مبادئ وأساسيات الشبكات

م. هاشم بن مستور الشريف
عضو هيئة التدريب بالكلية التقنية بحائل

١٤٤٦هـ

مقدمة:

تعتبر شبكات الحاسب الآلي من أهم المواضيع التي يتم دراستها في علوم الحاسب إذ تشكل أساساً مهماً للاتصال بين الأجهزة الحاسوبية وتبادل المعلومات والبيانات بينها. وتعتبر مادة مبادئ شبكات الحاسب الآلي هي الأساس الذي يجب على الطالب في كافة تخصصات الحاسب الآلي معرفته وفهمه بشكل جيد لمعرفة كيف تتواصل الأجهزة مع بعضها البعض سواء في نطاق الشبكات المحلية أو على نطاق أوسع مثل شبكة الانترنت.

يعتبر هذا الكتاب محاولة جمع وتبسيط لأساسيات ومبادئ شبكات الحاسب الآلي وعند الحديث عن أنظمة التشغيل كان التركيز على أجهزة Cisco ويتكون الكتاب من عدة فصول تغطي مجموعة واسعة من الموضوعات، بدءاً من تعريف الشبكات وأنواعها، وصولاً إلى تصميم وتطبيقات الشبكات وأدوات الشبكات المختلفة والأمان في الشبكات.

يمثل هذا الكتاب الجزء الأساسي لموضوعات شبكات الحاسب الآلي، بحيث يستطيع الطلاب الاستفادة منه كأساس ينطلق من خلاله إلى فهم المفاهيم الأساسية والتحليل العميق للمواضيع المتقدمة.

أسأل الله سبحانه وتعالى أن يجعل هذا العمل خالصاً لوجه وأن يجد فيه أبنائنا الطلاب شيئاً مفيداً ونافعاً وأعلم تمام العلم أن الكمال لله عز وجل وأن عمل الأنسان مهما بذل فيه من جهد ووقت يبقى ناقص ويعتريه القصور والخطأ.

ختاماً .. أشكر الأخ الحبيب المهندس رائد بن سليم الحربي ، على تفضله ومراجعته وتزويده لي بالملاحظات الجوهرية والمفيدة والتي أثمرت في خروج هذه النسخة الأولى من الكتاب فلا حرمه ربي الأجر وأسأل الله له التوفيق والسداد

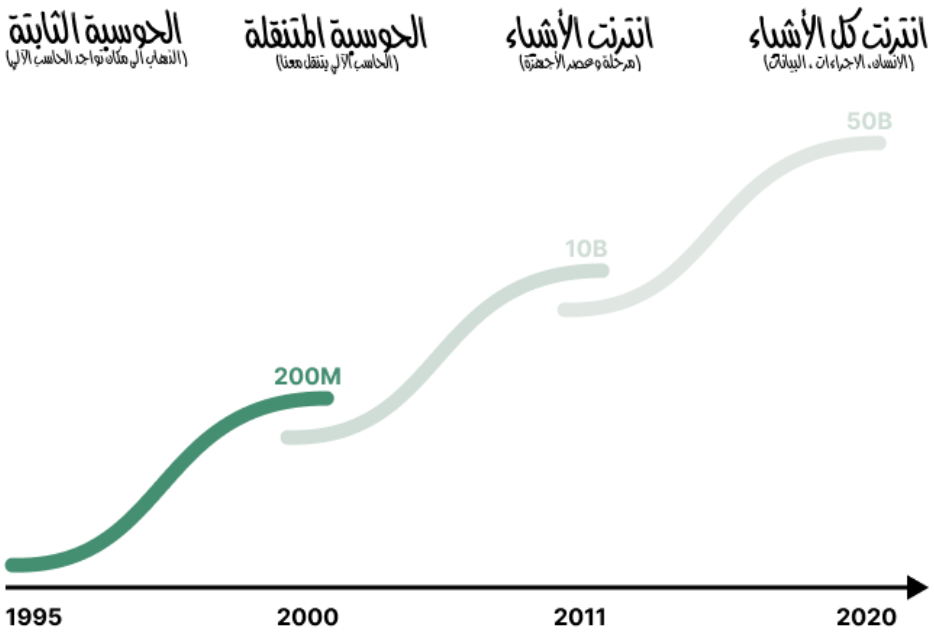
المهندس / هاشم بن مستور الشريف

الشبكات في الماضي وفي حياتنا الحالية:

يعود تاريخ بداية دراسة شبكات الحاسب إلى عقود مضت، حيث بدأت الأبحاث الأولى في هذا المجال في الستينيات والسبعينيات من القرن الماضي. وفي ذلك الوقت، كان الهدف الرئيسي للأبحاث هو توصيل أجهزة الحاسب الآلي ببعضها البعض لتسهيل تبادل المعلومات والبيانات بينها، وتطوير طرق التواصل بينها.

ومع تطور أجهزة الحاسب الآلي والتكنولوجيا بدأت شبكات الحاسب في الانتشار والتطور بشكل كبير حتى أصبحت تستخدم في العديد من المجالات مثل الأعمال التجارية والترفيه والتعليم والخدمات الحكومية أي انها تحولت من مجرد أسلوب لتبادل المعلومات بين أجهزة الحاسب الآلي إلى جزء أساسي من الحياة اليومية لا يمكن الاستغناء عنه وأصبحت قادرة على وتوصيل الأفراد ببعضهم البعض في جميع أنحاء العالم.

واليوم تمتد مجالات تخصص شبكات الحاسب إلى تصميم وتطوير البرمجيات والأجهزة والبنية التحتية للشبكات وحماية الأمن السيبراني.



من الأشياء التي تدعمها شبكات الحاسب في حياتنا اليومية ونلمسها بوضوح :

- ☐ دعم طريقة التعلم
- ☐ دعم طريقة التواصل
- ☐ دعم طريقة العمل
- ☐ دعم طريقة اللعب

أحجام شبكات الحاسب:

تختلف أحجامها بشكل كبير اعتمادًا على نوع الشبكة والاستخدام الذي يراد منها فقد تكون ذات حجم صغير مثل الشبكات المنزلية التي توفر الاتصال بين الأجهزة في منزل واحد أو مكتب صغير وقد تكون ذات حجم أكبر مثل الشبكات الموجودة في الحرم الجامعي والتي تربط أجهزة الحاسب الآلي في مكان واحد أو تلك الموجودة في المستشفيات وقد تكون أكبر حجمًا مثل الشبكات الواسعة النطاق التي تغطي مناطق كبيرة وتربط أجهزة الحاسب الآلي في مدن أو دول بأكملها.

يمكن أن تشمل شبكات الحاسب أيضًا عددًا كبيرًا من الأجهزة بما في ذلك أجهزة الحاسب الآلي والهواتف الذكية والأجهزة اللوحية وغيرها، وتتوفر اليوم شبكات ضخمة تضم الملايين من الأجهزة في جميع أنحاء العالم مثل الإنترنت والسحابة الحاسوبية وشبكات التواصل الاجتماعي


Small Home Networks


Small Office/Home Office Networks


Medium to Large Networks

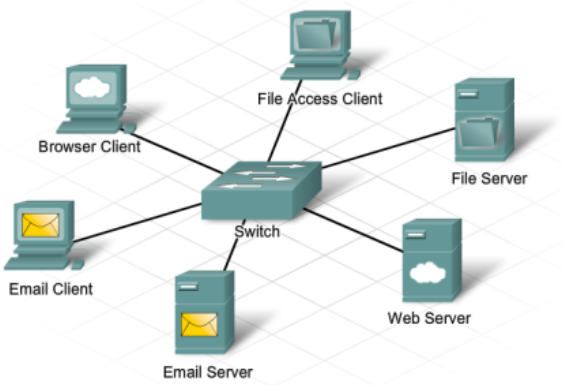

World Wide Networks

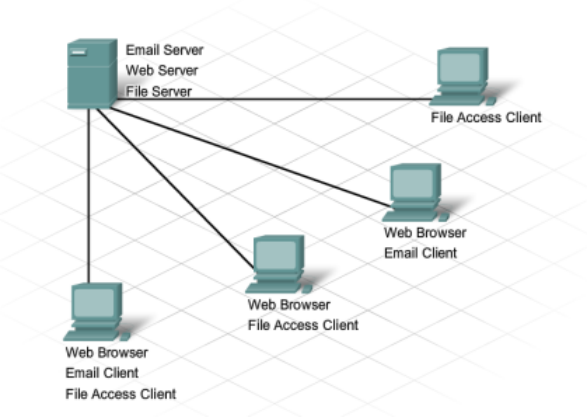
ماذا يقصد بمصطلح (العملاء والخوادم) في شبكات الحاسب :

يشير مصطلح العميل والخادم (Client-Server) إلى علاقة تفاعلية بين جهازي حاسب أو برمجيات، حيث يعمل الجهاز الأول (العميل) على طلب الخدمات أو الموارد التي يريدها من الجهاز الثاني (الخادم) والذي بدوره يستجيب لهذه الطلبات ويقدم الموارد المطلوبة.

وعليه فيمكن أن تكون العلاقة بين العميل والخادم في صورة طلب واستجابة مباشرة حيث يقوم العميل بإرسال طلباته إلى الخادم وتتم الاستجابة لها بشكل فوري ويمكن أن يكون الاتصال بين العميل والخادم على شكل دائم ومستمر بحيث يقوم العميل بالتواصل بشكل دوري مع الخادم لتحديث المعلومات أو الحصول على الموارد الجديدة.

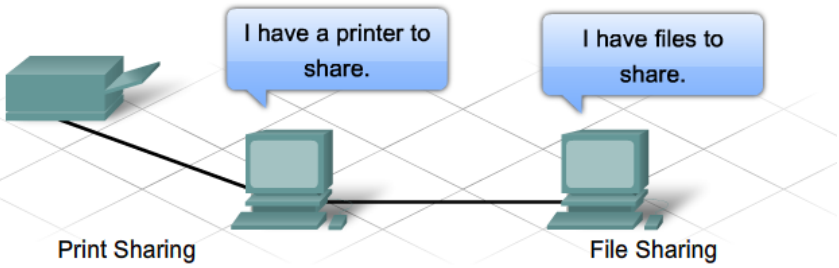
وتستخدم هذه العلاقة في العديد من التطبيقات والخدمات على الإنترنت مثل البريد الإلكتروني والمواقع الإلكترونية والتطبيقات السحابية بحيث يتم استخدام الخادم لتخزين وتوفير الموارد والخدمات المطلوبة من قبل العميل





شبكات (نظير إلى نظير) :

شبكات نظير إلى نظير (P2P) هي نموذج آخر للاتصال بين أجهزة الحاسب الآلي والتطبيقات التي تتيح التواصل والتبادل المباشر للموارد فيما بينها ودون الحاجة إلى وجود خادم مركزي.



ويتم في هذا النموذج توزيع العمل بين الأجهزة المشاركة حيث يمكن لأي جهاز في الشبكة الوصول للموارد المتاحة وتوفير الموارد المطلوبة للجهاز الآخر أي أنه يمكن لأي جهاز أن يكون عميلاً وخادماً في ذات الوقت ويعتبر هذا النموذج مناسبًا لتحميل الملفات وتوزيع المحتوى على المستخدمين وللتواصل الفوري مثل تطبيقات المحادثة.

ويتم استخدام شبكات نظير إلى نظير في العديد من التطبيقات الشائعة، مثل تبادل الملفات عبر الإنترنت والعمليات المالية المشفرة والألعاب عبر الإنترنت.

مكونات الشبكة الأساسية:

تتكون الشبكة من ثلاث مكونات أساسية وهي:

١. **الأجهزة:** وتشمل الأجهزة المستخدمة في الشبكة مثل أجهزة الحاسب الآلي والموجهات (Router) والمبدلات (Switch) والخوادم (Server) وغيرها. وتسمح هذه الأجهزة بتوصيل الأجهزة المختلفة ببعضها البعض في الشبكة ونقل البيانات والمعلومات بينها.

٢. **الخدمات (البرمجيات):** وتشمل البرمجيات المستخدمة في الشبكة مثل برامج إدارة الشبكة وبرامج الحماية وبرامج التشغيل والتطبيقات المختلفة التي تستخدمها الأجهزة في الشبكة.

٣. **الوسائط:** وتشمل الكابلات المستخدمة لربط الأجهزة في الشبكة مثل الكابلات النحاسية والألياف الضوئية وغيرها كما تشمل أيضاً الموجات اللاسلكية التي تعتمد على تقنية WiFi للاتصال بالشبكة.

تتفاعل هذه المكونات مع بعضها البعض لتشكل الشبكة الأساسية وتتيح للأجهزة التواصل ونقل البيانات والمعلومات فيما بينها

أنواع الأجهزة المستخدمة في شبكات الحاسب:

يوجد نوعين من الأجهزة المستخدمة في شبكات الحاسب وهما:

١. **الأجهزة الوسيطة (البينية):** هي الأجهزة التي تستخدم لربط الأجهزة الطرفية (End Devices) مع بعضها البعض في الشبكة، وتساعد في تحسين أداء الشبكة وزيادة سرعة نقل البيانات. وتشمل الأجهزة الوسيطة الأشهر في شبكات الحاسب هي الموجهات (Router) والمبدلات (Switch) ومكررات الإشارة (Hubs) ونقاط الوصول اللاسلكية (Wireless Access Points) بحيث تعمل هذه الأجهزة على توجيه حركة المرور في الشبكة وتوزيع البيانات والمعلومات بين الأجهزة الطرفية فتحسين أداء الشبكة عن طريق تحسين سرعة النقل وتحسين تدفق البيانات وزيادة كفاءة الاتصالات. وتلعب الأجهزة الوسيطة دورًا مهمًا في تصميم الشبكة، حيث يعتبر جزء أساسي في تصميم الشبكة تحديد المكان المثالي لوضعها وتحديد أنواعها وعددها واختيار الأجهزة الأفضل لتلبية احتياجات الشبكة وتحقيق أعلى مستويات الأداء.

٢. **الأجهزة الطرفية:** الأجهزة الطرفية (End Devices) في شبكات الحاسب هي الأجهزة التي تتصل بالشبكة لتلقي الخدمات وإرسال البيانات إليها. وتشمل الأجهزة الطرفية أي جهاز يتصل بالشبكة ويستخدمه المستخدم النهائي لأغراضه الشخصية أو العملية، مثل أجهزة الحاسب الآلي (الشخصية أو المحمولة) والهواتف الذكية والأجهزة اللوحية والأجهزة الذكية الأخرى. وتلعب

الأجهزة الطرفية دورًا حيويًا في الشبكات حيث تشكل جزءاً أساسياً من التطبيقات والخدمات التي توفرها الشبكات للمستخدمين. وتختلف متطلبات الأجهزة الطرفية وخصائصها وفقاً للدور الذي تقوم به ونوع الشـبكة الموجود فيها وعادة ما يتم تصـميم الشـبكة بناءً على متطلبات الأجهزة الطرفية المختلفة واحتياجات المستخدمين.

أنواع البرمجيات (الخدمات) المستخدمة في شبكات الحاسب:

تتنوع البرمجيات المستخدمة في شبكات الحاسب حسب الغرض من الاستخدام، ومن بين أهم أنواع البرمجيات المستخدمة في شبكات الحاسب:

١. **أنظمة التشغيل (Operating Systems):** وتشمل البرامج التي تدير عمليات أجهزة الحاسب الآلي والأجهزة الأخرى في الشبكة، وتشمل أنظمة التشغيل المختلفة مثل ويندوز ولينكس وماك أو إس.

٢. **برامج الحماية والأمان (Security Software):** وتتضمن البرامج المصممة لحماية الشبكة والأجهزة الموصولة بها من الهجمات الإلكترونية والفيروسات والبرامج الخبيثة، مثل برامج الحماية من الفيروسات والجدران النارية (Firewalls) وأدوات الكشف عن الاختراق.

٣. **برامج الخوادم (Server Software):** وتشمل البرامج التي تستخدم لتشغيل الخوادم في الشبكة، مثل برامج البريد الإلكتروني وخوادم الملفات وخوادم الويب وخوادم قواعد البيانات.

٤. **برامج إدارة الشبكة (Network Management Software):** وتشمل البرامج التي تساعد في إدارة ومتابعة أداء الشبكة، وتشمل أدوات المتابعة والتشخيص وأدوات إدارة الموارد وأدوات إدارة الاعدادات.

٥. **برامج التطبيقات (Applications Software):** وتشمل البرامج التي تستخدم لتشغيل التطبيقات المختلفة على الشبكة مثل برامج المكالمات الصوتية والفيديو والتطبيقات الإلكترونية المختلفة.

وهناك العديد من البرامج الأخرى التي تستخدم في شبكات الحاسب وتختلف بحسب نوع الشبكة وحجمها وأهدافها ومتطلبات المستخدمين.

أنواع الوسائط المستخدمة في شبكات الحاسب:

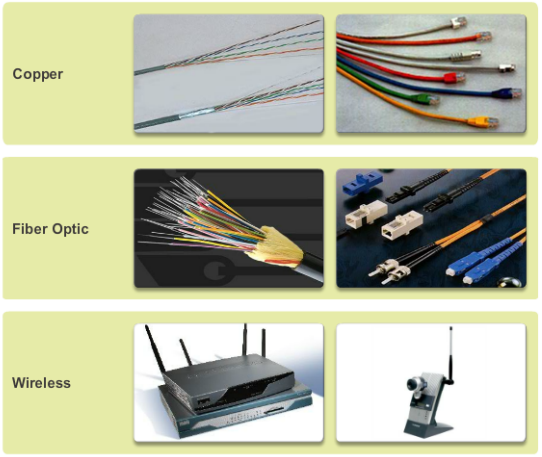
يمكن استخدام عدة أنواع من الوسائط لتوصيل شبكات الحاسب، ومن بين هذه الوسائط:

١. **الكابلات النحاسية:** وتشمل الكابلات النحاسية مثل الكابلات المحورية (Coaxial) والكابلات الغير محمية (UTP) والكابلات المحمية (STP) ويستخدم حالياً (UTP) و (STP) بشكل شائع في شبكات الحاسب المحلية.

٢. **الألياف الضوئية:** وتعتبر الألياف الضوئية أسرع وأكثر كفاءة من الكابلات النحاسية حيث تسمح بنقل البيانات على مسافات طويلة وبشكل أسرع وتستخدم هذه الوسائط في الشبكات الكبيرة مثل شبكات المؤسسات وشبكات الاتصالات الواسعة.

٣. **الموجات اللاسلكية:** تستخدم بعض الأجهزة اللاسلكية مثل الأجهزة الهواتف الذكية وأجهزة الحاسب الآلي المحمولة والأجهزة اللوحية خاصية الاتصال بالشبكة باستخدام إشارات الراديو وترددات اللاسلكي.

ويختلف كل نوع من الوسائط المستخدمة لتوصيل شبكات الحاسب من حيث المميزات والعيوب والتطبيقات المناسبة لكل نوع ويتم اختيار الوسيطة المناسبة حسب حاجة الشبكة واحتياجات المستخدمين.

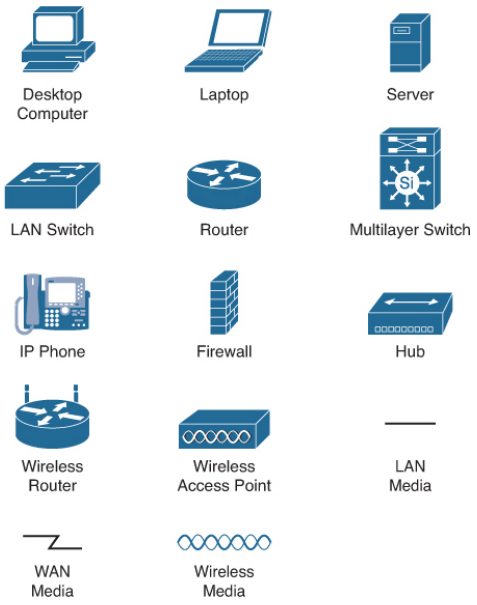


تمثيل الشبكة رسومياً (الأيقونات والرموز):

تلعب الأيقونات المستخدمة لتمثيل الشبكة وأجهزتها دورًا هاماً في فهم وتصور الشبكة والأجهزة الموجودة فيها حيث تمثل هذه الأيقونات الأجهزة والمكونات المختلفة للشبكة بشكل واضح وسهل الفهم.

وتتيح هذه الأيقونات التواصل بين المتخصصين في مجال شبكات الحاسب والأشخاص العاديين الذين يستخدمون الشبكة حيث يمكن استخدامها في الرسومات والتخطيطات والأشكال التوضيحية لتوضيح مكونات الشبكة وعلاقاتها ببعضها البعض مما يساعد على فهم أساسيات الشبكة وعملها بشكل أفضل.

علاوة على ذلك فإن استخدام الأيقونات الموحدة يجعل من السهل فهم التصميم العام للشبكة حيث يسهل استخدام نفس الأيقونات للمستخدمين والمتخصصين على حد سواء فهم تصميم الشبكات المختلفة والتواصل فيما بينهم .



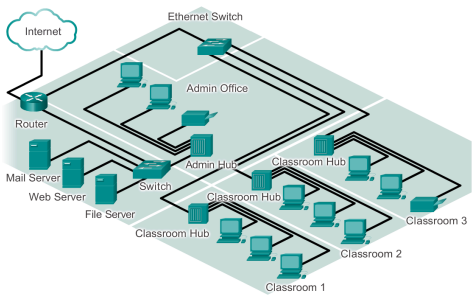
المخططات الهيكلية للشبكة:

- **المخطط الفيزيائي للشبكة (Physical Network Diagram)** يوضح كيفية توصيل الأجهزة والمعدات المختلفة في الشبكة ويصف الاتصالات الفعلية بينها فهو يعرض المخطط الفيزيائي للمكان وللأجهزة الفعلية في الشبكة والتوصيلات بينها.

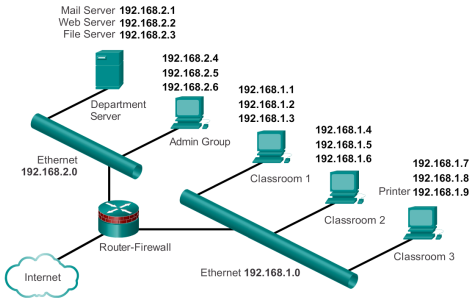
- **المخطط المنطقي للشبكة (Logical Network Diagram)** يركز على كيفية تبادل البيانات بين الشبكات أو بين الأجهزة في الشبكة الواحدة فهو يركز على عناوين الـ IP وعلى الشبكات الفرعية والشبكات الظاهرية (VLANs) وما أشبه ذلك.

بشكل عام، المخطط الفيزيائي يركز على تفاصيل الشبكة والأجهزة الفعلية المستخدمة فيها، في حين أن المخطط المنطقي يركز على الاتصالات العامة والخدمات التي توفرها الشبكة. وبالتالي فإن كل منهما يعرض جانباً مختلفاً من الشبكة ويساعد على فهم كيفية عمل الشبكة بشكل أفضل.

Physical Topology



Logical Topology



أنواع شبكات الحاسب:

هناك عدة أنواع من شبكات الحاسب، وقد يكون أشهرها :

- **شبكات النطاق الشخصي (PAN) :** وهي شبكات صغيرة تغطي مساحة قريبة جداً من الشخص المستخدم لها مثل الهواتف الذكية وأجهزة الحاسب الآلي المحمولة والأجهزة اللوحية والسماعات اللاسلكية.

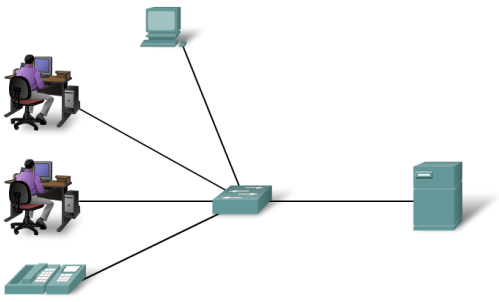
- **شبكات النطاق المحلي (LAN) :** وهي شبكات تغطي منطقة محدودة مثل مبنى أو مجموعة من المباني القريبة من بعضها وتستخدم بشكل شائع في المؤسسات والشركات الصغيرة والمتوسطة.

- **شبكات النطاق الواسع (WAN) :** وهي شبكات تغطي مناطق واسعة جداً مثل الدول والقارات وتستخدم بشكل شائع في الاتصالات العالمية والمؤسسات الكبيرة.

