



جامعة طنطا  
كلية التربية النوعية  
قسم تكنولوجيا التعليم  
المستوى الثالث (ساعات معتمدة)  
برنامج إعداد معلم حاسب آلي

# صيانة الشبكات

إعداد  
د / أميرة إبراهيم عبد الغني



رَفَعَ اللَّهُ دِينَكُمْ  
وَلَذِكْرُ الْوَالِدِ الْعَظِيمِ

### رسالة برنامج تكنولوجيا التعليم

تتص رسالة برنامج تكنولوجيا التعليم بتوفير بيئة تربوية تراعي الفروق الفردية لإعداد أخصائي تكنولوجيا التعليم متميز علمياً ومهنياً وفنياً مواكب متطلبات سوق العمل التكنولوجي وقادر على الإسهام في ر مجال تكنولوجيا ا والمنافسة البحثية وخدمة المجتمع لتحقيق أهداف التنمية المستدامة.

## وتتص أهداف برنامج تكنولوجيا التعليم على :

- ١- الإرتقاء بجودة أداء الكوادر البشرية من أخصائى تكنولوجيا التعليم للعمل فى المؤسسات التعليمية ومراكز التعليم الإلكتروني فى مجال تكنولوجيا التعليم.
- ٢- رفع كفاءة المنظومة التعليمية لزيادة القدرة التنافسية ومواكبة المستجدات ذات العلاقة بالتخصص، من خلال تحديث وتطوير البرامج التعليمية وأساليب وأدوات التعليم فى مؤسسات التعليم الجامعى وما قبل الجامعى.
- ٣- الريادة فى البحث العلمى والتميز والإبتكار فى مجالات تكنولوجيا التعليم.
- ٤- تفعيل الشراكات المجتمعية فى ضوء أهداف التنمية المستدامة من خلال رفع وعى الطلاب فى المشاركة فى أنشطة خدمة المجتمع، والتطوير التكنولوجى.
- ٥- وضع آلية للتحسين المستمر فى جميع عناصر العملية التعليمية والبحثية لتدويل برنامج تكنولوجيا التعليم.

# الباب الأول

## مقدمة في شبكات الحاسب



## أهداف الباب الأول

بعد الانتهاء من دراسة هذا الباب ينبغي أن يكون الطالب قادراً على أن:

- ١- يُعرف الشبكات.
- ٢- يعدد أهداف الشبكات.
- ٣- يقوم باستعراض خدمات العمل الشبكي التي يتيحها نظام التشغيل.
- ٤- يسترجع فائدة الشبكات في التعليم الالكتروني.
- ٥- يعدد أنواع الشبكات على حسب المساحة الجغرافية التي تغطيها.
- ٦- يعدد أنواع الشبكات المحلية ويعطي مثال على شبكات الحاسب المتوسطة.
- ٧- يميز من حيث الشكل بين البنى الطبوغرافية الأساسية للشبكات المحلية.
- ٨- يبرر السبب في أن شبكة الإنترنت هي الأكثر شيوعاً واستخداماً.
- ٩- يحدد أي نوع من الشبكات يمكن استخدامه على حسب طبيعة المكان والأجهزة المستخدمة في الشبكات.
- ١٠- يعدد أنواع الشبكات على حسب علاقة الأجهزة مع بعضها البعض.
- ١١- يعدد أنواع الشبكات على حسب التقنية المستخدمة في وسائط بين الأجهزة.
- ١٢- يُعرف الشبكات اللاسلكية.
- ١٣- يذكر آلية عمل الشبكات اللاسلكية.
- ١٤- يميز بين الشبكات السلكية واللاسلكية.
- ١٥- يفرق بين الأنماط المختلفة للشبكات اللاسلكية.
- ١٦- يعدد مزايا الشبكات اللاسلكية.
- ١٧- يُعرف مزود الخدمة ISP.
- ١٨- يُعرف الانترنت الفضائي ويعدد سلبياته وإيجابياته.
- ١٩- يحدد كيف يعمل الانترنت الفضائي.
- ٢٠- يعدد العوامل التي تؤثر على أداء الانترنت باستخدام الأقمار الصناعية.
- ٢١- يُعرف النطاق العريض Broadband.
- ٢٢- يفرق بين المصطلحات Bandwidth، Broadband.
- ٢٣- يُعرف معدل نقل البيانات Bandwidth.
- ٢٤- يميز الوحدة المستخدمة لقياس عرض النطاق.
- ٢٥- يحسب الزمن المستغرق لنقل ملف حجمه بالبايت عبر خط معين.
- ٢٦- يستنتج العوامل التي تؤثر على زمن نقل البيانات.

