إهداء

فهرس

مدخل الى المشروع:

مقدمة:

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 لكاقة المستخدمين داخل هذه الشركة بالحصول على الأذونات في التحكم\ أو تغيير الإعدادات أو الضبط وبالتالي تكون صلاحياتهم محصورة.

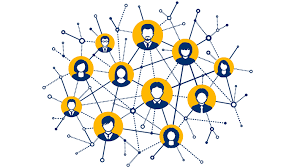
شرح المشروع:

ربط جامعة قرطبة جامعة حلب مع فرع القامشلي و التحكم بنقاط البث بشكل مركزي.

**الفصل الأول – الدراسة النظرية**

1.1 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

2.1أصناف 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

1.2.1شبكات 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.

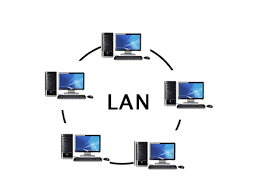
#### أين تستخدم شبكات ال LAN ؟

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

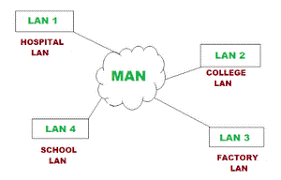
2.2.1الشبكات الحضرية أو المدنية :Metropolitan Area Network

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.



الشكل (3) شبكة MAN

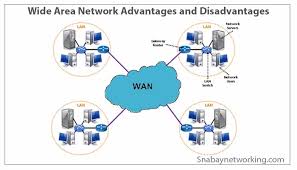
3.2.1شبكات بعيدة أو طويلة المدى :Wide Area Network

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 ؟

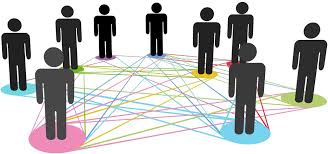
تتكون شبكة WAN من عدة شبكات MAN أو LAN يتم ربطهم من خلال الأقمار الصناعية المنتشرة عبر العالم كله على عكس الشبكات المحلية LAN والتي تعتمد على معداتها الخاصة في الاتصالات فإن شبكة WAN قد تستخدم أجهزة اتصالات عامة أو مستأجرة أو خاصة حيث يتم تجميعهم وبالتالي يمكن امتداد مساحة تغطية الشبكة عبر مساحات جغرافية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



الشكل (4) شبكةWAN

4.2.1الشبكات 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.

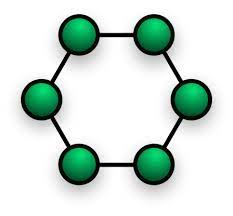


الشكل (5) شبكة شخصية

3.1أنواع الشبكات:

1.3.1  الحلقيRing :

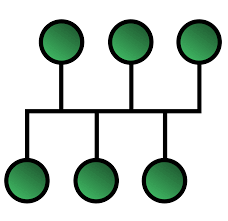
إن هذا النوع هو من الأنواع المعروفة حيث انه يعتمد على اتصال الجهاز أتوماتيكيا بالجهاز الذي قبله والجهاز الذي بعده ويكون هذا الاتصال مباشر حيث انه يكون مشكل في صورة دائرة مغلقة وهذا يكون في اتجاه واحد.



الشكل (6) الحلقي

2.3.1  الخطي Bus:

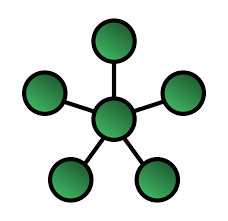
  أن هذا النوع هو من أقدم أنواع الشبكات حيث انه يقوم باتصال الشبكات بعضها البعض وذلك عن طريق خط رئيسي ولكن لا يسمح أن يتم تبادل البيانات بين جهازين وان حدث فذلك يؤدي إلى تصادم البيانات واتلافها.



الشكل (7) الخطي

3.3.1نجمية Star‏:

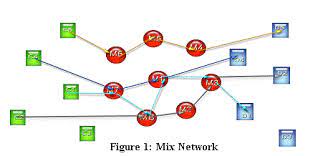
هي إحدى نماذج [الشبكات](https://ar.wikipedia.org/wiki/%D8%B7%D9%88%D8%A8%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7_%D8%B4%D8%A8%D9%83%D8%A9)، ويرتبط فيها كل جهاز بخط إلى خادم مركزي مثل [جهاز توزيع الشبكة](https://ar.wikipedia.org/wiki/%D9%85%D8%A8%D8%AF%D9%84_(%D8%B4%D8%A8%D9%83%D8%A7%D8%AA))، وترسل البيانات 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.



الشكل (8) النجمي

4.3.1مختلطة 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

**4.1فوائد 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 5.1**

**6.1أصناف عناوين IP:**

1.6.1تعريف 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

1.1.6.1مجالات الأصناف Classes:

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

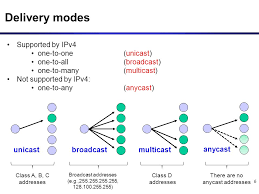
|  |  |  |
| --- | --- | --- |
|  |  | الجدول(1) IPv4 |

2.1.6.1 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

**Private ip public ip**

**127 ip**

**Mac address**

2.6.1تعريف ال**IPv6:**

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.

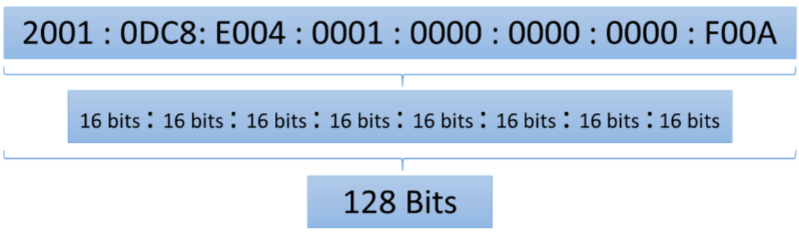
يتم تمثيل عناوين IPv6 في شكل ثماني مجموعات من أربعة أرقام سداسية عشرية لكل منها ، مفصولة بنقطتين. قد يتم تقصير التمثيل الكامل.

**1.2.6.1الخصائص 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.



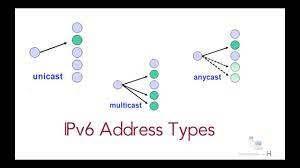
الشكل (11) IPv6

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

**3.6.1مقارنة 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.

**1.3.6.1مساحة 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.

**2.3.6.1الإرسال المتعدد**

بنية الإرسال المتعدد في IPv6

الإرسال المتعدد ، وهو نقل الحزمة إلى وجهات متعددة في عملية إرسال واحدة ، هو جزء من المواصفات الأساسية في IPv6. في IPv4 هذه ميزة اختيارية (على الرغم من تنفيذها بشكل شائع). تتميز معالجة الإرسال المتعدد لـ IPv6 بميزات وبروتوكولات مشتركة مع البث المتعدد IPv4 ، ولكنها توفر أيضًا تغييرات وتحسينات من خلال التخلص من الحاجة إلى بروتوكولات معينة. لا ينفذ IPv6 بث IP التقليدي ، أي إرسال حزمة إلى جميع المضيفين على الرابط المرفق باستخدام عنوان بث خاص ، وبالتالي لا يحدد عناوين البث. في IPv6 ، يتم تحقيق نفس النتيجة عن طريق إرسال حزمة إلى مجموعة الإرسال المتعدد لجميع العقد المحلية للارتباط على العنوان ff02 :: 1 ، وهو ما يماثل الإرسال المتعدد IPv4 لعنوان 224.0.0.1. يوفر IPv6 أيضًا تطبيقات جديدة للبث المتعدد ، بما في ذلك تضمين عناوين نقطة الالتقاء في عنوان مجموعة الإرسال المتعدد IPv6 ، مما يبسط نشر الحلول بين المجالات.

في IPv4 ، من الصعب جدًا على المنظمة الحصول حتى على تعيين مجموعة متعددة البث عالميًا واحدًا ، كما أن تنفيذ الحلول بين المجالات أمر غامض. تعيينات عناوين أحادية الإرسال بواسطة سجل إنترنت محلي لـ IPv6 لها بادئة توجيه 64 بت على الأقل ، مما ينتج عنه أصغر حجم شبكة فرعية متاح في IPv6 (أيضًا 64 بت). باستخدام مثل هذا التعيين ، من الممكن تضمين بادئة العنوان الأحادي في تنسيق عنوان الإرسال المتعدد IPv6 ، مع الاستمرار في توفير كتلة 32 بت ، أو وحدات البت الأقل أهمية من العنوان ، أو ما يقرب من 4.2 مليار معرف مجموعة الإرسال المتعدد. وبالتالي فإن كل مستخدم لشبكة IPv6 الفرعية لديه تلقائيًا مجموعة من مجموعات الإرسال المتعدد الخاصة بالمصدر والقابلة للتوجيه عالميًا لتطبيقات البث المتعدد.

**3.3.6.1التكوين التلقائي للعنوان عديم الحالة (SLAAC)**

عنوان IPv6 التكوين التلقائي للعنوان عديم الحالة

يقوم مضيفو IPv6 بتكوين أنفسهم تلقائيًا. تحتوي كل واجهة على عنوان ارتباط محلي يتم إنشاؤه ذاتيًا ، وعند الاتصال بشبكة ، يتم تنفيذ حل التعارض وتوفر أجهزة التوجيه بادئات الشبكة عبر إعلانات جهاز التوجيه. [19] يمكن تحقيق التكوين عديم الحالة للموجهات باستخدام بروتوكول خاص لإعادة ترقيم جهاز التوجيه. [20] عند الضرورة ، قد يقوم المضيفون بتكوين عناوين إضافية ذات حالة عبر الإصدار 6 من بروتوكول التكوين الديناميكي للمضيف (DHCPv6) أو العناوين الثابتة يدويًا.