- **شبكات النطاق المحلي اللاسلكي (WLAN):** وهي شبكات لاسلكية تستخدم نفس تقنيات الاتصال اللاسلكي التي تستخدمها شبكات الجيل الثالث (3G) والجيل الرابع (4G)، وتغطي مناطق محدودة مثل مباني أو غرف معينة.

الشبكة المحلية (LAN):

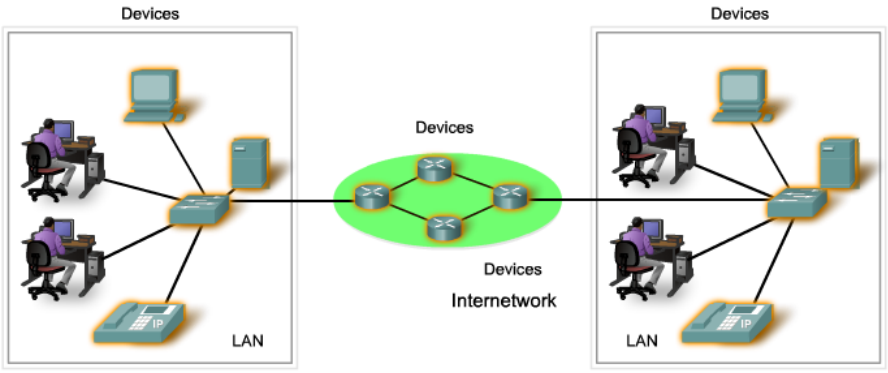
يقصد بالشبكة المحلية Local Area Network (LAN) الشبكة الصغيرة المحدودة النطاق والمستخدمة لربط الأجهزة في مكان معين مثل مبنى أو مكتب أو مدرسة أو مجموعة من المباني المتجاورة. وعادة ما تكون LAN خاصة بمؤسسة تعمل في مكان واحد وتستخدم لتبادل الملفات والموارد المشتركة بين الأجهزة الموجودة في نطاقها.



الشبكة الواسعة (WAN):

يقصد بالشبكة الواسعة Wide Area Network (WAN) الشبكة التي تغطي منطقة واسعة جغرافيًا، وهي عادة ما تغطي مناطق واسعة مثل مدن أو دول أو حتى قارات. وتتكون WAN من مجموعة من شبكات الحاسب المحلية LAN وغيرها من الشبكات الصغيرة المرتبطة بشبكة أكبر. وعادة ما تعتمد WANعلى تقنيات الاتصالات السلكية واللاسلكية مثل خطوط الهاتف والكابلات البحرية والأقمار الصناعية وخدمات الاتصالات اللاسلكية وتستخدم شبكات WAN على نطاق واسع في الأعمال

والحكومات والمؤسسات لربط مواقعها المنتشرة جغرافيًا وتمكين تبادل البيانات والمعلومات والخدمات بينها.



تهديدات الأمان:

وتتضمن التهديدات الخارجية الشائعة التي تتعرض لها شبكات الحاسب:

- الفيروسات وأحصنة طروادة
- برامج التجسس وبرامج الإعلانات المتسلسلة
- هجمات المتسللون
- هجمات رفض الخدمة (DoS)
- اعتراض البيانات والسرقة
- انتحال الهوية

حلول الأمان:

عادة ما تتضمن مكونات أمان الشبكة ما يلي:

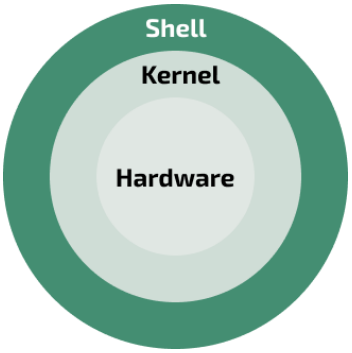
- برنامج مكافحة الفيروسات وبرنامج مكافحة التجسس
- أنظمة الجدر النارية (Firewalls)
- قوائم التحكم في الوصول (ACL)
- أنظمة منع الهجمات (IPS)
- أنظمة كشف الهجمات (IDS)
- شبكات ظاهرية خاصة (VPNs)

أنظمة التشغيل:

نظام التشغيل (Operating System) هو البرنامج الأساسي الذي يدير الموارد ويوفر الخدمات اللازمة للتطبيقات والبرامج. يعمل النظام على التفاعل مع الأجهزة المختلفة في الحاسب مثل المعالج والذاكرة والأقراص والطابعات ويسمح للمستخدم بإدارة وتنظيم الملفات والمجلدات وتشغيل التطبيقات المختلفة.

يتكون أي نظام تشغيل من ثلاثة أجزاء أساسية:

١. (Shell) : الواجهة التي يستخدمها الـــ End User وقد تكون واجهة رسومية وقد تكون واجهة سطر أوامر
٢. (Kernel) : الطبقة الوسطى والتي تربط بين الطبقتين وتسمى النواة
٣. (Hardware) : المعدات والأجهزة المستخدمة



هناك عدة أنواع من أنظمة التشغيل مثل:

- **نظام التشغيل Windows** الذي يعمل على أجهزة الحاسب الآلي الشخصية والأجهزة اللوحية والهواتف الذكية. وهو يتميز بواجهة رسومية سهلة الاستخدام وكذلك بدعمه لتشغيل العديد من التطبيقات المختلفة.
- **نظام التشغيل macOS** الذي يعمل على أجهزة الحاسب المصنعة من قبل شركة Apple وهو يتميز بتصميم أنيق في واجهته الرسومية وكذلك بأداء عالي وقدرات فائقة في التعامل مع الوسائط المتعددة.
- **نظام التشغيل Linux** الذي يعتبر مفتوح المصدر ومتاح للجميع وهو يتميز بالأمان والاستقرار والقدرة على التعامل مع الشبكات والخوادم ويدعم كلاً من الواجهات الرسومية وواجهات سطر الأوامر
- **نظام التشغيل iOS** الذي يعمل على أجهزة الهواتف الذكية والأجهزة اللوحية المصنعة من قبل Apple ويتميز بالأداء العالي والأمان العالي وواجهة رسومية سهلة الاستخدام.
- **نظام التشغيل Android** الذي يعمل على العديد من الأجهزة الذكية والأجهزة اللوحية ويتميز بالمرونة ودعمه لتطبيقات Google Play الواسعة وواجهته الرسومية.

نظام تشغيل أجهزة Cisco :

نظام التشغيل Internetwork Operating System (IOS) : وهو نظام تشغيل متكامل وقابل للبرمجة يتم استخدامه في مجموعة واسعة من أجهزة الشبكات التي تشمل الموجهات (Router) والمبدلات (Switch) وغيرها ويستخدم نظام التشغيل IOS نظام سطر الأوامر لإدارة وإعداد الأجهزة

وتشخيص المشاكل والأخطاء في الشبكة ويوفر مجموعة كبيرة من المميزات والوظائف للمستخدمين لإدارة شبكاتهم بكفاءة.

يتم تخزين نظام IOS في ذاكرة Flash وهي ذاكرة تخزين غير متطايرة فلا يتم فقد البيانات منها عند انقطاع التيار الكهربائي ويمكن كذلك تغييرها أو استبدالها حسب الحاجة.

وظائف نظام تشغيل شبكات Cisco :

تعتبر موجهات (Router) ومبدلات (Switch) شركة Cisco أجهزة مهمة في شـبكات الحاسـب وتتميز بوظائف رئيسية متعددة، من أهمها:

- **تمكين اتصـالات الشـبكة:** حيث تعتبر هذه الأجهزة مسـؤولة عن توصـيل الأجهزة المختلفة في الشبكة مع بعضها البعض.

- **توجيه حركة البيانات:** حيث تسـتخدم الموجهات (Router) لتوجيه حركة حزم البيانات بين الشبكات المختلفة، وذلك باستخدام بروتوكولات التوجيه المختلفة.

- **تحسـين الأداء:** تسـاعد المبدلات (Switch) في تحسـين أداء الشـبكة حيث تعمل على توزيع إطارات البيانات بشكل أفضل وتحسن السرعة.

- **توفير الأمان:** حيث تقدم الموجهات (Router) والمبدلات (Switch) خيارات متعددة لتحسـين الأمان في الشبكة وذلك من خلال توفير الحماية والتشفير والتحكم في الوصول إلى الموارد.

- **إدارة الشـبكة:** حيث تقدم بعض برمجيات Cisco واجهات مسـتخدم سـهلة الاسـتخدام وأدوات إدارة شاملة للشبكة مما يجعل من السهل إدارة الشبكة ومتابعة الأداء والأمان.

أساليب الوصول إلى وحدة التحكم:

أكثر الطرق شيوعاً للوصول إلى واجهة سطر الأوامر ومن ثم التحكم في نظام التشغيل والأجهزة

١. منفذ وحدة التحكم Console
٢. بروتوكولي الوصول عن بعد Telnet أو SSH
٣. منفذ Aux (مساعد)

منفذ وحدة التحكم Console :

- يمكّن من الوصول إلى التحكم في الجهاز حتى في حال عدم وجود خدمات الشبكات.
- يحتاج إلى كابل خاص
- يسمح بإدخال أوامر الإعداد
- يجب أن يكون مؤمن ضد الوصول غير المرخص باستخدام كلمات مرور قوية.

بروتوكولي الوصول عن بعد Telnet أو SSH

Telnet

- طريقة للوصول عن بُعد إلى CLI عبر شبكة
- يتطلب خدمات شبكات نشطة وواجهة واحدة نشطة تم تكوينها

Secure Shell (SSH)

- طريقة أخرى للوصول عن بُعد يماثل Telnet ولكنه يستخدم المزيد من الأمان
- لديه مصادقة أقوى لكلمة المرور
- يستخدم التشفير عند نقل البيانات

منفذ Aux (مساعد) :

- اتصال خارج النطاق الترددي
- يستخدم خط الهاتف
- يمكن استخدامه كمنفذ لوحدة التحكم

أوضاع تشغيل Cisco IOS :

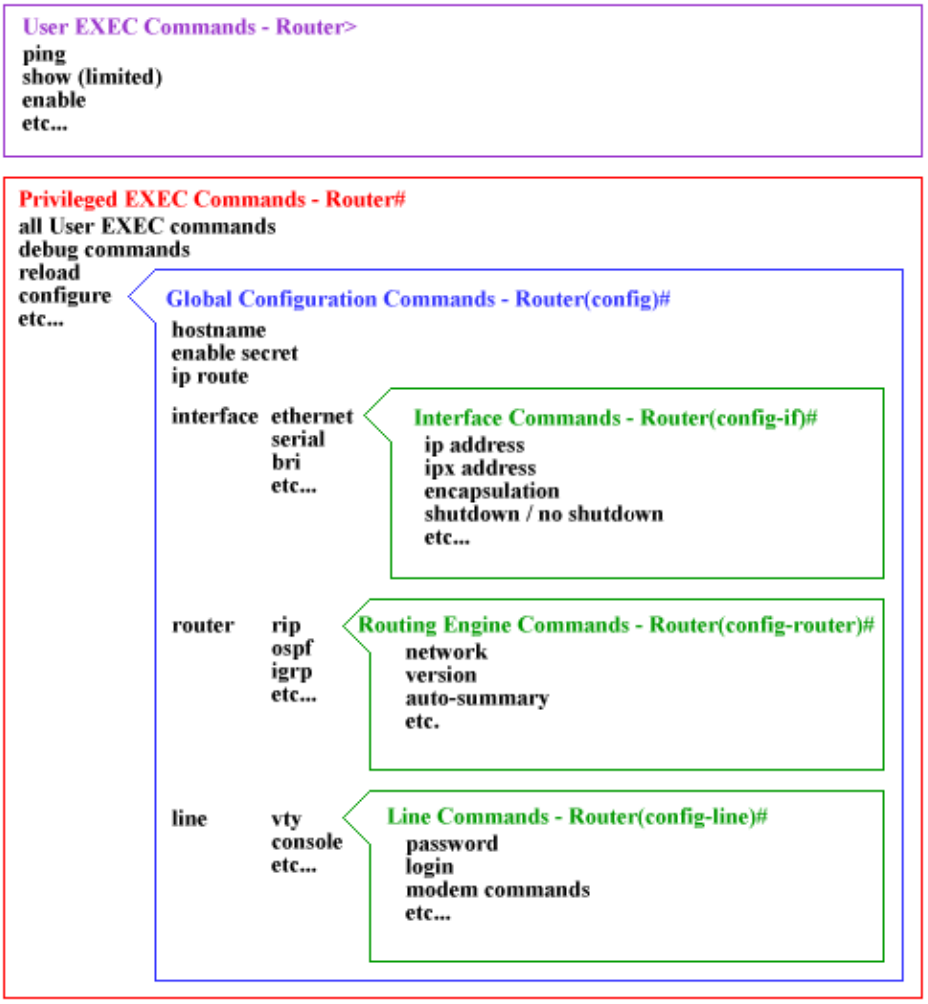
يحتوي Cisco IOS على عدة وضعيات تشغيل تسمح للمستخدمين بالوصول إلى مجموعة مختلفة من الأوامر والإعدادات:

١. **وضع المستخدم العادي (User mode):** هو وضع الدخول الافتراضي للمستخدم، ويسمح للمستخدم بعرض الحالة العامة للجهاز وبعض المعلومات الأساسية حول الوضع الحالي للجهاز.

٢. **وضع الامتياز (Privileged mode):** وضع الإعداد هو وضع الوصول الكامل إلى جهاز Cisco. يمكن المستخدمين من الوصول إلى جميع الأوامر المتاحة لاعداد وتشغيل الجهاز.

٣. **وضـع الاعداد العام (Global configuration mode):** يسـمح هذا الوضـع للمسـتخدمين بتكوين خصائص الجهاز، مثل عناوين IP وإعدادات المنافذ والأمان والتوجيه والتبديل.

٤. **وضع الاعداد الخاص (sub-configuration mode):** يستخدم هذا الوضع لتكوين خصائص أمر ووضع محددة.



بنية أوامر IOS

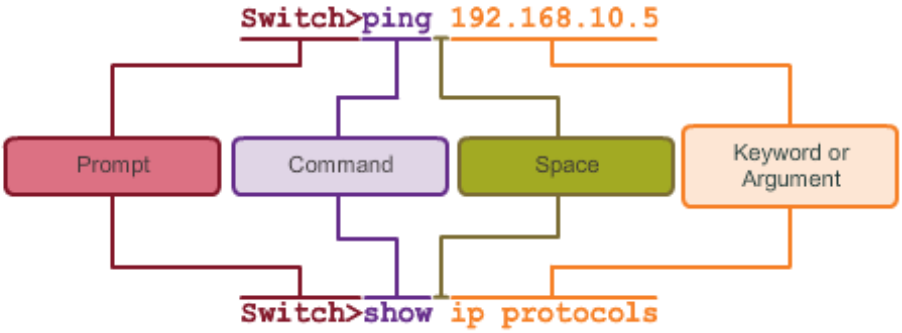
يحتوي نظام التشغيل على بنية الأوامر الخاصة به والتي تتضمن عدة أجزاء كالتالي:

- **الأمر (Command):** هو الجزء الأساسي من الأوامر والذي يشير إلى الإجراء الذي يراد تنفيذه مثل "show" أو "configure".
- **الخيارات (Options):** يستخدم لتحديد الإعدادات الإضافية للأوامر مثل "interface" أو " ip address".

- **المعاملات (Parameters):** يستخدم لتحديد القيم المطلوبة للإعدادات مثل عنوان IP المطلوب.

- **الفواصل (Delimiters):** يستخدم لفصل العناصر المختلفة في الأوامر مثل المسافات الفارغة.

يتم استخدام بنية الأوامر الخاصة بـــ IOS لتحديد الإجراءات والإعدادات المختلفة في أنظمة سيسكو وتشغيل الأجهزة المختلفة.

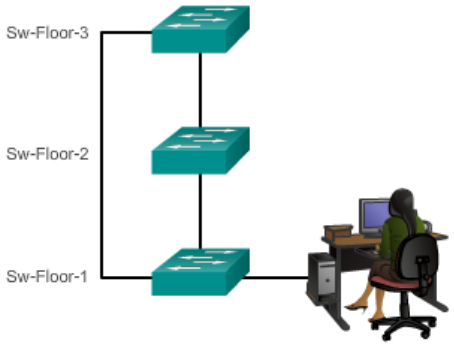


تسمية أجهزة الشبكة:

تعتبر تسمية أجهزة الشبكة مهمة جداً لعدة أسباب من بينها:

١. **التعرف على الأجهزة بســـهولة:** باســـتخدام أســـماء فريدة لكل جهاز في الشـــبكة بحيث يكون المستفيد الأول من تسمية الأجهزة هو مسؤول الشبكة فيستطيع التعرف على كل جهاز وموقعه بسرعة وسهولة وبالتالي يستطيع من إجراء ما يحتاج من إعدادات أو صيانة بشكل أسهل.
٢. **تسهيل الإدارة:** يسهل استخدام أسماء فريدة لتسمية الأجهزة في الشبكة عمليات الإدارة والتحكم في الشبكة بحيث يستطيع مسؤول الشبكة استخدام الأسماء للاتصال بالأجهزة وإعدادها وإدارتها عن بعد إذا رغب في ذلك.
٣. **تحسين الأمان:** يمكن استخدام التسمية لتطبيق سياسات الأمان وتحديد مستويات الوصول للأجهزة في الشبكة. على سبيل المثال، يمكن تعيين أسماء معينة للأجهزة المصرح لها الاتصال بخوادم الشبكة وتقييد الوصول إلى هذه الخوادم للأجهزة التي لا تحمل هذه الأسماء.

بشكل عام، تعتبر تسمية الأجهزة في الشبكة مهمة جدًا لتحسين إدارة الشبكة وتأمينها وتحديد أوجه القصور في حال حدوث مشاكل أو أعطال.



وهناك شروط يجب مراعاتها عند تسمية الأجهزة هي:

١. يجب أن يبدأ الاسم بحرف
٢. يجب ألا يحوي مسافات
٣. يجب أن ينتهي بحرف أو رقم
٤. يجب استخدام الأحرف والأرقام والشرطات الأفقية فقط
٥. يجب ان لا يتعدى طول الاسم 64 حرفًا

ولعمل ذلك نتبع الخطوات التالية:

```
Switch> enable
Switch#
Switch# config t
Switch(config)#
Switch(config)# hostname Hail
Hail(config)#
```

تأمين أجهزة الشبكة:

يعتبر تأمين الوصول إلى الأجهزة مهماً لعدة أسباب منها:

١. **حماية البيانات:** فإذا تم الوصـــول إلى الأجهزة بدون إذن فيمكن للمهاجم الوصـــول إلى البيانات المخزنة عليها والتلاعب بها أو سرقتها.

٢. **حماية الشـبكة:** فقد يتم الوصـول إلى الأجهزة الحسـاسـة مثل الموجهات (Router) والمبدلات (Switch) وتغيير إعداداتها والتي قد تؤدي إلى تعطيل الشبكة بشكل كامل.

٣. **حماية هوية المسـتخدمين:** حيث يجب تأمين حسـابات المسـتخدمين لمنع اختراقها والوصـول إلى الأجهزة الحساسة داخل الشبكة.

٤. **التزام القوانين:** ففي بعض الحالات تتطلب قوانين الأمن الســـيبراني الالتزام بمعايير الأمان وحماية الوصول إلى الأجهزة والبيانات.

لذلك يجب أن يتم تأمين الوصـــول إلى أجهزة الشـــبكة عن طريق إعداد كلمات المرور الآمنة وتقييد الوصول إلى الأجهزة بشكل مناسب عن طريق تحديد الأدوار والصلاحيات المختلفة للمستخدمين.

ولأجل القيام بذلك يجب التعرف على الأوامر الخاصة بذلك ومنها:

- كلمة المرور المستخدمة للانتقال من وضع المستخدم لوضع صاحب الامتيازات

```
R1(config)# enable password cisco
```

- كلمة المرور المشفرة والمستخدمة للانتقال من وضع المستخدم لوضع صاحب الامتيازات

```
R1(config)# enable secret cisco
```

- كلمة المرور المستخدمة للوصول للجهاز عن طريق منفذ وحدة التحكم (console)

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

- كلمة المرور المستخدمة للوصول للجهاز عن بعد VTY

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

مفهوم الاتصال في شبكات الحاسب:

يشير مفهوم الاتصال في شبكات الحاسب إلى العملية التي تسمح لأجهزة الشبكة المختلفة بالتواصل وتبادل البيانات بشكل فعال فيتم تحقيق الاتصال في شبكات الحاسب عن طريق إنشاء اتصالات بين الأجهزة المختلفة في الشبكة. وحتى يتم ضمان عملية الاتصال في شبكات الحاسب لابد من مراعاة العديد من العوامل التي يجب اتباعها وهي ما تم الاتفاق على تسميتها بالبروتوكولات.

طرق توجيه الحزم في شبكات الحاسب:

تختلف طرق توجيه الحزم (packets) في شبكات الحاسب وتنقسم الى ثلاثة صور أساسية:

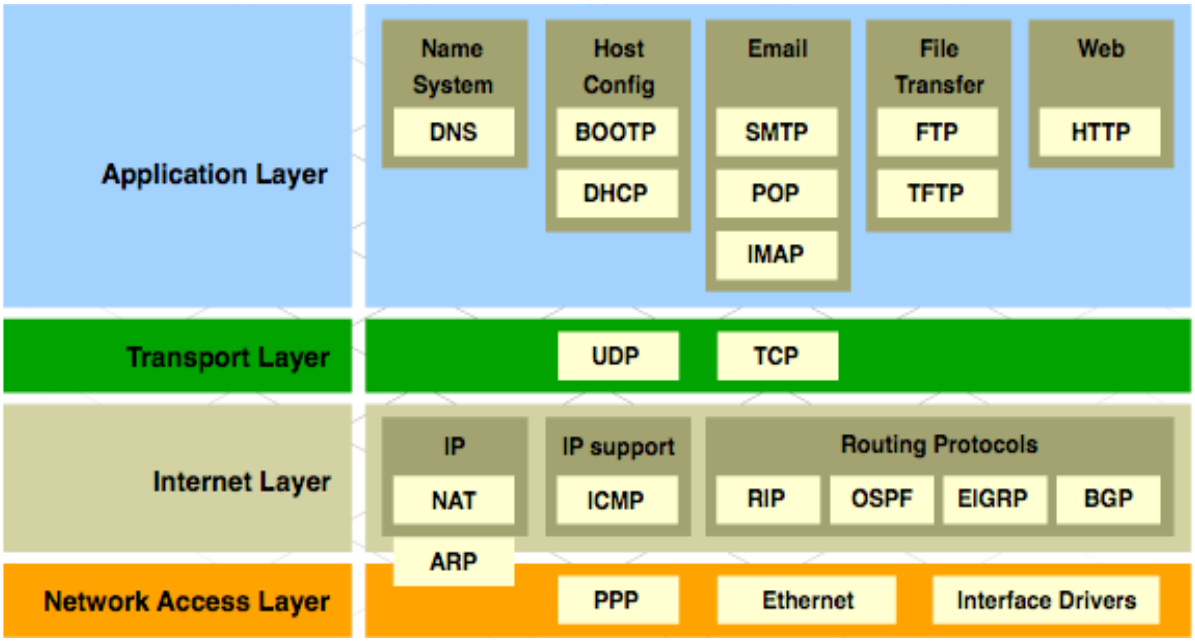
١. **Unicast:** هي عبارة عن توجيه حزمة من مصدر واحد إلى وجهة واحدة في الشبكة، حيث تتم المحادثة المباشرة بين الجهازين.
٢. **Multicast:** يتم توجيه الحزم من مصدر واحد إلى مجموعة متعددة من الأجهزة في الشبكة.
٣. **Broadcast:** هو عبارة عن توجيه حزمة من مصدر واحد إلى جميع الأجهزة المتصلة في الشبكة.

ما هي البروتوكولات في شبكات الحاسب:

يشير مصطلح البروتوكولات في شبكات الحاسب إلى مجموعة من القواعد والاتفاقيات التي تحكم التواصل وتبادل البيانات بين الأجهزة المختلفة في الشبكة. وتستخدم هذه البروتوكولات لتحديد كيفية نقل البيانات وتنظيم الاتصال بين الأجهزة المختلفة في الشبكة وضمان تسليم البيانات بشكل سليم وفعال. ويتم استخدام العديد من البروتوكولات في شبكات الحاسب والتي من بينها HTTP وSMTP وFTP.

