الجمهورية العربية السورية

جامعة قرطبة الخاصة

هندسة الاتصالات

تصميم شبكة ربط لجامعة قرطبة فرع حلب و القامشلي

الدكتور المشرف:

د.يوسف بياع د.محمد رواس

تقدمة الطالبان:

محمد بنيان مسلاتي صابوني عمر خالد عبدالحميد

إهداء

من عینیه الهادئتین ونظراته العمیقة شعرنا بالأمان والحكمة....

إلى قدوتي ومصدر قوتي في هذه الحیاة....

إلى من أحمل اسمه بكل افتخار....

إلى الذي أعطى وما ازل یعطي حب ا ودعم ا ....

إلى من أدین له ما حییت وسأقدم لسعادته ما أستطیع....

إلى الأسطورة والحقیقة....

أبي

إلى من حاكت سعادتي بخیوط منسوجة من قلبها....

إلى من أقف حائرة أمامها ولا أدري بماذا أكافئها....

إلى من أعطت كل شيء حتى ركع العطاء أمام قدمیها....

إلى من دع واتها سر نجاحي ورضاها غایتي في حیاتي....

إلى الغالیة التي أرى الأمل من عینیها....

هل یستطیع أحد أن یشكر الشمس لأنها أضاءت الدنیا...؟

إلى حبیبة قلبي الأولى

أمي

إلى شركاء طفولتي وشبابي

إلى الشموع المضیئة في سماء حیاتي إلى الذین قاسموني حبهم لأهدیهم قلبي إلى من نمت أحلامي في عیونهم وكبرت في قلوبهم

اخوتي وأخواتي

تذوقت معهم أجمل اللحظات...

من شاركوني وساندوني كل فكرة حتى غدت حقیقة ولم یتقاعسوا عن دعمي عندما احتجتهم

إلى من شاركني مشوار العلم إلى كل من أحببت إلى الذین أناروا أمامي طریق المستقبل

أصدقائي وزملائي

الفهرس

* الملخص
* الفصل الأول – مدخل الى المشروع
  + 1.1 المقدمة
  + 1.2 أهداف المشروع
* الفصل الثاني – الدراسة النظرية
  + 2.1 تعريف الشبكات
  + 2.2 أصناف الشبكات
    - 2.2.1 الشبكات المحليةLAN
    - 2.2.2 الشبكات الإقليمية MAN
    - 2.2.3 الشبكات بعيدة أو طويلة المدى WAN
    - 2.2.4 الشبكات الشخصية
  + 2.3 أنواع الشبكات
    - 2.3.1 الحلقي (Ring)
    - 2.3.2 الخطي (Bus)
    - 2.3.3 نجمية (Star)‏
    - 2.3.4 مختلطة Mix)‏(
  + 2.4 فوائد الشبكات
  + 2.5 Mac address
  + 2.6 أصناف Address IP
    - 1.6.2 تعريف الIPv4
      * 1.1.6.2 Private IP
      * 2.1.6.2 Public IP
      * 3.1.6.2 Reserved IP
    - 2.6.2 تعريف الIPv6
      * 1.2.6.2 الخصائص الرئيسية
    - 3.6.2 مقارنة IPv6مع IPv4
  + 2.7 أنواع وصلات الشبكة
    - 1.7.2 Straight
    - 2.7.2 Cross over
    - 3.7.2 Rollover
* الفصل الثالث - دراسة الأجهزة المستخدمة
  + 1.3 الموجه Router
  + 2.3 المبدل Switch
  + 3.3 وحدة تحكم الشبكة Network Controller
  + 4.3 الخادم Server
  + 5.3 هاتف نقل الصوت عبر الإنترنت Voice over IP
  + 6.3الجدار الناريFirewall
    - 1.6.3 تعريف جدار الحماية
    - 2.6.3 أنواع جدران الحماية
  + 7.3 نقطة الوصولAccess Point (AP)
  + 8.3 Meraki Server
    - 1.8.3 تعريف المصطلحات
* الفصل الرابع - دراسة البروتوكولات المستخدمة
  + 1.4البروتوكولات المستخدمة في ال Application Layer
    - DHCP 1.1.4بروتوكول التكوين الديناميكي
    - DNS 2.1.4بروتوكول نظام اسم المجال
    - 3.1.4 بروتوكول نقل الملفاتFTP
    - 4.1.4 بروتوكول TFTP
    - 5.1.4 بروتوكول HTTP
    - 6.1.4 بروتوكول HTTPS
    - 7.1.4 بروتوكول نقل البريدSMTP
    - 8.1.4 بروتوكول مضاهاة المحطة الطرفيةTelnet
    - 9.1.4 بروتوكول إدارة الشبكة البسيط SNMP
* الفصل الخامس - الدراسة العملية
  + 1.5 المشاكل التي واجهت المشروع
  + 2.5 الحلول المقترحة
  + 1.2.5 استخدام بروتوكول FTP
  + 2.2.5 استخدام بروتوكول HTTPS
  + 3.5 مخطط Flow chart
* الأهداف المستقبلية
* المراجع References

\

الملخص:

يهدف هذا المشروع إلى تصميم شبكة تربط بين فرعي جامعة قرطبة الخاصة حلب و القامشلي عن طريق انشاء قناة افتراضية و تشفير البيانات المارة من خلالها و تنظيم عملية مشاركة البيانات بين المستخدمين و توحيد مكان تخزين المعلومات و السماح للمستخدمين من الوصول الى المعلومات المصرحة لهم بسهولة و سرعة و سرية بالاضافة الى جعل موقع الجامعة يستخدم بروتوكول الHTTPS بدلا من بروتوكول الHTTP وذلك لمنع أي عملية اختراق لموقع الجامعة او أي عملية تنصت على المعلومات المدخلة من قبل المستخدمين.



**الفصل الأول مدخل الى المشروع**

|  |  |
| --- | --- |
| * **المقدمة** | * **أهداف المشروع** |

مقدمة: 1.1

انتشرت الشبكات بكل مناحي المعلومات فسيطرت على المجالات الاقتصادية والفنية والتعليمية والعسكرية وغيرها؛ هذه السيطرة والأهمية بعود لربطها العالم ببعضه البعض . مما أتاح وسرعة 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 والتصنت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة.