مثل IPv4 ، يدعم IPv6 عناوين IP الفريدة عالميًا. يهدف تصميم IPv6 إلى إعادة التأكيد على المبدأ الشامل لتصميم الشبكة الذي تم تصميمه في الأصل أثناء إنشاء الإنترنت المبكر من خلال جعل ترجمة عنوان الشبكة قديمة. لذلك ، يمكن معالجة كل جهاز على الشبكة عالميًا مباشرةً من أي جهاز آخر.

**7.1 أنواع وصلات الشبكة:**  
 **1.7.1 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**

**2.7.1 Cross over:**

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

**الطرف الاول :**

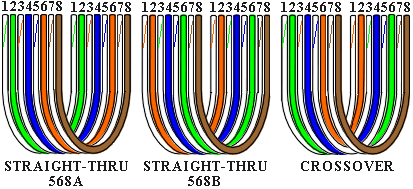
1. ابيض برتقالي Tx
2. برتقالى Tx
3. ابيض اخضر Rx
4. ازرق
5. ابيض ازرق
6. اخضر Rx
7. ابيض بنى
8. بنى

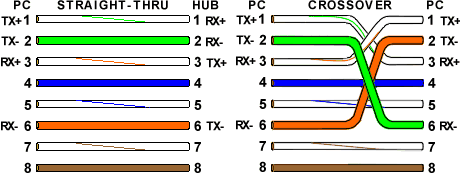
**الطرف الاخر :**

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

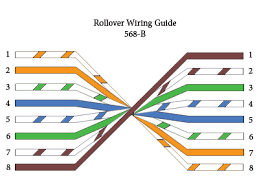
**3.7.1 Rollover:**

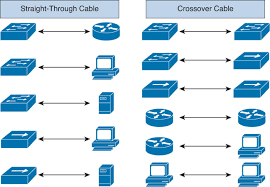
تُستخدم كبلات الrollover ، التي يشار إليها أحيانًا باسم كبلات Yost ، بشكل شائع للاتصال بمنفذ وحدة التحكم في الجهاز لإجراء تغييرات برمجية على الجهاز. على عكس الكابلات المتقاطعة والكابلات ذات الأسلاك المستقيمة ، لا يُقصد بكابلات التمرير لنقل البيانات ولكن بدلاً من ذلك إنشاء واجهة مع الجهاز.

[](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/)

الجدول(13) [](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/)كبلات Straight and Crossover

الجدول(14) Tx and Rx لكبلات Straight and Crossover

الجدول(15) Rollover



الجدول(16) أنواع الوصل بين الأجهزة

**الفصل الثاني- دراسة الأجهزة المستخدمة**

1.2 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 (71) Router

كيف يعمل جهاز التوجيه؟

فكر في 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.

ما هي أنواع الموجهات المختلفة؟

لتوصيل شبكة LAN بالإنترنت ، يحتاج جهاز التوجيه أولاً إلى الاتصال بمودم. هناك طريقتان أساسيتان للقيام بذلك:

1.1.2الموجه اللاسلكي:

يستخدم الموجه اللاسلكي كبل Ethernet للاتصال بمودم. يقوم بتوزيع البيانات عن طريق تحويل الحزم من الشفرة الثنائية إلى إشارات راديو ، ثم بثها لاسلكيًا باستخدام الهوائيات. لا تنشئ أجهزة التوجيه اللاسلكية شبكات LAN ؛ بدلاً من ذلك ، قاموا بإنشاء شبكات WLAN (شبكات المنطقة المحلية اللاسلكية) ، والتي تربط أجهزة متعددة باستخدام الاتصال اللاسلكي.

جهاز التوجيه السلكي: مثل جهاز التوجيه اللاسلكي ، يستخدم جهاز التوجيه السلكي أيضًا كبل Ethernet للاتصال بمودم. ثم يستخدم كبلات منفصلة للاتصال بجهاز واحد أو أكثر داخل الشبكة ، وإنشاء شبكة LAN ، وربط الأجهزة الموجودة داخل تلك الشبكة بالإنترنت.

بالإضافة إلى أجهزة التوجيه اللاسلكية والسلكية لشبكات LAN الصغيرة ، هناك العديد من الأنواع المتخصصة من أجهزة التوجيه التي تخدم وظائف محددة:

2.1.2جهاز التوجيه الأساسي:

على عكس أجهزة التوجيه المستخدمة في شبكة LAN منزلية أو تجارية صغيرة ، يتم استخدام جهاز توجيه أساسي من قبل الشركات الكبيرة والشركات التي تنقل حجمًا كبيرًا من حزم البيانات داخل شبكتها. تعمل أجهزة التوجيه الأساسية في "قلب" الشبكة ولا تتصل بالشبكات الخارجية.

3.1.2جهاز التوجيه Edge:

بينما يدير جهاز التوجيه الأساسي بشكل حصري حركة مرور البيانات داخل شبكة واسعة النطاق ، يتواصل جهاز التوجيه الحافة مع كل من أجهزة التوجيه الأساسية والشبكات الخارجية. تعيش أجهزة التوجيه Edge على "حافة" الشبكة وتستخدم BGP (بروتوكول بوابة الحدود) لإرسال واستقبال البيانات من شبكات LAN وشبكات WAN أخرى.

4.1.2جهاز التوجيه الافتراضي:

جهاز التوجيه الافتراضي هو تطبيق برمجي يؤدي نفس الوظيفة مثل جهاز التوجيه القياسي للأجهزة. قد يستخدم بروتوكول تكرار جهاز التوجيه الافتراضي (VRRP) لإنشاء أجهزة توجيه افتراضية أساسية ونسخ احتياطي ، في حالة فشل أحدها.

2.2المبدل Switch:



الشكل (81)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.

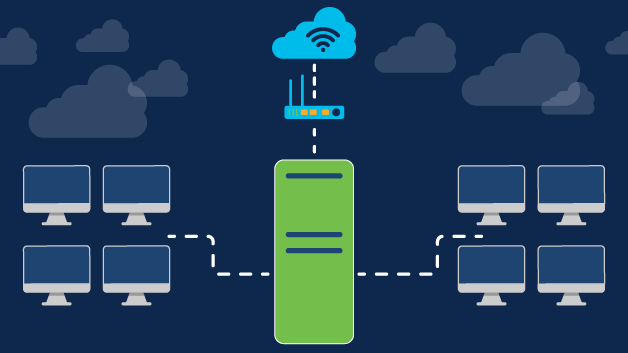
محولات Ethernet هي أكثر أشكال تبديل الشبكة شيوعًا. تم اختراع أول جسر في عام 1983 بواسطة مارك كيمبف ، وهو مهندس في مجموعة تطوير الشبكات المتقدمة التابعة لشركة Digital Equipment Corporation. تم تقديم أول منتج جسر ثنائي المنفذ (LANBridge 100) بواسطة تلك الشركة بعد فترة وجيزة. أنتجت الشركة لاحقًا محولات 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.

3.2وحدة تحكم الشبكة Network Controller:

ما هي وحدة تحكم الشبكة؟

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 (19) 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.

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.

لماذا تستخدم وحدات تحكم الشبكة؟

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.

كيف تطورت وحدات التحكم في الشبكة؟

كانت أنظمة إدارة العناصر (EMSs) واحدة من الأدوات المبكرة للتحكم في جهاز الشبكة. لقد ساعدوا وقاموا بمراقبة جوانب معينة من مجموعات محددة من أجهزة الشبكة ، ولم يكن من غير المعتاد العثور على أكثر من EMS واحد في شبكة كبيرة. على الرغم من أنها كانت مفيدة ، إلا أنها لا تستطيع التحكم في الشبكة بشكل كلي.

دمجت EMSs في النهاية المزيد من الوظائف ، والتي يشار إليها عادةً باسم الخطأ والتكوين والمحاسبة والأداء والأمن (FCAPS) ، وبدأت في استخدام واجهات برمجة التطبيقات المتجهة شمالًا للتكامل مع التطبيقات عالية المستوى. ومع ذلك ، كانوا مملوكين ويعملون فقط على مجموعات صغيرة من الأجهزة ، مما يحد من فائدتها.

تلبي وحدات التحكم في الشبكات المعرفة بالبرمجيات (SDN) حاجة مختلفة. يتم تشغيل وحدات التحكم هذه من خلال التطبيقات التي توفر الأتمتة والرشاقة للأجهزة التي تتحكم فيها. ومع ذلك ، لا توفر وحدات تحكم SDN العديد من الوظائف الأخرى الضرورية لبناء شبكة سريعة الاستجابة حقًا.

تجمع وحدات تحكم الشبكة وتتوسع في وظائف وحدات تحكم EMS و SDN. فهي تساعد فرق تكنولوجيا المعلومات على تحقيق عمليات أكثر بساطة ومركزية ورشيقة ، كما أنها توفر الأتمتة التي تشتد الحاجة إليها ، وتحليل الأداء ، واكتشاف الأخطاء وتصحيحها ، وبالتالي تساعد في تحقيق نتائج الأعمال المرغوبة.

