة من الإرسال:

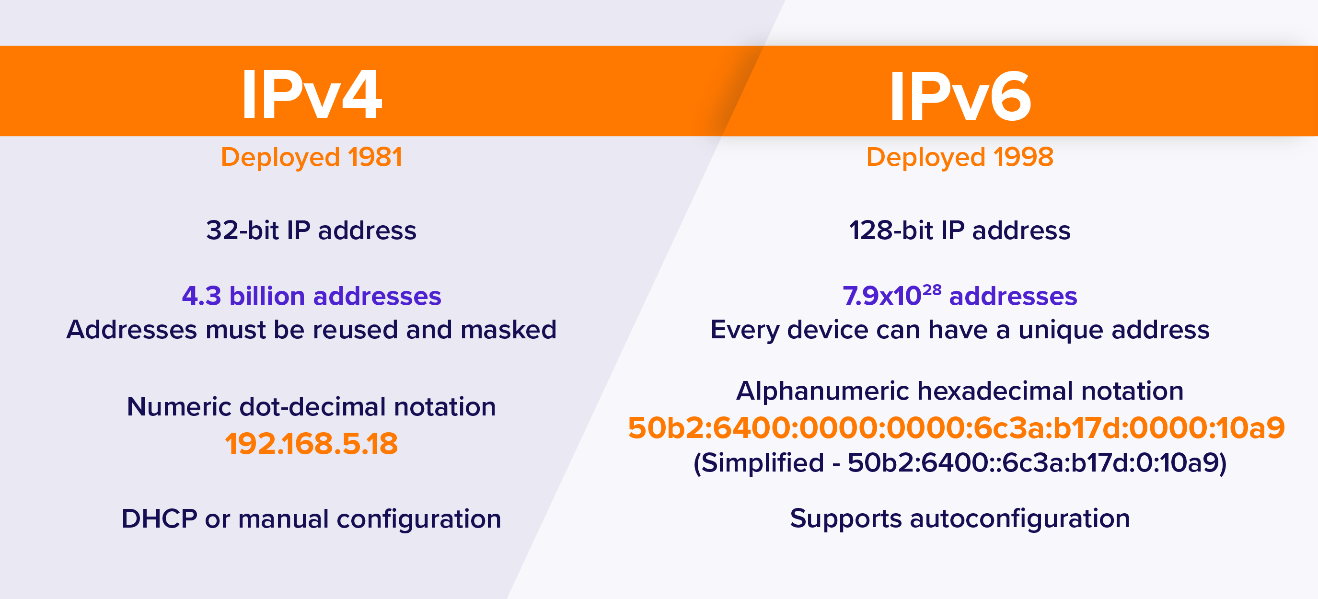
:Unicast هو نوع من الاتصال حيث يتم إرسال البيانات من كمبيوتر إلى كمبيوتر آخر.

: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

:2-6البروتوكولات المستخدمة في ال Application Layer:

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

الجدول(2) يعبر عن البروتوكولات المستخدمة

**:**2-6-1بروتوكول 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.

:2-6-2بروتوكول 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.

:2-6-3بروتوكول 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.

:2-6-4 بروتوكول نقل الملفات البسيط TFTP:

بروتوكول نقل الملفات البسيط (TFTP) هو بروتوكول بسيط لتبادل الملفات بين جهازي TCP / IP. تسمح خوادم TFTP بالاتصالات من عميل TFTP لإرسال الملفات واستلامها. يدعم بروتوكول TFTP عمليات إرسال الملفات واستلامها فقط. حذف الملف ونقله وإعادة تسميته غير مدعوم. نظرًا لقيوده ، يعد TFTP مكملاً لبروتوكول FTP العادي وليس بديلاً. يتم استخدامه فقط عندما تكون بساطته مهمة ، وافتقاره إلى الميزات أمر مقبول.

يمكن أيضًا استخدام خادم TFTP لتحميل صفحات HTML على خادم HTTP أو لتنزيل ملفات السجل على كمبيوتر بعيد. في هذه الحالة ، يجب استخدام مكون نظام الملفات ، ويجب تكوين خادم HTTP بشكل صحيح.