نموذج TCP/IP

نموذج TCP/IP هو نموذج مرجعي ومعياري يستخدمه الإنترنت. ويتكون هذا النموذج من مجموعة من الطبقات الوظيفية التي تقسم عملية الاتصالات الحاسوبية إلى مجموعة من الخطوات اللازمة لنقل البيانات بين أجهزة الحاسب ويشمل أربع طبقات كما هو مبين في الجدول أدناه:



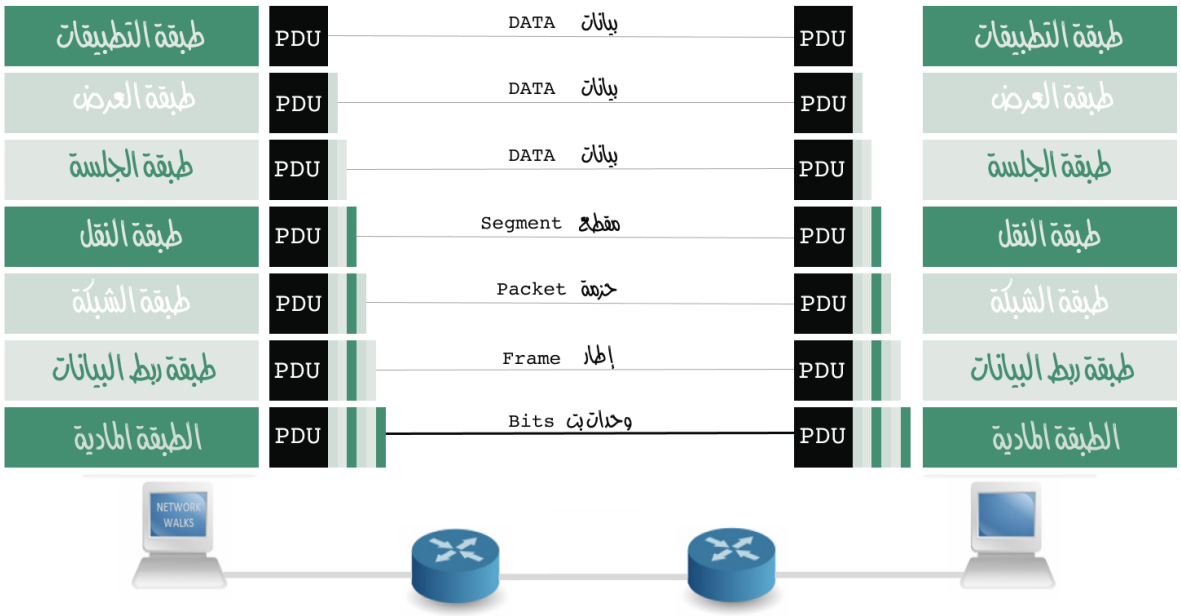
ويعتبر نموذج TCP/IP هو النموذج الأكثر استخدامًا في العالم، حيث يستخدم في إنشاء وإدارة الإنترنت والعديد من الشبكات الأخرى على مستوى العالم.

النموذج المرجعي OSI

النموذج المرجعي OSI هو اختصار لـ " Open Systems Interconnection"، وهو عبارة عن نموذج مرجعي للاتصالات الحاسوبية تم تطويره من قبل المنظمة الدولية للمعايير (ISO) في العام 1984. يتكون النموذج المرجعي من سبع طبقات تبدأ من الطبقة الفيزيائية إلى طبقة التطبيقات. ويهدف هذا النموذج إلى تسهيل فهم وتعليم عمل شبكات الحاسب للطلاب كما يقوم بتوفير إطار عمل موحد للشبكات المختلفة والأجهزة المختلفة، ويسمح للمطورين بتصميم تطبيقات وأجهزة شبكات الحاسب المتوافقة مع المعايير المعتمدة عالمياً. وباستخدام هذا النموذج، يمكن للمهندسين والمطورين العمل مع شبكات مختلفة وأجهزة مختلفة بشكل أسهل، كما يمكن للمستخدمين التواصل وتبادل المعلومات بشكل أفضل وأكثر فعالية.

وحدات بيانات البروتوكول (PDUs)

وحدة بيانات البروتوكول (PDU) هي مصطلح يستخدم في الاتصالات الشبكية للإشارة إلى حزمة البيانات التي تتم إرسالها في كل طبقة من طبقات النموذج المرجعي OSI. وتحتوي كل PDU على معلومات محددة لكل طبقة وتمر عبر الشبكة بين الأجهزة المختلفة. في نموذج OSI تتكون PDUs من الطبقات السبعة وتحتوي كل طبقة على PDU مختلفة وتتم إضافة معلومات التحكم والتوجيه لكل PDU لضمان التسليم الصحيح والسريع للبيانات. وفي نموذج OSI، تستخدم الـ PDUs التسمية (Data) في الطبقات الثلاث الأعلى وتستخدم الـ PDUs التسمية مقاطع (Segments) في طبقة النقل وتستخدم الـ PDUs التسمية حزم البيانات (Packets) في طبقة الشبكة والإطارات (Frames) في طبقة الربط بالشبكة.



طبقات النموذج المرجعي OSI:

طبقة التطبيقات
طبقة العرض
طبقة الجلسة
طبقة النقل
طبقة الشبكة
طبقة ربط البيانات
الطبقة المادية

سيتم الحديث عن هذا النموذج بالتفصيل في الصفحات التالية ابتداءً من الطبقة الأولى الطبقة المادية ووصولاً إلى الطبقة السابعة طبقة التطبيقات.

وكما مر سابقاً يعد OSI نموذجًا مرجعيًا يصف كيف يمكن لمكونات البرامج والأجهزة المختلفة في بيئة الحوسبة المتصلة بالشبكة أن تتواصل مع بعضها البعض وقد تم تطويره من قبل المنظمة الدولية للتوحيد القياسي (ISO) في الثمانينيات لتوفير إطار عمل مشترك لاتصالات الشبكة.

يتكون نموذج OSI من سبع طبقات كل منها مسؤول عن جانب معين من اتصالات الشبكة. هذه الطبقات هي:

١. **الطبقة المادية** - مسؤولة عن نقل بتات البيانات عبر الوسيط المادي مثل الكابلات النحاسية أو الألياف الضوئية أو الموجات اللاسلكية.

٢. **طبقة ارتباط البيانات** - مسؤولة عن النقل الموثوق لإطارات البيانات بين جهازين على نفس الشبكة المادية.

٣. **طبقة الشبكة** - مسؤولة عن توجيه حزم البيانات بين شبكات الحاسب المختلفة.

٤. **طبقة النقل** - مسؤولة عن توفير اتصال موثوق من طرف إلى طرف بين التطبيقات التي تعمل على أجهزة مختلفة.

٥. **طبقة الجلسة** - المسؤولة عن إنشاء الجلسات وصيانتها وإنهائها بين التطبيقات التي تعمل على أجهزة مختلفة.

٦. **طبقة العرض** - مسؤولة عن ترجمة البيانات بين طبقة التطبيق وطبقات المستوى الأدنى لنموذج OSI.

٧. **طبقة التطبيق** - مسؤولة عن تقديم الخدمات مباشرة إلى المستخدمين النهائيين مثل نقل الملفات أو البريد الإلكتروني.

وسيتم التفصيل في مهام كل طبقة على النحو التالي:

الطبقة المادية:

الطبقة الأولى من نموذج OSI هي الطبقة المادية. هذه الطبقة مسؤولة عن نقل بتات البيانات عبر وسيط مادي مثل الكابلات النحاسية أو الألياف الضوئية. تتمثل الوظيفة الأساسية لهذه الطبقة في تحديد الخصائص الفيزيائية لوسيط النقل بما في ذلك خصائصه الكهربائية والميكانيكية والوظيفية.

تحدد الطبقة المادية التوصيلات المادية مثل الكابلات والموصلات وترددات الراديو اللاسلكية المستخدمة لنقل البيانات. كما تحدد الإشارات الكهربائية التي يتم إرسالها عبر الوسيط بما في ذلك مستويات الجهد والتوقيت وأنظمة التشفير.

تتضمن أمثلة التقنيات التي تعمل في الطبقة المادية Ethernet و Wi-Fi و Bluetooth و USB.

باختصار الطبقة المادية هي أول طبقة في نموذج OSI وهي من يحدد الخصائص الفيزيائية لوسيط الإرسال المستخدم لنقل البيانات بين الأجهزة. وهي مسؤولة عن ضمان نقل البيانات بشكل موثوق ودقيق عبر الوسيط.

العناصر المادية في الشبكة:

العناصر المادية هي الأجهزة الإلكترونية والوسائط وسائر الموصلات الأخرى التي تقوم بإرسال الإشارات وحملها لتمثيل وحدات بت البيانات. فجميع المكونات المادية مثل بطاقات واجهة الشبكة NIC والواجهات والموصلات ومواد الكابلات وتصميمات الكابلات يتم تحديدها كلها في المعايير المقترنة بالطبقة المادية.

وسائط الشبكة:

مر سابقاً أنواع الوسائط المستخدمة في شبكات الحاسب هي:

١. الكابلات النحاسية
٢. الألياف الضوئية
٣. الموجات اللاسلكية

وقبل الحديث عنها هنا بمزيد من التفصيل يجدر توضيح مصطلح مهم يرد كثيراً عند الحديث عن الوسائط وهو النطاق الترددي (Bandwidth) والذي يقصد به قدرة الوسيط على حمل البيانات. فهو يعني كمية البيانات التي يمكنها التدفق من مكان إلى آخر خلال مدة زمنية معينة. ويقاس عادةً بوحدة الكيلوبت في الثانية (Kbps) أو ميجابت في الثانية (Mbps) أو جيجابت في الثانية (Gbps)

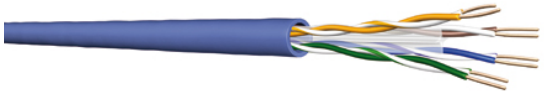
الكابلات النحاسية:

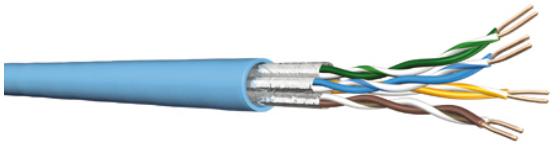
لقد ساهمت مؤسسات غير ربحية مختلفة معنية بوضع المعايير في تعريف الخصائص المادية والكهربائية للوسائط المتوفرة لاتصالات البيانات المختلفة. حيث تضمن هذه المواصفات عمل الكابلات والموصلات بشكل صحيح وكما هو متوقع منها.

فعلى سبيل المثال تم تعريف معايير الوسائط النحاسية لتشمل ما يلي:

- نوع الكابلات النحاسية المستخدمة
- عرض النطاق الترددي الخاص بالاتصال
- نوع الموصلات المستخدمة
- أوصاف الأسنان والرموز اللونية الخاصة بالاتصالات بالوسائط
- أقصى مسافة يستطيع الوسيط إيصال البيانات اليها.

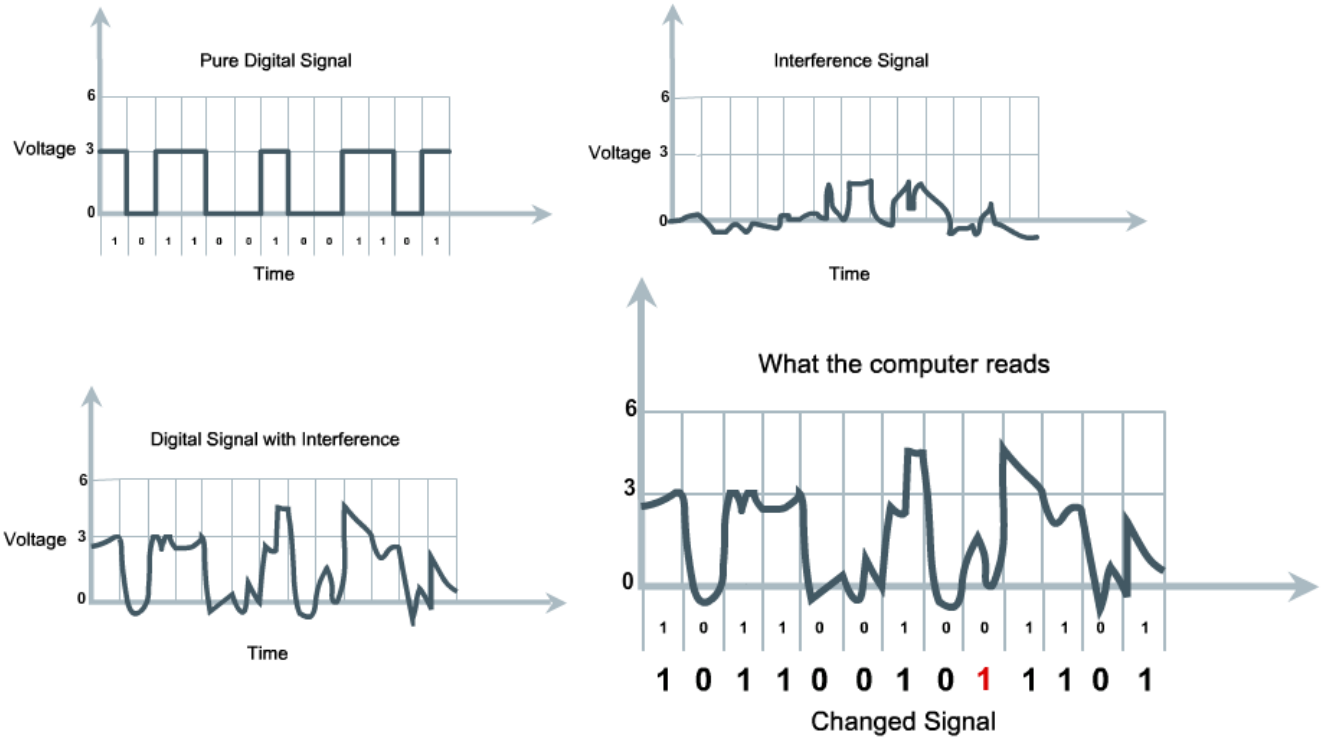
إن شبكات الحاسب تستخدم الوسائط النحاسية لأنها ليست باهظة الثمن وسهلة التركيب وتتمتع بمقاومة منخفضة للتيار الكهربي. ومع ذلك يوجد بعض العيوب في الوسائط النحاسية وهي محدودية المسافة فيها وتداخل الإشارات كذلك.





يتم إرسال البيانات عبر الكابلات النحاسية على شكل نبضات كهربائية ولابد من وجود كاشف أو قارئ على واجهة الشبكة الخاصة بالجهاز (NIC) بحيث تستقبل تلك النبضات الكهربائية وتفك ترميزها بشكل صحيح. ولكن مهم ان نعرف انه كلما انتقلت الإشارة إلى مسافة أطول انخفضت درجة جودتها. كما أن هناك عوامل أخرى تؤثر سلباً في جودة الاشارة مثل :

- التداخل الكهرومغناطيسي أو تداخل التردد اللاسلكي والناتجة عن مصابيح الفلوريسنت أو المحركات الكهربية
- تداخل الإشارات



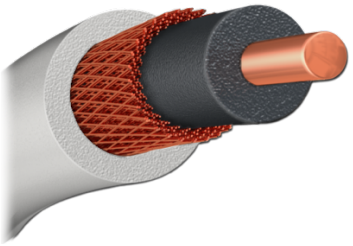
أنواع الكابلات النحاسية:

يوجد هناك ثلاثة أنواع أساسية للكابلات النحاسية وهي :

١. الكابل المحوري (Coaxial)
٢. الكابل المزدوج المجدول المحمي (STP)
٣. الكابل المزدوج المجدول غير المحمي (UTP)

الكابل المحوري (Coaxial) الكبل المحوري هو نوع من الكابلات الكهربائية التي لها موصل داخلي محاط بطبقة عازلة ودرع معدني وسترة خارجية. يستخدم بشكل شائع لنقل الإشارات عالية التردد وحالياً غالباً ما يستخدم في الاتصالات التلفزيونية. لم تعد تستخدم بشكل واسع في توصيل شبكات الحاسب لوجود بدائل أفضل.

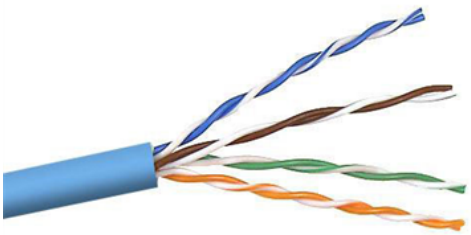
عادة ما يكون الموصل الداخلي مصنوعًا من النحاس. وهناك طبقة عازلة تحيط بالموصل الداخلي وتبقيه معزولا عن الدرع المعدني. حيث يعمل الدرع على حماية الموصل الداخلي من التداخل الكهرومغناطيسي ويساعد أيضًا على احتواء الإشارة داخل الكبل. الغلاف الخارجي مصنوع من مادة صلبة ومرنة توفر الحماية ضد التلف المادي والرطوبة.



الكابل المزدوج المجدول المحمي (STP) والذي يسمى Shielded Twisted Pair ، هو نوع من الكابلات النحاسية المستخدمة لنقل الإشارات. ويتكون من أربعة أزواج مجدولة من الأسلاك كل منهما معزول وملفوف بشكل فردي في درع معدني لتقليل التداخل الكهرومغناطيسي وتداخل الإشارات الكهربائية.

يمكن تصنيع الدرع المعدني من مجموعة متنوعة من المواد مثل رقائق الألومنيوم. يوفر هذا الدرع الحماية من مصادر التداخل الخارجية وتُستخدم بشكل شائع في شبكات Ethernet وتطبيقات اتصال البيانات الأخرى التي تتطلب معدلات نقل بيانات عالية وأداء موثوق.

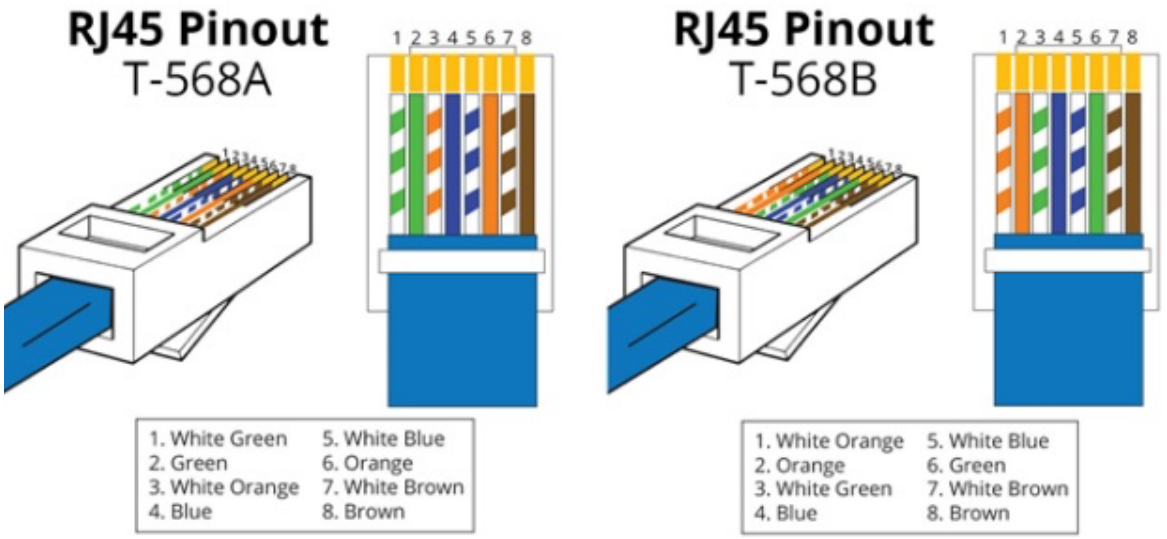
الكابل المزدوج المجدول غير المحمي (UTP) والذي يسمى Unshielded Twisted Pair ، لا يستخدم كابل UTP أي غلاف للتصدي للتداخل الكهرومغناطيسي وتداخل الإشارات الكهربائية. بل لقد اكتشف مصممو الكابلات أن بإمكانهم الحد من الأثر السلبي لتداخل الإشارات من خلال وضع أسلاك مزدوجة في دائرة. عند وضع سلكين في دائرة كهربائية بشكل متلاصق، تصبح الحقول الممغنطة في الاتجاه المعاكس تمامًا لكل منهما. ومن ثَم، يقوم الحقلان المغناطيسيان بإلغاء بعضهما وإلغاء أية إشارات خارجية أيضًا.



كلى نوعي الكابلات النحاسية (STP) و (UTP) يستخدمان نفس المقبس والموصل والذي يسمى (RJ45)

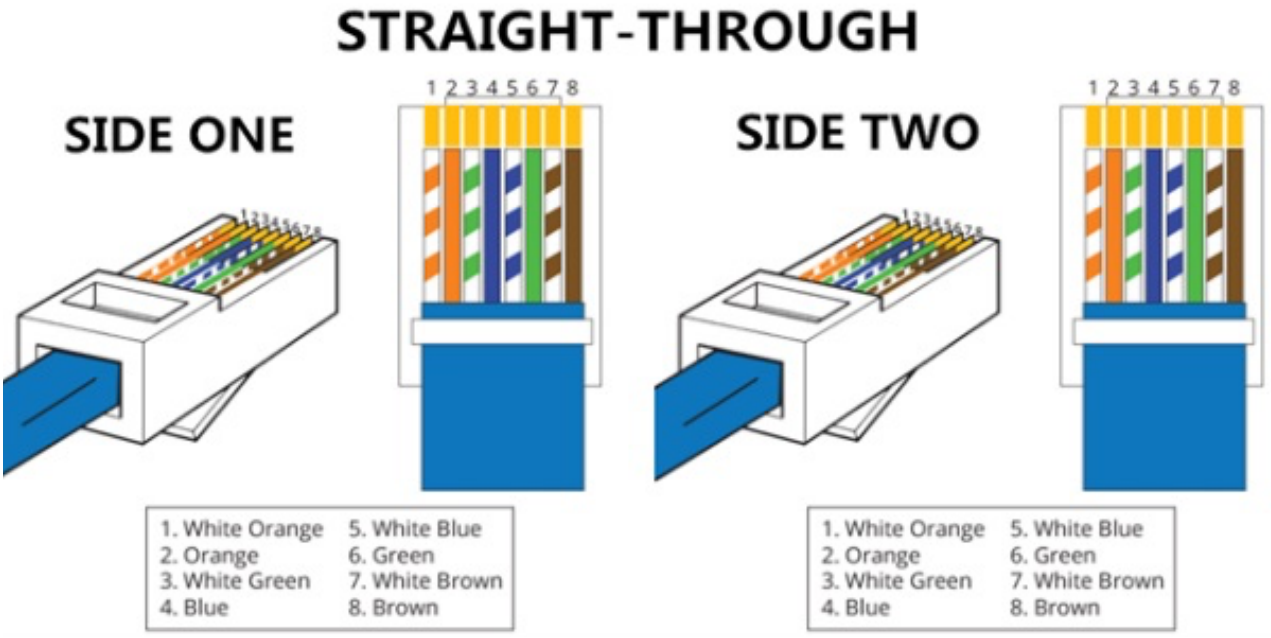
هناك معيارين أساسيين لتوزيع الأسلاك الخاصة بكيبلي (STP) و (UTP) داخل مقبس (RJ45) وهما:

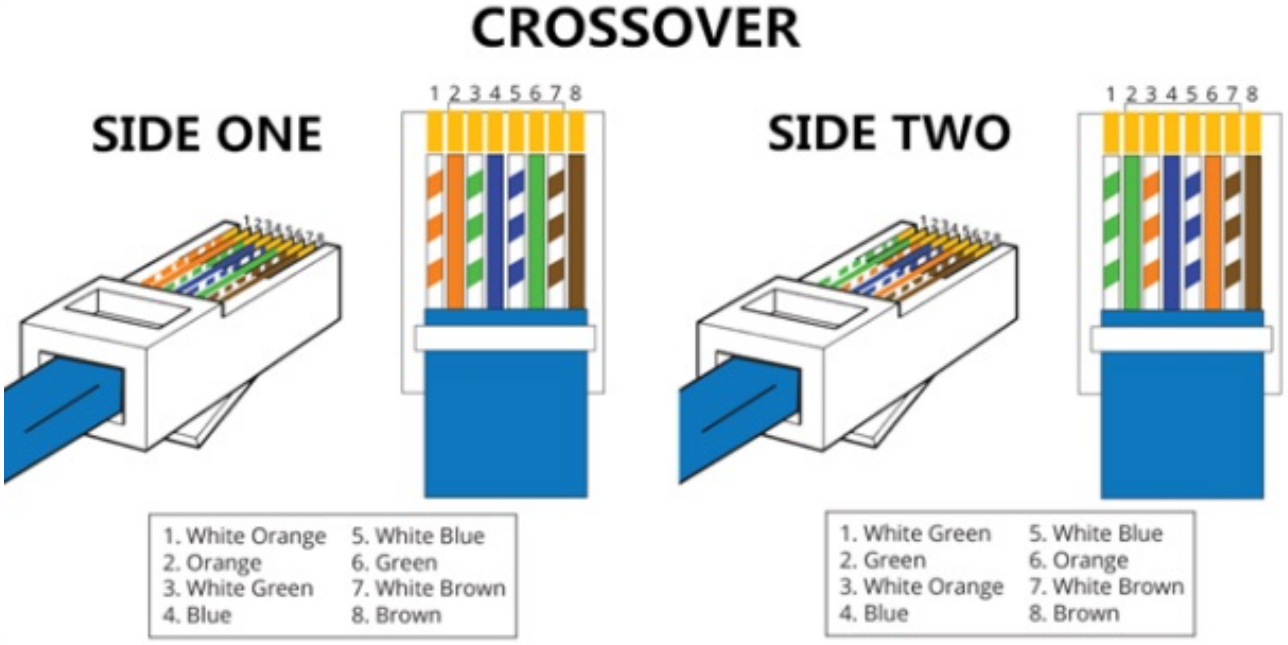
١. معيار (T-568A)
٢. معيار (T-568B)



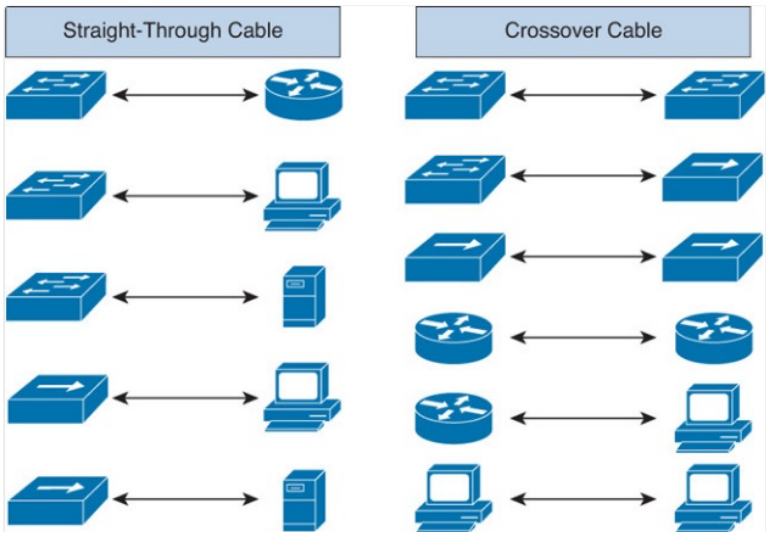
ونستطيع من خلال المعيارين السابقين انشاء نوعين مختلين من الكابلات وهما:

١. الكبل (**STRAIGHT-THROUGH**) : وهو الكبل الذي يكون طرفاه من نفس المعيار أي ان كلى الطرفين من المعيار (T-568A) أو كلاهما من المعيار (T-568B)
٢. الكبل (**CROSSOVER**) : وهو الكبل الذي يكون طرفاه من معيارين مختلفين فأحدهما من المعيار (T-568A) والآخر من المعيار (T-568B)





وتكمن فائدة وجود نوعي الكابلات المذكورة أعلاه في كون كل نوع منها قادر على توصيل أنواع محددة من الأجهزة الموجودة في الشبكة.. الصورة أدناه توضح الأجهزة التي يقوم بتوصيلها كل نوع منهما:



من المهم دائماً اختبار جودة توصيل وتمديد الكابلات باستخدام بعض الأجهزة المخصصة لذلك مثل الموضحة في الصورة أدناه وذلك للتأكد من:

- صحة تعيين الأسلاك وفق المعايير المذكورة أعلاه.
- مناسبة طول الكابل.
- مدى فقد الإشارة والناتج عن ضعف الاتصال.
- مدى وجود تداخل الإشارات.

الألياف الضوئية:

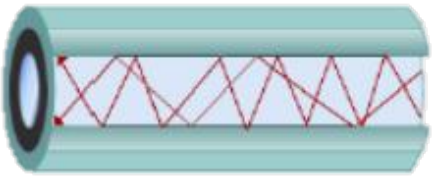
تتيح الألياف الضـوئية نقل البيانات عبر مسـافات أطول وبنطاقات ترددية أعلى من الكابلات النحاسـية. وعلى عكس الكابلات النحاسية تستطيع الألياف الضوئية نقل الإشارات مع الحماية الكاملة من التداخل الكهرومغناطيسي والترددات اللاسلكية.
وتتسم الألياف الضوئية بالمرونة، فهي عبارة عن جديلة شفافة رقيقة للغاية مكونة من الزجاج النقي ولا يزيد حجمها كثيراً عن حجم شـعرة الإنسـان ويتم ترميز وحدات بت البيانات على الألياف كنبضـات ضوئية.

أنواع الألياف الضوئية:

يوجد هناك نوعين من الألياف الضوئية وهما :
١. أحادي الوضع (Single-mode fiber)
٢. متعدد الأوضاع (Multimode fiber)

<u>أحادي الوضع (Single-mode fiber)</u> تم تصميمها لتحمل شعاعاً واحداً من الضوء على طول الألياف. وتُستخدم عادةً للاتصالات بعيدة المدى ولها قطر أساسي صغير يبلغ حوالي 9 ميكرون وتعد أعلى تكلفة من النوع الثاني من الألياف متعددة الأوضـاع ولكنها قادرة على نقل البيانات بشـكل أسرع وعبر مسـافات أطول ومع فقدان إشارة أقل وغالباً من تكون الإشارة الضوئية المستخدمة فيه عبارة عن أشعة ليزر.

<u>متعدد الأوضاع (Multimode fiber)</u> تم تصميمها لتحمل حزم متعددة من الضوء على طول الألياف. وقطرها الأساسي يبلغ حوالي من 50 الى 62.5 ميكرون مما يسمح لحزم متعددة من الضوء بالانتقال عبر الألياف وعادةً ما تُسـتخدم للمسـافات الأقصر مقارنة بالنوع الأول من الألياف أحادي الوضـع وهي أيضـاً أقل تكلفة من أحادية الوضـع ولا يمكنها نقل البيانات عبر مسـافات طويلة بسرـعات عالية مثل أحادية الوضع.



أخطاء توصيل الألياف الضوئية:

هناك ثلاثة أنواع شائعة لأخطاء توصيل الألياف الضوئية، هي:

١. **المحاذاة الخاطئة:** عدم محاذاة الألياف الضوئية بعضها ببعض بدقة عند توصيلها.
٢. **الفجوة الطرفية:** عدم ملامسة الألياف الضوئية تمامًا عند نقطة الاتصال أو التوصيل.
٣. **النهاية الطرفية:** عدم تنظيف طرفي الألياف الضوئية بشكل جيد عند أطراف التوصيل.

مقارنة بين الكابلات النحاسية والألياف الضوئية:

يوفر هذا الجدول مقارنة عامة بين الكابلات النحاسية والألياف الضوئية:

نطاق المقارنة	الكابلات النحاسية	الألياف الضوئية
المادة المستخدمة	النحاس	الزجاج أو البلاستيك
النطاق التردد	محدود	عالي
السرعة	بطيئة	سريعة
المسافة	قصيرة	طويلة
مقاومة التداخل الكهرومغناطيسي	ضعيفة	قوية
حجم والوزن	أسمك وأثقل	أنحف وأخف
الأمان	عرضة للتنصت	أكثر أمانًا بسبب
التكلفة	أرخص	أغلى
الاعداد	أسهل	أصعب وتتطلب الخبرة

الموجات اللاسلكية:

هي نوع من الإشعاع الكهرومغناطيسي. والذي يستخدم على نطاق واسع في شبكات الاتصالات الحديثة بما في ذلك شبكات الحاسب اللاسلكية ويتراوح طولها الموجي من حوالي 1 مليمتر إلى 100 كيلومتر ، وترددها منخفض ويتراوح من حوالي 3 كيلوهرتز إلى 300 جيجا هيرتز.

في شبكات الحاسب اللاسلكية تُستخدم الموجات اللاسلكية لنقل المعلومات بين الأجهزة فعندما يرسل جهاز يتم تحويل البيانات أولاً إلى إشارة رقمية ومن ثم يتم تشكيل هذه الإشارة على موجة حاملة وهو تردد محدد للموجة ثم يتم إرسال الموجة الحاملة المعدلة عبر الهواء إلى جهاز الاستقبال.

تعتبر قوة وجودة الإشـــارة أمراً بالغ الأهمية لأداء الشـــبكة فيمكن أن تؤثر عدة عوامل في ذلك مثل طول المسافة والعوائق والتداخل مع مصادر الموجات الأخرى على قوة الإشارة وجودتها.

طبقة ارتباط البيانات:

الطبقة الثانية من نموذج OSI هي طبقة ارتباط البيانات. هذه الطبقة مسؤولة عن توفير نقل موثوق للبيانات بين الأجهزة المتصـلة مباشرة ببعضـها البعض. تسـمى البيانات في طبقة ارتباط البيانات بالإطارات (Frame) وهي وحدات بيانات يتم نقلها بين الأجهزة. لا تحتوي الإطارات على البيانات التي يتم إرسـالها فحسـب بل تحتوي أيضـاً تحتوي على معلومات إضـافية مثل المزامنة واكتشـاف الأخطاء ومعلومات التحكم. وتسـتخدم طبقة ارتباط البيانات هذه الأجزاء الإضـافية من المعلومات لضمان نقل البيانات بشكل موثوق وبالترتيب الصحيح.
وتتمثل الوظيفة الأسـاسـية لهذه الطبقة في ضـمان نقل البيانات بدون أخطاء وبتسلسل صحيح.

تنقسم طبقة ارتباط البيانات إلى طبقتين فرعيتين:

١. **الطبقة الفرعية للتحكم في الوصول إلى الوسائط (MAC)**
٢. **الطبقة الفرعية للتحكم في الارتباط المنطقي (LLC)**

الطبقة الفرعية للتحكم في الوصول إلى الوسائط (MAC):
هي المسـؤولة عن التحكم في كيفية وصـول الأجهزة الموجودة على نفس الشـبكة المادية إلى وسـيط الإرسال. فهو المسؤول عن:

١. تعامل الأجهزة فيما يخص الوصول إلى الوسيط (كرت واجهة الشبكة) (NIC).
٢. ضمان عدم إرسال جهازين في نفس الوقت (تجنب الاصطدام) (CSMA/CD).
٣. التعامل مع الاصطدامات في ارسال البيانات عند حدوثها (اكتشاف الاصطدام) (CSMA/CA).
٤. تعيين عناوين مادية فريدة (MAC Address) لكل وحدة تحكم في واجهة الشـبكة (NIC) من أجل تحديد كل جهاز على الشبكة.

خاصية تجنب الاصطدام (CSMA/CD): الوصول المتعدد المستشعر للناقل مع اكتشاف التصادم يستخدم في شبكات Ethernet لإدارة الوصول إلى وسيط الإرسال مثل الكبل المحوري المشترك.

وفيه يستمع كل جهاز على الشبكة لإشارة الناقل لتحديد ما إذا كان وسيط الإرسال متاحاً أم لا. فإذا كان الوسـيط خاملاً يمكن أن يبدأ الجهاز في إرسـال بياناته. فإذا صـادف وحاول أكثر من جهاز نقل البيانات في تلك اللحظة أي في وقت واحد يحدث تصادم وتفقد البيانات.

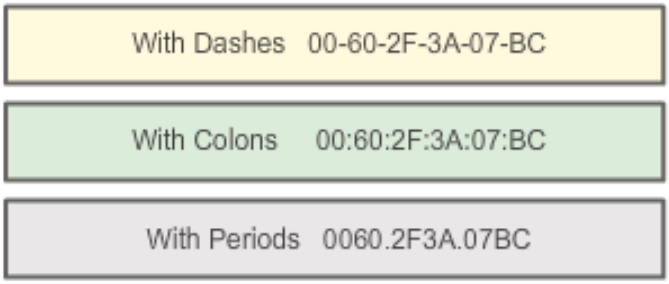
وعند حدوث التصـــادم تتوقف كل الأجهزة عن الإرســـال وتنتظر جميع الأجهزة فترة عشـــوائية من الوقت قبل محاولة إعادة إرسـال بياناتها. يسـاعد هذا التأخير العشـوائي على ضـمان عدم اصـطدام البيانات مرة أخرى مع بعضها بشكل متكرر مما يتسبب في ازدحام الشبكة.

يعد CSMA/CD طريقة فعالة للتحكم في الوصـول إلى وسـيط إرسـال مشـترك. ولكن مع زيادة حجم الشبكة تزداد احتمالية حدوث تصادمات أيضاً مما قد يقلل من أداء الشبكة.

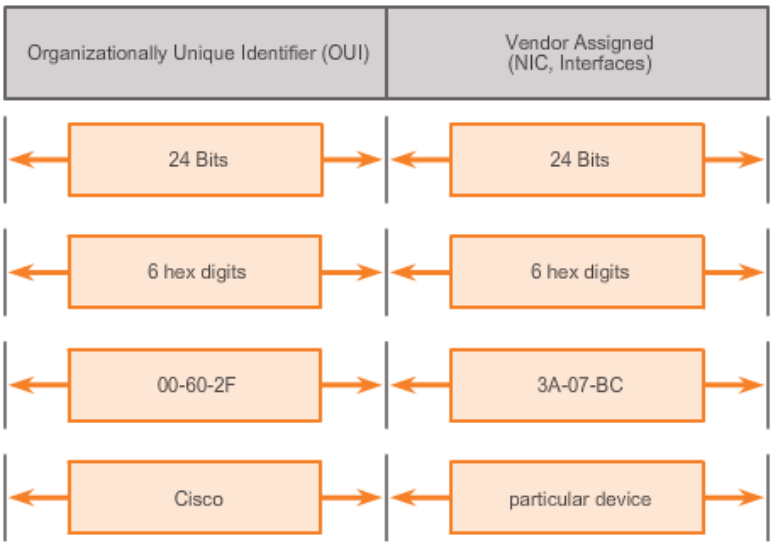
خاصـية اكتشـاف الاصـطدام (CSMA/CA): الوصـول المتعدد مع تجنب الاصـطدام يسـتخدم في شـــبكات الحاســـب اللاســـلكية مثل Wi-Fi ، لإدارة الوصـــول إلى وســـيط الإرســـال. على عكس CSMA/CD الذي يسـتخدم في شـبكات Ethernet السـلكية فقد تم تصـميم CSMA/CA لتجنب الاصطدامات تماماً بدلاً من اكتشافها بعد حدوثها.

ففيه يستمع كل جهاز على الشبكة لإشارة الناقل لتحديد ما إذا كان وسيط الإرسال متاحاً. ومع ذلك فقبل إرســـال البيانات يرســـل الجهاز حزمة طلب إرســـال (RTS) إلى جهاز الاســـتقبال المقصـــود. فيستجيب جهاز الاستقبال ويرد بحزمة (CTS) والتي تعني (Clear to Send) إذا كان وسيط الإرسال متاحاً. ويمكن للجهاز بعد ذلك نقل بياناته ويتعين على الأجهزة الأخرى الانتظار حتى اكتمال الإرسـال قبل محاولة الإرسال.

عناوين (MAC Address): عنوان التحكم في الوصـــول إلى الوســـائط (MAC) هو عنوان فريد يتم تعيينه لوحدة تحكم واجهة الشـبكة (NIC) لاسـتخدامه كعنوان شـبكة في الاتصـالات داخل قطاع الشبكة. يُشار إليه أحيانًا بالعنوان الفيزيائي أو المادي أو عنوان Ethernet.

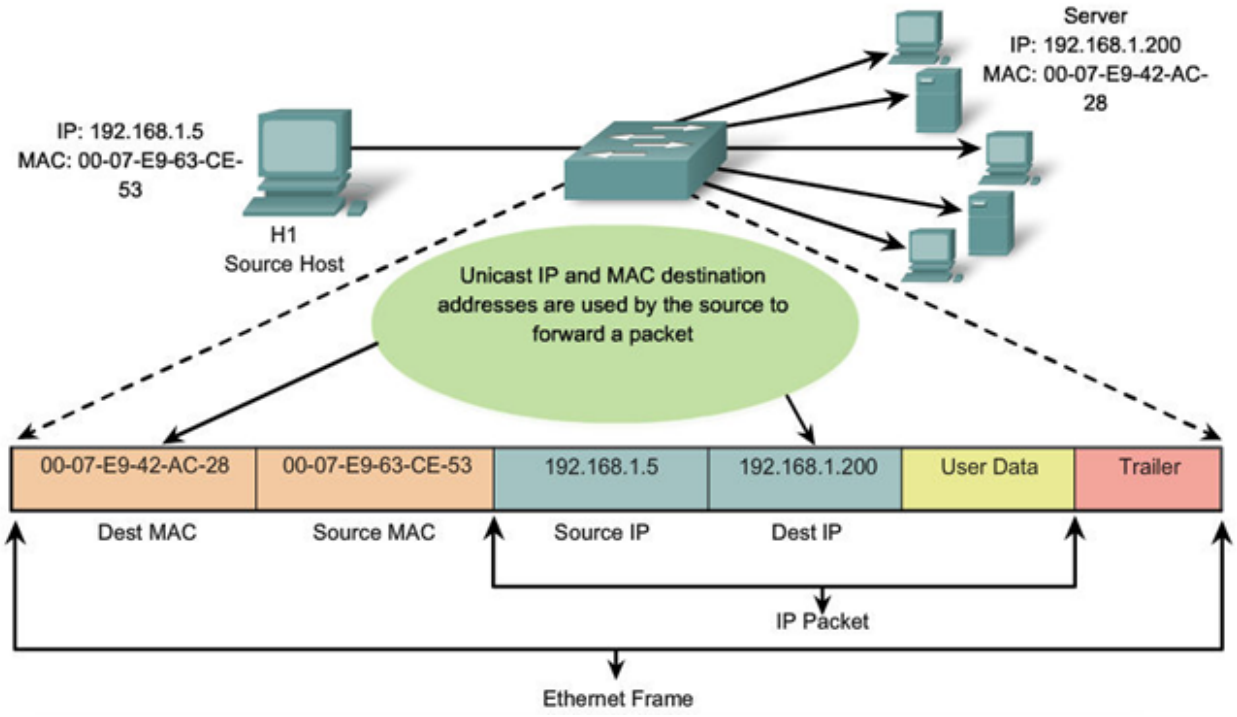


عنوان الـ MAC مكون من 48 بت (تُمثل بتنسيق ست عشري) ويتألف من ست مجموعات ومن رقمين لكل منها مفصـولة بنقطتين أو شرطات أو أربعة أرقام مفصـولة بنقطة كما هو موضـح في الصـورة أعلاه. تمثل المجموعات الثلاث الأولى ما يسمى (OUI) والذي يحدد الشركة المصنعة للـ NIC بينما يتم تعيين المجموعات الثلاث الأخيرة من قبل الشركة المصنعة وتمثل الرقم التسلسلي للجهاز أو المعرف الفريد.

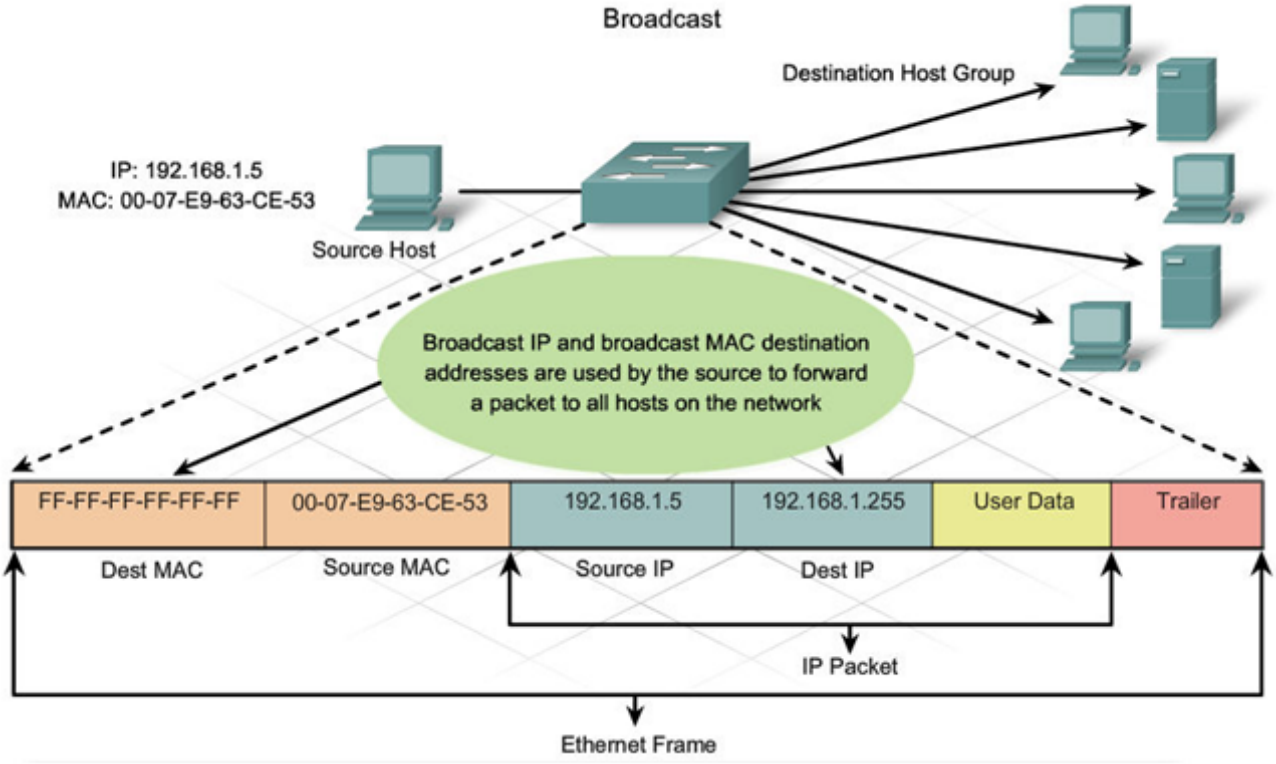


يتم استخدام عناوين MAC بواسطة طبقة ارتباط البيانات (الطبقة 2) لنموذج OSI لتحديد الأجهزة داخل شبكة محلية بحيث يتم استخدامها لضمان إرسال البيانات إلى الجهاز الصحيح على الشبكة ولمنع تصادم البيانات بين الأجهزة.