## مفهوم الشبكات

في سياق التغير التكنولوجي والانتقال إلى التعامل مع آليات العمل المفتوحة والمنافسة الشديدة ، توجد عدة تحديات تواجه العملية التعليمية في كل أنحاء العالم تتمثل في تقديم فرص تعليمية متزايدة تكون في مقدرة كل المتعلمين. وقد بدأ كثير من المنظمات والمؤسسات التعليمية مواجهة هذا التحدي بتطوير برامج المقررات التعليمية Courseware، لكي تتاح وتمد عن بعد من خلال شبكات المعلومات وخاصة عبر شبكة الانترنت.

والشبكة الكمبيوترية هي عبارة عن منظومة من الحواسيب والأجهزة الخارجية متصلة معاً. والهدف من الشبكة أن يتمكن كل مستخدم من المشاركة في الملفات على الحواسيب الأخرى أو على حاسوب مركزي يسمى الحاسوب الخا Ser، أما الحواسيب ا Clients أو محطات العمل Workstations. كما يمكن إشراك مستخدمي الشبكة أيضاً في الأجهزة الخارجية مثل أجهزة الطابعات وأجهزة التوقيع وأجهزة المسح المتصلة بالحاسوب الخادم.

وتتكون الشبكة من حاسوبين أو أكثر متصلين معاً من أجل مشاركة الموارد وتبادل ملفات البيانات وتوفير الاتصالات الالكترونية. ويمكن ربط الحاسبات داخل الشبكة من خلال كوابل أو خطوط الهاتف أو موجات الراديو أو الأقمار الصناعية. أي أن الشبكات هي عبارة عن ربط بين الحواسيب مع أدوات وبرامج مخصصة للعمل الشبكي وذلك لإتاحة التشارك فيما بينها وتتدفق



المعلومات عبر الشبكة على شكل إشارات كهربائية ويتم نقلها في صورة حزم من المعلومات .

وتعتبر شبكة الانترنت شبكة الحاسبات الأكبر والأعظم قوة في الوقت الحالي. وتشتمل هذه الشبكة على أكثر من خمسة عشر مليون حاسب مضيف Host Computers لها عناوين انترنت ويستخدمها أكثر من مائة مليون شخص في معظم دول العالم. وحالياً يرتبط الأفراد والمدارس والجامعات وغير ذلك من منظمات بشبكة الانترنت. وتفتح شبكة الانترنت مجالاً واسعاً للخدمات والتطبيقات التعليمية على الخط، حيث يوجهها خبراء التربية والتعليم فيما يتصل بتوظيف التعليم الالكتروني، بهدف التغلب على قيود ومحددات المسافة والوقت حتى يستطيع الطلاب والباحثين الوصول إلى مصادر التعلم، بالإضافة إلى تعزيز وتحسين التعليم المستمر والتعلم مدى الحياة أما بالنسبة للمعلم الاتصال بالشبكة العنكبوتية كن المعلم من الوصول إلى خب وتجارب تعليمية يصعب الوصول إليها بطرق أخرى.

ولم تظهر الانترنت على الصعيد العام إلا في مطلع العقد الأخير من القرن العشرين، وفي عام ١٩٩٣ على وجه التحديد. ويشكل ظهورها علامة بارزة في مسيرة تطوير تقنيات المعلومات. وبصفة عامة فإن الانترنت تشكل نظاماً عالمياً لتدفق المعلومات في مختلف المجالات وعلى اختلاف المستويات. ويمكن من خلالها أداء ما يلي:

١- النشر الالكتروني.

- ٢- استرجاع البيانات الورقية.
- ٣- استرجاع الحقائق والنصوص.
- ٤- البريد الالكتروني.
- ٥- المؤتمرات عن بعد. ٦- تبادل الملفات والبرامج.
- ٧- استخدام الحاسبات عن بعد.