:2-6-5بروتوكول نقل النص التشعبي :(HTTP)

HTTP هو بروتوكول طبقة تطبيق يستخدم لأنظمة المعلومات الموزعة والتعاونية والوسائط التشعبية. إنه يعمل على نموذج خادم العميل ، حيث يعمل متصفح الويب كعميل. تتم مشاركة البيانات مثل النصوص والصور وملفات الوسائط المتعددة الأخرى عبر شبكة الويب العالمية باستخدام HTTP. كبروتوكول نوع الطلب والاستجابة ، يرسل العميل طلبًا إلى الخادم ، والذي تتم معالجته بعد ذلك بواسطة الخادم قبل إرسال استجابة مرة أخرى إلى العميل.

HTTP هو بروتوكول عديم الحالة ، مما يعني أن العميل والخادم على دراية ببعضهما البعض فقط بينما يكون الاتصال بينهما سليمًا. بعد ذلك ، ينسى كل من العميل والخادم وجود بعضهما البعض. بسبب هذه الظاهرة ، لا يمكن للعميل والخادم الاحتفاظ بالمعلومات بين الطلبات.

:2-6-6بروتوكول 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).

7-6-:2 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.

8-6-:2 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.

9-6-:2 بروتوكول إدارة الشبكة البسيط (SNMP):

SNMP هو بروتوكول طبقة تطبيق يستخدم لإدارة العقد ، مثل الخوادم ومحطات العمل والموجهات والمحولات وما إلى ذلك ، على شبكة IP. يمكّن SNMP مسؤولي الشبكة من مراقبة أداء الشبكة ، وتحديد مواطن الخلل في الشبكة ، واستكشاف الأخطاء وإصلاحها. يتكون بروتوكول SNMP من ثلاثة مكونات: جهاز مُدار ، ووكيل SNMP ، ومدير SNMP.

يوجد وكيل SNMP على الجهاز المُدار. الوكيل عبارة عن وحدة برمجية لديها معرفة محلية بمعلومات الإدارة ، ويترجم تلك المعلومات إلى نموذج متوافق مع مدير SNMP. يقدم مدير SNMP البيانات التي تم الحصول عليها من وكيل SNMP ، مما يساعد مسؤولي الشبكة على إدارة العقد بفعالية.

يوجد حاليًا ثلاثة إصدارات من SNMP v1 :SNMP و SNMP v2 و SNMP v3 يحتوي كلا الإصدارين 1 و 2 على العديد من الميزات المشتركة ، ولكن SNMP v2 يقدم تحسينات مثل عمليات البروتوكول الإضافية. يضيف الإصدار 3 من SNMP (SNMP v3) إمكانات الأمان والتكوين عن بُعد للإصدارات السابقة.

**الفصل الثالث - الأجهزة المستخدمة**

1-3: 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). شبكة LAN هي مجموعة من الأجهزة المتصلة التي تقتصر على منطقة جغرافية معينة. تتطلب شبكة LAN عادةً موجهًا واحدًا.



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.

2-3: المبدل (Switch):



الشكل (15)Switch

مبدل الشبكة (يُطلق عليه أيضًا مركز التبديل ، ولوحة الوصل ، وجسر MAC بواسطة IEEE) هو جهاز للشبكات يربط الأجهزة على شبكة الكمبيوتر باستخدام تبديل الحزمة لتلقي البيانات وإعادة توجيهها إلى الجهاز الوجهة.