كيف تحل أجهزة التحكم في الشبكة تحديات تكنولوجيا المعلومات؟

* تقليل تكاليف التشغيل:

إحدى أكبر المشكلات التي تواجه تكنولوجيا المعلومات اليوم هي التكلفة المتزايدة للعمليات. هذه التكاليف هي نتيجة تقديم الخدمات لعدد متزايد من المستخدمين والأجهزة التي تتصل بالشبكة من المكاتب والمنازل والمقاهي والمطارات وغيرها ، والتطبيقات التي يتم توزيعها في مراكز البيانات الخاصة والسحابات العامة. هذا النمو يفوق قدرات تكنولوجيا المعلومات وجهود الإدارة اليدوية. تعمل وحدات التحكم في الشبكة على أتمتة العمليات التي تؤدي إلى توسيع نطاق أفضل وتقليل الوقت والقضاء على الأخطاء وتقليل التكاليف.

* زيادة التوفر:

تجمع وحدة التحكم في الشبكة حركة مرور الشبكة وتحللها لاكتشاف أي مشكلات محتملة بشكل استباقي قبل أن تصبح مشكلات حقيقية. يمكنه إجراء تحليل السبب الجذري وتنبيه عمليات تكنولوجيا المعلومات التي يمكنها اتخاذ خطوات تصحيحية ووقائية لضمان بقاء خدمات الشبكة متاحة دائمًا.

* تحسين خفة الحركة:

تعمل وحدة التحكم في الشبكة على جعل الشبكات أكثر مرونة واستجابة لاحتياجات العمل. يقوم بتنفيذ التغييرات المطلوبة على جميع أجهزة الشبكة بشكل متسق وعالمي دون الحاجة المستهلكة للوقت لتكوينات كل جهاز على حدة.

* تعزيز الأمن:

قد يكشف التحليل الشامل لوحدة التحكم في الشبكة لحركة مرور الشبكة عن تهديدات أمنية محتملة. يمكن لوحدة التحكم بعد ذلك أن تعمل على عزل التهديد ومنع انتشاره.

4.2الخادم Server:



الشكل (20) Servers

ما هو الخادم؟

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.

كيف تعمل الخوادم؟

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.

برنامج الخادم:

كحد أدنى ، يتطلب الخادم مكونين برمجيين: نظام تشغيل وتطبيق. يعمل نظام التشغيل كمنصة لتشغيل تطبيق الخادم. يوفر الوصول إلى موارد الأجهزة الأساسية ويوفر خدمات التبعية التي يعتمد عليها التطبيق.

يوفر نظام التشغيل أيضًا وسائل للعملاء للاتصال بتطبيق الخادم. يتم تعيين عنوان IP الخاص بالخادم واسم المجال المؤهل بالكامل ، على سبيل المثال ، على مستوى نظام التشغيل.

أجهزة كمبيوتر سطح المكتب مقابل الخوادم:

هناك أوجه تشابه واختلاف بين أجهزة الكمبيوتر المكتبية والخوادم. تعتمد معظم الخوادم على وحدات المعالجة المركزية X86 / X64 ويمكنها تشغيل نفس الرمز مثل كمبيوتر سطح المكتب X86 / X64. على عكس معظم أجهزة الكمبيوتر المكتبية ، غالبًا ما تشتمل الخوادم الفعلية على مآخذ متعددة لوحدة المعالجة المركزية وذاكرة تصحيح الأخطاء. تدعم الخوادم أيضًا بشكل عام قدرًا أكبر من الذاكرة مقارنة بمعظم أجهزة كمبيوتر سطح المكتب.

نظرًا لأن أجهزة الخادم تعمل عادةً على تشغيل أحمال عمل حرجة للمهام ، فإن مصنعي أجهزة الخوادم يصممون الخوادم لدعم المكونات الزائدة عن الحاجة. قد يكون الخادم مزودًا بمصادر طاقة زائدة عن الحاجة وواجهات شبكة زائدة عن الحاجة. تسمح هذه المكونات المكررة للخادم بالاستمرار في العمل حتى في حالة فشل أحد المكونات الرئيسية.

تختلف أجهزة الخادم أيضًا عن أجهزة سطح المكتب من حيث عامل الشكل الخاص بها. غالبًا ما توجد أجهزة كمبيوتر سطح المكتب الحديثة كأبراج صغيرة ، مصممة لتوضع تحت مكتب. على الرغم من وجود بعض البائعين الذين يقدمون خوادم برجية ، إلا أن معظم الخوادم مصممة ليتم تركيبها على حامل.

5.2هاتف نقل الصوت عبر الإنترنت Voice over IP:



الشكل (21) Voip Phone

ما هو مزود الهاتف VoIP؟

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.

هل يمكن لهاتف VoIP استقبال الرسائل النصية؟

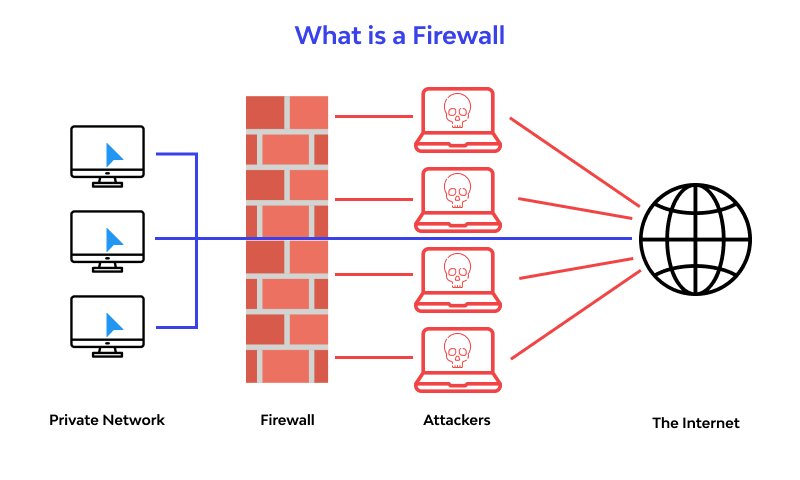
نعم ، يمكن لهاتف VoIP استقبال الرسائل النصية. أسهل طريقة لإرسال واستقبال الرسائل النصية على رقم هاتف VoIP الخاص بك هي استخدام تطبيق برمجي ، مثل NextivaONE. باستخدام NextivaONE ، يمكنك تحويل أي كمبيوتر أو جهاز محمول إلى هاتف يمكنه إجراء مكالمات أو إرسال واستقبال الرسائل النصية.

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).

6.2الجدار الناريFirewall :



الشكل (22) Firewall

1.6.2تعريف 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.

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).

2.6.2أنواع 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.

**1.2.6.2جدران الحماية من الجيل التالي Next-generation firewalls (NGFW) :**

تدمج تقنية جدار الحماية التقليدية مع وظائف إضافية ، مثل فحص حركة المرور المشفرة وأنظمة منع التطفل ومكافحة الفيروسات والمزيد. والجدير بالذكر أنه يشمل فحص الحزمة العميق (DPI). بينما تنظر جدران الحماية الأساسية فقط إلى رؤوس الحزم ، يفحص فحص الحزمة العميق البيانات الموجودة داخل الحزمة نفسها ، مما يمكّن المستخدمين من تحديد الحزم التي تحتوي على بيانات ضارة أو تصنيفها أو إيقافها بشكل أكثر فعالية. تعرف على Forcepoint NGFW هنا.

**2.2.6.2جدران الحماية الوكيل Proxy firewalls :**

تعمل على تصفية حركة مرور الشبكة على مستوى التطبيق. على عكس جدران الحماية الأساسية ، يعمل الوكيل كوسيط بين نظامين طرفيين. يجب على العميل إرسال طلب إلى جدار الحماية ، حيث يتم تقييمه بعد ذلك وفقًا لمجموعة من قواعد الأمان ثم يتم السماح به أو حظره. والجدير بالذكر أن جدران الحماية الوكيل تراقب حركة المرور لبروتوكولات الطبقة 7 مثل HTTP و FTP ، وتستخدم كلاً من فحص الحزمة حسب الحالة والعميق لاكتشاف حركة المرور الضارة.

**3.2.6.2جدران حماية ترجمة عناوين الشبكة (NAT) :**

تسمح للأجهزة المتعددة التي لها عناوين شبكة مستقلة بالاتصال بالإنترنت باستخدام عنوان IP واحد ، مع إبقاء عناوين IP الفردية مخفية. نتيجة لذلك ، لا يستطيع المهاجمون الذين يقومون بفحص الشبكة بحثًا عن عناوين IP التقاط تفاصيل محددة ، مما يوفر أمانًا أكبر ضد الهجمات. تشبه جدران حماية NAT جدران الحماية الوكيل من حيث أنها تعمل كوسيط بين مجموعة من أجهزة الكمبيوتر وحركة المرور الخارجية.

**4.2.6.2جدران الحماية بفحص متعدد الطبقات (SMLI):**

تقوم بترشيح حزم في طبقات الشبكة والنقل والتطبيق ، ومقارنتها بالحزم الموثوقة المعروفة. مثل جدران الحماية NGFW ، يفحص SMLI الحزمة بأكملها ويسمح لهم بالمرور فقط إذا اجتازوا كل طبقة على حدة. تقوم جدران الحماية هذه بفحص الحزم لتحديد حالة الاتصال (وبالتالي الاسم) للتأكد من أن جميع الاتصالات التي بدأت تحدث فقط مع مصادر موثوقة.

7.2نقطة 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.



الشكل (23)Access Point

ما هي نقطة الوصول؟

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.