يهدف المشروع إلى رفع المستوى الأمني و ربط بين فرعي جامعة قرطبة بين حلب و القامشلي عن طريق تطبيق مجموعة من البروتوكولات والتقنيات التي تستخدم لزيادة المستوى الأمني للجامعة وبالتالي رفع نسبة الحماية فيها بشكل كبير من الاختراقات التي تعطلها عن مهامها وأعمالها . أو أعمال التجسس على الإعدادات وكلمات المرور . وعدم السماح لكافة المستخدمين داخل هذه الشركة بالحصول على الأذونات في التحكم\ أو تغيير الإعدادات أو الضبط وبالتالي تكون صلاحياتهم محصورة.

أهداف المشروع: 2.1

ربط فرعي جامعة قرطبة حلب و القامشلي.

انشاء قناة خاصة لنقل البيانات بين الفرعين.

تشفير جميع البيانات المارة ضمن القناة.

تنظيم عملية مشاركة البيانات بين المستخدمين

تنظيم عملية مشاركة البيانات بين المستخدمين

جعل موقع الجامعة أكثر حماية باستخدام بروتوكول الHTTPS .



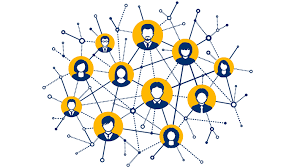
**الفصل الثاني الدراسة النظرية**

|  |  |
| --- | --- |
| * **تعريف الشبكات** | * **Mac address** |
| * **أصناف الشبكات** | * **أصناف IP address** |
| * **أنواع الشبكات** | * **أنواع وصلات الشبكة** |
| * **فوائد الشبكات** |

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.

يبين الشكل التالي الشبكة:



الشكل (2-1)

22. أصناف الشبكات :Scope 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. الشبكات المحلية LAN (Local Area Networks)
2. الشبكات الإقليمية MAN (Metropolitan Area Network)
3. الشبكات الواسعة WAN (Wide Area Networks)
4. الشبكات الشخصية :Personal Area Network

21.2. 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

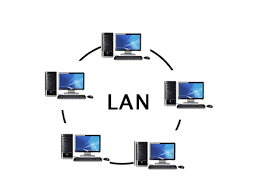
تستخدم شبكات LAN في محيط التجارة والأعمال حيث يكون هناك ارتباط بين عدة أجهزة للعمل بصورة تعاونية مثل شبكة المعلومات داخل ورش العمل داخل مصنع أو بنك حيث يكون هناك جهاز واحد له سعة تخزينية فائقة وسرعة عالية جدا يسمى server ومجموعة من الأجهزة الفرعية تسمى clients .   
عادة لدى الشبكات المحلية LAN معدلات 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.

يبين الشكل التالي شبكة LAN:



الشكل (2-2)

22.2. الشبكات الحضرية أو المدنية :Metropolitan Area Network

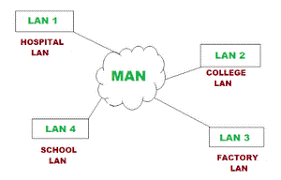
هي تكون شبكات متوسطة أي بمعنى أدق أنها تقوم بتغطية مناطق متوسطة المساحة مثل تغطية مدنية على سبيل المثال فهي تكون أكبر من الشبكات المحلية وأصغر من الشبكات طويلة المدى.

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.

**مثال على ذلك:**  
يمكن ربط البنوك الموجودة في مدينة ما من خلال ربط بنوك كل مقاطعة في شبكة LAN ثم ربط شبكات LANs لتكوين شبكة .MAN

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.

يبين الشكل التالي شبكة MAN:



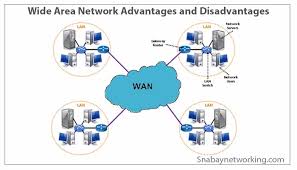
الشكل (2-3)

3.2.2شبكات 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.  
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.

يبين الشكل التالي شبكة WAN

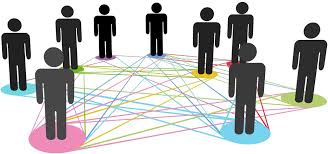


الشكل (2-4)

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.

يبين الشكل التالي الشبكة الشخصية:



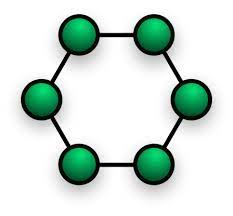
الشكل (2-5)

3.2أنواع الشبكات:

1.3.2  الحلقيRing :

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.

يبين الشكل التالي الشكل الحلقي:

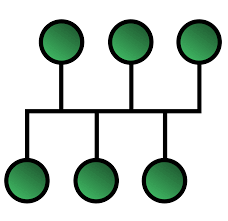


الشكل (2-6)

2.3.2  الخطي 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.

يبين الشكل التالي الشكل الخطي:

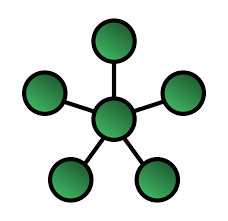


الشكل (2-7)

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.

يبين الشكل التالي الشكل النجمي:

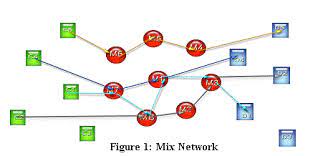


الشكل (2-8)

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.

يبين الشكل التالي الشكل المختلطة:



الشكل (2-9)

**4.2فوائد 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).

**:Mac address 5.2**

هو معرف فريد يتم تعيينه لوحدة تحكم واجهة الشبكة(NIC) لاستخدامه كعنوان شبكة في الاتصالات داخل قطاع الشبكة.

يتم تعيين عناوين MAC بشكل أساسي من قبل الشركات المصنعة للأجهزة وبالتالي يشار إليها غالبًا باسم العنوان المنسوخ أو كعنوان جهاز Ethernet ، أو عنوان الجهاز أو العنوان الفعلي.

يمكن تخزين كل عنوان في الأجهزة مثل ذاكرة البطاقة للقراءة فقط ، أو بواسطة آلية البرامج الثابتة.

**6.2أصناف عناوين IP:**

1.6.2تعريف ال**IPv4:**

الـ  IPيوفر عدد هائل من العناوين فالأصدار 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 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 Class A.

Network . Host . Host . Host

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

Network . Network . Host . Host

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

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

1.1.6.2مجالات الأصناف Classes:

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

|  |  |  |
| --- | --- | --- |
|  |  | الجدول(1) IPv4 |

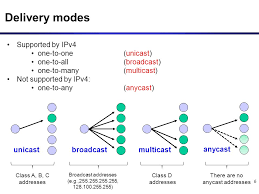
2.1.6.2 أنواع ارسال البيانات في الشبكة IPv4 :

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.