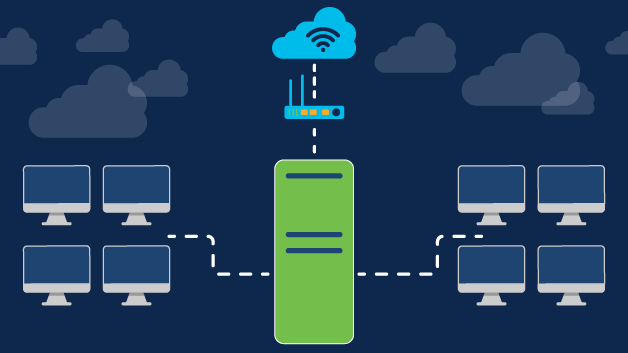
مبدل الشبكة هو جسر شبكة متعدد المنافذ يستخدم عناوين MAC لإعادة توجيه البيانات في طبقة ارتباط البيانات (الطبقة 2) لنموذج OSI. يمكن لبعض المحولات أيضًا إعادة توجيه البيانات في طبقة الشبكة (الطبقة 3) من خلال دمج وظائف التوجيه بشكل إضافي. تُعرف هذه المبدلات عمومًا باسم مفاتيح تبديل الطبقة 3 أو المفاتيح متعددة الطبقات.

محولات Ethernet هي أكثر أشكال تبديل الشبكة شيوعًا. تم اختراع أول جسر في عام 1983 بواسطة مارك كيمبف ، وهو مهندس في مجموعة تطوير الشبكات المتقدمة التابعة لشركة Digital Equipment Corporation. تم تقديم أول منتج جسر ثنائي المنفذ (LANBridge 100) بواسطة تلك الشركة بعد فترة وجيزة. أنتجت الشركة لاحقًا محولات متعددة المنافذ لكل من Ethernet و FDDI مثل GigaSwitch. قررت شركة Digital ترخيص براءة اختراع MAC Bridge الخاصة بها على أساس خالٍ من حقوق الملكية وغير تمييزي سمح بتوحيد IEEE. سمح هذا لعدد من الشركات الأخرى بإنتاج محولات متعددة المنافذ ، بما في ذلك كالبانا. كانت Ethernet في البداية وسيلة وصول مشتركة ، لكن إدخال جسر MAC بدأ في التحول إلى شكل نقطة إلى نقطة الأكثر شيوعًا دون مجال تصادم. توجد أيضًا المحولات لأنواع أخرى من الشبكات بما في ذلك القناة الليفية ووضع النقل غير المتزامن و InfiniBand.

بخلاف محاور إعادة الإرسال ، التي تبث نفس البيانات من كل منفذ وتسمح للأجهزة باختيار البيانات الموجهة إليها ، يتعرف مفتاح الشبكة على هويات الأجهزة المتصلة ثم يعيد توجيه البيانات فقط إلى المنفذ المتصل بالجهاز الذي هو عليه معالجة.

3-3: وحدة التحكم في الشبكة (Network Controller):

تم تطويره كبرنامج لتنظيم وظائف الشبكة ، تعمل وحدة التحكم في الشبكة كوسيط بين الأعمال والبنية التحتية للشبكة. عندما تدخل منظمة أهداف العمل المرغوبة في وحدة التحكم ، فإنها تنشئ الشبكة لتحقيق هذه الأهداف.

[](javascript:void(0);)

الشكل (16) Network Controller

كيف تعمل وحدات التحكم في الشبكة؟

وحدة تحكم الشبكة هي برنامج ينظم وظائف الشبكة. يعمل كوسيط بين الأعمال والبنية التحتية للشبكة. تدخل المنظمة أهداف العمل المرغوبة في وحدة التحكم والتي بدورها تنشئ الشبكة لتحقيق هذه الأهداف.

4-3: الخادم (Server):



الشكل (71) Servers

الخادم 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.