ويمكن تعريف شبكة الانترنت على أنها شبكة ضخمة تضم ملايين من أجهزة الحاسوب من مختلف أنحاء العالم تتفاهم هذه الأجهزة مع بعضها البعض من خلال بروتوكولات للتفاهم والاتصال، وتعمل الأجهزة بواسطتها على تبادل الخبرات في جميع المجالات (الثقافية - الاقتصادية - الاجتماعية - الدينية - التجارية - السياسية - العسكرية - التعليمية)، كما تساعد الملايين من الأشد لى تحقيق أهداف متد

### دور الشبكات في التعليم الالكتروني

مع انتشار الشبكات وارتباطها بشبكة الانترنت، وبصفة خاصة الشبكة العنكبوتية- توسع استخدام التعليم للشبكات في مستويات متعددة أدناها الإفادة من المعلومات المتاحة على ملايين المواقع المنتشرة على شبكة الانترنت في إثراء عملية التعليم والتعلم، والإفادة من مصادر التعليم والتعلم الالكترونية المتاحة على هذه المواقع. وصولاً إلى أقصى مستويات الإفادة بالاعتماد كاملاً على الشبكات في تقديم الخدمة التعليمية، وتعلم المستفيدين منها .

ويعد البريد الإلكتروني E-Mail أكثر تطبيقات الانترنت شيوعاً، حيث يمكن من خلاله إرسال أي رسالة لأشخاص في أي مكان من العالم في عدة ثوان وبتكلفة زهيدة لا تتعدى تكلفة الربط بالشبكة. أما الشبكة الدولية للمعلومات World Wide Web فهي أكثر تطبيقات الانترنت جاذبية ومتعة، لأسباب كثيرة أهمها سهولة استخدامه، كما تقوم بربط الوثائق ذات العلاقة ، مما يتيح عملية التجول بين الموضوعات المختلفة بسهولة، كما تدعم عرض الوثائق والصور إضافة إلى الأصوات ولقطات الفيديو.

وتعد الشبكة الدولية للمعلومات من أدوات التعليم الإلكتروني المعتمدة على الانترنت ويطلق عليها مسميات عديدة منها الشبكة العنكبوتية، الشبكة النسيجية، والويب.

### ومن استخدامات التربية لشـ خدمات الدولية ما يلي:

١- نشر المقررات الإلكترونية E-Courses وجعلها متاحة للفئات المستفيدة منها.

٢- مساعدة المعلم والطلاب في الحصول على خطط لدروس الكترونية E-lessons في كافة التخصصات العلمية.

٣- الحصول على المعلومات من خلال خدمة الاشتراك في المكتبات الإلكترونية Digital Libraries.

٤- التنقل والإبحار الافتراضي بين المواقع التاريخية والأماكن الجغرافية ذات الأهمية الدولية مثل المتاحف والمعارض.

٥- مساعدة كل من المعلم والمتعلم في الحصول على بنوك أسئلة في تخصصات علمية مختلفة.

ويمكن توظيف الانترنت في التدريس وتقديم المناهج ويقصد بعملية التوظيف هو تقديم المنهج والتدريس للتلاميذ في صورة برنامج تعليمي منشور على الانترنت أو صفحة تعليمية على الشبكة تستخدم كمصدر أساسي في التعليم والتعلم، أو كمصدر تعزيزي للتعلم الصفي، ويمكن الدخول على هذه الصفحة من قبل الطلاب.

ويمكن أن يحتوي البرنامج على خصائص الوسائط المتعددة التي تسمح بالتفاعل والمشاركة والاستماع والقراءة والإجابة على أسئلة وتدريب حول الدروس. ومع تطور أدوات إنشاء الصفحات على الشبكة أصبح بإمكان المعلم بناء مواقع وصفحات لتوجيه الطلاب من خلالها، وهذا بدوره جعل من السهل تحديث المعلومات المتضمنة بها، وبهذا يكون التدريس بواسطة الانترنت قابل للتعديل والتطوير لمواكبة التغيير السريع في المعلومات الدراسية .