يبين الشكل التالي الشكل أنواع ارسال البيانات IPv4:



الشكل (2-10)

Private IP 1.6.1.1:

تحتوي أجهزة التوجيه المنزلية على عنوان IP عام، ولكن يقوم مزود خدمة الإنترنت أيضًا بتعيين رقم عنوان IP خاص للجهاز. يُشار إليه أيضًا باسم عنوان IP المحلي.

:Public IP 2.6.1.1

عندما تحصل على جهاز توجيه لشبكتك المنزلية ، فإن مهمة مزود خدمة الإنترنت (ISP) هي تعيين عنوان IP عام لها. يمكن الوصول إلى هذا العنوان مباشرة من بقية الإنترنت.

الحصول على عنوان IP عام يشبه الحصول على رقم الصندوق بدلاً من استخدام عنوان منزلك. إنه أكثر أمانًا إلى حد ما ويمنع الأشخاص من معرفة عنوانك الحقيقي.

:Reserved IP 3.6.1.1

ضمن بنية عناوين الإنترنت، حجزت فرقة عمل هندسة الإنترنت (IETF) وهيئة الأرقام المخصصة للإنترنت(IANA) العديد من عناوين بروتوكول الإنترنت (IP) لأغراض خاصة.

بشكل عام، لا يتم استخدام عناوين IP المحجوزة لبناء شبكة الإنترنت الأساسية، ونتيجة لذلك، لا يتم نقلها عبر الإنترنت. يمكن استخدامها فقط على شبكة خاصة أو جهاز كمبيوتر محلي.

2.6.2تعريف 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. تم تطوير IPv6 من قبل فريق هندسة الإنترنت (IETF) للتعامل مع المشكلة التي طال انتظارها لاستنفاد عنوان IPv4 ، ويهدف إلى استبدال IPv4. في ديسمبر 1998 ، أصبح IPv6 مسودة معيار لـ IETF ، والذي صدق عليه لاحقًا كمعيار إنترنت في 14 يوليو 2017.

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. بحلول عام 1998 ، قامت IETF بإضفاء الطابع الرسمي على البروتوكول التالي. يستخدم IPv6 عناوين 128 بت ، مما يسمح نظريًا بـ 2128 ، أو 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.

يوفر IPv6 مزايا تقنية أخرى بالإضافة إلى مساحة عنونة أكبر. على وجه الخصوص ، يسمح بطرق تخصيص العنوان الهرمي التي تسهل تجميع المسارات عبر الإنترنت ، وبالتالي تحد من توسيع جداول التوجيه. يتم توسيع وتبسيط استخدام عنونة الإرسال المتعدد ، ويوفر تحسينًا إضافيًا لتقديم الخدمات. تمت مراعاة جوانب تنقل الجهاز وأمنه وتكوينه في تصميم البروتوكول.

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

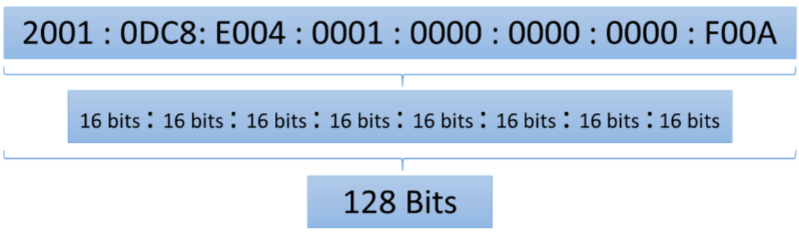
**1.2.6.2الخصائص الرئيسية:**

مسرد المصطلحات المستخدمة لعناوين IPv6

IPv6 هو بروتوكول طبقة الإنترنت للعمل على الإنترنت بتبديل الحزمة ويوفر نقل مخطط البيانات من طرف إلى طرف عبر شبكات IP متعددة ، مع الالتزام الوثيق بمبادئ التصميم التي تم تطويرها في الإصدار السابق من البروتوكول ، الإصدار 4 من بروتوكول الإنترنت (IPv4).

بالإضافة إلى تقديم المزيد من العناوين ، يقوم IPv6 أيضًا بتنفيذ ميزات غير موجودة في IPv4. فهو يبسط جوانب تكوين العنوان ، وإعادة ترقيم الشبكة ، وإعلانات جهاز التوجيه عند تغيير موفري اتصال الشبكة. يبسط معالجة الحزم في أجهزة التوجيه من خلال وضع مسؤولية تجزئة الحزمة في نقاط النهاية. يتم توحيد حجم الشبكة الفرعية لـ IPv6 عن طريق تثبيت حجم جزء معرف المضيف الخاص بالعنوان على 64 بت.

يبين الشكل التالي الشكل IPv6:



الشكل (2-11)

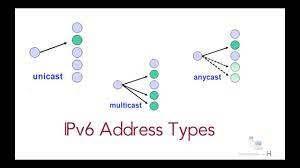
تم تعريف بنية العنونة الخاصة بـ IPv6 في RFC 4291 وتسمح بثلاثة أنواع مختلفة من الإرسال:

: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.

يبين الشكل التالي الشكل أنواع ارسال البيانات IPv6:



الشكل (2-12)

**3.6.2مقارنة IPv6مع IPv4:**

على الإنترنت ، يتم نقل البيانات في شكل حزم شبكة. يحدد IPv6 تنسيق حزمة جديد ، مصمم لتقليل معالجة رأس الحزمة بواسطة أجهزة التوجيه. نظرًا لاختلاف رؤوس حزم IPv4 وحزم IPv6 اختلافًا كبيرًا ، فإن البروتوكولين غير قابلين للتشغيل البيني. ومع ذلك ، فإن معظم بروتوكولات طبقة النقل والتطبيق تحتاج إلى القليل من التغيير أو لا تحتاج إلى أي تغيير لتعمل عبر IPv6 ؛ الاستثناءات هي بروتوكولات التطبيقات التي تضم عناوين طبقة الإنترنت ، مثل بروتوكول نقل الملفات (FTP) وبروتوكول وقت الشبكة (NTP) ، حيث قد يتسبب تنسيق العنوان الجديد في حدوث تعارض مع بنية البروتوكول الحالية.

**1.3.6.2مساحة عنوان أكبر**

الميزة الرئيسية لـ IPv6 عبر IPv4 هي مساحة العنوان الأكبر. حجم عنوان IPv6 هو 128 بت ، مقارنة بـ 32 بت في IPv4. وبالتالي فإن مساحة العنوان لها 2128 = 340،282،366،920،938،463،463،374،607،431،768،211،456 عنوانًا (حوالي 3.4 × 1038). بعض الكتل في هذه المساحة وبعض العناوين المحددة محجوزة لاستخدامات خاصة.