ما هو موسع النطاق؟

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.

لماذا تعتبر نقاط الوصول أفضل للشركات؟

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.

8.2Meraki 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.



الشكل (24) Meraki

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.

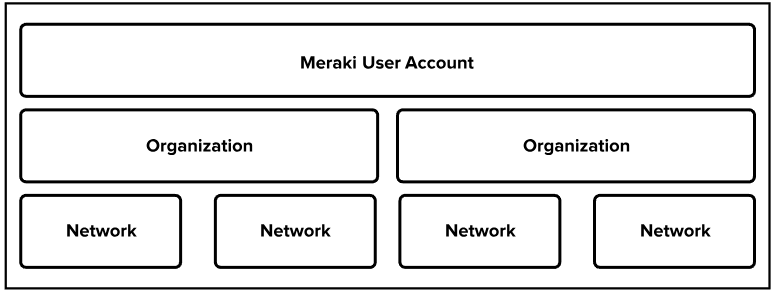
1.8.2 تعريف المصطلحات

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.

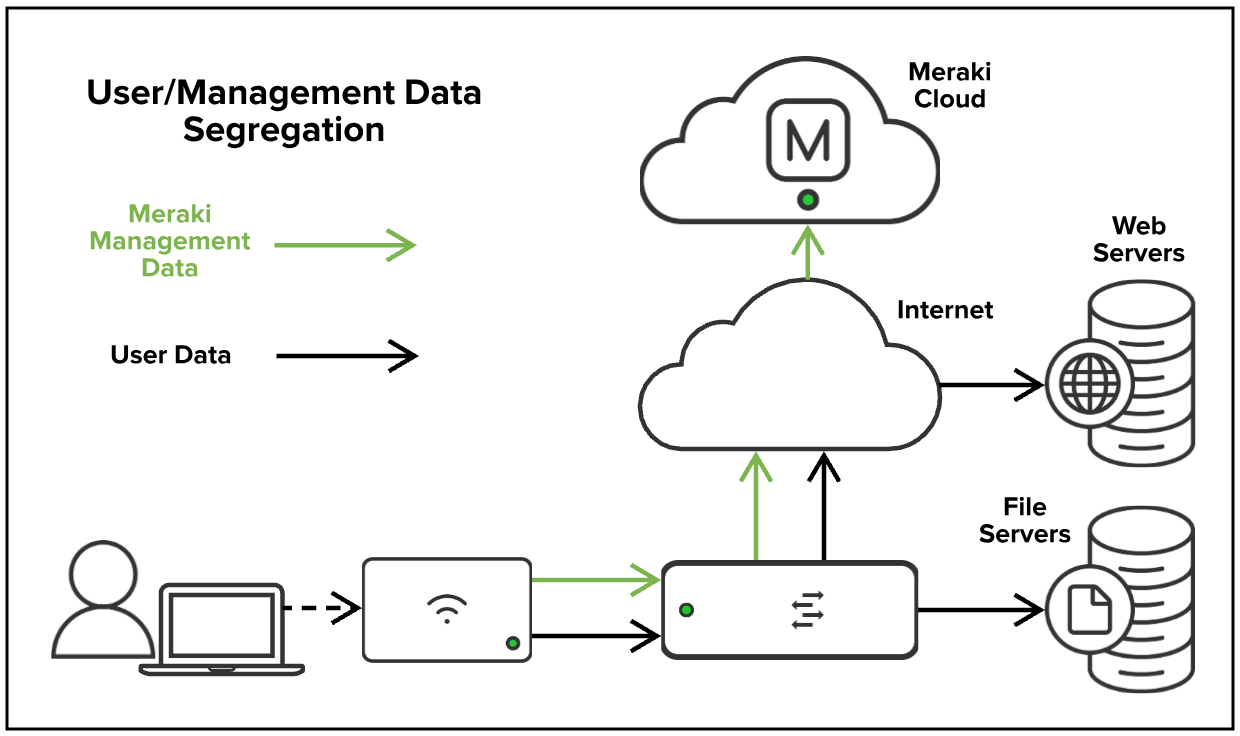
الشبكة: حاوية منطقية لمجموعة من أجهزة وخدمات Meraki المدارة مركزيًا.



الشكل (25) الشبكة

بيانات الإدارة: البيانات (التكوين والإحصاءات والمراقبة وما إلى ذلك) التي تتدفق من أجهزة Meraki (نقاط الوصول اللاسلكية والمفاتيح وأجهزة الأمان) إلى سحابة Meraki عبر اتصال إنترنت آمن.

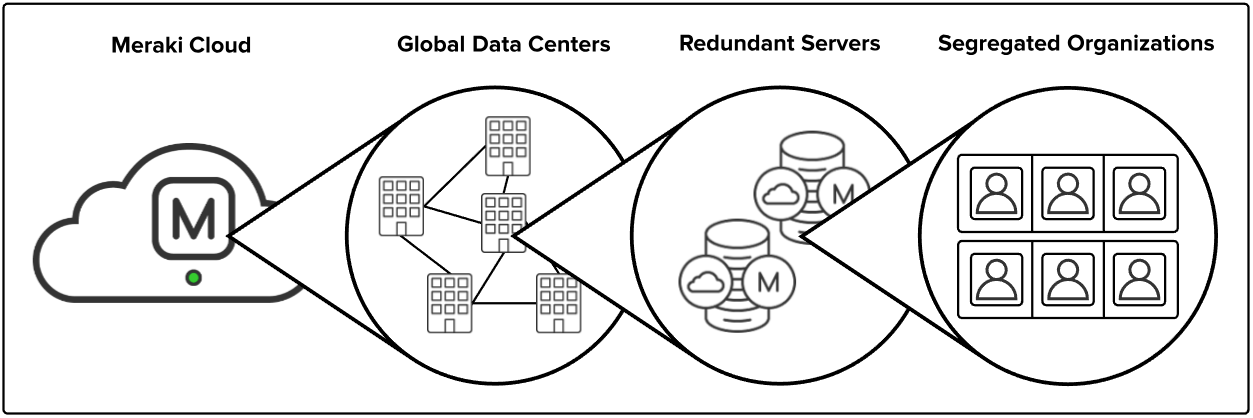
بيانات المستخدم: البيانات المتعلقة بحركة المستخدم (تصفح الويب ، والتطبيقات الداخلية ، وما إلى ذلك). لا تتدفق بيانات المستخدم عبر سحابة Meraki ، بل تتدفق مباشرة إلى وجهتهم على شبكة LAN أو عبر WAN.



الشكل (26) بيانات المستخدم

2.8.2 معمارية Meraki Cloud

سحابة Meraki هي العمود الفقري لحل إدارة Meraki. هذه "السحابة" عبارة عن مجموعة من الخوادم الموثوق بها متعددة المستأجرين الموزعة بشكل استراتيجي حول العالم في مراكز بيانات Meraki. الخوادم في مراكز البيانات هذه عبارة عن أجهزة كمبيوتر استضافة قوية تتكون من العديد من حسابات المستخدمين المنفصلة. يطلق عليهم خوادم متعددة المستأجرين لأن الحسابات تشترك (متساوية) في موارد الحوسبة على مضيفها (الخادم). ومع ذلك ، على الرغم من مشاركة هذه الحسابات في الموارد ، يضمن Meraki الحفاظ على أمان معلومات العميل من خلال تقييد وصول المؤسسة استنادًا إلى مصادقة الحساب ، بالإضافة إلى تجزئة معلومات المصادقة مثل كلمات مرور المستخدم أو مفاتيح واجهة برمجة التطبيقات.



الشكل (27) معمارية Meraki

3.8.2 مراكز البيانات

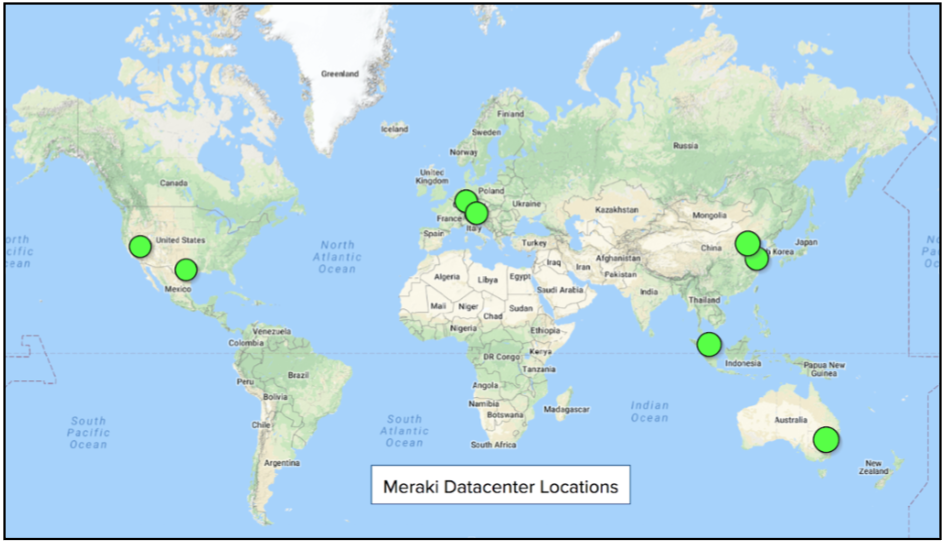
يتم نسخ بيانات إدارة العملاء عبر مراكز بيانات مستقلة في نفس المنطقة في الوقت الفعلي. يتم أيضًا نسخ نفس البيانات في النسخ الاحتياطية الأرشيفية التلقائية التي تستضيفها خدمات التخزين السحابية التابعة لجهات خارجية في المنطقة. لا تقوم سحابة Meraki بتخزين بيانات المستخدم الخاصة بالعميل. يمكن العثور على مزيد من المعلومات حول أنواع البيانات المخزنة في سحابة Meraki في قسم "بيانات الإدارة" أدناه.