ويتنوع استخدام الانترنت في التعليم في المراحل التعليمية المختلفة حسب طبيعة الاستخدامات والتسميات، حيث تسمى في المراحل المدرسية الثلاث (الابتدائية والمتوسطة والثانوية) بـ (تعليم الدفاتر الالكترونية) وفي المرحلة الجامعية (التعليم عن بعد) وفي التعليم بشكل عام (التعليم الالكتروني)، وهذا كله أعطى دفعة قوية للنهوض بالتعليم للأمام وتحديثه ونقله نقلات نوعية من النظريات والتطبيقات التقليدية إلى آفاق التطبيقات التكنولوجية الحديثة التي تأخذ في الاعتبار تحقيق أهداف التربية بمفهومها الشامل، وليس مجرد تقليد أعمى تصاحبه نتائج عكسية وسلبية.

ومن فوائد شبكة الانترنت في العملية التعليمية التعلمية الالكترونية ما يلي:-

١- استخدام شبكة الانترنت في التعليم الالكتروني من خلال إنشاء مواقع لمقررات دراسية ومواقع لدورات تعليمية على الشبكة تكون متاحة في كل وقت وفي أي مكان.

٢- مصدر ثري للمعلومات ، حيث توفر شبكة الانترنت كمية كبيرة جداً من المعلومات العلمية والبحوث والدراسات المتخصصة في جميع مجالات المعرفة.

صل بين المعلمين في عينة أو في دول عدة لتبادل الأفكار والخطط التدريسية، والمشاركة في المناقشات التربوية.

٤- تسهيل اتصال الطلاب فيما بينهم ، وتبادل المعلومات والأفكار التربوية، وإتاحة تواصلهم مع طلاب دول أخرى.

٥- الاستفادة من البرمجيات التعليمية المجانية أو التجريبية المتاحة على شبكة الانترنت وتوظيفها في المجال التعليمي.

٦- تسهل للطلاب والمعلمين نشر إبداعاتهم وأعمالهم من خلال إنشاء المواقع الشخصية على الشبكة .

## أنواع الشبكات

أولاً: من حيث النطاق الجغرافي:

أي حسب المساحة الجغرافية التي تغطيها ، وتنقسم إلى :

- الشبكات المحلية (LAN) .
- شبكة الحاسب المتوسطة (MAN).
- شبكة الحاسب الموسعة (WAN)

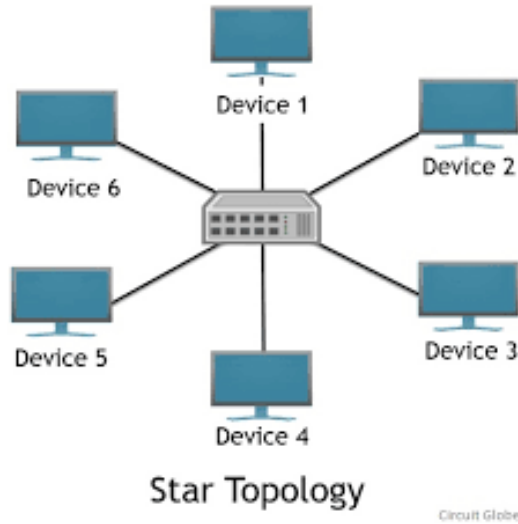
### (أ) شبكة الحاسب المحلية (LAN) Local Area Networks:

مخصصة لمساحة مكانية محدودة ، مثل شبكة المعمل المدرسي للحاسب ، أو قاعة ، أو مبنى شركة ، عدد الأجهزة فيها محدوداً ، وسهولة الاتصال بين الأجهزة عالية ؛ نظراً لقصر المسافات بين الأجهزة .

### أنواع الشبكات المحلية :-

#### ١ - شبكة النجمة (Star)

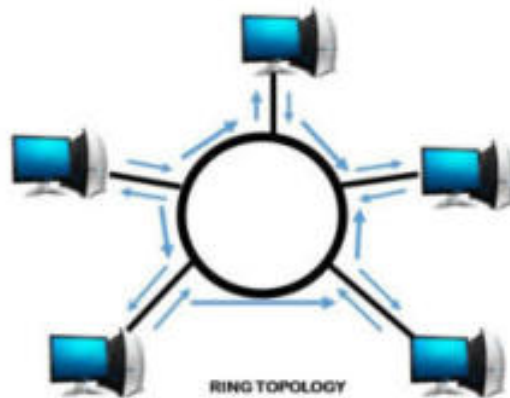
وتكون أجهزة الحاسب فيها مرتبطة مع بعضها عن طريق جهاز يسمى (Hub) حيث يتم وصله مع الجهاز الرئيسي والذي يقوم بتنظيم عملية تمرير الإشارات من الأجهزة المختلفة واليها وبهذه الطريقة فان تعطل أي جهاز لا يعني تعطل الأجهزة الأخرى. ويمكن استخدام هذا الشكل لربط أجهزة تكون موزعة بشكل غير منتظم و بعيدة نسبياً عن بعضها البعض.