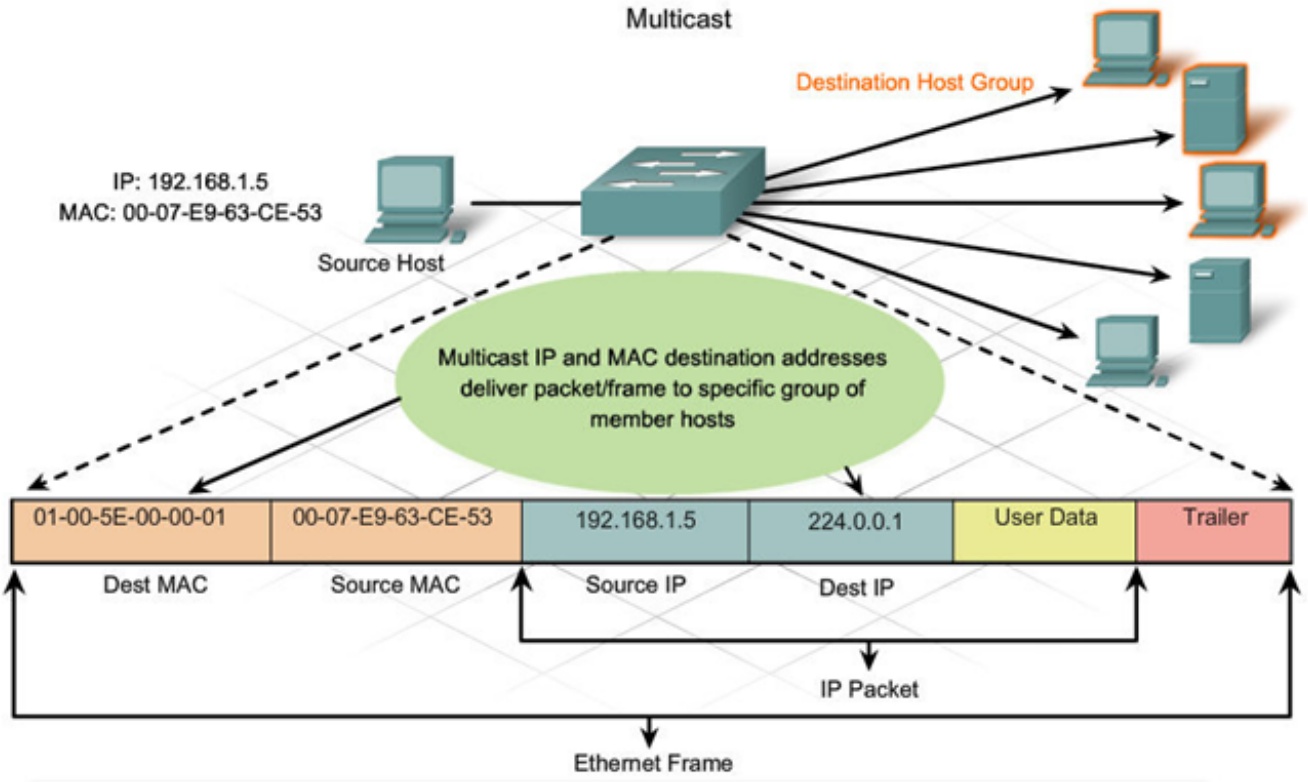
عنوان MAC للبث الأحادي:



عنوان MAC للبث:



عنوان MAC للبث المتعدد:



الطبقة الفرعية للتحكم في الارتباط المنطقي (LLC):

هي المسؤولة عن توفير التحكم في التدفق وفحص الأخطاء بين الأجهزة. تقوم بما يلي:

١. تجزئة البيانات
٢. إعادة تجميع البيانات
٣. ضمان نقل البيانات بالترتيب الصحيح.

بروتوكول تحليل العنوان (ARP):

هو بروتوكول يُستخدم في شبكات الكمبيوتر لمعرفة وتعيين عنوان الـ (MAC) من خلال معرفة عنوان ال (IP) فقط. فعندما يريد أحد الأجهزة إرسال البيانات إلى جهاز آخر على شبكة محلية فإنه يحتاج إلى معرفة عنوان MAC الخاص به. فيقوم الجهاز أولاً بالتحقق من ذاكرة التخزين المؤقت المحلية له لـ ARP ، وهو جدول يخزن عناوين IP المستخدمة مؤخرًا والمقابلة لعناوين MAC. فإذا لم يكن عنوان MAC المطلوب موجوداً في ذاكرة التخزين المؤقت وانما كان هناك فقط عنوان IP للجهاز المطلوب فحينها يرسل الجهاز رسالة بث (Broadcast) تحوي طلب ARP إلى جميع الأجهزة على الشبكة بحيث يُطلب فيها عنوان MAC المرتبط بعنوان IP الذي يريد الاتصال به.

تحتوي رسالة طلب ARP على عنوان IP للجهاز صاحب الطلب وعنوان IP للجهاز الذي يريد الاتصال به. تتلقى جميع الأجهزة الموجودة على الشبكة طلب ARP ولكن الجهاز الذي يحمل عنوان IP المطابق فقط هو الذي يستجيب للطلب ويقوم بالرد عن طريق إرسال رسالة رد ARP مرة أخرى إلى الجهاز الطالب. تحتوي رسالة رد ARP على عنوان MAC الخاص بالجهاز المستجيب والذي يتم إضافته إلى ذاكرة التخزين المؤقت ARP للجهاز الطالب للاستخدام في المستقبل.

طبقة الشبكة:

طبقة التطبيقات
طبقة العرض
طبقة الجلسة
طبقة النقل
طبقة الشبكة
طبقة ربط البيانات
الطبقة المادية

الطبقة الثالثة من نموذج OSI هي المسؤولة عن توفير العنونة المنطقية وتوجيه الحزم بين الأجهزة على الشبكة وتتمثل الوظيفة الأساسية لطبقة الشبكة في تمكين الاتصال من طرف إلى طرف بين الأجهزة التي قد لا تكون متصلة بشكل مباشر.

ولتحقيق ذلك توفر طبقة الشبكة عنواناً منطقياً لكل جهاز على الشبكة يُعرف باسم عنوان IP. تُستخدم عناوين IP لتعريف كل جهاز بشكل فريد على الشبكة ولتمكين توجيه البيانات بين الأجهزة.

تسمى البيانات في طبقة الشبكة بالحزم (Packet) وهي وحدات بيانات يتم نقلها بين الأجهزة على الشبكة. تحدد طبقة الشبكة أيضًا البروتوكولات المستخدمة لتوجيه البيانات عبر شبكات الحاسب وهذا يتضمن التوجيه داخل الشبكة (داخل شبكة واحدة) والتوجيه بين شبكات متعددة.

وظيفة أخرى مهمة لطبقة الشـــبكة هي تجزئة وإعادة تجميع حزم البيانات بحيث تقوم طبقة الشـــبكة بتقسـيم البيانات إلى أجزاء أصـغر تسـهل من نقل هذه الأجزاء بشـكل فردي وإعادة تجميعها كذلك عند الطرف المستقبل.

عناوين الـــ (IP) والتي تعمل على طبقة الشبكة يوجد منها حالياً إصدارين هما IPv4 و IPv6 كما يعمل في هذه الطبقة أيضـــاً بروتوكول رســـائل التحكم في الإنترنت (ICMP) وبروتوكول إدارة مجموعة الإنترنت (IGMP).

باختصـــار طبقة الشـــبكة هي الطبقة الثالثة من نموذج OSI وهي مســـؤولة عن توفير العنونة المنطقية وتوجيه البيانات بين الأجهزة على الشـبكة ويحدد البروتوكولات المسـتخدمة لتوجيه الحزم عبر شـبكات الحاسب ويمكن الاتصال من طرف إلى طرف بين الأجهزة.

خصائص IP :

١. **غير متصل (Connectionless) :** هو بروتوكول غير متصل أي أنه لا ينشئ اتصالاً مخصصاً من طرف إلى طرف أي بين المرســل والمســتقبل قبل إرســال البيانات. بل يتم التعامل مع كل حزمة بشكل مستقل ويتم توجيهها بناءً على عنوان IP الوجهة الموجود في رأس الحزمة.

٢. **أفضـل جهد (Best effort) :** هو بروتوكول لا يضـمن تسـليم البيانات ولا يضـمن جودة الخدمة (QoS) المقدمة للحزم وهذا لأنه مصـــمم ليكون بروتوكول خفيف الوزن ومرن يمكنه العمل عبر مجموعة واسعة من تقنيات وظروف الشبكة.

٣. **مسـتقل عن الوسـائط (Media independent) :** هو بروتوكول مسـتقل عن الوسـائط أي أنه قادر على العمل والانتقال عبر أنواع الوســائط المختلفة في الشــبكة مثل الكابلات النحاســية أو الألياف الضوئية أو الموجات اللاسلكية.

ما هو IPv4 :

هو بروتوكول طبقة الشـبكة ويسـتخدم على نطاق واسـع بحيث يوفر الأسـاس للاتصـال على الإنترنت والعديد من شـبكات الحاسـب الأخرى ويمثل الإصـدار الرابع من بروتوكول الإنترنت وقد تم تطويره في أوائل الثمانينيات من قبل فريق هندسة الإنترنت (IETF).

وعلى الرغم من اســتخدامه على نطاق واســع إلا أن به العديد من القيود والمحدودية التي تعيبه مثل محدودية أعداد العناوين المتاحة منه حيث يبلغ إجمالي عدد عناوين IPv4 حوالي ٤,٣ مليار. والســبب في ذلك يعود لبنية هذه العناوين حيث أنها عبارة عن أرقام عشـرية تتكون من 32 بت مما يعني أن هناك إجمالي 2^{32} أو (4294967296) عنوان متاح.

ومع ذلك ليســت كل هذه العناوين متاحة للاســتخدام العام حيث يوجد منها ما هو محجوز لأغراض خاصــة مثل الشــبكات الخاصــة وعناوين الإرســال المتعدد (Multicast) وعناوين الاســترجاع (Loopback).

ومع كثرة اســتخدام هذه العناوين وبروز مرحلة "انترنت الأشــياء" فقد أدى ذلك إلى نقص عدد العناوين المتاحة والذي بدوره أســهم في تطوير أنظمة عنونة بديلة مثل ترجمة عنوان الشــبكة (NAT) عناوين IPv6 الأحدث والتي وفرت عدد هائل جداً من العناوين تمثل 2^{128} أو (304×10^{38}) ، **فعدد عناوين IPv6 أكثر من عدد حبيبات الرمل على الأرض.**

الموجه (Router) عبارة عن جهاز حاسب:

غالباً ما يشار إلى أجهزة التوجيه على أنها أجهزة حاسب لأن لها العديد من الخصائص المشتركة مع أنظمة الحاسب التقليدية. فكليهما يحتوي على وحدة معالجة وذاكرة وتخزين وتستخدم برامج لأداء وظائفها.

ومع ذلك فهناك العديد من الاختلافات الرئيسية بين أجهزة التوجيه وأجهزة الحاسب مثل:

الغرض والهدف: فقد تم تصــميم أجهزة التوجيه خصــيصــاً لإعادة توجيه حركة مرور البيانات بين الشبكات بينما تم تصميم أجهزة الحاسب التقليدية للحوسبة ذات الأغراض العامة.

نظام التشـغيل: تسـتخدم أجهزة التوجيه نظام تشـغيل خاص ومصـمم لوظائف شـبكات الحاسـب بينما تسـتخدم أجهزة الحاسـب التقليدية أنظمة تشـغيل أخرى للأغراض العامة مثل Windows أو macOS أو Linux.

ومع ذلك يمكن اعتبار أجهزة التوجيه أنها أنواع متخصصة من أجهزة الحاسب الآلي تم تحسينها لوظائف أخرى.

ولدى الموجة أنواع متعددة من الذواكر كما هو الحال لأجهزة الحاسب مع بعض الاختلافات البسيطة

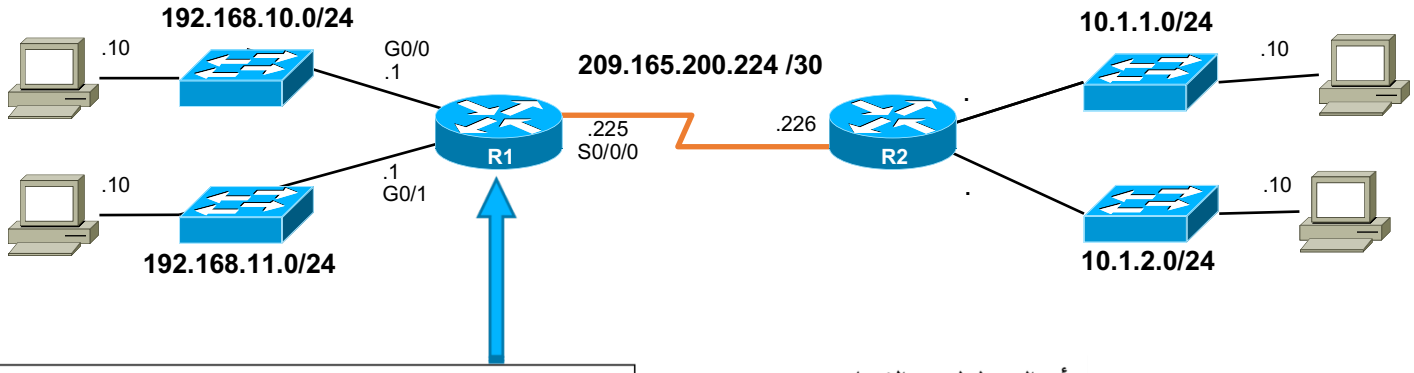
الذاكرة	نوعها	الغرض منها
ذاكرة الوصول العشوائي (RAM)	متطايرة	☐ IOS الجاري تشغيله ☐ ملف التكوين الحالي ☐ جداول توجيه IP وARP ☐ مخزن الحزم المؤقت
ROM	غير متطايرة	☐ تعليمات التمهيد ☐ POST
NVRAM	غير متطايرة	☐ ملف تكوين بدء التشغيل
Flash	غير متطايرة	☐ IOS ☐ ملفات نظام أخرى