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



الشكل (81) Voip Phone

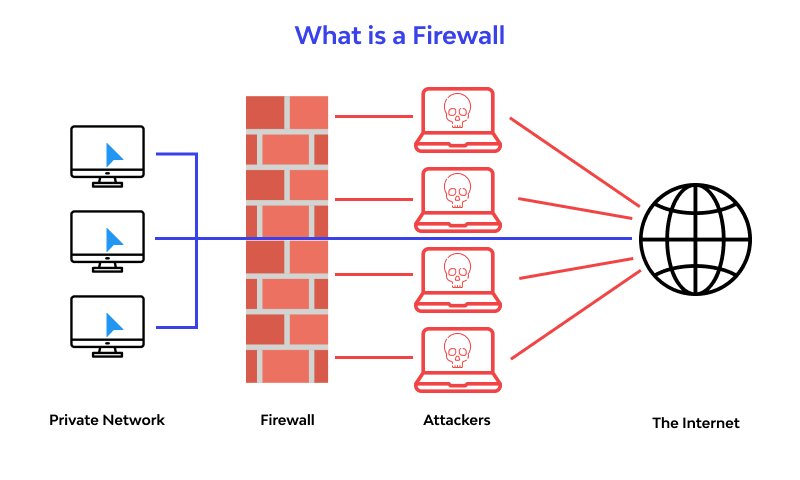
يشبه مزود هاتف VoIP إلى حد كبير شركة الهاتف التقليدية الخاصة بك من حيث أنه يدعم خطة الهاتف الخاصة بك ، ولكن مزود الهاتف VoIP (الصوت عبر بروتوكول الإنترنت) يتعامل مع المكالمات الهاتفية التي تحدث عبر اتصال الإنترنت ، بدلاً من خطوط الهاتف التقليدية. يمكنك الحصول على خطة مكالمات هاتفية وجهاز هاتف VoIP وأي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

ما هي ميزات هاتف VoIP الشائعة للأعمال؟

تتمتع هواتف VoIP بالعديد من ميزات VoIP الشائعة والشائعة للأعمال. تشمل ميزات هاتف VoIP الأكثر شيوعًا للأعمال التجارية البريد الصوتي المرئي ، وإعادة توجيه المكالمات ، وتوجيه المكالمات ، والوكلاء الظاهريون الأذكياء ، والمراسلة النصية للأعمال. يعتمد الأمر حقًا على احتياجات عملك لتحديد الميزات التي تريد التسوق من أجلها. تحقق من هذه القائمة الكاملة المكونة من 40 ميزة من أفضل ميزات VoIP لبدء قائمة رغباتك.

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 ، وليس عبر شبكة الهاتف العامة (PSTN) ، والمعروفة أيضًا باسم خدمة الهاتف القديم العادي (POTS).

3-6: 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.

كيف يعمل جدار الحماية؟

تقوم جدران الحماية بتحليل حركة المرور الواردة بعناية استنادًا إلى القواعد المحددة مسبقًا وتصفية حركة المرور القادمة من مصادر غير آمنة أو مشبوهة لمنع الهجمات. تحرس جدران الحماية حركة المرور عند نقطة دخول الكمبيوتر ، والتي تسمى المنافذ ، حيث يتم تبادل المعلومات مع الأجهزة الخارجية. على سبيل المثال ، يُسمح "لعنوان المصدر 172.18.1.1 بالوصول إلى الوجهة 172.18.2.1 عبر المنفذ 22.

مثلا عناوين IP كمنازل ، وأرقام المنافذ كغرف داخل المنزل. يُسمح فقط للأشخاص الموثوق بهم (عناوين المصدر) بالدخول إلى المنزل (عنوان الوجهة) على الإطلاق - ثم تتم تصفيته أكثر بحيث يُسمح للأشخاص داخل المنزل فقط بالوصول إلى غرف معينة (منافذ الوجهة) ، اعتمادًا على ما إذا كانوا المالكين أو طفل أو ضيف. يُسمح للمالك بالدخول إلى أي غرفة (أي منفذ) ، بينما يُسمح للأطفال والضيوف بدخول مجموعة معينة من الغرف (منافذ محددة).

يمكن أن تكون جدران الحماية عبارة عن برامج أو أجهزة ، على الرغم من أنه من الأفضل أن يكون لديك كلاهما. جدار حماية البرنامج هو برنامج يتم تثبيته على كل كمبيوتر وينظم حركة المرور من خلال أرقام المنافذ والتطبيقات ، بينما جدار الحماية الفعلي هو جزء من المعدات المثبتة بين شبكتك والبوابة.

تقوم جدران الحماية التي تعمل بفلترة الحزم ، وهي أكثر أنواع جدار الحماية شيوعًا ، بفحص الحزم وتمنعها من المرور إذا لم تتطابق مع مجموعة قواعد أمان محددة. يتحقق هذا النوع من جدار الحماية من عناوين IP لمصدر ووجهة الحزمة. إذا كانت الحزم تتطابق مع تلك الخاصة بقاعدة "مسموح بها" على جدار الحماية ، فمن الوثوق بالدخول إلى الشبكة.