في حين أن مساحة العنوان هذه كبيرة جدًا ، لم يكن قصد مصممي IPv6 ضمان التشبع الجغرافي بعناوين قابلة للاستخدام. بدلاً من ذلك ، تعمل العناوين الأطول على تبسيط تخصيص العناوين ، وتمكين تجميع المسار الفعال ، والسماح بتنفيذ ميزات العنونة الخاصة. في IPv4 ، تم تطوير طرق التوجيه بين المجالات المعقدة (CIDR) لتحقيق أفضل استخدام لمساحة العنوان الصغيرة. الحجم القياسي للشبكة الفرعية في IPv6 هو 264 عنوانًا ، أي حوالي أربعة مليارات ضعف مساحة عنوان IPv4 بالكامل. وبالتالي ، سيكون استخدام مساحة العنوان الفعلي صغيرًا في IPv6 ، ولكن تم تحسين إدارة الشبكة وكفاءة التوجيه من خلال مساحة الشبكة الفرعية الكبيرة وتجميع المسار الهرمي.

**7.2 أنواع وصلات الشبكة:**

**1.7.2 Straight:**

وهو يكون بين جهازين مختلفين مثلاً : Pc + Switch أو Switch + Router و غيرها

ويكون الترتيب للأسلاك كالتالي :   
وهذه الألوان هي المتعارف عليها والتي تعمل بين جهاز الكمبيوتر والراوتر أو المودم:

1. ابيض برتقالى Tx
2. برتقالى Tx
3. ابيض أخضر Rx
4. ازرق
5. ابيض ازرق
6. اخضر Rx
7. ابيض بني
8. بني

ويوجد ترتيب مختلف عن ذلك بالنسبة للتوصيل  **Straight** ولكن هذا هو الشائع على ما اعتقد و اى ترتيب يجب مراعاه فيه رقم 1 و 2 و 3 و 6 حيث انهم هم المتخصصين فى استقبال ونقل البيانات.**DATA**

**2.7.2 Cross over:**

وهو لتوصيل جهازين متشابهين ببعض مثل ( **Router** + **Router** ) او غيرها وكذلك للدخول **Console**  على اى Devicesو ترتيبها كالتالى :

**الطرف الاول :**

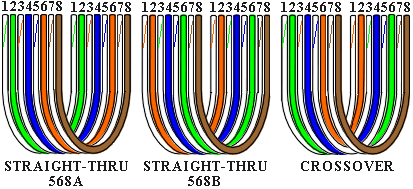
1. ابيض برتقالي Tx
2. برتقالى Tx
3. ابيض اخضر Rx
4. ازرق
5. ابيض ازرق
6. اخضر Rx
7. ابيض بنى
8. بنى

**الطرف الاخر :**

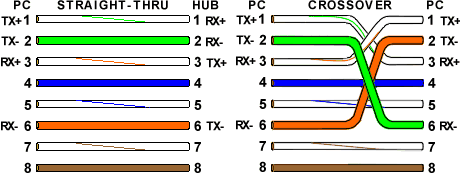
1. ابيض اخضر Rx
2. اخضر Rx
3. ابيض برتقالى
4. ازرق Tx
5. ابيض ازرق
6. برتقالى Tx
7. ابيض بنى
8. بنى

**3.7.2 Rollover:**

تُستخدم كبلات الrollover ، التي يشار إليها أحيانًا باسم كبلات Yost ، بشكل شائع للاتصال بمنفذ وحدة التحكم في الجهاز لإجراء تغييرات برمجية على الجهاز. على عكس الكابلات المتقاطعة والكابلات ذات الأسلاك المستقيمة ، لا يُقصد بكابلات التمرير لنقل البيانات ولكن بدلاً من ذلك إنشاء واجهة مع الجهاز.

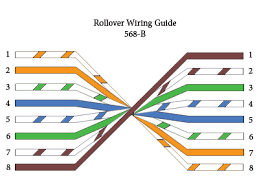
يبين الشكل التالي الشكل كبلات Straight and Crossover:[](https://www.hd-tch.com/%d8%a7%d9%86%d9%88%d8%a7%d8%b9-%d8%aa%d9%88%d8%b5%d9%8a%d9%84%d8%a7%d8%aa-%d9%83%d8%a7%d8%a8%d9%84-%d8%a7%d9%84%d8%b4%d8%a8%d9%83%d8%a9-utp/%d8%a7%d9%86%d9%88%d8%a7%d8%b9-%d8%a7%d9%84%d8%aa%d9%88%d8%b5%d9%8a%d9%84%d8%a7%d8%aa-%d9%84%d9%83%d9%8a%d8%a8%d9%84%d8%a7%d8%aa-%d8%a7%d9%84%d8%b4%d8%a8%d9%83%d8%a91/)

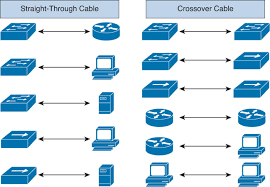
الشكل (2-13)

يبين الشكل التالي الشكلTx and Rx لكبلات Straight and Crossover:[](https://www.hd-tch.com/%d8%a7%d9%86%d9%88%d8%a7%d8%b9-%d8%aa%d9%88%d8%b5%d9%8a%d9%84%d8%a7%d8%aa-%d9%83%d8%a7%d8%a8%d9%84-%d8%a7%d9%84%d8%b4%d8%a8%d9%83%d8%a9-utp/%d8%a7%d9%86%d9%88%d8%a7%d8%b9-%d8%a7%d9%84%d8%aa%d9%88%d8%b5%d9%8a%d9%84%d8%a7%d8%aa-%d9%84%d9%83%d9%8a%d8%a8%d9%84%d8%a7%d8%aa-%d8%a7%d9%84%d8%b4%d8%a8%d9%83%d8%a9/)

الشكل (2-14)

يبين الشكل التالي الشكل Rollover:

الشكل (2-15) 

يبين الشكل التالي الشكل أنواع الوصل بين الأجهزة:

الشكل (2-16)



**الفصل الثالث دراسة الأجهزة المستخدمة**

|  |  |  |
| --- | --- | --- |
| * الموجه Router | * هاتف نقل الصوت عبر الإنترنت Voice over IP | |
| * المبدل Switch | * الجدار الناريFirewall | |
| * وحدة تحكم الشبكة Network Controller | * نقطة الوصولAccess Point (AP) | |
| * الخادم Server | * Meraki Server |

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.