واجهات LAN

واجهات WAN

واجهات Console

خطوات إعداد جهاز التوجيه :




```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

أمر الدخول لوضع الامتياز

أمر الدخول لوضع الإعداد العام

أمر إعطاء الجهاز أسم جديد (R1)

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

أمر إعطاء كلمة مرور مشفرة للوصول لوضع الامتياز

أوامر إعطاء كلمة مرور لمنفذ الـ Console

أوامر إعطاء كلمة مرور للوصول عن بعد الـ vty

أمر تشفير جميع كلمات المرور

طبقة النقل :

طبقة النقل هي الطبقة الرابعة في نموذج OSI وتوفر خدمات نقل البيانات من طرف إلى طرف والتي تضمن نقلاً موثوقاً وخالياً من الأخطاء للبيانات بين التطبيقات التي تعمل على أجهزة شبكات مختلفة وتعتبر طبقة النقل مسؤولة عن إدارة تدفق البيانات بين التطبيقات وإنشاء الاتصالات وإنهائها بين الأجهزة والتأكد من تسليم البيانات دون أخطاء وبالترتيب الصحيح.

هناك نوعان من البروتوكولات الرئيسية التي تعمل في طبقة النقل:

١. بروتوكول التحكم في الإرسال (TCP).
٢. بروتوكول مخطط بيانات المستخدم (UDP).
٣.

بروتوكول (TCP) : يوفر نقلاً موثوقاً للبيانات عن طريق إنشاء اتصال بين المرسل والمستقبل وإجراء فحص لمعرفة الأخطاء وإعادة إرسال الحزم المفقودة وكذلك التأكد من استلام البيانات بالترتيب الصحيح ويستخدم بشكل شائع للتطبيقات التي تتطلب موثوقية ودقة عالية مثل نقل الملفات والبريد الإلكتروني وتصفح الويب بحيث يتم ذلك من خلال مجموعة متنوعة من الآليات مثل أرقام التسلسل وأرقام الإقرار وإعادة الإرسال.

فعندما يرسل المرسل حزمة بيانات فهو يقوم بتعيين رقم تسلسلي فريد لتلك الحزمة ويقوم في المقابل جهاز الاستقبال عند استلام الحزمة بإرسال حزمة إقرار (ACK) إلى المرسل مع رقم التسلسل المتوقع أن يصله في الارسال التالي فيشير هذا الإقرار إلى أن جهاز الاستقبال قد استقبل جميع الحزم حتى الحزمة التي تحتوي على رقم التسلسل الأخير المقر بوصوله.

وإذا لم يستلم المرسل حزمة ACK التي تقر بالوصول لحزمة معينة وذلك بعد فترة زمنية محددة فإنه سوف يفترض أن الحزمة قد فقدت وسيعيد إرسال الحزمة بنفس رقم التسلسل وهذا يضمن أن المتلقي يتلقى جميع الحزم وبالترتيب الصحيح.

بالإضافة إلى ذلك يستخدم بروتوكول (TCP) آليات التحكم في التدفق والتحكم في الازدحام لمنع فقدان الحزم والتأكد من أن الشبكة ليست مثقلة بحركة المرور وذلك عن طريق ما يسمى بحجم النافذة (Window Size) والذي سيتم الحديث عنه في الأسطر القادمة.

بروتوكول (UDP) : يوفر أفضل خدمة توصيل لكن دون التحقق من الأخطاء أو إعادة الإرسال أو التحكم في التدفق فهو يستخدم بشكل شائع للتطبيقات التي تتطلب نقل بيانات لا يحتمل التأخير أي أنه عالي السرعة مثل تدفق الفيديو والصوت والألعاب عبر الإنترنت والاتصالات في الوقت الفعلي.

توفر طبقة النقل إضافة الى ذلك العديد من الوظائف المهمة الأخرى بما في ذلك:

- **مضاعفة الإرسال (Multiplexing):** يتيح ذلك لتطبيقات متعددة مشاركة نفس اتصال الشبكة عن طريق تعيين معرفات فريدة تسمى أرقام المنافذ وذلك لكل تدفق بيانات. بحيث يصبح بالإمكان أن يحوي المتصفح عدة نوافذ متصلة وفعالة في نفس الوقت أحدها مثلاً للاطلاع على البريد الالكتروني في حين يكون الآخر لزيارة موقع معين وهكذا.
- **التحكم في التدفق (Flow control):** وهذا يدير ويتحكم بمعدل نقل البيانات لأجل منع ازدحام الشبكة وضمان الاستخدام الفعال لموارد الشبكة.
- **التحكم في الازدحام (Congestion control):** وهذا يكتشف ازدحام الشبكة ويديره لمنع فقدان الحزمة وضمان نقل البيانات بسلاسة.
- **كشف الأخطاء وتصحيحها (Error detection and correction):** وهذا يحدد ويصحح الأخطاء في نقل البيانات لضمان سلامة البيانات ودقتها.

بشكل عام تلعب طبقة النقل دورًا مهمًا في ضمان نقل موثوق وفعال للبيانات بين التطبيقات والأجهزة الموجودة على الشبكة.

المنافذ (Ports) :

في طبقة النقل تستخدم التطبيقات أرقام منافذ محددة للتواصل مع بعضها البعض عبر الشبكة وهذه المنافذ هي قنوات افتراضية تسمح للتطبيقات المتعددة باستخدام نفس اتصال الشبكة مع الاحتفاظ ببياناتها منفصلة عن بعضها البعض بحيث يتم تحديد كل منفذ برقم مميز وفريد يتراوح بين 0 و 65535.

هناك نوعان من المنافذ المستخدمة في طبقة النقل:

١. **المنافذ المعروفة:** وهي مخصصة لخدمات أو تطبيقات معينة ومحددة وهي مرقمة بين 0 و 1023. مثل المنفذ 80 والمحجوز لحركة مرور HTTP (تصفح الويب) والمنفذ 443 والمحجوز لحركة مرور HTTPS (تصفح الويب المشفر) ، والمنفذ 21 والمحجوز لحركة مرور FTP (نقل الملفات) والمنفذ 25 والمحجوز لحركة SMTP (البريد الإلكتروني).

٢. **المنافذ الديناميكية أو الخاصة:** وهي أرقام منافذ مؤقتة تستخدمها تطبيقات العميل لبدء الاتصالات مع تطبيقات الخادم. يتم ترقيم المنافذ الديناميكية بين 1024 و 65535 ويتم تعيينها عشوائيًا بواسطة نظام التشغيل عندما يبدأ تطبيق العميل الاتصال.

يُعرف الجمع بين عنوان IP ورقم المنفذ باسم (socket).

192.168.10.10:443

تسمح (socket) للتطبيقات بإنشاء اتصال بجهاز بعيد وتبادل البيانات عبر الشبكة. على سبيل المثال عندما تتصفح موقع ويب يفتح متصفح الويب الخاص بك socket لعنوان IP لخادم الويب على المنفذ 80 لإرسال بيانات HTTP واستلامها كما واضح في المثال أعلاه.

يسمح استخدام المنافذ في طبقة النقل لتطبيقات متعددة بالتواصل مع بعضها البعض عبر نفس اتصال الشبكة دون التداخل مع بيانات بعضها البعض. كما يسمح لمسؤولي الشبكة بالتحكم في الخدمات التي يُسمح لها بالاتصال عبر الشبكة عن طريق حظر أو تصفية أرقام منافذ معينة.

رسائل المصافحة ثلاثية الاتجاهات :

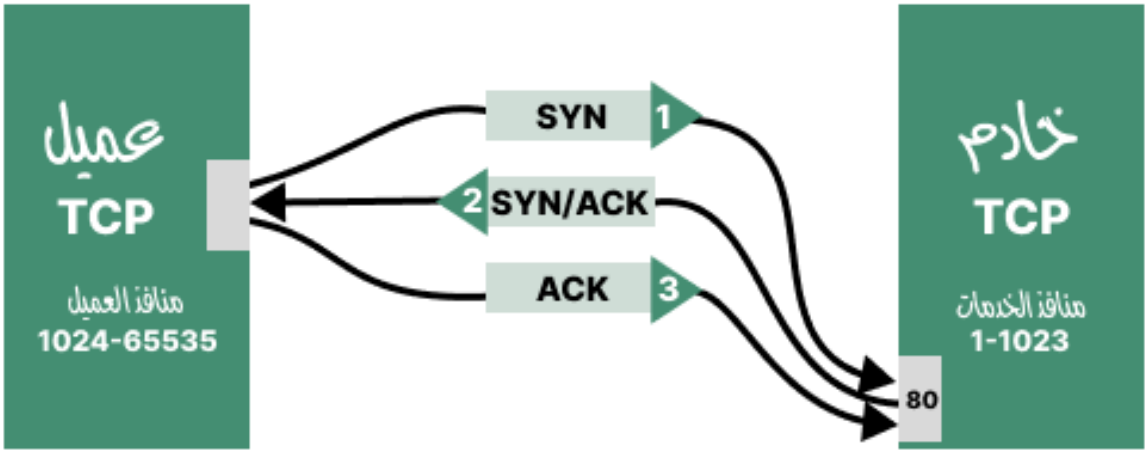
المصافحة ثلاثية الاتجاهات (المعروفة أيضًا باسم المزامنة ثلاثية الاتجاهات) هي عملية يستخدمها بروتوكول التحكم في الإرسال (TCP) لإنشاء اتصال بين جهازي شبكة تتضمن عملية الاتصال ثلاثي الاتجاهات سلسلة من ثلاث رسائل متبادلة بين المرسل والمستقبل لمزامنة حالة اتصالهما والتأكيد على استعدادهما لإرسال البيانات واستلامها.

الرسائل الثلاث التي تم تبادلها أثناء تبادل الإشارات الثلاثية هي:

١. **SYN:** يبدأ المرسل الاتصال عن طريق إرسال رسالة SYN (مزامنة) إلى الجهاز المستقبل. تتضمن هذه الرسالة رقم تسلسل عشوائي يستخدمه المرسل لتحديد الحزم التي يرسلها.

٢. **SYN-ACK:** إذا كان الجهاز المستقبل متاحاً وراغباً في إنشاء الاتصال فإنه يرسل رسالة SYN-ACK مرة أخرى إلى المرسل تتضمن هذه الرسالة رقم إقرار يؤكد استلام رسالة SYN الأولى للمرسل ورقم تسلسل جديد يستخدمه المستلم لتحديد الحزم التي يرسلها.

٣. **ACK:** في الختام يرسل المرسل رسالة ACK (إقرار) مرة أخرى إلى المستقبل لتأكيد استلامه لرسالة SYN-ACK. تتضمن هذه الرسالة رقم الإقرار من رسالة المستقبل والذي يؤكد أن الاتصال قد تم إنشاؤه.



بمجرد اكتمال تأكيد الاتصال ثلاثي الاتجاهات تتم مزامنة المرسل والمستقبل ويكونان جاهزين لتبادل البيانات عبر الاتصال. يمكن للمرسل البدء في إرسال البيانات وسيقوم المستلم بالإعلام بكل حزمة يتلقاها فإذا احتاج أي من الطرفين إلى إنهاء الاتصال فيمكنه إرسال رسالة FIN (إنهاء) إلى الطرف الآخر مما يؤدي إلى تشغيل تسلسل مماثل من الرسائل لإغلاق الاتصال بأمان.

تعتبر عملية الاتصال ثلاثي الاتجاهات عملية مهمة في TCP فهي تستخدم في ضمان نقل البيانات بشكل موثوق وفعال بين أجهزة الشبكة حيث يتم فيها الاتفاق فيها على ما يسمى (Window Size) والذي سيتم توضيحه بعد قليل ، وهي تؤكد على استعداد كلا الطرفين لتبادل البيانات ومنع الأخطاء وإعادة إرسال الحزم المفقودة والمشكلات الأخرى التي يمكن أن تؤثر على موثوقية نقل البيانات.

حجم النافذة (Window Size) :

في سياق TCP والمصافحة ثلاثية الاتجاهات يشير حجم النافذة إلى كمية البيانات التي يُسمح للمرسل بإرسالها دون تلقي إقرار من الجهاز المستقبل.

فأثناء تبادل تأكيد الاتصال ثلاثي الاتجاهات يتفاوض المرسل والمستقبل على حجم النافذة كجزء من رسالة SYN-ACK. وتشير قيمة حجم النافذة إلى عدد البايتات التي يرغب الجهاز المستقبل في تخزينها مؤقتاً قبل أن يتعين عليه إرسال إقرار بالاستلام مرة أخرى إلى المرسل. ويمكن ضبط هذه القيمة أثناء سير الاتصال بناءً على ظروف الشبكة ومقدار مساحة المخزن المؤقت المتاحة.

حجم النافذة مهم لأنه يساعد على تحسين تدفق البيانات بين المرسل والمستقبل فإذا كان حجم النافذة صغير جداً فقد يحتاج المرسل إلى انتظار الإقرارات قبل أن يتمكن من إرسال المزيد من البيانات مما قد يؤدي إلى إبطاء معدل الإرسال أما إذا كان حجم النافذة كبير جداً فقد يغمر الجهاز المستقبل بالبيانات ويبدأ الأخير في إسقاط الحزم مما قد يتسبب في إعادة الإرسال ومشكلات أخرى في الأداء. وعليه فمن خلال التفاوض على حجم النافذة كجزء من تبادل الاتصال ثلاثي الاتجاهات يضمن بروتوكول TCP إمكانية تبادل البيانات بين المرسل والمستقبل بكفاءة وموثوقية على مدار الاتصال كاملاً.

ملاحظة : يبدأ تكوين جلسة اتصال TCP بمصافحة ثلاثية الاتجاه بينما يتم إنهاء الجلسة بمصافحة رباعية الاتجاه.

يتم إنهاء الاتصال باستخدام مصافحة رباعية الاتجاه والتي تتضمن أربع رسائل بين المرسل والمستقبل للتأكد من أن كلا الطرفين جاهز لإغلاق الاتصال.

١. يرسل المرسل حزمة FIN (إنهاء) إلى المستلم لطلب إنهاء الاتصال.
٢. يستجيب المستقبل بحزمة ACK للإقرار بالطلب ولإبلاغ المرسل بأنه جاهز لإغلاق الاتصال.
٣. يرسل المستقبل حزمة FIN إلى المرسل لطلب إنهاء الاتصال من جانبه.
٤. يستجيب المرسل بحزمة ACK للإقرار بالطلب ولإبلاغ المستقبل بأنه جاهز للإغلاق من جانبه.

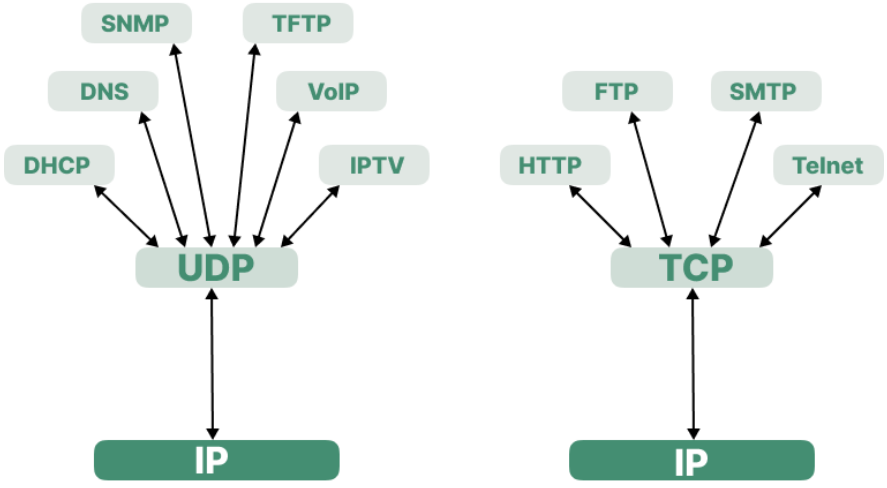
والسبب في تأكيد الاتصال رباعي الاتجاه هو التأكد من إرسال جميع البيانات قبل إغلاق الاتصال بحيث تقر حزمة ACK النهائية من المرسل إلى المستقبل باستلام جميع البيانات ويمكن إنهاء الاتصال بأمان.

هل يمكن الاستغناء بأحد بروتوكولات النقل عن الآخر؟

لا. وذلك لأن بروتوكولات النقل TCP و UDP تخدم أهدافاً مختلفة ولها نقاط قوة وضعف مختلفة. فمثلاً يوفر TCP تسليماً موثوقاً ومرتباً للبيانات مع آليات التحكم في التدفق والتحكم في الازدحام وهذا يجعله مناسباً للتطبيقات التي تتطلب نقل كميات كبيرة من البيانات بأقل قدر من الفقدان أو التلف مثل تصفح الويب والبريد الإلكتروني ونقل الملفات بينما يوفر UDP نقلاً منخفض السلامة وغير موثوق به للبيانات وهذا يجعله مناسباً للتطبيقات التي تتطلب السرعة في النقل مع التسامح في فقدان بعض البيانات أو تلفها مثل الألعاب عبر الإنترنت ووسائط البث.

البروتوكولات التي تستخدم TCP و UDP

بحسب المميزات الخاصة بكل منهما تستخدم البروتوكولات الأخرى أحدهما بحسب الحاجة والاستخدام كما هو موضح من الرسم أدناه



أنظمة العد:

أنظمة العد هي طرق تستخدم لتمثيل ومعالجة الأرقام بناء على قاعدة أو أساس معين فالأساس يعتبر عدد الرموز أو الأرقام المميزة المستخدمة في هذا النظام ومن أكثر أنظمة العد شيوعاً واستخداماً اليوم هو النظام العشري (الأساس 10) والثنائي (الأساس 2) والست عشري (الأساس 16).

نظام العد		
النظام	القاعدة	الأرقام او الأحرف المستخدمة
الثنائي	2	0 1
العشري	10	0 1 2 3 4 5 6 7 8 9
الست عشري	16	0 1 2 3 4 5 6 7 8 9 A B C D E F

في نظام العد **ذي الأساس العشري** نستخدم عشرة أرقام مميزة هي (9,8,7,6,5,4,3,2,1,0) وذلك لتمثيل جميع الأرقام الممكنة يستخدم هذا النظام على نطاق واسع في الحياة اليومية مثل البيع والشراء أو تتبع الوقت.

في نظام العد **ذي الأساس الثنائي** نستخدم رقمين مميزين (1,0) لتمثيل جميع الأرقام الممكنة. يستخدم هذا النظام في الحوسبة والإلكترونيات الرقمية لسهولة تنفيذه في الدوائر الإلكترونية كما أنه يبسط عمليات المنطق الرقمي.

في نظام العد **ذي الأساس الست عشري** نستخدم ستة عشر رقماً حرفاً مميزاً (F,E,D,C,B,A,9,8,7,6,5,4,3,2,1,0) لتمثيل كل ما هو ممكن من أعداد.

التحويل من النظام الثنائي للنظام العشري:

لتحويل رقم ثنائي إلى رقم عشري يمكن استخدام الخطوات التالية:

١. اكتب الرقم الثنائي وليكن على سبيل المثال 10110001.

1	0	1	1	0	0	0	1

٢. قم بتعيين قيمة مكانية لكل رقم في العدد الثنائي بدءاً من اليمين وزيادة بمقدار الضعف في كل مرة. فتصبح على النحو

1	0	1	1	0	0	0	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

٣. اضرب كل رقم في الرقم الثنائي بالقيمة المكانية المقابلة له ثم اجمع كل حاصل الضرب للحصول على القيمة العشرية المكافئة.

(128X1)+(64X0)+(32X1)+(16X1)+(8X0)+(4X0)+(2X0)+(1X1)
=128+0+32+16+0+0+0+1=128+32+16+1=**177**

التحويل من النظام العشري للنظام الثنائي:

لتحويل رقم عشري إلى رقم ثنائي يمكن استخدام الخطوات التالية:

١. قم بقسمة الرقم العشري على ٢ واكتب حاصل القسمة (القسمة الصحيحة) والباقي. استمر في قسمة حاصل القسمة على ٢ حتى يصبح حاصل القسمة صفراً. وليكن على سبيل المثال الرقم العشري ١٩٢

القسمة على 2	خارج القسمة	الباقي
192/2	96	0
96/2	48	0
48/2	24	0
24/2	12	0
12/2	6	0
6/2	3	0
3/2	1	1
1/2	0	1

٢. اكتب باقي القسمة من الخطوة ١ بترتيب عكسي، ستمثل هذه الأرقام الثنائية الرقم الثنائي المكافئ فيكون الناتج (1100000) ويمكن كتابته ايضاً هكذا (01100000) للمحافظة على كون الرقم ٨ خانات

بنية عنوان IPv4:

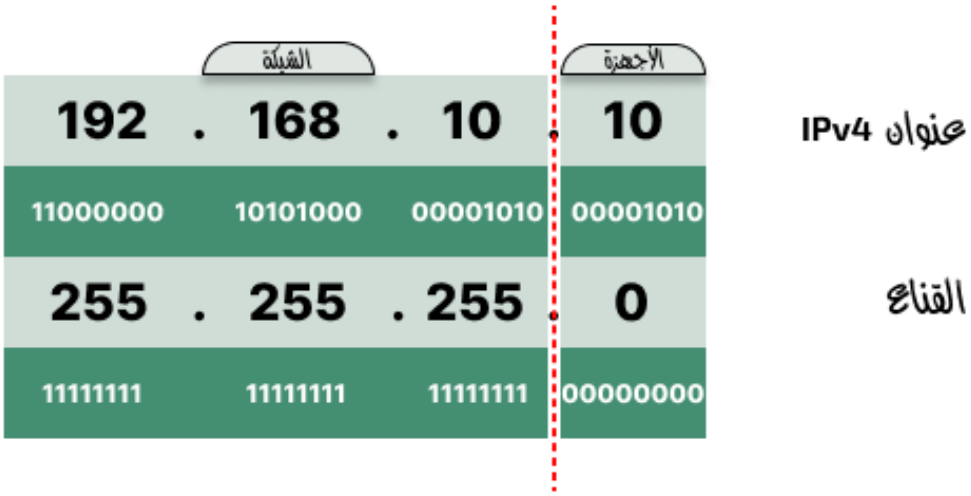
كما مر بنا سابقاً فإن عناوين IPv4 هي عناوين 32 بت تُستخدم لتعريف الأجهزة الموجودة على شبكة الحاسب الآلي بحيث تتم كتابة عنوان IPv4 عن طريق نظام العد العشري ويتكون العنوان من أربعة أرقام مفصولة بنقاط بحيث يمثل كل رقم 8bit (أو 1byte) من العنوان بحيث تكتب على هذه الصورة على سبيل المثال 192.168.10.12

يمكن تقسيم بنية عنوان IPv4 إلى جزأين:

١. جزء الشبكة: يحدد هذا الجزء من العنوان الشبكة التي ينتمي إليها الجهاز.
٢. جزء الأجهزة: يحدد هذا الجزء من العنوان الجهاز المحدد على تلك الشبكة.

يتم فصل جزء الشبكة وجزء الأجهزة بواسطة ما يسمى بقناع الشبكة الفرعية والذي يمثل أيضاً قيمة 32 بت مكتوبة بنظام العد العشري. بحيث يحتوي قناع الشبكة الفرعية على سلسلة من الـ 1 متبوعة بسلسلة من الـ 0 بحيث تشير الـ 1 إلى جزء الشبكة من العنوان بينما تشير الـ 0 إلى جزء الأجهزة من العنوان.

مثال: يعني قناع الشبكة الفرعية 255.255.255.0 أن الأرقام الثلاثة الأولى في عنوان IPv4 تمثل جزء الشبكة ويمثل الرقم الأخير جزء الجهاز.