يتم أيضًا نسخ جميع خدمات Meraki (لوحة القيادة وواجهات برمجة التطبيقات) عبر العديد من مراكز البيانات المستقلة ، بحيث يمكن تجاوز الفشل بسرعة في حالة حدوث فشل كارثي في مركز البيانات.

توجد مراكز بيانات Meraki في جميع أنحاء العالم ، مما يتيح إمكانية احتواء البيانات المحلية عالية التوفر لسيادة البيانات في البلدان والمناطق الحساسة ، والاتصالات عالية السرعة لتسهيل الاتصال الموثوق به لإدارة السحابة. تحمل مراكز البيانات هذه شهادات مثل PCI و SAS70 Type II / SSAE و PCI و ISO27001. بالإضافة إلى ذلك ، تخضع جميع مراكز بيانات Meraki لاختبارات اختراق يومية من قبل طرف ثالث مستقل. تتضمن المزيد من ميزات مركز البيانات الرئيسية ما يلي:

* اتفاقية مستوى خدمة وقت التشغيل بنسبة 99.99٪
* الكشف التلقائي عن الأعطال على مدار الساعة طوال أيام الأسبوع
* تكرار البيانات في الوقت الحقيقي بين مراكز البيانات
* يتم تجزئة جميع البيانات الحساسة (مثل كلمات المرور) على الخوادم

4.8.2 مواقع مراكز البيانات:



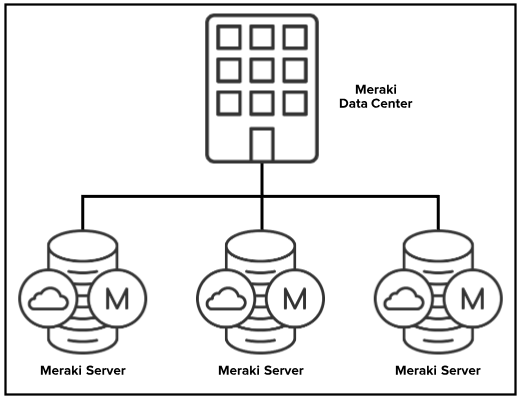
الشكل (28) مواقع مراكز البيانات

تحتوي كل منطقة (أمريكا الشمالية والجنوبية وأوروبا وآسيا والصين) ، على الأقل ، على زوج متطابق جغرافيًا (لتجاوز الفشل) من مراكز البيانات حيث يوجد أي خادم Meraki الأساسي لنقطة النهاية. يوضح الجدول أدناه تفاصيل مراكز البيانات التي تغطي كل منطقة من مناطق لوحة المعلومات.

عند إنشاء الحساب ، يمكن للعملاء تحديد المنطقة التي يتم استضافة بياناتهم فيها. بالنسبة للعملاء الذين لديهم شبكات متفرقة عالميًا ، يجب إنشاء مؤسسات منفصلة لكل منطقة تخزين بيانات (أمريكا الشمالية وأمريكا الجنوبية وأوروبا وآسيا والصين). يمكن العثور على منطقة الاستضافة لكل حساب في الجزء السفلي من صفحات لوحة معلومات Meraki عند تسجيل دخول المستخدم.

5.8.2 تخزين مركز البيانات

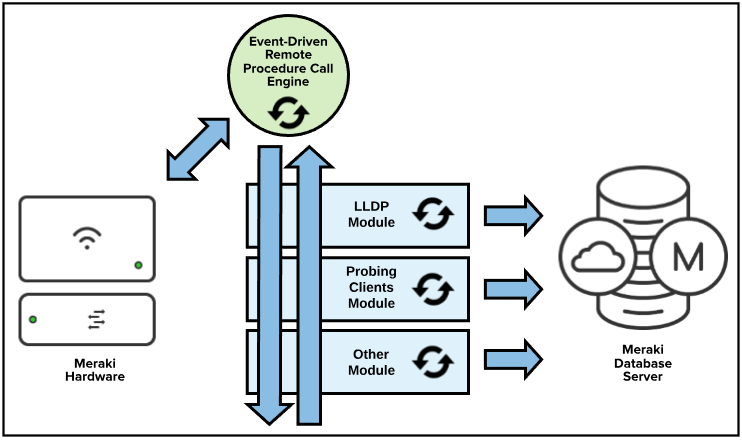
تحتوي مراكز بيانات Meraki على بيانات تكوين جهاز Meraki النشطة وبيانات استخدام الشبكة التاريخية. تضم مراكز البيانات هذه خوادم حوسبة متعددة ، حيث يتم احتواء بيانات إدارة العملاء. لا تخزن مراكز البيانات هذه بيانات المستخدم الخاصة بالعملاء. يتم تناول أنواع البيانات هذه بمزيد من التفصيل في قسم "البيانات" أدناه.



الشكل (29) تخزين مركز البيانات

6.8.2 اتصالات من جهاز إلى سحابة من Meraki:

يستخدم Meraki محرك استدعاء إجراء بعيد (RPC) مدفوع بالحدث لأجهزة Meraki للاتصال بلوحة القيادة وخوادم Meraki لإرسال البيانات واستلامها. تعمل أجهزة Meraki كخادم / مستقبل لأن سحابة Meraki تبدأ المكالمات إلى الأجهزة لجمع البيانات ونشر التكوين. البنية التحتية السحابية هي البادئ ، لذلك يمكن تنفيذ التكوينات في السحابة قبل أن تكون الأجهزة متصلة بالفعل أو حتى يتم نشرها فعليًا.



الشكل (30) اتصالات من جهاز إلى سحابة من Meraki

في حالة فقدان الاتصال السحابي (والذي يحدث غالبًا بسبب مزود خدمة الإنترنت المحلي أو فشل الاتصال) ، سيستمر جهاز Meraki في العمل بآخر تكوين معروف له حتى يتم استعادة الاتصال السحابي.

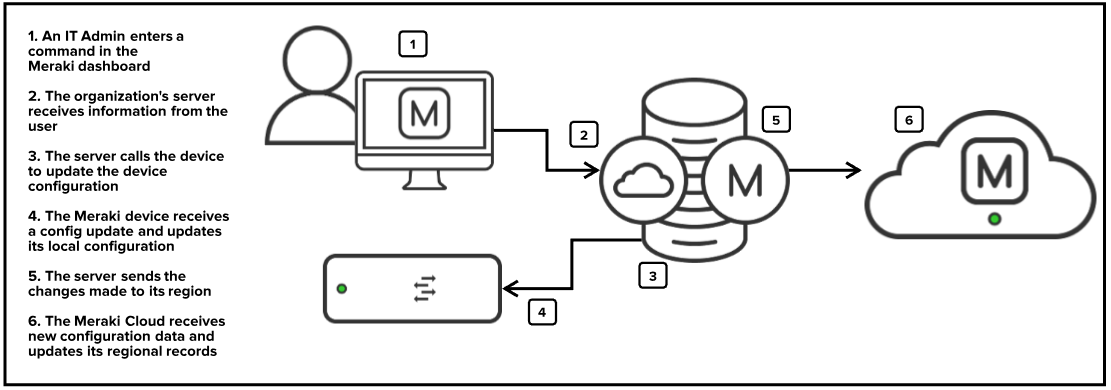
7.8.2 عملية التواصل

إذا كان الجهاز غير متصل بالإنترنت ، فسيستمر في محاولة الاتصال بسحابة Meraki حتى يكتسب الاتصال. بمجرد اتصال الجهاز بالإنترنت ، يتلقى تلقائيًا أحدث إعدادات التكوين من سحابة Meraki. إذا تم إجراء تغييرات على تكوين الجهاز أثناء اتصال الجهاز بالإنترنت ، فسيتلقى الجهاز هذه التغييرات ويحدثها تلقائيًا. تتوفر هذه التغييرات بشكل عام على الجهاز في غضون ثوانٍ. ومع ذلك ، قد تستغرق الكميات الكبيرة من التغييرات وقتًا أطول للوصول إلى أجهزتها. إذا لم يتم إجراء أي تغييرات على التكوين من قبل المستخدم ، فسيستمر الجهاز في البحث بشكل دوري عن تحديثات التكوين الخاصة به من تلقاء نفسه.

أثناء تشغيل الجهاز على الشبكة ، سيقوم بتوصيل تحليلات استخدام الجهاز والشبكة مرة أخرى إلى سحابة Meraki. يتم تحديث تحليلات لوحة المعلومات المستندة إلى هذه المعلومات ، في شكل رسوم بيانية ومخططات ، بانتظام في سحابة Meraki ويتم عرضها في لوحة معلومات المستخدمين عندما يشاهدون هذه المعلومات.