تنقسم جدران الحماية لتصفية الحزم إلى فئتين: ذات حالة وعديمة الحالة. تقوم جدران الحماية عديمة الحالة بفحص الحزم بشكل مستقل عن بعضها البعض وتفتقر إلى السياق ، مما يجعلها أهدافًا سهلة للقراصنة. في المقابل ، تتذكر جدران الحماية ذات الحالة الخاصة المعلومات حول الحزم التي تم تمريرها سابقًا وتعتبر أكثر أمانًا.

بينما يمكن أن تكون جدران الحماية لتصفية الحزم فعالة ، فإنها توفر في النهاية حماية أساسية جدًا ويمكن أن تكون محدودة للغاية على سبيل المثال ، لا يمكنها تحديد ما إذا كانت محتويات الطلب الذي يتم إرساله ستؤثر سلبًا على التطبيق الذي يصل إليه. إذا كان الطلب الخبيث الذي تم السماح به من عنوان مصدر موثوق يؤدي .

7-3: 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.

1-7-3: الأنواع التي تستخدمها وحدات التحكم الفعلية:

1- نشر مركزي:

النوع الأكثر شيوعًا من أنظمة الشبكات اللاسلكية ، 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.

2- التوزيع الموزع:

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.

8-3: نقطة الوصول(Access Point) :



الشكل (21)Access Point

لقد تحسنت تقنية WiFi بشكل كبير في السنوات الأخيرة ، ولكنها ليست مقاسًا واحدًا يناسب الجميع ، لا سيما عندما يتعلق الأمر بالأعمال التجارية. عادةً ما تستخدم المساحات المكتبية الكبيرة ذات حركة المرور الكثيفة نقاط وصول WiFi ، بينما من المرجح أن تحتوي المكاتب الصغيرة ذات المستخدمين المحدودين على أجهزة توجيه WiFi وموسعات النطاق. دعنا نلقي نظرة على كيفية مقارنة ميزاتها للعثور على أفضل حل WiFi لك.

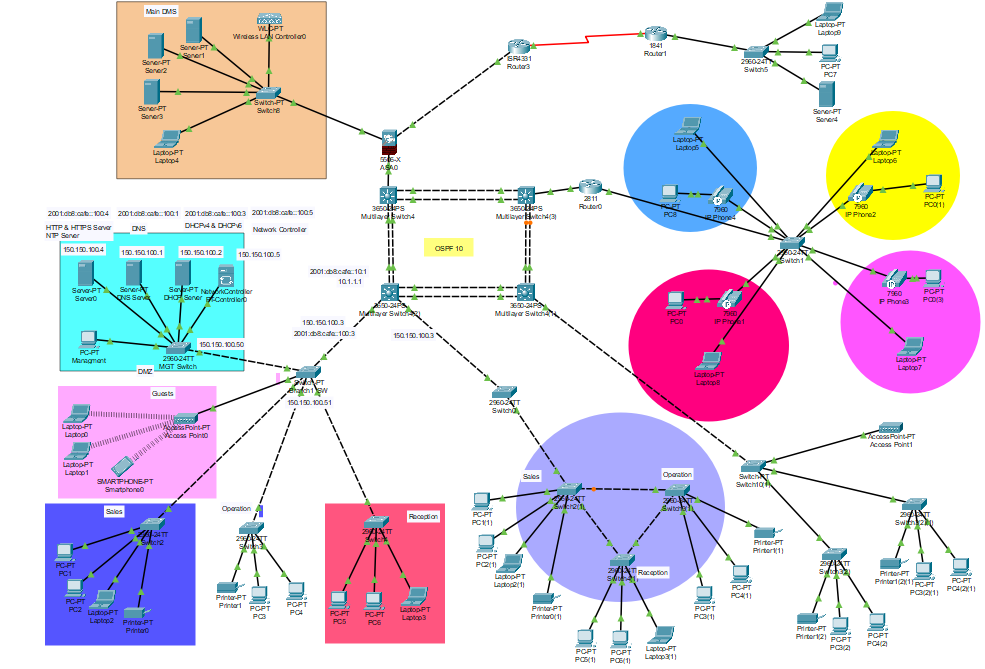
نقطة الوصول هي جهاز يقوم بإنشاء شبكة محلية لاسلكية ، أو WLAN ، عادة في مكتب أو مبنى كبير. تتصل نقطة الوصول بجهاز توجيه أو مفتاح أو محور سلكي عبر كابل Ethernet ، وتعرض إشارة WiFi إلى منطقة معينة. على سبيل المثال ، إذا كنت ترغب في تمكين وصول WiFi في منطقة الاستقبال الخاصة بشركتك ولكن ليس لديك جهاز توجيه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