تمثل العدد الأول أو ما يمكن تسـميته بالثمانية الأولى (octet) من عنوان IPv4 الفئة التي ينتمي لها العنوان والتي تحدد قناع الشـبكة الفرعية الافتراضي والحد الأقصى لعدد الأجهزة المضـيفة التي يمكن توصيلها بالشبكة. هناك خمس فئات من عناوين IPv4:

Address Class	1st octet	Network & Host	Default subnet mask	Number of network & host
A	1-127	N.H.H.H	255.0.0.0	128 net 16777214 host
B	128-191	N.N.H.H	255.255.0.0	16384 net 65534 host
C	192-223	N.N.N.H	255.255.255.0	2097150 net 254 host
D	224-239	Multicast		
E	240-255	Experiments		

ولتوضـيح الفكرة يمثل الجدول أدناه عناوين IP مختلفة ومن فئات مختلفة وكيفية اسـتنتاج كامل مواصفات الشبكة من خلال الثمانية الأولى لهذه العناوين:

IP Address	class	Net No	1st IP	Last IP
192.168.12.22	C	192.168.12.0	192.168.12.1	192.168.12.254
1.122.22.12	A	1.0.0.0	1.0.0.1	1.255.255.254
190.12.233.55	B	190.12.0.0	190.12.0.1	190.12.255.254
130.223.34.87	B	130.223.0.0	130.223.0.1	130.223.255.254
111.121.222.11	A	111.0.0.0	111.0.0.1	111.255.255.254

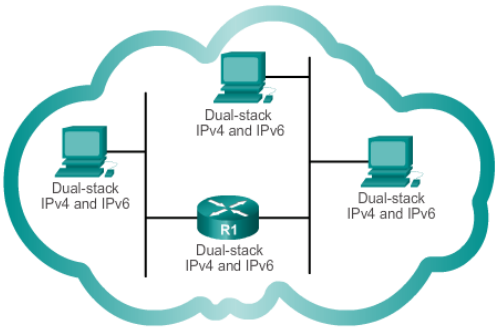
لماذا تم إيجاد اصدار جديد من عناوين IP ليكون IPv6:

السبب الرئيسي لإيجاد عناوين IPv6 هو استنفاد أعداد العناوين التي يوفرها IPv4 يستخدم IPv4 والتي توفر ما يصل إلى 4.3 مليار عنوان فريد وغير مكرر ومع ذلك. والسبب في ذلك هو النمو الهائل للإنترنت وانتشار الأجهزة الشبكية وبروز ما يسمى بإنترنت الأشياء (IoT) فلم يعد هذا الرقم كافياً. ومن هنا جاءت الحاجة للتحديث وجاءت العناوين IPv6 والتي تتكون من 128 بت وتوفر مسـاحة عناوين كبيرة جداً تصل إلى(340000000000000000000000000000000000000) عنوان تقريباً.

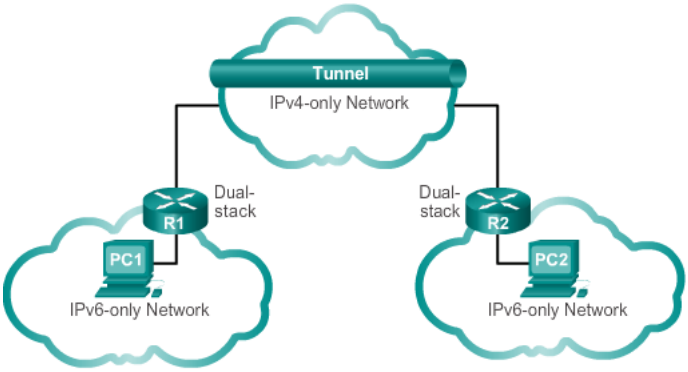
كيف يمكن التوفيق بين شبكات الحاسب التي تعمل بـ IPv4 *وتلك التي تعمل بـ* IPv6 *:*

IPv4 و IPv6 غير متوافقين بشـــكل مباشر لأنهما بروتوكولات مختلفة تســـتخدم تنســـيقات عناوين مختلفة. ومع ذلك هناك العديد من الآليات التي تم تطويرها لتمكين الاتصال بين شبكات IPv4 و IPv6:

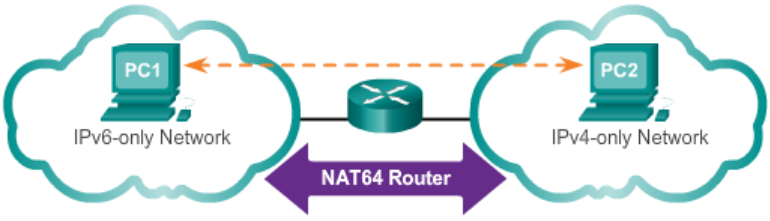
١. **التكدس الثنائي (Dual-Stack):** تتمثل إحدى الطرق في تشـغيل كل من IPv4 و IPv6 على نفس الجهاز باستخدام تقنية تسمى التكدس الثنائي أو المزدوج. بحيث يحتوي الجهاز على عنوان IPv4 وعنوان IPv6 ، ويمكنه الاتصال بكل من شبكات IPv4 و IPv6.



٢. **الاتصال النفقي:** تتمثل هذه الطريقة في استخدام الاتصال النفقي لتغليف حزم IPv6 داخل حزم IPv4 ، أو العكس. يسمح ذلك بنقل حركة مرور IPv6 عبر شبكة IPv4 ، أو العكس.



٣. **الترجمة:** الترجمة هي طريقة أخرى يمكن استخدامها لتمكين الاتصال بين شبكات IPv4 و IPv6. في هذا النهج تُترجم الحزم من بروتوكول إلى آخر في بوابة الشبكة.



بنية عنوان IPv6 *:*

عناوين IPv6 هي عناوين 128 بت يتم تمثيلها وفق نظام العد الست عشري. ينقسم العنوان إلى ثمانية كتل من ١٦ بت مفصولة بنقطتين بحيث تمثل كل كتلة بأربعة أرقام سداسية عشرية.
مثال 2001:0DB8:000A:1000:0000:0000:0000:0100

يمكن أيضًا اختصار عناوين IPv6 باستخدام عدة تقنيات:

١. **الأصفار البادئة:** يمكن حذف الأصفار البادئة في الكتلة فعلى سبيل المثال يمكن اختصار "2001:0DB8" لتكون "2001:DB8" كما هو موضح أدناه.

العنوان كاملاً	2001 : 0DB8 : 000A : 1000 : 0000 : 0000 : 0000 : 0100
حذف الأصفار	2001 : DB8 : A : 1000 : 0 : 0 : 0 : 100
ضغط العنوان	2001 : DB8 : A : 1000 : 0 : 0 : 0 : 100

٢. **الكتل الصفرية المتتالية:** يمكن استبدال الكتل المتتالية من الأصفار بنقطتين مزدوجتين (: :). على سبيل المثال يمكن اختصار "2001:0DB8:000A:1000:0000:0000:0000:0100" إلى "2001:0DB8:000A:1000::0100".

ملاحظة: في حال وجود أكثر من مقطع من الكتل الصفرية فلا يمكن تطبيق القاعدة الثانية الامرة واحدة على أحد هذه الكتل كما هو موضح في المثال أدناه.

العنوان كاملاً	2001 : 0DB8 : 0000 : 0000 : ABCD : 0000 : 0000 : 0100
حذف الأصفار	2001 : DB8 : 0 : 0 : ABCD : 0 : 0 : 100
ضغط العنوان	2001 : DB8 : : ABCD : 0 : 0 : 100
	أو
	2001 : DB8 : 0 : 0 : ABCD : : 100

ما الفرق بين Traceroute *و* Ping *:*

يعد كل من Traceroute و Ping من أدوات تشخيص الشبكة لكنهما يخدمان أهدافاً مختلفة ويستخدمان تقنيات مختلفة.

Ping هي أداة بسيطة تُستخدم لاختبار الاتصال بين جهازين موجودين في شبكة عن طريق إرسال حزمة ICMP (بروتوكول رسائل التحكم في الإنترنت) إلى الجهاز المستهدف وانتظار حزمة رد ICMP.
يقيس الأمر ping وقت الرحلة ذهابًا وإيابًا بين المرسل والجهاز الهدف ويبلغ عن أي فقد للحزمة. غالبًا ما تُستخدم هذه الأداة للتحقق مما إذا كان يمكن الوصول إلى الجهاز واستجابته على الشبكة.

بينما Traceroute هي أداة تستخدم لتتبع المسار الذي تسلكه الحزم من الجهاز المصدر إلى الجهاز الوجهة وتحديد أي مشكلات في الشبكة تصادفه على طول الطريق. يعمل Traceroute عن طريق إرسال حزم ذات قيم TTL (مدة البقاء) إلى الجهاز المستهدف. عندما تمر كل حزمة عبر جهاز توجيه

تنخفض قيمة TTL ويرسل جهاز التوجيه رسالة ICMP "تجاوز الوقت" إلى الجهاز المصدر عندما تصل قيمة TTL إلى الصفر. من خلال إرسال حزم مع قيم TTL المتناقصة بشكل متكرر يكون traceroute قادرًا على تعيين مسار الشبكة من الجهاز المصدر إلى الجهاز المستهدف وتحديد أي أجهزة توجيه أو روابط قد تسبب زمن انتقال الشبكة أو فقدان الحزمة.

باختصار يتم استخدام Ping لاختبار الاتصال وقياس وقت الذهاب والإياب بينما يتم استخدام Traceroute لتعيين مسار الشبكة وتحديد مشكلات الشبكة. توفر كلتا الأداتين معلومات تشخيصية قيمة لاستكشاف مشكلات الشبكة وإصلاحها.

تقسيم الشبكة الى شبكات فرعية :

يعني تقسيم الشبكة إلى شبكات فرعية أن يتم تقسيم شبكة كبيرة إلى شبكات فرعية أصغر وأكثر قابلية للإدارة ولكل منها عنوان الشبكة الفريد الخاص بها يتم ذلك عادةً لتحسين كفاءة الشبكة وأمانها.

عند تقسيم الشبكة إلى شبكات فرعية يكون لكل شبكة فرعية نطاق عناوين خاص بها وتعمل الشبكات الفرعية أيضًا على تحسين أمان الشبكة عن طريق تقييد مجال البث. فمن خلال تقسيم الشبكة إلى شبكات فرعية أصغر يتم تقليل مجال البث مما يساعد على منع عواصف البث وتحسين الأداء الكلي للشبكة.

هناك طرق عديدة لاستخدام الشبكات الفرعية في المساعدة في إدارة أجهزة الشبكة. فبإمكان مسؤولي الشبكة تقسيم الشبكة الى شبكات فرعية اعتماداً على عدة اعتبارات مثل:

١. الموقع، مثل الطوابق في أحد المباني
٢. الإدارات التنظيمية
٣. أنواع الأجهزة

عند الحديث عن تقسيم الشبكات فهناك طريقتان للقيام بذلك، الأولى وهي الأسهل ولكن ينقصها الدقة التي قد تكون مهمة في بعض الحالات أما الثانية فهي تتطلب العديد من العمليات الحسابية الأساسية والبسيطة ولكنها أكثر دقة والطريقتان هما:

١. تقسيم الشبكات إلى شبكات فرعية على مستوى الحد الثماني المتمثل في 8/ و16/ و24/
٢. تقسيم الشبكات إلى شبكات فرعية على مستوى البت.

مثال للطريقة الأولى:

نفترض أن شركة اختارت العنوان الخاص 10.0.0.0/8 ليكون عنوان الشـــبكة الداخلية لها وهذا العنوان لأنه من الفئة A كما مر معنا سـابقاً يمكنه ربط 16777214 جهازاً في مجال بث واحد. وهذا لا يُعد إجراء مثالي وجيد للشركة. ولمعالجة ذلك يمكن للشركة تقسـيم الشـبكة 10.0.0.0/8 إلى شـبكات فرعية عند الحد الثماني 16/ ليصبح عنوان الشبكة الجديد هو 10.0.0.0/16

عنوان الشبكة الفرعية	مدى العناوين	عنوان البث
10.0.0.0/16	**10.0**.255.254- **10.0**.0.1	**10.0**.255.255
10.1.0.0/16	**10.1**.255.254- **10.1**.0.1	**10.1**.255.255
10.2.0.0/16	**10.2**.255.254- **10.2**.0.1	**10.2**.255.255
10.3.0.0/16	**10.3**.255.254- **10.3**.0.1	**10.3**.255.255
10.4.0.0/16	**10.4**.255.254- **10.4**.0.1	**10.4**.255.255
10.5.0.0/16	**10.5**.255.254- **10.5**.0.1	**10.5**.255.255
...	...	...
10.255.0.0/16	**10.255**.0.254- **10.255**.0.1	**10.255**.255.255

يمكن أن يوفر هذا الإجراء للشـركة القدرة على تعريف وإيجاد ما يصـل إلى 256 شـــبكة فرعية (أي: من 10.0.0.0/16 إلى 10.255.0.0/16) بحيث تستطيع كل شبكة فرعية ربط 65443 جهاز. لاحظ كيف تحدد الـ البايتان الأوليان جزء الشبكة للعنوان بينما تمثل البايتان الأخيرتان عناوين IP للمضيف.

أو بدلاً من ذلك، يمكن للشركة أن تختار تقسـيم الشـبكة إلى شـبكات فرعية عند الحد الثماني 24/. وذلك يُمكّن الشركة من ايجاد 65536 شبكة فرعية تكون كل منها قادرة على ربط ٢٥٤ جهاز.

عنوان الشبكة الفرعية	مدى العناوين	عنوان البث
10.0.0.0/24	**10.0.0**.254- **10.0.0**.1	**10.0.0**.255
10.0.1.0/24	**10.0.1**.254- **10.0.1**.1	**10.0.1**.255
10.0.2.0/24	**10.0.2**.254- **10.0.2**.1	**10.0.2**.255
...	...	...
10.0.255.0/24	**10.0.255**.254- **10.0.255**.1	**10.0.255**.255
10.1.0.0/24	**10.1.0**.254- **10.1.0**.1	**10.1.0**.255
...	...	...
10.255.255.0/24	**10.255.255**.254- **10.255.255**.1	**10.255.255**.255

إن الحد 24/ شائع للغاية في تقسيم الشبكات إلى شبكات فرعية نظرًا لأنه يتّسع لعدد مناسب ومعقول من الأجهزة كما أنه يقسم الشبكات إلى شبكات فرعية عند الحد الثماني بطريقة سهلة.

مثال للطريقة الثانية:

قبل ضرب المثال لهذه الطريقة يجب إيضـاح القاعدة التي يتم الاعتماد عليها عند تقسـيم الشـبكة الى شبكات فرعية على مستوى البت.

لحسـاب عدد الشـبكات الفرعية المتحصـل عليها من اسـتعارة 1 بت من جزء الأجهزة واعطاؤه لجزء الشبكة

192.	168.	1.	0	0000000

تمت استعارة 1 بت

القاعدة هي : عدد الشبكات الفرعية = $2^{\text{عدد البتات المستعارة}}$

وعليه فعند استعارة 1 بت فقط سيكون عدد الشبكات الفرعية المتحصل عليها هو 2 لأن

$$2^1=2$$

ولحسـاب عدد الأجهزة في كل شـبكة الفرعية والمتحصـل عليها من اسـتعارة 1 بت من جزء الأجهزة واعطاؤه لجزء الشبكة

192.	168.	1.	0	0000000

عدد البتات المتبقية 7

القاعدة هي : عدد الأجهزة في كل شبكة فرعية = $2^{\text{عدد البتات المتبقية}}$ -2

وعليه فعند استعارة 1 بت فقط سيكون عدد الأجهزة في كل شبكة فرعية هو 126 لأن

$$2^7-2=126$$

مثال آخر للطريقة الثانية:

ماذا يحدث عند استعارة وحدتي بت من جزء الأجهزة وإضافتها لجزء الشبكة.

القاعدة هي : عدد الشبكات الفرعية = $2^{\text{عدد البتات المستعارة}}$

$$2^2=4$$

هذا يعني أننا سنتحصل على 4 شبكات فرعية وعدد الأجهزة في كل شبكة فرعية يمكن حسابه من خلال

القاعدة هي : عدد الأجهزة في كل شبكة فرعية = $2^{\text{عدد البتات المتبقية}}$ -2

$$2^6-2=62$$

اعتبارات تقسيم الشبكة إلى شبكات فرعية:

هناك اعتبارين أساسيين يجب مراعاتهما عن تقسيم الشبكة إلى شبكات فرعية هما:

١. عدد الشبكات الفرعية المطلوبة.
٢. عدد عناوين الأجهزة المضيفة المطلوبة.

أولاً: الخطوات اللازمة لتقسيم الشبكة باعتبار عدد الشبكات الفرعية المطلوبة هي:

١. التأكد من الجزء الذي سنقوم بالعمل عليه وهل هو جزء الشبكة أو جزء الأجهزة وفي حالتنا هذه سنعمل على جزء الشبكة والذي يمثله (1's)
٢. نحدد عدد البتات (Bits) التي سنقوم باستعارتها من جزء الأجهزة ونعطيه لجزء الشبكات ونستخدم هذه القاعدة:

$$2^{?} \geq \text{عدد الشبكات المطلوبة}$$

٣. نحدد القناع الجديد بعد الاستعارة.
٤. نحدد الـ Block size والذي يمثل العدد الثابت الذي نريده لمعرفة أرقام الشبكات ونستخدم لذلك هذه القاعدة:

$$\text{Block size} = 2^{\text{Zero's}}$$

٥. نحدد الشبكات الجديدة الفرعية ونوضح تفاصيلها.

مثال١: قسم الشبكة 192.168.11.0/24 الى شبكتين فرعية

الحل:

١. التأكد من الجزء الذي سنقوم بالعمل عليه وهل هو جزء الشبكة أو جزء الأجهزة وفي حالتنا هذه سنعمل على جزء الشبكة والذي يمثله (1's)

٢. نحدد كم بت سنقوم باستعارته من جزء الأجهزة ونعطيه لجزء الشبكات ونستخدم القاعدة

$$2^{?} \geq \text{عدد الشبكات المطلوبة}$$

$$2^{?} \geq 2$$

$$2^{1} \geq 2$$

وعليه فإن عدد البتات (Bits) المستعارة هو 1

٣. نحدد الآن القناع الجديد بعد الاستعارة

11111111.11111111.11111111.**1**0000000
192.168.11.0/25 أو 255.255.255.128

٤. نحدد الـ Block size والذي يمثل العدد الثابت الذي نريده لمعرفة أرقام الشبكات والقاعدة

Block size= $2^{Zero's}$

Block size= 2^7

Block size= 128

٥. نحدد الشبكات الجديدة الفرعية ونوضح تفاصيلها

S1 192.168.11.0/25
S2 192.168.11.128/25

IP Address	1st	Last	Broadcast
192.168.11.0	192.168.11.1	192.168.11.126	192.168.11.127
192.168.11.128	192.168.11.129	192.168.11.254	192.168.11.255

مثال٢: قسم الشبكة 192.168.3.128/25 الى أربعة شبكات فرعية

الحل:

١. التأكد من الجزء الذي سنقوم بالعمل عليه وهل هو جزء الشبكة أو جزء الأجهزة وفي حالتنا هذه سنعمل على جزء الشبكة والذي يمثله (1's)

٢.

٣. نحدد كم بت سنقوم باستعارته من جزء الأجهزة ونعطيه لجزء الشبكات ونستخدم القاعدة

عدد الشبكات المطلوبة $\leq 2^?$

$2^? \geq 4$

$2^2 \geq 4$

وعليه فإن عدد البتات (Bits) المستعارة هو 2

٤. نحدد الآن القناع الجديد بعد الاستعارة

11111111.11111111.11111111.**11**00000
192.168.3.128/27 أو 255.255.255.224

٥. نحدد الـ Block size والذي يمثل العدد الثابت الذي نريده لمعرفة أرقام الشبكات والقاعدة

Block size= $2^{Zero's}$

Block size= 2^5

Block size= 32

٦. نحدد الشبكات الجديدة الفرعية ونوضح تفاصيلها

S1 192.168.3.128/27
S2 192.168.3.160/27
S3 192.168.3.192/27
S4 192.168.3.224/27

IP Address	1st	Last	Broadcast
192.168.3.128	192.168.3.129	192.168.3.158	192.168.3.159
192.168.3.160	192.168.3.161	192.168.3.190	192.168.3.191
192.168.3.192	192.168.3.193	192.168.3.222	192.168.3.223
192.168.3.224	192.168.3.225	192.168.3.254	192.168.3.255

مثال٣: قسم الشبكة 19.0.0.0/8 الى خمس شبكات فرعية

الحل:

١. التأكد من الجزء الذي سنقوم بالعمل عليه وهل هو جزء الشبكة أو جزء الأجهزة وفي حالتنا هذه سنعمل على جزء الشبكة والذي يمثله (1's)

٢.

٣. نحدد كم بت سنقوم باستعارته من جزء الأجهزة ونعطيه لجزء الشبكات ونستخدم القاعدة

عدد الشبكات المطلوبة $\leq 2^{?}$

$2^{?} \geq 5$

$2^{3} \geq 5$

وعليه فإن عدد البتات (Bits) المستعارة هو 3

٤. نحدد الآن القناع الجديد بعد الاستعارة

11111111.**111**00000.00000000.00000000

19.0.0.0/11 أو 255.224.0.0

٥. نحدد الـ Block size والذي يمثل العدد الثابت الذي نريده لمعرفة أرقام الشبكات والقاعدة