8.8.2 حاويات التكوين

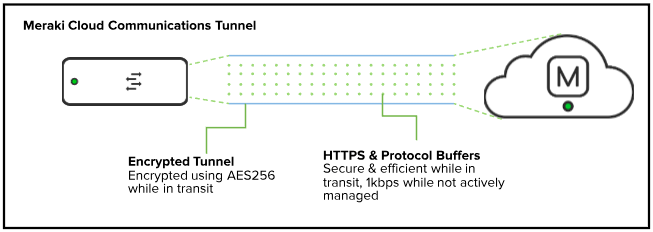
يتم تخزين تكوينات الجهاز كحاوية في خلفية Meraki. عندما يتم تغيير تكوين الجهاز بواسطة مسؤول الحساب عبر لوحة التحكم أو واجهة برمجة التطبيقات ، يتم تحديث الحاوية ثم دفعها إلى الجهاز المرتبطة به الحاوية عبر اتصال آمن. تقوم الحاوية أيضًا بتحديث سحابة Meraki بتغيير تكوينها لتجاوز الفشل والتكرار.



الشكل (31) حاويات التكوين

9.8.2 اتصال آمن للأجهزة

بالنسبة للأجهزة للاتصال بالسحابة ، تستفيد Meraki من نفق مشفر خفيف الوزن مملوك باستخدام تشفير AES256 أثناء نقل بيانات الإدارة. داخل النفق نفسه ، تستفيد Meraki من HTTPS والمخازن المؤقتة للبروتوكول للحصول على حل آمن وفعال ، يقتصر على 1 كيلو بت في الثانية لكل جهاز عندما لا تتم إدارة الجهاز بشكل فعال.

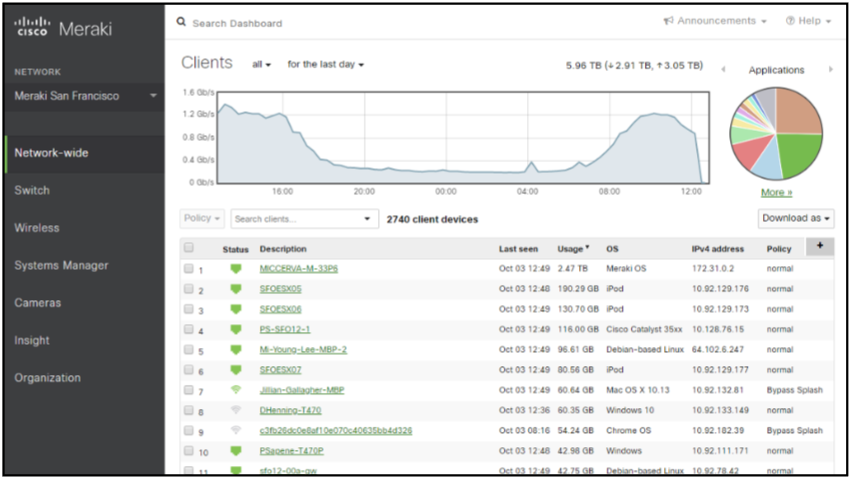


الشكل (32) اتصال آمن للأجهزة

10.8.2 واجهات التكوين

1.10.8.2 لوحة القيادة Meraki

2.10.8.2 لوحة معلومات Meraki هي أداة حديثة قائمة على مستعرض الويب تستخدم لتكوين أجهزة وخدمات Meraki.



الشكل (33) واجهات التكوين

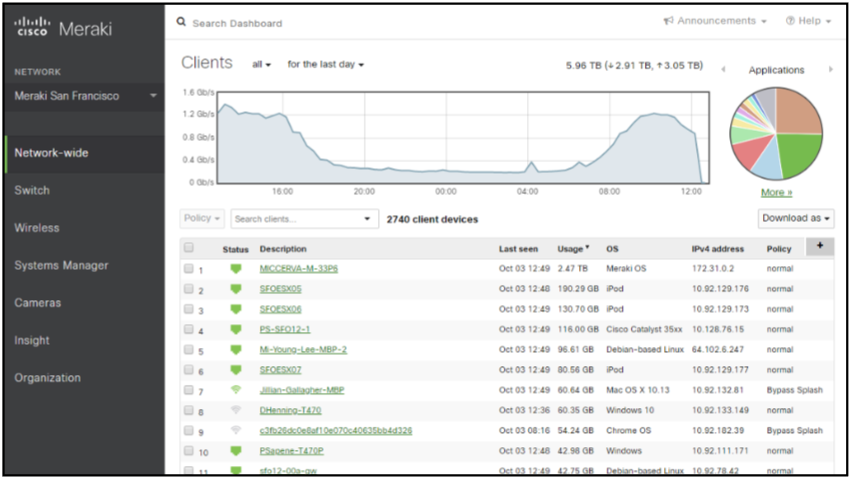
1.10.8.2 لوحة معلومات Meraki هي البديل المرئي لسطر الأوامر التقليدي ، والذي يستخدم لإدارة العديد من أجهزة التوجيه والمحولات وأجهزة الأمان والمزيد. بدلاً من ذلك ، يضع Meraki جميع الأجهزة داخل الشبكات في مكان واحد ويسمح للمستخدمين بتطبيق التغييرات بتنسيق بسيط وسهل الاستخدام.

بالإضافة إلى تبسيط إدارة الجهاز ، تعد لوحة المعلومات أيضًا منصة لعرض تحليلات الشبكة ، وتطبيق أذونات الشبكة ، وتتبع المستخدمين. تسمح لوحة القيادة للمستخدمين بمشاهدة تدفقات الكاميرا وإدارة الأجهزة المحمولة وأجهزة الكمبيوتر الخاصة بالمستخدمين وتعيين قواعد المحتوى ومراقبة الاتصالات الأولية من مكان واحد.

1.10.8.2 واجهات برمجة تطبيقات Meraki

توفر واجهات برمجة تطبيقات Meraki التحكم في حل Meraki بطريقة قابلة للبرمجة ، وتمكين الإجراءات التي قد لا تكون ممكنة مع لوحة المعلومات ، أو إثبات المزيد من التحكم الدقيق. واجهات برمجة تطبيقات Meraki هي واجهات برمجة تطبيقات RESTful تستخدم HTTPS للنقل و JSON لتسلسل الكائن.

من خلال توفير إمكانية الوصول إلى واجهة برمجة التطبيقات المفتوحة ، تستفيد Meraki من قوة النظام الأساسي السحابي على مستوى أعمق لإنشاء حلول أكثر كفاءة وقوة. من خلال Meraki APIs ، يمكن للمستخدمين أتمتة عمليات النشر ومراقبة شبكاتهم وبناء حلول إضافية أعلى لوحة معلومات Meraki.



الشكل (34) Meraki API

ترتبط مفاتيح API بحساب مستخدم معين من خلال منصة Meraki. إذا كان لدى الفرد حق الوصول الإداري إلى العديد من مؤسسات Meraki ، فيمكن لمفتاح واحد تكوين هذه المؤسسات المتعددة والتحكم فيها.

11.8.2 المصداقية والتواجد

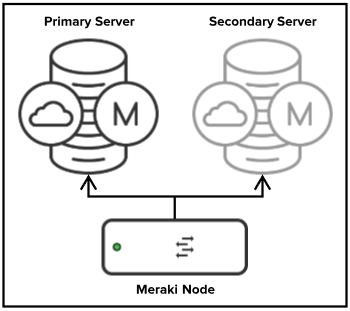
تتيح Meraki بنية عالية الإتاحة (HA) بطرق متعددة لضمان إمكانية الخدمة العالية لعملائنا. اتصالات الشبكة من خلال مراكز البيانات لدينا عالية في النطاق الترددي ومرنة للغاية. تضمن هياكل HA المشتركة توفر البيانات في حالة حدوث عطل محلي ، وتضمن بنية النسخ الاحتياطي لمركز البيانات لدينا توفر بيانات إدارة العملاء دائمًا في حالة الفشل الذريع. يتم تخزين هذه النسخ الاحتياطية على خدمات التخزين السحابية لجهات خارجية. تقوم خدمات الجهات الخارجية هذه أيضًا بتخزين بيانات Meraki استنادًا إلى المنطقة لضمان الامتثال للوائح تخزين البيانات الإقليمية.

12.8.2 توفر عالي لاتصال الارتباط الصاعد لمركز البيانات

تراقب Meraki باستمرار الاتصالات للتأكد من سلامتها باستخدام اتصالات متعددة عالية السرعة من مراكز البيانات الخاصة بها. يقوم اتصال شبكة Meraki بإجراء اختبارات لإمكانية الوصول إلى DNS لتحديد أن مراكز التكامل والبيانات ستنتقل إلى الارتباطات الثانوية في حالة الارتباط المتدهور.

13.8.2 التوفر العالي لخادم Meraki

يتصل جهاز واحد بخوادم Meraki متعددة في نفس الوقت ، مع التأكد من تحديث جميع البيانات في حالة الحاجة إلى تجاوز الفشل. يتحقق اتصال خادم Meraki الثانوي هذا من سلامة تكوين الجهاز وبيانات استخدام الشبكة التاريخية في حالة فشل خادم Meraki.

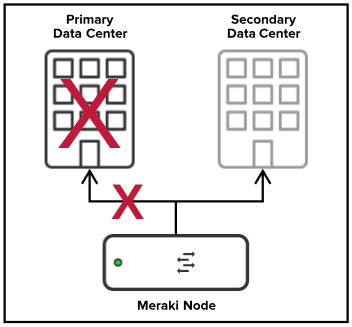


الشكل (35) التوفر العالي لخادم Meraki

في حالة فشل الخادم أو فقد الاتصال ، يمكن أن يتجاوز اتصال العقدة بالخادم الثانوي. عند استعادة الخادم الأساسي ، سيتم إعادة إنشاء الاتصال دون تأثير ملحوظ على العقد المتصلة.