1-8-3: مزايا استخدام نقاط الوصول اللاسلكية:

* يمكن تثبيت نقاط الوصول على مستوى الأعمال في أي مكان يمكنك فيه تشغيل كبل Ethernet. تتوافق الطرز الأحدث أيضًا مع Power over Ethernet Plus أو +PoE (مزيج من Ethernet وسلك الطاقة) ، لذلك ليست هناك حاجة لتشغيل خط طاقة منفصل أو تثبيت منفذ بالقرب من نقطة الوصول.
* تشمل الميزات القياسية الإضافية دعم البوابة المقيدة وقائمة التحكم في الوصول (ACL) ، بحيث يمكنك تقييد وصول الضيف دون المساس بأمان الشبكة ، بالإضافة إلى إدارة المستخدمين بسهولة داخل شبكة WiFi الخاصة بك.
* تتضمن نقاط الوصول المحددة ميزة التجميع وهي نقطة واحدة يمكن لمسؤول تكنولوجيا المعلومات من خلالها عرض شبكة WiFi ونشرها وتكوينها وتأمينها ككيان واحد بدلاً من سلسلة من تكوينات نقطة الوصول المنفصلة.

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

:Commands :4-1



**الفصل الخامس - الاستنتاجات والعمل المستقبلي**

1-5 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.

2-5 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.

**Key Words**

**http:**

فهرس عملي

**References المراجع**

1. [https://www.almrsal.com/](C:\\Users\\E\\AppData\\Roaming\\Microsoft\\Word\\ip address شرح | المرسال (almrsal.com)" \o "https://www.almrsal.com/)
2. <https://wikiarab.com/>
3. [ما هي أنواع شبكات الحاسوب والانترنت types of networks (safaaemam.com)](https://www.safaaemam.com/2022/01/types-of-networks.html#:~:text=%D8%A3%D9%86%D9%88%D8%A7%D8%B9%20%D8%A7%D9%84%D8%B4%D8%A8%D9%83%D8%A7%D8%AA%20%D8%AD%D8%B3%D8%A8%20%D8%A7%D9%84%D9%85%D8%B3%D8%A7%D8%AD%D8%A9%20%D8%A7%D9%84%D8%AA%D9%8A%20%D8%AA%D8%BA%D8%B7%D9%8A%D9%87%D8%A7%20%D8%AA%D9%86%D9%82%D8%B3%D9%85%20%D8%A5%D9%84%D9%8A,Network%203%20%D8%A7%D9%84%D8%B4%D8%A8%D9%83%D8%A7%D8%AA%20%D8%A7%D9%84%D9%88%D8%A7%D8%B3%D8%B9%D8%A9%20WAN%3D%3E%20Wide%20Area%20Networks)
4. [Subcarriers: أصناف عناوين الـ IP](https://subcarriers.blogspot.com/2013/12/ip.html)
5. [Application layer protocols | Various Protocols of Applications layers (educba.com)](https://www.educba.com/application-layer-protocols/)
6. <https://www.cisco.com/>
7. <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-network-controller.html#~faqs>
8. <https://www.techtarget.com/whatis/definition/server>
9. https://www.forcepoint.com/cyber-edu/firewall