Block size= $2^{Zero's}$

Block size= 2^{5}

Block size= 32

٦. نحدد الشبكات الجديدة الفرعية ونوضح تفاصيلها

S1 19.0.0.0/11
S2 19.32.0.0/11

S3 19.64.0.0/11
S4 19.96.0.0/11
S5 19.128.0.0/11

IP Address	1st	Last	Broadcast
19.0.0.0	19.0.0.1	19.31.255.254	19.31.255.255
19.32.0.0	19.32.0.1	19.63.255.254	19.63.255.255
19.64.0.0	19.64.0.1	19.95.255.254	19.95.255.255
19.96.0.0	19.96.0.1	19.127.255.254	19.127.255.255
19.128.0.0	19.128.0.1	19.159.255.254	19.159.255.255

ثانياً: الخطوات اللازمة لتقسيم الشبكة باعتبار عدد الأجهزة المطلوبة في كل شبكة فرعية هي:

١. التأكد من الجزء الذي سنقوم بالعمل عليه وهل هو جزء الشبكة أو جزء الأجهزة وفي حالتنا هذه سنعمل على جزء الشبكة والذي يمثله (0's)
٢. نحدد عدد البتات (Bits) التي سنقوم بالاحتفاظ بها لجزء الأجهزة ونعطي المتبقي لجزء الشبكات ونستخدم هذه القاعدة:

$$2^{?} \geq \text{عدد الأجهزة المطلوبة} + 2\text{Bit's}$$

٣. نحدد القناع الجديد بعد الاستعارة.
٤. نحدد الـ Block size والذي يمثل العدد الثابت الذي نريده لمعرفة أرقام الشبكات ونستخدم لذلك هذه القاعدة:

$$\text{Block size} = 2^{\text{Zero's}}$$

٥. نحدد الشبكات الجديدة الفرعية ونوضح تفاصيلها.

مثال١: قسم الشبكة 192.168.30.0/24 بحيث يكون في كل شبكة خمسة أجهزة

الحل:
١. التأكد من الجزء الذي سنقوم بالعمل عليه وهل هو جزء الشبكة أو جزء الأجهزة وفي حالتنا هذه سنعمل على جزء الأجهزة والذي يمثله (0's)

٢. نحدد كم بت سنقوم بالاحتفاظ به للأجهزة وإعطاء الباقي للشبكة ونستخدم هذه القاعدة

$$2^{?} \geq \text{عدد الأجهزة المطلوبة} + 2\text{Bit's}$$

$$2^{?} \geq 5 + 2\text{Bit's}$$

$$2^{?} \geq 7$$

$$2^{3} \geq 7$$

وعليه فإن عدد البتات (Bits) التي سنحتفظ بها هو 3

٣. نحدد القناع الجديد بعد الاستعارة

11111111.11111111.11111111.11111**000**
192.168.30.0/29 أو 255.255.255.0

٤. نحدد الـ Block size والذي يمثل العدد الثابت الذي نريده لمعرفة أرقام الشبكات والقاعدة

Block size= $2^{Zero's}$

Block size= 2^3

Block size= 8

٥. نحدد الشبكات الجديدة الفرعية ونوضح تفاصيلها

S1 192.168.30.0/29
S2 192.168.30.8/29
S3 192.168.30.16/29
S4 192.168.30.24/29
S5 192.168.30.32/29
S6 192.168.30.40/29
S7 192.168.30.48/29
S8 192.168.30.56/29
S9 192.168.30.64/29
S10 192.168.30.72/29

IP Address	1st	Last	Broadcast
192.168.30.0	192.168.30.1	192.168.30.6	192.168.30.7
192.168.30.8	192.168.30.9	192.168.30.14	192.168.30.15
192.168.30.16	192.168.30.17	192.168.30.22	192.168.30.23
192.168.30.24	192.168.30.25	192.168.30.30	192.168.30.31
192.168.30.32	192.168.30.33	192.168.30.38	192.168.30.39
192.168.30.40	192.168.30.41	192.168.30.46	192.168.30.47
192.168.30.48	192.168.30.49	192.168.30.54	192.168.30.55
192.168.30.56	192.168.30.57	192.168.30.62	192.168.30.63
...	...	...	...
192.168.30.248	192.168.30.249	192.168.30.254	192.168.30.255

مثال٢: قسم الشبكة 149.0.0.0/16 بحيث يكون في كل شبكة 1000 جهاز

الحل:

١. التأكد من الجزء الذي سنقوم بالعمل عليه وهل هو جزء الشبكة أو جزء الأجهزة وفي حالتنا هذه سنعمل على جزء الأجهزة والذي يمثله (0's)

٢. نحدد كم بت سنقوم بالاحتفاظ به للأجهزة وإعطاء الباقي للشبكة ونستخدم هذه القاعدة

$2^{?} \geq$ عدد الأجهزة المطلوبة+2Bit's

$2^{?} \geq 1000+2Bit's$

$2^{?} \geq 1002$

$2^{10} \geq 1002$

وعليه فإن عدد البتات (Bits) التي سنحتفظ بها هو 10

٣. نحدد القناع الجديد بعد الاستعارة

11111111.11111111.11111100.00000000

149.0.0.0/22 أو 255.255.252.0

٤. نحدد الـ Block size والذي يمثل العدد الثابت الذي نريده لمعرفة أرقام الشبكات والقاعدة

$Block\ size = 2^{Zero's}$

$Block\ size = 2^{2}$

$Block\ size = 4$

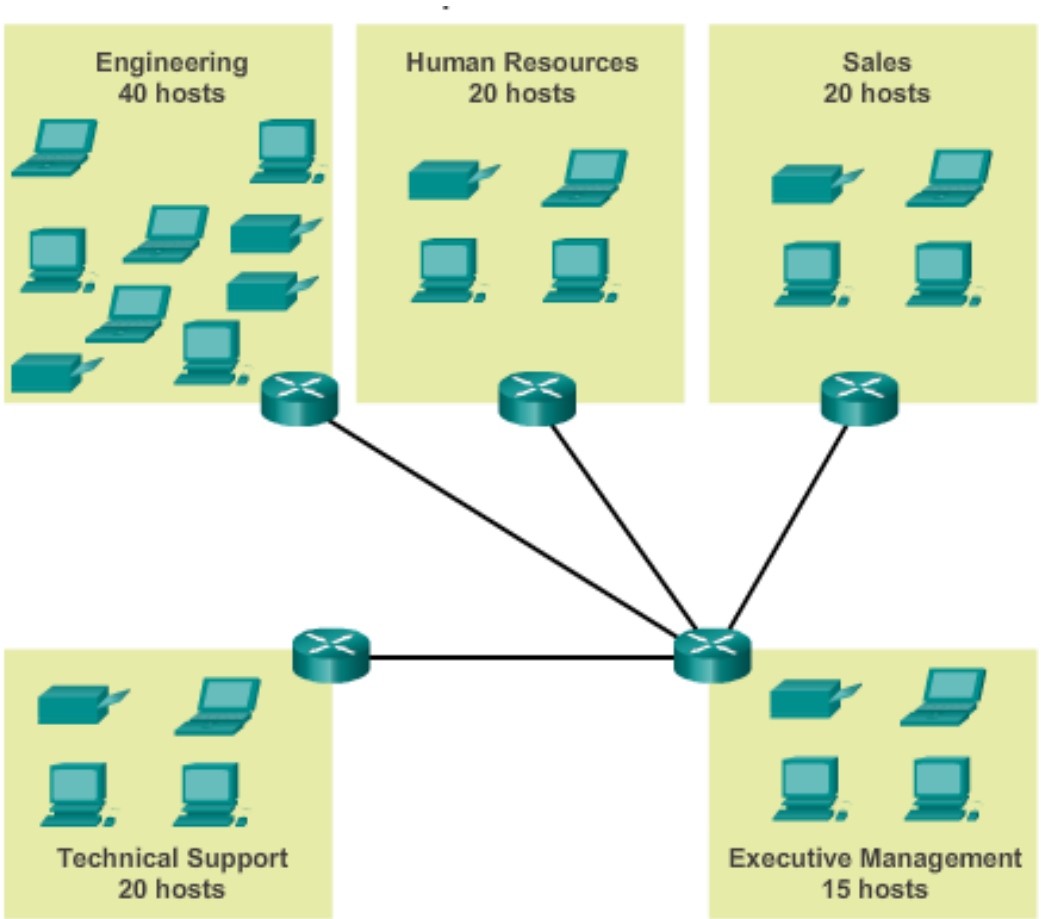
٥. نحدد الشبكات الجديدة الفرعية ونوضح تفاصيلها

S1 149.0.0.0/22
S2 149.0.4.0/22
S3 149.0.8.0/22
S4 149.0.12.0/22
S5 149.0.16.0/22
S6 149.0.20.0/22
S7 149.0.24.0/22
S8 149.0.28.0/22
S9 149.0.32.0/22
S10 149.0.36.0/22

IP Address	1st	Last	Broadcast
149.0.0.0/22	149.0.0.1/22	149.0.3.254/22	149.0.3.255/22
149.0.4.0/22	149.0.4.1/22	149.0.7.254/22	149.0.7.255/22
149.0.8.0/22	149.0.8.1/22	149.0.11.254/22	149.0.11.255/22
149.0.12.0/22	149.0.12.1/22	149.0.15.254/22	149.0.15.255/22
149.0.16.0/22	149.0.16.1/22	149.0.19.254/22	149.0.19.255/22
149.0.20.0/22	149.0.20.1/22	149.0.23.254/22	149.0.23.255/22
149.0.24.0/22	149.0.24.1/22	149.0.27.254/22	149.0.27.255/22
149.0.28.0/22	149.0.28.1/22	149.0.31.254/22	149.0.31.255/22
...	...	...	...

ملاحظة:

الاعتبارين اللذين تمت مناقشتهما أعلاه تقسم لنا الشبكة إلى شبكات فرعية متساوية في الحجم سواء باعتبار عدد الشبكات أو باعتبار عدد الأجهزة وفي الواقع العملي قد نحتاج الى تقسيم الشبكة إلى شبكات فرعية مختلفة الاحجام وهذا ما يسمى بالـ VLSM كما هو موضح بالصورة أدناه:



VLSM تقنية أو طريقة تستخدم في تقسيم الشبكات إلى شبكات فرعية أصغر ذات أحجام مختلفة بدلاً من استخدام نفس الحجم لجميع الشبكات الفرعية.

مر معنا سابقاً تقسيم الشبكة إلى شبكات فرعية متساوية بحيث يكون لكل منها نفس عدد عناوين IP. وهذا غالبًا ما يؤدي إلى اســـتخدام غير فعال لعناوين IP حيث قد تحتوي بعض الشـــبكات الفرعية على عدد كبير من عناوين IP بينما قد يكون لدى البعض الآخر عدد قليل.

باستخدام VLSM يمكن لمسؤولي الشبكة استخدام أقنعة شبكة فرعية مختلفة لشبكات فرعية مختلفة اعتمادًا على عدد الأجهزة التي تحتاج إلى الاتصال بتلك الشبكة الفرعية المحددة. يسمح هذا باستخدام أكثر كفاءة لعناوين IP حيث يمكن تخصيص كل شبكة فرعية للعدد الدقيق للأجهزة التي ستدعمها.

على سبيل المثال افترض أننا نرغب في إنشاء شبكتين فرعيتين الأولى بها 100 جهاز والثانية بها 50 جهاز فقد لا يكون منا سب استخدام الطريقة التقليدية التي تقسم الشبكات إلى شبكات فرعية متساوية وانما يفضل استخدام الـــ VLSMفي هذه الحالة بحيث نستخدم قناع شبكة فرعية يسمح بما لا يقل عن 128 عنوان IP والذي سيكون في هذه الحالة (X.X.X.X/25) هذا القناع سيوفر لنا 128عنوان نستخدم منها الـــ 100 التي نحتاج ثم نستخدم قناع شبكة فرعية آخر يوفر لنا ما لا يقل عن 50 عنوان والذي سيكون في حالتنا هذه (X.X.X.X/26) هذا القناع سيوفر لنا 64 عنوان نستخدم منها الـ 50 التي نحتاج.

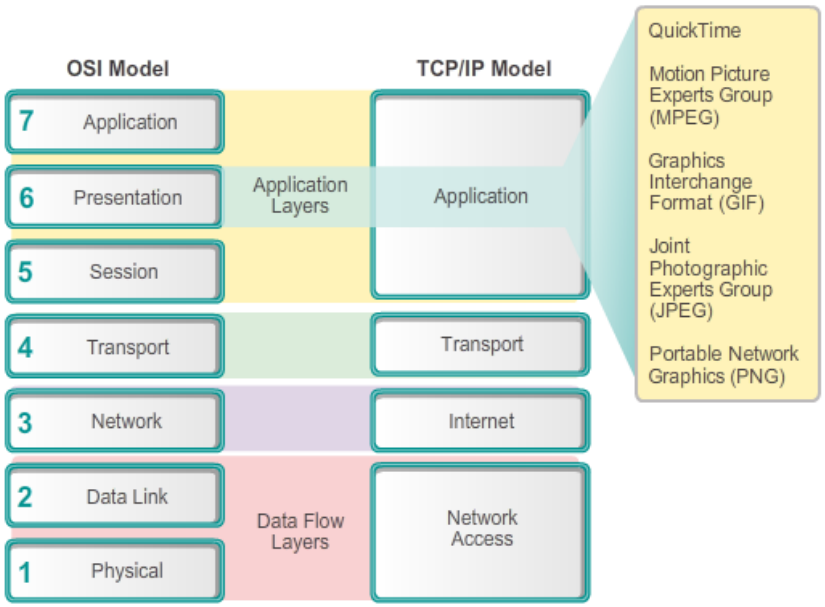
طبقات الجلسة والعرض والتطبيقات:

تقوم طبقة الجلسة بعدد من المهام الأساسية وهي:

- تعمل الوظائف على إنشاء حوارات بين تطبيقات المصدر والوجهة والحفاظ عليها.
- تقوم بعملية تبادل المعلومات لبدء الحوارات والحفاظ على نشاطها وإعادة تشغيل الجلسات.

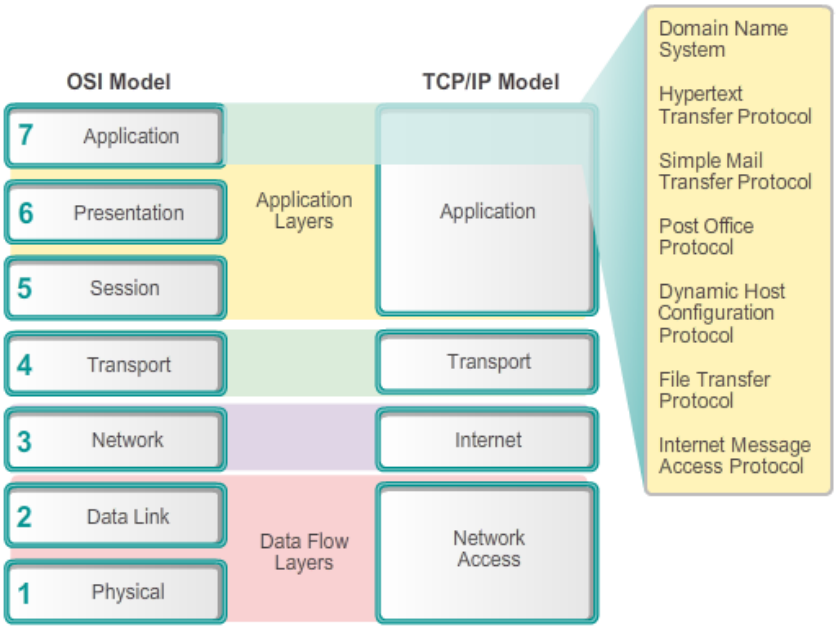
تقوم طبقة العرض بثلاث وظائف رئيسية وهي:

١. ترميز وتحويل بيانات طبقة التطبيق
٢. ضغط البيانات
٣. تشفير البيانات لعملية الإرسال وإلغاء تشفيرها فور استلامها من قِبل جهاز الوجهة



تقوم طبقة التطبيقات بشكل رئيسي بتقديم الخدمات لتطبيقات المستخدم النهائي فهي تقوم بـ :

- توفير الوصول إلى خدمات الشبكة.
- تعريف البروتوكولات لتطبيقات معينة.
- تمكين تبادل البيانات بين التطبيقات.
- دعم الأمان على مستوى التطبيق.



هناك العديد من البروتوكولات التي تعمل في طبقة التطبيق والتي ســـتعرض هنا باختصـــار في حين سيتم توضيح بعضها بشيء من التفصيل وهي كالتالي:

بروتوكول خدمة اسم المجال (DNS) - يستخدم لتحليل أسماء الإنترنت إلى عناوين IP

Telnet - هو أحد بروتوكولات المحاكاة الطرفية ويستخدم لتوفير إمكانية الوصول عن بُعد لأجهزة الخوادم وأجهزة شبكات الحاسب

بروتوكول روتين التمهيد (BOOTP) - يسبق بروتوكول DHCP، وهو بروتوكول شبكات يستخدم للحصول على معلومات عنوان IP أثناء التمهيد

بروتوكول التحكم في المضيف الديناميكي (DHCP) - يستخدم لتخصيص عنوان IP وقناع الشبكة الفرعية والعبّارة الافتراضية وخادم DNS إلى مضيف

بروتوكول نقل النص التشعبي (HTTP) - يستخدم لنقل الملفات التي تتكون منها صفحات الويب على شبكة الويب العالمية

بروتوكول نقل الملفات (FTP) - يستخدم لنقل الملفات بصورة تفاعلية بين الأنظمة

بروتوكول نقل الملفات المبسط (TFTP) - يستخدم لنقل الملفات الفعال دون اتصال

بروتوكول نقل البريد البسيط (SMTP) - يستخدم لنقل رسائل البريد والمرفقات

بروتوكول مكتب البريد (POP) - يستخدم بواسطة عملاء البريد الإلكتروني للحصول على البريد الإلكتروني من خادم بعيد

بروتوكول الوصول إلى الرسائل عبر الإنترنت (IMAP) - بروتوكول آخر لاستعادة البريد الإلكتروني

بروتوكول نقل النص التشعبي (HTTP):

HTTP (بروتوكول نقل النص التشعبي) و HTTPS (بروتوكول نقل النص التشعبي الآمن) هما بروتوكولات تستخدم للتواصل بين العميل (مثل مستعرض الويب) والخادم (مثل موقع الويب).

HTTP هو أساس اتصال البيانات على شبكة الانترنت بحيث يتم استخدامه لنقل البيانات. يعمل HTTP وفق نموذج TCP/IP.

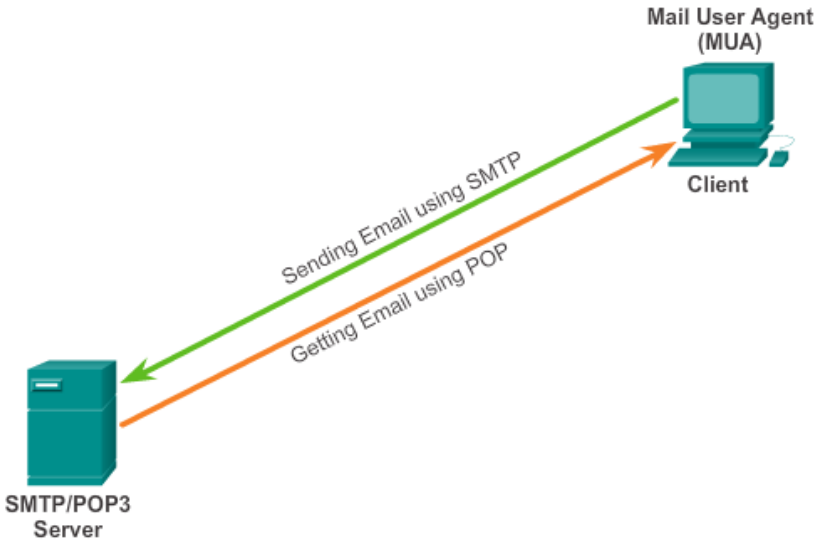
HTTPS هو امتداد لـ HTTP يستخدم التشفير لتأمين الاتصال بين العميل والخادم. يتم تحقيق التشفير باستخدام بروتوكولات SSL/TLS والتي تضمن عدم اعتراض البيانات التي يتم إرسالها أو العبث بها من قبل طرف ثالث. فعند زيارة موقع ويب يستخدم HTTPS سيقوم المتصفح أولاً بإنشاء اتصال آمن بالخادم باستخدام بروتوكولات SSL/TLS. يتم إنشاء هذا الاتصال الآمن من خلال تبادل الشهادات الرقمية والتي تتحقق من هوية الخادم وتشفير البيانات التي يتم إرسالها. وعليه فإن HTTPS يوفر تجربة تصفح أكثر أمانًا وخصوصية من HTTP خاصة عند التعامل مع المعلومات الحساسة مثل كلمات المرور وأرقام بطاقات الائتمان والمعلومات الشخصية.

بروتوكولات البريد الالكتروني (SMTP,POP,IMAP):

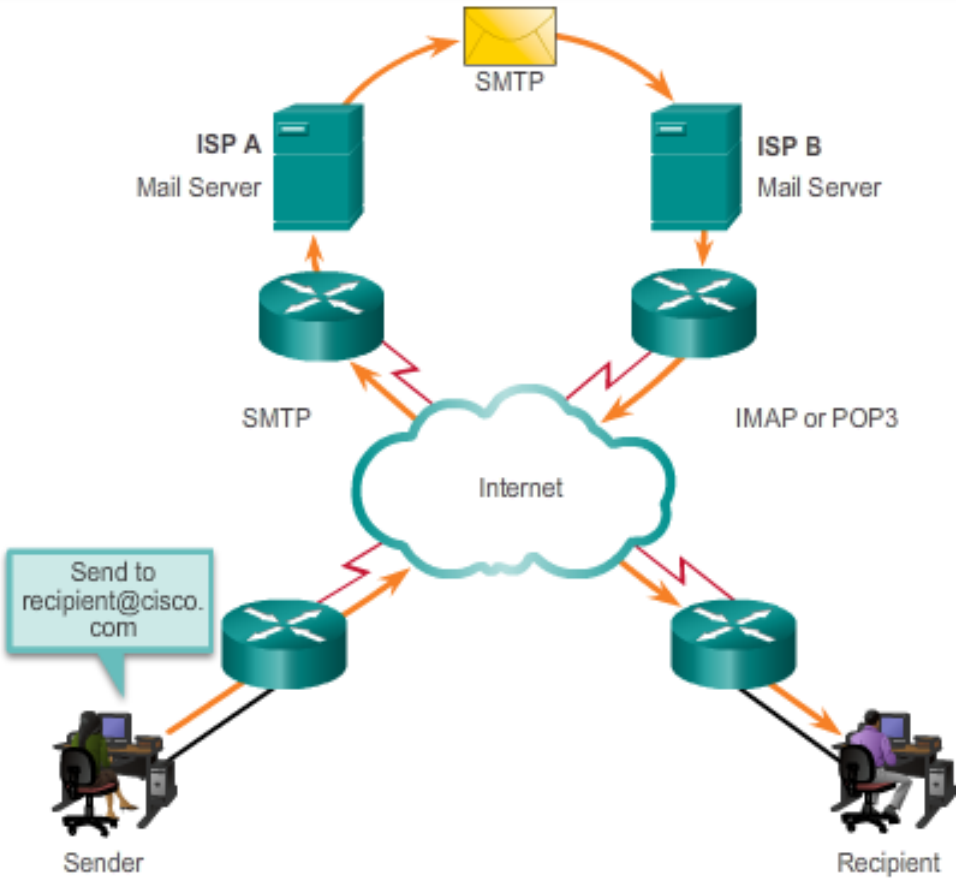
SMTP (بروتوكول نقل البريد البسـيط) و POP (بروتوكول مكتب البريد) و IMAP (بروتوكول الوصـول إلى الرسائل عبر الإنترنت) هي ثلاثة بروتوكولات مستخدمة للاتصال عبر البريد الإلكتروني.

يتم استخدام SMTP لإرسال رسائل البريد الإلكتروني من العميل (مثل تطبيق البريد الإلكتروني) إلى خادم (مثل خادم البريد). فهو بروتوكول يعمل على المنفذ 25 أو 587 وهو مسـؤول عن تسـليم رسـائل البريد الإلكتروني إلى خادم بريد المستلم المناسب. (بروتوكول دفع)

يسـتخدم بروتوكول POP لاسـترداد رسـائل البريد الإلكتروني من الخادم إلى العميل. إنه بروتوكول يقوم بتنزيل رسـائل البريد الإلكتروني من خادم إلى جهاز محلي مثل الكمبيوتر أو الهاتف المحمول. يعمل على المنفذ 110 ويسـتخدم آلية مصـادقة بسـيطة تعتمد على اسـم المسـتخدم وكلمة المرور. (بروتوكول سحب)

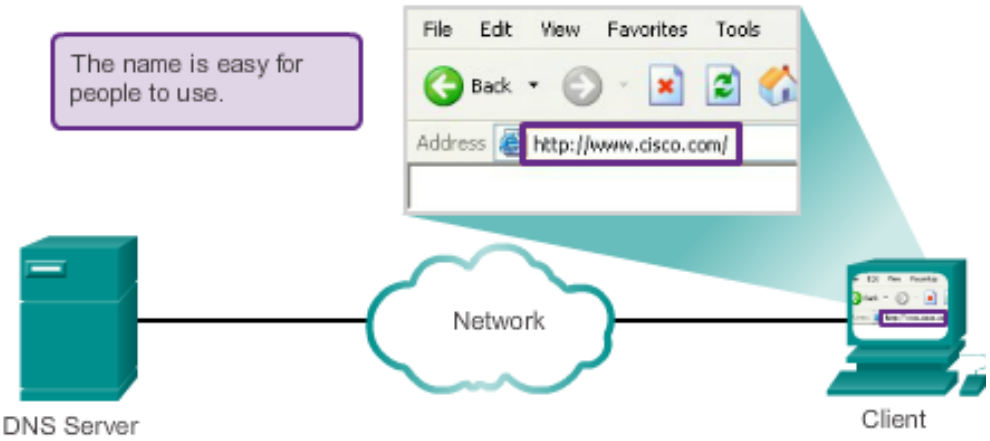


IMAP هو بروتوكول آخر يسـتخدم لاسـترداد رسـائل البريد الإلكتروني من خادم إلى عميل. ويختلف عن سـابقه بأنه يسـمح للمسـتخدم بالوصـول إلى رسـائل البريد الإلكتروني على الخادم دون تنزيلها على جهاز محلي. هذا يعني أنه يمكن للمسـتخدم الوصـول إلى بريده الإلكتروني من أجهزة متعددة وأي إجراءات يتم اتخاذها (مثل وضـع علامة على رسـالة بريد إلكتروني كمقروءة) سـتنعكس على جميع الأجهزة. يعمل IMAP على المنفذ 143 أو 993 (لاتصـالات SSL/TLS الآمنة) ويوفر ميزات أكثر تقدمًا من POP ، مثل إدارة المجلدات وعلامات الرسائل. (بروتوكول سحب)

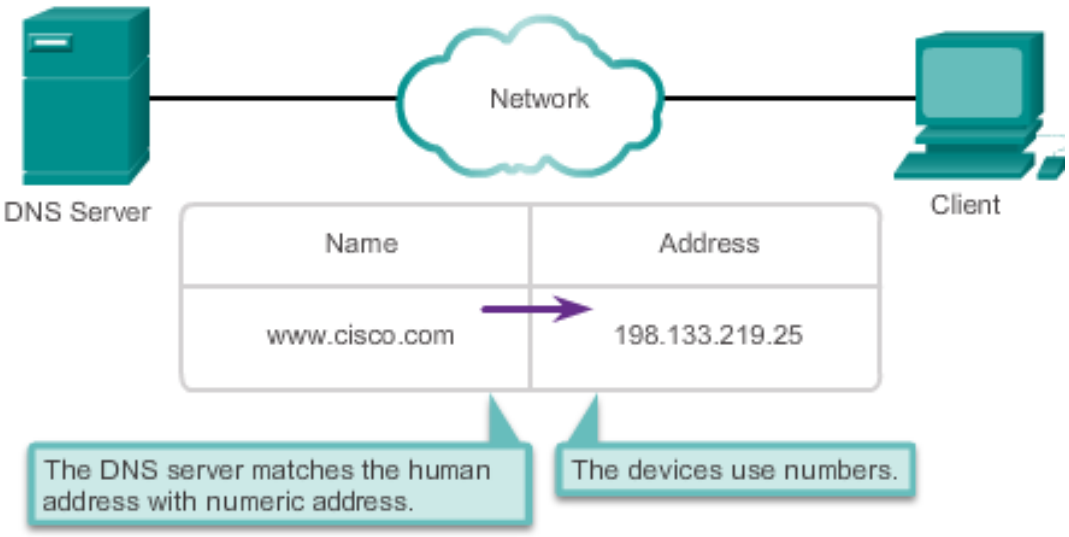


بروتوكول خدمة اسم المجال (DNS)

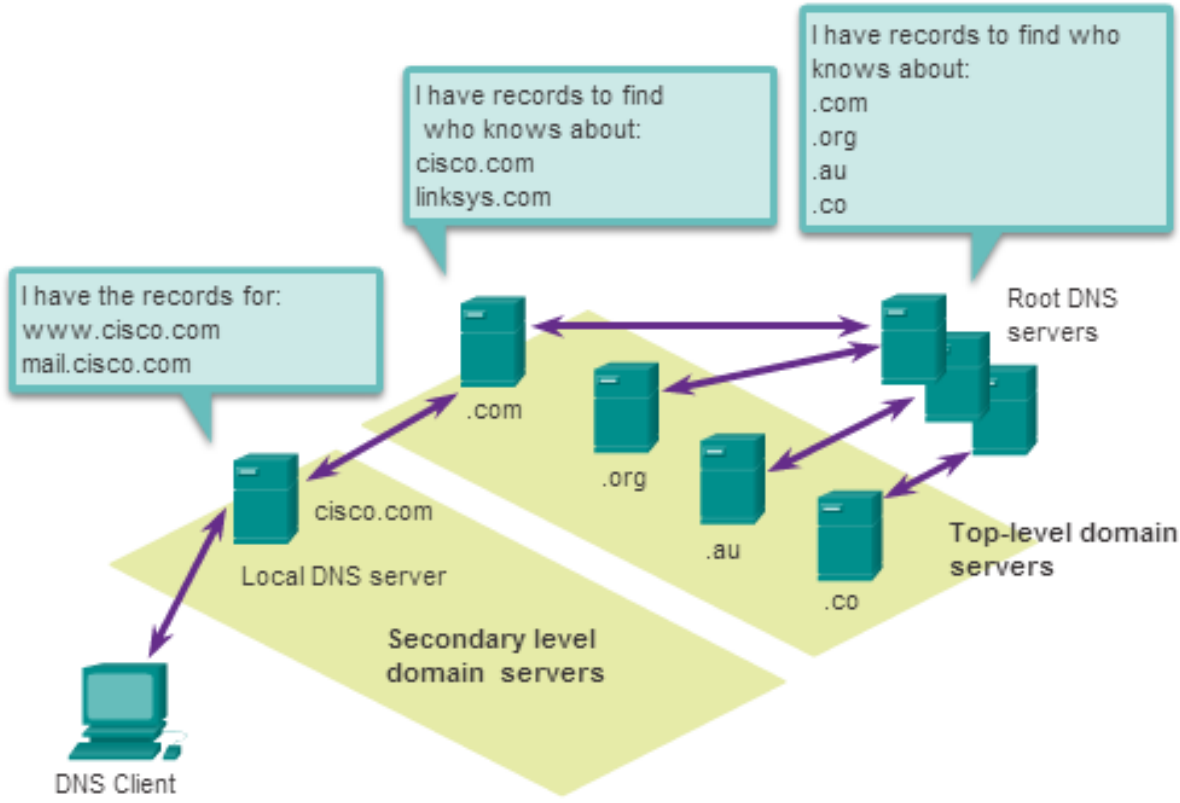
DNS (نظام اسم المجال) هو نظام تسمية موزع يستخدم لترجمة أسماء المجالات (مثل www.example.com) إلى عناوين IP (مثل 192.168.1.1).



عندما نكتب اسم الموقع الذي نريد الوصول اليه في متصفح الانترنت يحتاج الجهاز إلى إيجاد عنوان الـ IP الخاص باسم الموقع هذا وذلك حتى يتم التواصل مع خادم الويب الذي يستضيف هذا الموقع. وهذا هو الدور الذي يقوم به DNS. فهو من يزود الجهاز بعنوان الـ IP المقابل للموقع الذي كُتب في المتصفح.



يعمل DNS وفق نظام هرمي للخوادم حيث يكون كل خادم مسـؤولاً عن جزء معين من نظام اسـم المجال. عندما يحتاج الجهاز إلى حل اسم المجال فسيقوم أولاً بالاستعلام من DNS محلي (عادةً ما يتم توفيره بواسطة مزود خدمة الإنترنت أو مسؤول الشبكة). فإذا لم يكن هناك إجابة فسيقوم بالاستعلام عن خادم DNS ذي مستوى أعلى حتى يصل في النهاية إلى خادم DNS الموثوق للمجال.



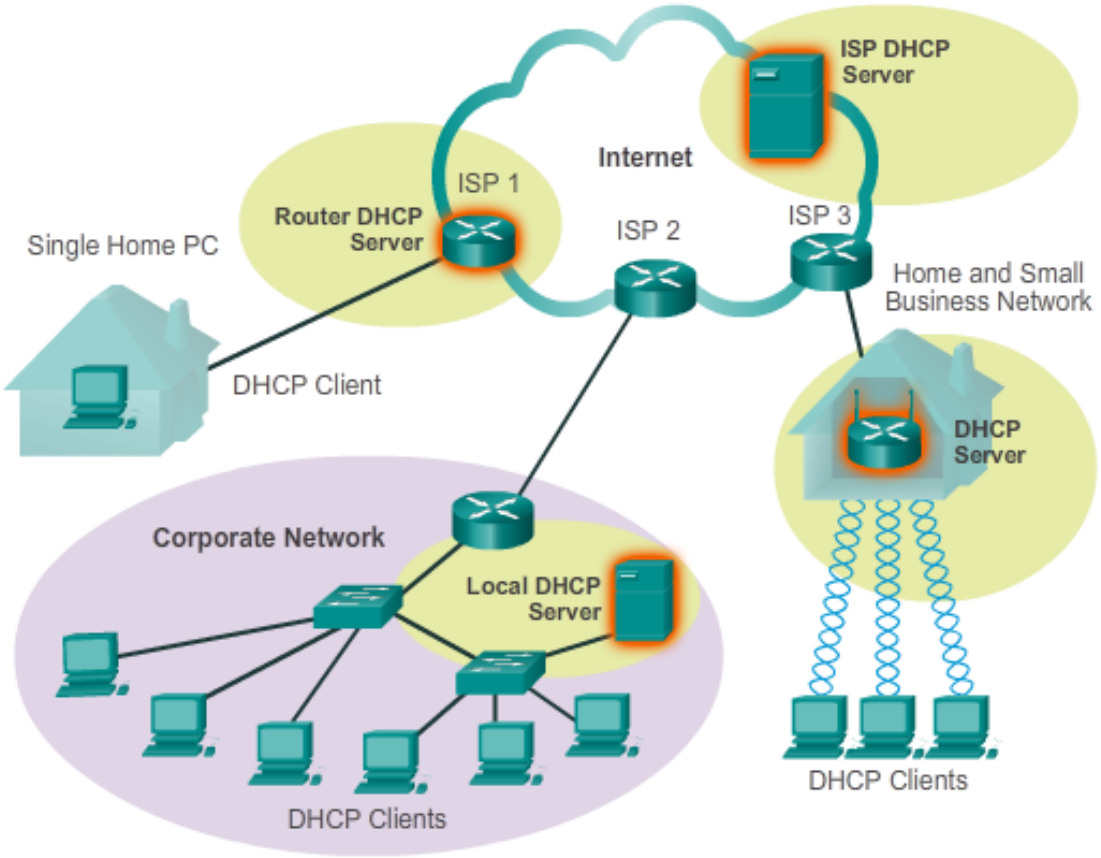
خادم DNS الموثوق هو المسـؤول عن توفير عنوان IP المرتبط باسـم المجال. بمجرد أن يتلقى الجهاز عنوان IP من خادم DNS الموثوق يمكنه اسـتخدام هذه المعلومات للتواصـل مع خادم الويب الذي يستضيف موقع الانترنت المراد.

يعد DNS مكونًا مهمًا للبنية التحتية للإنترنت ويسـتخدم لمجموعة واسـعة من التطبيقات مثل البريد الإلكتروني ونقل الملفات والألعاب عبر الإنترنت.

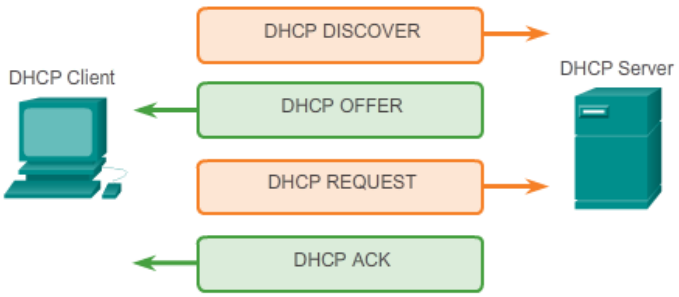
وبدون DNS سيحتاج المستخدمون إلى تذكر عناوين IP واستخدامها للوصول إلى مواقع الويب وخدمات الإنترنت الأخرى الأمر الذي سيكون صعبًا وغير عملي.

بروتوكول التحكم في المضيف الديناميكي (DHCP)

DHCP (بروتوكول الاعداد الديناميكي للمضيف) هو بروتوكول شبكة يُستخدم لتعيين عناوين IP ومعلمات تكوين الشبكة الأخرى تلقائياً للأجهزة الموجودة على الشبكة.



يُستخدم بروتوكول DHCP عادةً في شبكات الحاسب المحلية (LAN) لأتمتة عملية تخصيص عنوان IP. عندما تتصل أحد الأجهزة بشبكة فإنها ترسل رسالة بث (Broadcast) تطلب عنوان IP. يستجيب خادم DHCP على الشبكة بعد ذلك بعرض عنوان IP إلى جانب معلومات التكوين الأخرى مثل قناع الشبكة الفرعية والعبّارة الافتراضية وخوادم DNS.



بمجرد قبول الجهاز للعرض يتم تعيين عنوان IP له ويمكنه التواصـل مع الأجهزة الأخرى على الشـبكة. يعد بروتوكول DHCP مفيدًا لإدارة تخصيص عنوان IP في شبكات الحاسب الكبيرة لأنه يلغي الحاجة إلى قيام مسؤولي الشبكة بتعيين عناوين IP يدوياً لكل جهاز.

يدعم DHCP أيضًـا مفهوم وقت التأجير والذي يسـمح لخادم DHCP بتخصـيص عناوين IP لفترة زمنية محددة وعند انتهاء مدة التأجير يجب أن يطلب الجهاز عنوان IP جديد. يسـمح هذا لخادم DHCP باستعادة عناوين IP غير المستخدمة وإعادة استخدامها للأجهزة الأخرى على الشبكة.

جدول المحتويات