14.8.2 التوفر العالي للنسخ الاحتياطي لمركز البيانات

يحتفظ Meraki ببيانات إدارة العملاء النشطة في مركز بيانات أساسي وثانوي في نفس المنطقة. يتم فصل مراكز البيانات جغرافيًا لتجنب الكوارث المادية أو الانقطاعات التي قد تؤثر على نفس المنطقة. تتم مزامنة البيانات المخزنة في مراكز البيانات هذه في الوقت الفعلي. في حالة فشل مركز البيانات ، سيفشل مركز البيانات الأساسي في الوصول إلى مركز البيانات الثانوي مع تخزين أحدث تكوين.



الشكل (36) التوفر العالي للنسخ الاحتياطي لمركز البيانات

15.8.2 خطة التعافي من الكوارث

يعد تخزين بيانات إدارة العملاء وموثوقية لوحة المعلومات وخدمات واجهة برمجة التطبيقات من الأولويات الأساسية لشركة Meraki. للمساعدة في منع فقدان البيانات في حالة وقوع كارثة ، لدى Meraki العديد من نقاط التكرار الرئيسية. يتم إقران كل مركز بيانات Meraki مع مركز بيانات آخر في نفس المنطقة. إذا تم محو مركز البيانات تمامًا ، فيمكن إنشاء النسخ الاحتياطية في غضون دقائق في مركز البيانات الآخر في المنطقة. بعد ذلك ، في حالة تأثر مركزي البيانات ، يمكن استخدام النسخ الاحتياطية الليلية المستضافة في خدمتين مختلفتين للتخزين السحابي لجهة خارجية ، لكل منهما نسخ احتياطية للتخزين المادي ، لاستعادة البيانات.

16.8.2 بيانات الإدارة

تجمع سحابة Meraki وتخزن أنواعًا معينة من بيانات "الإدارة" لتمكين حلولها. يتم تشفير جميع أشكال البيانات أثناء النقل من وإلى خوادم Meraki. هناك أربعة أنواع رئيسية من البيانات المخزنة في سحابة Meraki:

1. سجلات المستخدم: تتضمن البريد الإلكتروني للحساب واسم الشركة أو معلومات اختيارية أخرى مثل اسم المستخدم والعنوان.
2. بيانات التكوين: تتضمن إعدادات الشبكة والتكوينات التي أجراها العملاء في لوحة معلومات Meraki.
3. بيانات التحليلات: تتضمن بيانات تحليلات العميل وحركة المرور والموقع ، مما يوفر تصورات ورؤى للشبكة في أنماط حركة المرور عبر مواقع العملاء.
4. الأصول المحملة بواسطة العميل: تشمل مخططات الطوابق المخصصة وشعارات البداية.

17.8.2 فصل بيانات الخادم

يتم فصل بيانات المستخدم على خوادم Meraki بناءً على أذونات المستخدم. تتم مصادقة كل حساب مستخدم بناءً على عضوية المؤسسة ، مما يعني أن كل مستخدم لديه فقط حق الوصول إلى المعلومات المرتبطة بالمؤسسات التي تمت إضافته إليها كمستخدمين. يضيف مسؤولو المؤسسة المستخدمين إلى مؤسساتهم الخاصة ، ويقوم هؤلاء المستخدمون بتعيين اسم المستخدم وكلمة المرور الآمنة الخاصة بهم. ثم يتم ربط هذا المستخدم بالمعرف الفريد لتلك المؤسسة ، وبعد ذلك يكون قادرًا فقط على تقديم طلبات إلى خوادم Meraki للحصول على البيانات التي تم تحديد نطاقها لمعرفات المؤسسة المعتمدة الخاصة بهم.

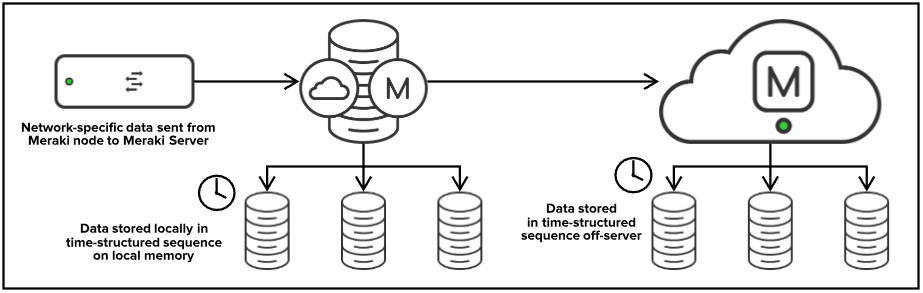
بالإضافة إلى ذلك ، تمتلك فرق تطوير Meraki خوادم منفصلة للتطوير والإنتاج ، لذلك لا تستخدم Meraki أبدًا بيانات العملاء الحية للاختبار أو التطوير. لا يمكن الوصول إلى بيانات مستخدم Meraki أبدًا للمستخدمين الآخرين أو تخضع لتغييرات التطوير.

18.8.2 فصل بيانات الشبكة والإدارة

يفصل مستوى التحكم Meraki "خارج النطاق" بيانات الإدارة عن بيانات المستخدم. تتدفق بيانات الإدارة من أجهزة Meraki (مثل نقاط الوصول اللاسلكية والمفاتيح وأجهزة الأمان) إلى سحابة Meraki عبر اتصال إنترنت آمن. لا تتدفق بيانات المستخدم (حركة مرور الشبكة ، وتصفح الويب ، والتطبيقات الداخلية ، وما إلى ذلك) عبر سحابة Meraki ، وبدلاً من ذلك تتدفق مباشرة إلى الوجهة على الشبكة المحلية أو عبر WAN.

19.8.2 الاحتفاظ ببيانات استخدام الشبكة

يقوم Meraki بتخزين بيانات الإدارة مثل استخدام التطبيق وتغييرات التكوين وسجلات الأحداث داخل نظام الواجهة الخلفية. يتم تخزين بيانات العملاء لمدة 14 شهرًا في منطقة الاتحاد الأوروبي ولمدة 26 شهرًا في باقي أنحاء العالم. تعتمد الفترات الزمنية لتخزين بيانات Meraki على ميزات إعداد التقارير السنوية في لوحة المعلومات (فترات 12 شهرًا) ، بالإضافة إلى وقت إضافي لضمان إزالة البيانات من النسخ الاحتياطية من Meraki عند الحذف (شهرين). يستخدم Meraki نظام قاعدة بيانات خاص لإنشاء بيانات قابلة للبحث والرجوع بسهولة.



الشكل (37) الاحتفاظ ببيانات استخدام الشبكة

20.8.2 أصول المستخدم المنفصلة

تقوم Meraki بتخزين الأصول التي تم تحميلها بواسطة العملاء مثل مخططات الطوابق المخصصة وشعارات البداية. يتم الاستفادة من هذه العناصر داخل لوحة معلومات Meraki لشبكة العملاء المحددة فقط ، وبالتالي يتم تقسيمها بشكل آمن بناءً على أذونات المستخدم القياسية المرتبطة بالوصول إلى معرف الشبكة أو المؤسسة. يمكن فقط للمستخدمين المصادق عليهم للوصول إلى الشبكة المضيفة الوصول إلى الأصول التي تم تحميلها.

21.8.2 أمن البيانات

يتم نقل جميع البيانات المنقولة من وإلى أجهزة وخوادم Meraki عبر نفق اتصالات آمن خاص (راجع قسم "الاتصال الآمن" أعلاه). يتم تشفير بيانات الاتصالات أثناء النقل عبر هذا النفق. تحتوي جميع اتصالات إدارة العميل (لوحة القيادة / واجهة برمجة التطبيقات) بسحابة Meraki على تشفير TLS آمن لجميع حركة مرور التطبيقات.

بالإضافة إلى ذلك ، يتم تشفير النسخ الاحتياطية لبيانات Meraki بالكامل باستخدام AES256 ولها وصول مقيد (راجع قسم "الأمن الداخلي المادي والتشغيلي").

22.8.2 خصوصية البيانات

يستلزم الاتصال بحل السحابة تخزين بيانات محددة في السحابة لسهولة الاستخدام والوصول. للحفاظ على النزاهة والأمان ، يجب أن تأخذ البنية التحتية السحابية في الاعتبار قواعد الحساسية والامتثال لتلك البيانات. تمتلك صناعات ومناطق جغرافية معينة قوانين لحماية بيانات المستخدم التي تعالجها Meraki من خلال البنية التحتية السحابية المرنة.

تقوم Meraki بتضمين الخصوصية حسب التصميم في تطوير منتجاتها وميزاتها بالإضافة إلى ممارسات الأعمال. الخصوصية هي جزء لا يتجزأ من عملية تصميم Meraki وهي اعتبار من تصميم المنتج الأولي وصولاً إلى تنفيذ المنتج. تقدم Meraki مجموعة كاملة من الميزات التي تعتمد على الخصوصية لجميع العملاء على مستوى العالم. تتيح هذه الميزات لعملائنا إدارة متطلبات الخصوصية والمساعدة في دعم مبادرات الخصوصية الخاصة بهم. يمكن للعملاء قراءة المزيد حول بعض ميزات خصوصية Meraki في مقالة خصوصية البيانات وميزات الحماية.