يبين الشكل التالي الشكل Router:



الشكل (1-3)

جهاز التوجيه باعتباره جهاز تحكم في الحركة الجوية وحزم البيانات مثل الطائرات المتجهة إلى مطارات (أو شبكات) مختلفة. تمامًا كما أن لكل طائرة وجهة فريدة وتتبع مسارًا فريدًا ، يجب توجيه كل حزمة إلى وجهتها بأكبر قدر ممكن من الكفاءة. بنفس الطريقة التي يضمن بها مراقب الحركة الجوية وصول الطائرات إلى وجهاتها دون الضياع أو المعاناة من اضطراب كبير على طول الطريق ، 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.

2.3المبدل Switch:

يبين الشكل التالي الشكل Switch:



الشكل (2-3)

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.

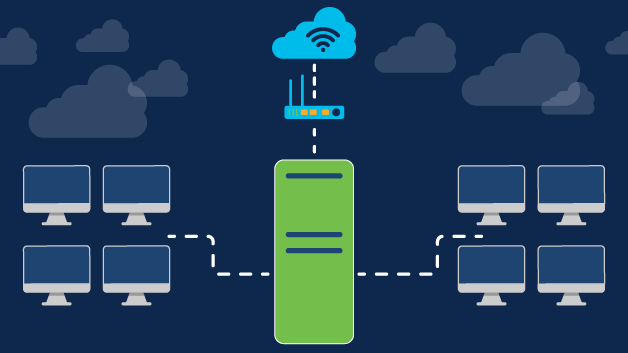
مبدل الشبكة هو جسر شبكة متعدد المنافذ يستخدم عناوين MAC لإعادة توجيه البيانات في طبقة ارتباط البيانات (الطبقة الثانية) لنموذج OSI. يمكن لبعض المحولات أيضًا إعادة توجيه البيانات في طبقة الشبكة (الطبقة الثالثة) من خلال دمج وظائف التوجيه بشكل إضافي. تُعرف هذه المبدلات عمومًا باسم مفاتيح تبديل الطبقة 3 أو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

3.3وحدة تحكم 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.

يبين الشكل التالي الشكل Network Controller:[](javascript:void(0);)

الشكل (3-3)

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.

يقوم مراقبو الشبكة بعملهم من خلال:

* الاحتفاظ بجرد للأجهزة في الشبكة وحالتها
* أتمتة عمليات الجهاز مثل التكوينات وتحديثات الصور.
* تحليل عمليات الشبكة وتحديد المشكلات المحتملة واقتراح الحلول.
* توفير منصة للتكامل مع التطبيقات الأخرى مثل أنظمة التقارير.

الشبكة هي شريان الحياة لأي منظمة حديثة. لا توفر الشبكة الاتصال الأساسي فحسب ، بل توفر أيضًا الأمان والتعاون المعزز والجودة واستمرارية الخدمة ، وما إلى ذلك. لذا فإن البنية والبنية التحتية وإدارة الشبكة تعتبر حيوية ومرتبطة بشكل متزايد بنجاح الأعمال.

تقوم وحدة التحكم في الشبكة بإدارة وتنظيم جميع جوانب الشبكة مع التأكد من أنها تعمل بشكل لا تشوبه شائبة وتؤدي إلى تحقيق أهداف العمل. لفهم دور وحدات التحكم هذه بشكل أفضل ، ضع في اعتبارك كيف تطورت إدارة الشبكة.

4.3الخادم Server:

يبين الشكل التالي الشكل Servers:



الشكل (4-3)

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.

الخوادم المادية والافتراضية:

الخادم المادي هو ببساطة جهاز كمبيوتر يتم استخدامه لتشغيل برنامج الخادم.

الخادم الافتراضي هو تمثيل افتراضي لخادم فعلي. مثل الخادم الفعلي ، يشتمل الخادم الافتراضي على نظام التشغيل والتطبيقات الخاصة به. يتم الاحتفاظ بها منفصلة عن أي خوادم افتراضية أخرى قد تعمل على الخادم الفعلي.

تتضمن عملية إنشاء أجهزة افتراضية تثبيت مكون برنامج خفيف الوزن يسمى برنامج Hypervisor على خادم فعلي. تتمثل مهمة المشرف الفائق في تمكين الخادم الفعلي من العمل كمضيف افتراضي. يجعل مضيف المحاكاة الافتراضية موارد أجهزة الخادم الفعلي - مثل وقت وحدة المعالجة المركزية والذاكرة والتخزين وعرض النطاق الترددي للشبكة - متاحة لجهاز ظاهري واحد أو أكثر.

تمنح وحدة التحكم الإدارية للمسؤولين القدرة على تخصيص موارد أجهزة محددة لكل خادم افتراضي. يساعد هذا في خفض تكاليف الأجهزة بشكل كبير لأن خادمًا ماديًا واحدًا يمكنه تشغيل عدة خوادم افتراضية ، على عكس كل حمل عمل يحتاج إلى خادم فعلي خاص به.

5.3هاتف نقل الصوت عبر الإنترنت Voice over IP:

يبين الشكل التالي الشكل VOIP Phone:



الشكل (5-3)

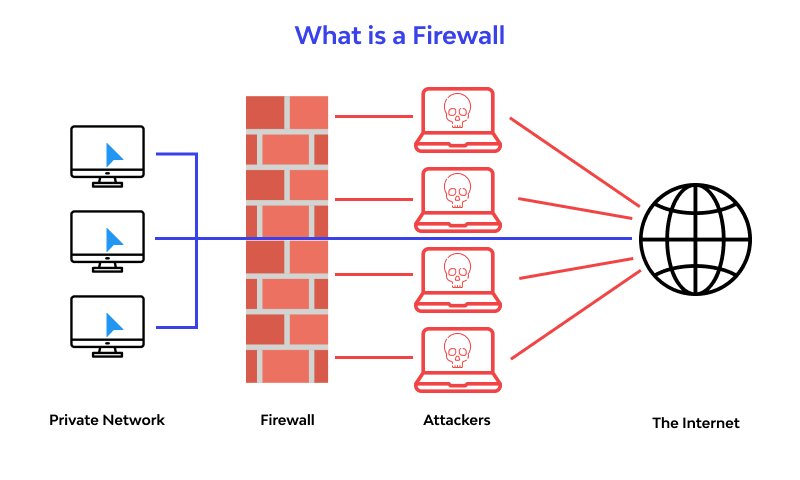
يشبه مزود هاتف VoIP إلى حد كبير شركة الهاتف التقليدية الخاصة بك من حيث أنه يدعم خطة الهاتف الخاصة بك ، ولكن مزود الهاتف VoIP (الصوت عبر بروتوكول الإنترنت) يتعامل مع المكالمات الهاتفية التي تحدث عبر اتصال الإنترنت ، بدلاً من خطوط الهاتف التقليدية. يمكنك الحصول على خطة مكالمات هاتفية وجهاز هاتف VoIP وأي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

يمكن لهاتف VoIP استقبال الرسائل النصية. أسهل طريقة لإرسال واستقبال الرسائل النصية على رقم هاتف VoIP الخاص بك هي استخدام تطبيق برمجي ، مثل NextivaONE. باستخدام NextivaONE ، يمكنك تحويل أي كمبيوتر أو جهاز محمول إلى هاتف يمكنه إجراء مكالمات أو إرسال واستقبال الرسائل النصية.

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.

6.3الجدار الناريFirewall :

يبين الشكل التالي الشكل Firewall:



الشكل (6-3)

1.6.3تعريف جدار الحماية:

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.

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).

2.6.3أنواع جدران الحماية:

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 ، على سبيل المثال ، إلى حذف قاعدة البيانات ، فلن يكون لجدار الحماية أي وسيلة لمعرفة ذلك. الجيل التالي من جدران الحماية وجدران الحماية الوكيل أكثر تجهيزًا لاكتشاف مثل هذه التهديدات.

7.3نقطة الوصولAccess Point (AP) :

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.

يبين الشكل التالي الشكل Access Point:



الشكل (7-3)

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.

كما يوحي اسمه ، يعمل موسع النطاق على إطالة مدى وصول شبكة WiFi الحالية. نظرًا لأن موسعات النطاق تتصل لاسلكيًا بأجهزة توجيه WiFi ، فيجب وضعها حيث تكون إشارة موجه WiFi قوية بالفعل ، وليس في موقع النقطة الميتة الفعلية. على سبيل المثال ، إذا كان جهاز التوجيه الخاص بك في الطابق السفلي من مبنى مكون من طابقين ، فإن تثبيت موسع النطاق في الطابق الأرضي (حيث لا تزال التغطية من جهاز توجيه WiFi قويًا) سيقضي على المناطق الميتة المحتملة في الطابق الثاني.

على الرغم من أن موسعات النطاق رائعة لشبكات WiFi المنزلية ، إلا أنها ليست فعالة للشركات الحديثة. هذا لأنه لا يمكنها دعم سوى عدد محدود من الأجهزة في وقت واحد ، لا يزيد عادةً عن 20. بينما تزيد موسعات النطاق من تغطية جهاز توجيه WiFi ، فإنها لا تزيد من عرض النطاق الترددي المتاح. اعتمادًا على عدد الأجهزة التي قمت بتوصيلها في وقت واحد ، يمكن أن ينتهي موسع النطاق بثقل اتصالك.

من ناحية أخرى ، يمكن لنقاط الوصول التعامل مع أكثر من 60 اتصالًا متزامنًا لكل منها. من خلال تثبيت نقاط الوصول في جميع أنحاء المكتب ، يمكن للمستخدمين التجول بحرية من غرفة إلى أخرى دون التعرض لانقطاعات في الشبكة. أثناء تنقلهم عبر المبنى ، تنتقل أجهزتهم بسلاسة من نقطة وصول إلى أخرى دون قطع الاتصال - لن يدركوا حتى أنهم يبدلون بين الشبكات.

مزايا استخدام نقاط الوصول اللاسلكية:

عندما يكون لديك موظفون وضيوف متصلون بأجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمولة والهواتف المحمولة والأجهزة اللوحية ، فإن 20 جهازًا على شبكة لاسلكية تضيف المزيد بسرعة. من خلال 60 اتصالاً متزامنًا لكل منها ، تمنحك نقاط الوصول الحرية في قياس عدد الأجهزة المدعومة على شبكتك. ولكن هذه ليست سوى واحدة من مزايا استخدام معززات الشبكة ضع في اعتبارك النقاط التالية:

* 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.

8.3Meraki Server :

Save translation

Cisco Meraki هي شركة تكنولوجيا معلومات مُدارة عبر السحابة ومقرها في سان فرانسيسكو ، كاليفورنيا. تشمل منتجاتها الشبكات اللاسلكية والتبديل والأمان وإدارة التنقل المؤسسي (EMM) والكاميرات الأمنية ، وكلها تدار مركزيًا من الويب. استحوذت شركة Cisco Systems على Meraki في ديسمبر 2012.

حل Meraki السحابي عبارة عن خدمة إدارة مركزية تتيح للمستخدمين إدارة جميع أجهزة شبكة Meraki الخاصة بهم عبر منصة واحدة بسيطة وآمنة.

يبين الشكل التالي الشكل Meraki:



الشكل (8-3)

يمكن للمستخدمين نشر أجهزة Meraki الخاصة بهم ومراقبتها وتكوينها عبر واجهة ويب لوحة معلومات Meraki أو عبر واجهات برمجة التطبيقات. بمجرد قيام المستخدم بإجراء تغيير في التكوين ، يتم إرسال طلب التغيير إلى سحابة Meraki ثم يتم دفعه إلى الجهاز (الأجهزة) ذات الصلة.

1.8.3 تعريف المصطلحات

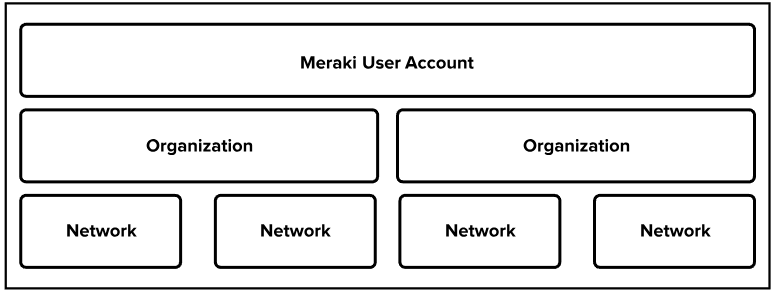
لوحة معلومات Meraki: أداة حديثة قائمة على مستعرض الويب تُستخدم لتكوين أجهزة وخدمات Meraki.

الحساب: حساب مستخدم Meraki ، يُستخدم للوصول إلى مؤسسات Meraki وإدارتها.