23.8.2 PCI

يوفر Meraki حلاً شاملاً لضمان بيئة متوافقة مع PCI يتم الالتزام بها وفقًا للمعايير الصارمة لتدقيق المستوى 1 PCI (مستوى التدقيق الأكثر صرامة). تتناول مجموعة ميزات الأمان الغنية جميع معايير أمان بيانات PCI ، مما يساعد العملاء على بناء شبكة آمنة والحفاظ عليها ، والحفاظ على برنامج إدارة الثغرات الأمنية ، وتنفيذ تدابير قوية للتحكم في الوصول ، ومراقبة أمان الشبكة.

24.8.2 حماية

أمان العميل هو أولوية قصوى لشركة Meraki. تحافظ الاستثمارات الضخمة في الأدوات والعمليات والتقنيات على أمان مستخدمينا وشبكاتهم ، بما في ذلك ميزات مثل المصادقة الثنائية للوصول إلى لوحة المعلومات وبنية إدارة السحابة خارج النطاق.

بالإضافة إلى فرق الأمن الداخلي في Meraki و Cisco ، تستفيد Meraki من الأطراف الثالثة لتوفير أمان إضافي. يتم تضمين الاحتياطات مثل عمليات الفحص اليومية للثغرات الأمنية من جهة خارجية واختبار التطبيق واختبار الخادم في برنامج أمان Meraki. بدأت Meraki أيضًا برنامج مكافآت الثغرات الأمنية لكل من الأجهزة والبرامج ، مما يشجع الباحثين الخارجيين على التعاون مع فريق الأمان لدينا للحفاظ على أمان بنيتنا التحتية وعملائنا. يمكن العثور على مزيد من المعلومات حول هذا البرنامج على صفحة برنامج Bugcrowd.

تعمل البنية التحتية الأمنية الذكية من Meraki على التخلص من تعقيدات الإدارة والاختبار اليدوي وتحديات الصيانة المستمرة التي تؤدي إلى نقاط الضعف. تُعد ميزات الأمان البديهية والفعالة من حيث التكلفة مثالية لمسؤولي الشبكات ، في حين أن أدوات الإدارة القوية والدقيقة ، وحماية الحساب ، وعمليات التدقيق ، وتغيير الإدارة تناشد كبار مسؤولي أمن المعلومات.

25.8.2 أمن الأجهزة والبرامج

تستفيد Meraki من التكنولوجيا مثل التمهيد الآمن وتوقيع صورة البرامج الثابتة ومثبتات ثقة الأجهزة كجزء من دورة حياة Cisco Secure Development للحفاظ على تكامل الأجهزة والبرامج.

26.8.2 الأمن الداخلي المادي والتشغيلي

تلتزم Meraki بالحفاظ على أمان المستخدم من خلال توفير التدريب الأمني التشغيلي الإلزامي لجميع الموظفين. تم وضع برامج رسمية للتوعية بأمن المعلومات لجميع الموظفين. بالإضافة إلى ذلك ، يتعين على جميع الموظفين والمقاولين الامتثال لسياسة فحص الخلفية الخاصة بشركة Cisco والالتزام بسياسة أمان معلومات Meraki واتفاقيات السرية القياسية للصناعة.

يتم الوصول عن بعد إلى خوادم Meraki عبر IPSec VPN و SSH. يتم تحديد نطاق الوصول وتقييده من قبل فرق الأمن الداخلي والبنية التحتية لدينا بناءً على قواعد صارمة لاحتياجات العمل.

للوصول إلى خوادم Meraki السحابية وقواعد البيانات والرمز ، هناك نماذج وصول قائمة على الأدوار لوصول المستخدم وأذونات محددة في المكان. يتم فرض المصادقة الثنائية لجميع المستخدمين الذين لديهم حق الوصول إلى هذه الأنظمة ، داخليًا وعن بُعد.

27.8.2 الأمن الداخلي المادي والتشغيلي

تلتزم Meraki بالحفاظ على أمان المستخدم من خلال توفير التدريب الأمني التشغيلي الإلزامي لجميع الموظفين. تم وضع برامج رسمية للتوعية بأمن المعلومات لجميع الموظفين. بالإضافة إلى ذلك ، يتعين على جميع الموظفين والمقاولين الامتثال لسياسة فحص الخلفية الخاصة بشركة Cisco والالتزام بسياسة أمان معلومات Meraki واتفاقيات السرية القياسية للصناعة.

يتم الوصول عن بعد إلى خوادم Meraki عبر IPSec VPN و SSH. يتم تحديد نطاق الوصول وتقييده من قبل فرق الأمن الداخلي والبنية التحتية لدينا بناءً على قواعد صارمة لاحتياجات العمل.

للوصول إلى خوادم Meraki السحابية وقواعد البيانات والرمز ، هناك نماذج وصول قائمة على الأدوار لوصول المستخدم وأذونات محددة في المكان. يتم فرض المصادقة الثنائية لجميع المستخدمين الذين لديهم حق الوصول إلى هذه الأنظمة ، داخليًا وعن بُعد.

يتم تأمين الوصول المادي إلى البنية التحتية السحابية Meraki في جميع الأوقات ، عن طريق دوريات خدمة الحراسة ، ويحتوي على مراقبة فيديو خارجية وداخلية مع مراقبة في الوقت الفعلي. للوصول المادي ، تحتوي جميع مراكز البيانات على نظام بطاقة مفتاح عالي الأمان وأجهزة قراءة المقاييس الحيوية. لا يُمنح الوصول إلى مراكز البيانات هذه إلا للمستخدمين الذين يحتاجون الأعمال للوصول إليها ، والاستفادة من مصادقة PKI والمصادقة الثنائية للتحقق من الهوية. يقتصر هذا الوصول على عدد قليل جدًا من الموظفين ويتم تدقيق وصول المستخدم شهريًا.

**الفصل الثالث- دراسة البروتوكولات المستخدمة**

1.3 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

1.1.3 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.

**مزايا استخدام :DHCP**

* إدارة مركزية لعناوين .IP
* إضافة عملاء جدد بشكل سلس إلى الشبكة.
* إعادة استخدام عناوين IP ، وتقليل العدد الإجمالي لعناوين IP المطلوبة.

**عيوب استخدام :DHCP**

* يصبح تتبع نشاط الإنترنت مملاً ، حيث يمكن أن يكون للجهاز نفسه عدة عناوين IP خلال فترة زمنية.
* لا يمكن استخدام أجهزة الكمبيوتر المزودة بـ DHCP كخوادم ، حيث تتغير عناوين IP الخاصة بها بمرور الوقت.

2.1.3 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.

**مزايا استخدام:**DNS

* يسهل الوصول إلى الإنترنت.
* يلغي الحاجة إلى حفظ عناوين. IP

**سلبيات استخدام :**DNS

* لا تحمل استعلامات DNS معلومات تتعلق بالعميل الذي بدأها. هذا لأن خادم DNS لا يرى سوى عنوان IP من حيث جاء الاستعلام ، مما يجعل الخادم عرضة للتلاعب من المتسللين.
* يمكن لخوادم جذر DNS ، إذا تم اختراقها ، تمكين المتسللين من إعادة التوجيه إلى صفحات أخرى لبيانات التصيد الاحتيالي.

3.1.3 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.

**مزايا استخدام :FTP**

* يتيح مشاركة الملفات الكبيرة والدلائل المتعددة في نفس الوقت.
* يتيح لك استئناف مشاركة الملفات إذا تمت مقاطعتها.
* يتيح لك استعادة البيانات المفقودة وجدولة نقل الملفات.

**سلبيات استخدام :FTP**

* يفتقر بروتوكول نقل الملفات إلى الأمان. يتم نقل البيانات وأسماء المستخدمين وكلمات المرور بنص عادي ، مما يجعلها عرضة للجهات الضارة.
* يفتقر FTP إلى إمكانات التشفير ، مما يجعله غير متوافق مع معايير الصناعة.

4.1.3 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.

5.1.3 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.

**مزايا استخدام :HTTP**

* استخدام الذاكرة واستخدام وحدة المعالجة المركزية منخفضان بسبب الاتصالات المتزامنة الأقل.
* يمكن الإبلاغ عن الأخطاء بدون إغلاق الاتصالات.
* بسبب اتصالات TCP الأقل ، يتم تقليل ازدحام الشبكة.

**سلبيات استخدام :HTTP**

* يفتقر HTTP إلى إمكانات التشفير ، مما يجعله أقل أمانًا.
* يتطلب HTTP مزيدًا من القوة لإنشاء اتصال ونقل البيانات.

6.1.3 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).

7.1.3 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.

**مزايا استخدام :SMTP**

* سهولة التركيب.
* يتصل بأي نظام دون أي قيود.
* لا يحتاج إلى أي تطوير من جانبك.

**سلبيات استخدام :SMTP**

* يمكن للمحادثات ذهابًا وإيابًا بين الخوادم أن تؤخر إرسال رسالة ، كما تزيد أيضًا من فرصة عدم تسليم الرسالة.
* يمكن لبعض جُدر الحماية أن تحجب المنافذ المستخدمة مع .SMTP

8.1.3 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.

**مزايا استخدام Telnet:**

* متوافق مع أنظمة تشغيل متعددة.
* يوفر الكثير من الوقت بسبب اتصاله السريع بالأجهزة البعيدة.

**سلبيات استخدام Telnet:**

* تفتقر Telnet إلى إمكانات التشفير وترسل عبر المعلومات الهامة بنص واضح ، مما يسهل على الجهات الضارة.
* باهظة الثمن بسبب سرعات الكتابة البطيئة.

9.1.3 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.

الخلاصة:

الأهداف المستقبلية:

استخدام IMAP بدل Pop3

المراجع:

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/