المؤسسة: حاوية منطقية لشبكات Meraki يديرها حساب واحد أو أكثر.

الشبكة: حاوية منطقية لمجموعة من أجهزة وخدمات Meraki المدارة مركزيًا.

يبين الشكل التالي الشكل الشبكة:



الشكل (9-3)



**الفصل الرابع دراسة البروتوكولات المستخدمة**

v

|  |  |  |
| --- | --- | --- |
| * DHCP بروتوكول التكوين الديناميكي | * بروتوكول نقل البريدSMTP | |
| * DNSبروتوكول نظام اسم المجال | * بروتوكول مضاهاة المحطة الطرفيةTelnet | |
| * بروتوكول نقل الملفاتFTP | * بروتوكول إدارة الشبكة البسيط SNMP | |
| * بروتوكول TFTP |  | |
| * بروتوكول HTTP (Hyper Text Transfer Protocol) * بروتوكول HTTPS(Hyper Text Transfer Protocol Security) | |

1.4 البروتوكولات 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](https://en.wikipedia.org/wiki/Teleprinter) Network. |
| * SMNP: Simple Network Management Protocol. |

الجدول(2) يعبر عن البروتوكولات المستخدمة

1.1.4 DHCP بروتوكول التكوين الديناميكي للمضيف:

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.

2.1.4 DNSبروتوكول نظام اسم المجال:

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.

3.1.4 بروتوكول 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.

4.1.4 بروتوكول 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.

5.1.4 بروتوكول :HTTP (Hyper Text Transfer Protocol)

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.

6.1.4 بروتوكول HTTPS(Hyper Text Transfer Protocol Security):

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).

7.1.4 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.

8.1.4 بروتوكول مضاهاة المحطة الطرفية: 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.

9.1.4 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 الخامس الدراسة العملية**

|  |  |
| --- | --- |
| * **المشاكل التي واجهت المشروع** | * **الحلول المقترحة** |
| * **مخطط Flow Chart** | * **الأهداف المستقبلية** |

1.5 المشاكل التي واجهت المشروع:

العديد من الأبحاث والمشاريع التي تعنى بمجال الشبكات تواجه غالبا مشكلة تخزين البيانات.

بالإضافة الى مشكلة أخرى ألا و هي اختراق موقع الجامعة بسبب استخدامه لبروتوكول ال.HTTP

نبحث في هذا الفصل عن أفضل الطرق و الوسائل التي تتغلب عن هذه المشاكل في الشكل الذي يفضي الى انتاج بينية قادرة على التغلب على مشاكل التخزين و الوصول غير الامن الى البيانات.

2.5 الحلول المقترحة:

2.5.1 استخدام بروتوكول FTP:

بروتوكول نقل الملفات FTP هو [بروتوكول اتصال](https://en.wikipedia.org/wiki/Communication_protocol) قياسي يُستخدم لنقل [ملفات الكمبيوتر](https://en.wikipedia.org/wiki/Computer_file) من خادم إلى عميل على [شبكة كمبيوتر](https://en.wikipedia.org/wiki/Computer_network) . تم بناء FTP على بنية [نموذج العميل والخادم](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) باستخدام تحكم منفصل واتصالات البيانات بين العميل والخادم.  قد يصادق مستخدمو FTP أنفسهم باستخدام بروتوكول تسجيل الدخول [بنص واضح](https://en.wikipedia.org/wiki/Clear_text) ، عادةً في شكل اسم مستخدم وكلمة مرور ، ولكن يمكنهم الاتصال بشكل مجهول إذا تم تكوين الخادم للسماح بذلك. للإرسال الآمن الذي يحمي اسم المستخدم وكلمة المرور ، ويشفّر المحتوى.

محاسن بروتوكول الFTP :

سهل الاستخدام ويمكن لمعظم المستخدمين تعلمه بسهولة.

سرعات نقل عالية يمكن لـ FTP نقل الملفات الكبيرة بسرعة ، مما يجعلها وسيلة فعالة لنقل كميات كبيرة من البيانات.

آمن يمكن تكوين FTP لاستخدام تشفير SSL / TLS لتأمين عمليات النقل وحماية البيانات الحساسة أثناء عمليات النقل.

فعال تم تحسين FTP لعمليات النقل عالية السرعة ، مما يقلل الوقت المستغرق لنقل الملفات الكبيرة عبر الإنترنت.

عمليات نقل الدُفعات يسمح FTP بنقل ملفات متعددة في وقت واحد ، مما يجعله أكثر كفاءة لعمليات النقل على نطاق واسع.

و باستخدامنا لهذا البروتوكول امكننا توحيد مكان تخزين المعلومات و سهولة احضارها و الحفاظ على نسخة احتياطية للمعلومات في حال فقدانها و حيث يمكن لأي مستخدم مصرح له الوصول لهذه المعلومات بسرية تامة و بسرعة عالية.

مساوئ بروتوكول الFTP :

لا توجد وسيلة تشفير على جميع خوادم FTP ، مما يعني أنه لا يمكن حماية نقل البيانات.

يمكن اختراق كلمات المرور الضعيفة ، حيث يقوم قراصنة مختلفون لكلمة المرور باختراق كلمة المرور الخاصة بك.

من بين جميع المعلومات التي تحتوي عليها الملفات ، مثل البيانات وأسماء المستخدمين وكلمات المرور ، سيتمكن المتسللون من سرقة معلوماتك الشخصية ومعلوماتك الحساسة.

يمكن حذف أو إزالة أو تحديث الملفات الهامة عن طريق الخطأ من الخادم.

2.2.5 استخدام بروتوكول HTTPS:

بروتوكول نقل النص التشعبي الآمن  HTTPS هو امتداد [لبروتوكول نقل النص التشعبي](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) .HTTP يستخدم [التشفير](https://en.wikipedia.org/wiki/Encryption) من أجل [الاتصال الآمن](https://en.wikipedia.org/wiki/Secure_communications) عبر [شبكة الكمبيوتر](https://en.wikipedia.org/wiki/Computer_network) ، ويستخدم على نطاق واسع على [الإنترنت](https://en.wikipedia.org/wiki/Internet) . في HTTPS ، يتم تشفير [بروتوكول الاتصال](https://en.wikipedia.org/wiki/Communication_protocol) باستخدام [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 الذي](https://en.wikipedia.org/wiki/Website)[تم](https://en.wikipedia.org/wiki/Data_integrity) الوصول إليه وحماية خصوصية [وسلامة](https://en.wikipedia.org/wiki/Information_privacy) البيانات المتبادلة أثناء نقلها. إنه يحمي من [هجمات man-in-the-middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack)[،](https://en.wikipedia.org/wiki/Tamper-evident#Tampering) كما أن [تشفير الكتلة](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation) ثنائي الاتجاه للاتصالات بين العميل والخادم يحمي الاتصالات من [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). كانت هذه من الناحية التاريخية عملية باهظة الثمن ، مما يعني أن اتصالات HTTPS المصادق عليها بالكامل عادة ما يتم العثور عليها فقط في خدمات معاملات الدفع المضمونة وأنظمة معلومات الشركات الأخرى المؤمنة على شبكة الويب [العالمية](https://en.wikipedia.org/wiki/World_Wide_Web) . في عام 2016 ، أدت حملة من قبل  [Electronic Frontier Foundation](https://en.wikipedia.org/wiki/Electronic_Frontier_Foundation)بدعم من مطوري [مستعرض الويب](https://en.wikipedia.org/wiki/Web_browser) إلى انتشار البروتوكول بشكل أكبر.  يتم استخدام HTTPS الآن في كثير من الأحيان بواسطة مستخدمي الويب أكثر من HTTP الأصلي غير الآمن ، وذلك لحماية مصداقية الصفحة على جميع أنواع مواقع الويب ، والحسابات الآمنة ، والحفاظ على خصوصية اتصالات المستخدم ، والهوية ، وتصفح الويب.

محاسن بروتوكول الHTTPS :

الأمان يقوم HTTPS بتشفير البيانات التي يتم إرسالها بين العميل والخادم ، مما يوفر الحماية ضد التنصت والعبث والأنشطة الضارة الأخرى.

المصادقة يتحقق HTTPS من هوية موقع الويب الذي يتم الوصول إليه ، ويمنع هجمات man-in-the-middle ويضمن أن المستخدمين يتواصلون مع موقع الويب المقصود.

الموثوقية يتضمن HTTPS أن البيانات المنقولة بين العميل والخادم لم يتم العبث بها ، مما يحمي من تلف البيانات والعبث بها

الخصوصية يحمي HTTPS المعلومات الحساسة للمستخدمين ، مثل بيانات اعتماد تسجيل الدخول والمعلومات المالية ، من أن يتم اعتراضها من قبل أطراف غير مصرح لها.

تحسين مُحسّنات محرّكات البحث: صرحت Google بأن HTTPS عبارة عن إشارة ترتيب خفيفة الوزن في خوارزميات البحث الخاصة بها ، ومن المحتمل أن توفر تعزيزًا صغيرًا لترتيب مواقع الويب المؤمنة باستخدام HTTPS.

و بالتالي باستخدامنا لبروتوكول الHTTPS في المشروع يمنع أي عملية اختراق على موقع الجامعة و يمنع عملية التنصت على المعلومات و خاصة المعلومات الخطيرة مثل كلمات المرور.

مساوئ بروتوكول الHTTPS :

التكلفة تحتاج إلى شراء شهادة SSL تختلف الأسعار اعتمادًا على عدد المجالات أو المجالات الفرعية التي ستغطيها الشهادة وكذلك على مستوى التحقق من الهوية

الشهادة لها مدة محدودة إذا نفدت الشهادة و / أو لم يتم تجديدها ، فسيعرض الموقع أخطاء أو قد لا يتم عرضه على الإطلاق ما لم تتم إعادته مرة أخرى إلى HTTP

التأخير في بعض الحالات ، يمكن أن يتسبب HTTPS في حدوث تأخيرات

مشكلة وسائط مختلطة أثناء تصفح الويب ، ربما تكون قد تلقيت تحذيرًا يفيد بأن الموقع يقدم محتوى غير آمن. هذا ليس لأنهم يقومون بأي شيء سيء ، ولكن لأنهم يقومون بتحميل من مواقع أو خدمات أخرى ، مثل وسائل التواصل الاجتماعي أو أدوات الدردشة ، غير المشفرة

مشاكل التخزين المؤقت للوكيل عادة ما يؤثر على المواقع الكبيرة. لا يمكن أن يحدث أي تخزين مؤقت عام قد يحدث. لن يتمكن مزودو خدمة الإنترنت وغيرهم من تخزين المحتوى المشفر مؤقتًا

3.5 مخطط Flow Chart:

4.5 الأهداف المستقبلية:

* استخدام قناة تشفير بين الفرعين حلب و القامشلي باستخدام بروتوكول ipsec.
* استخدام بروتوكول HSRP وذلك لتحقيق .
* منع الاتصال باستخدام بروتوكول ال Telnet السماح فقط الدخول الى الأجهزة باستخدام بروتوكول ال SSH وذلك لجعل كامل الاتصال مشفر.

: References المراجع

* [https://www.almrsal.com/](C:\\Users\\E\\AppData\\Roaming\\Microsoft\\Word\\ip address شرح | المرسال (almrsal.com)" \o "https://www.almrsal.com/)
* <https://wikiarab.com/>
* [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)
* [Subcarriers: أصناف عناوين الـ IP](https://subcarriers.blogspot.com/2013/12/ip.html)
* [Application layer protocols | Various Protocols of Applications layers (educba.com)](https://www.educba.com/application-layer-protocols/)
* <https://www.cisco.com/>
* <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-network-controller.html#~faqs>
* <https://www.techtarget.com/whatis/definition/server>
* <https://www.forcepoint.com/cyber-edu/firewall>
* <https://www.ip-insider.de/was-ist-ospf-open-shortest-path-first-a-905626/>
* <https://ar.wikipedia.org/wiki/>
* arageek.com/l/أنواع-الشبكات
* <https://www.lifesize.com/blog/tcp-vs-udp/#:~:text=TCP%20is%20a%20connection%2Doriented,is%20only%20possible%20with%20TCP>.
* <https://www.geeksforgeeks.org/differences-between-tcp-and-udp/>
* <https://www.cisco.com/c/en/us/products/routers/product-listing.html>
* <https://de.wikipedia.org/wiki/Switch_(Netzwerktechnik)>
* Networks: The Definitive Guide, 2nd Edition. Matthew 802.11 O’Reilly Media. ISBN #0-596-10052-3, Gast Network Site Surveying, Cisco Press. ISBN #1- 802.11 587-05164-8.
* Network Protocols Handbook.
* Collision Probability in Saturated IEEE 802.11 Networks (Taka Sakurai).
* Simulation of IEEE 802.11 PCF function in GloMoSim (Michael Cloran).