شكل (١-١) يوضح الشبكة النجمية.

## ٢- شبكة الحلقة (Ring)

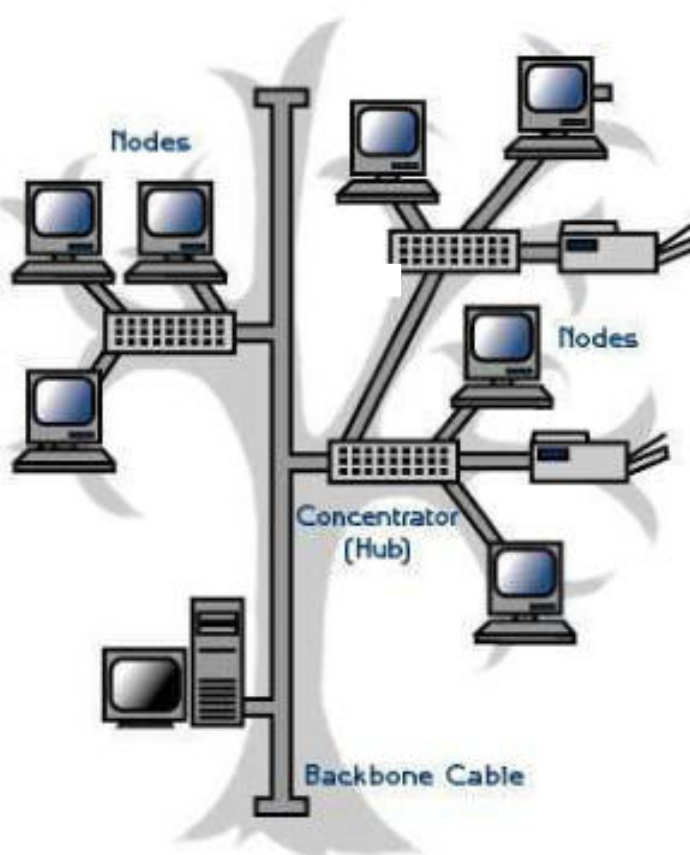
وفي هذا الشكل ترتبط الأجهزة مع بعضها البعض عن طريق كوابل لها مواصفات خاصة وبالنهاية ترتبط مع الجهاز الرئيسي على التوالي. وفي حالة تعطل من الأجهزة تتعطل الشبكة كما أن تمرير إشارة يكون طريق تمريرها إلى الجهاز الذي قبله مما يقلل من السرعة بعكس شبكة النجمة.



شكل (١-٢) يوضح ارتباط الأجهزة على شكل حلقة.

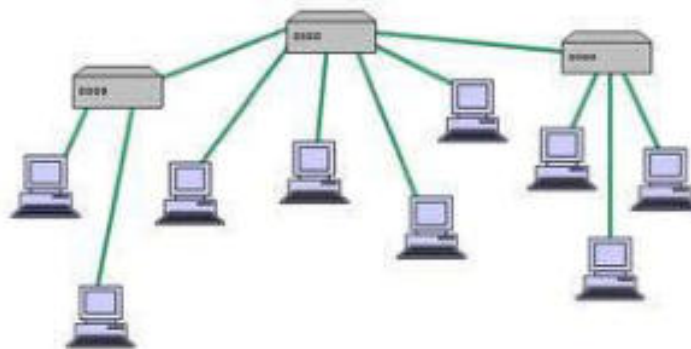
## ٣- شبكة الشجرة (Tree)

وفيها ترتبط الأجهزة على شكل الجذر الذي يمثل الجهاز الرئيسي والأفرع والتي تمثل الأجهزة المستفيدة. وفي هذه الحالة يكون كل جهاز مرتبطاً بعدد من الأجهزة الأخرى والتي بدورها ترتبط بعدد آخر من الأجهزة وهكذا وفي حالة تعطل جهاز تتعطل الأجهزة المرتبطة به مباشرة فقط دون التأثير على الأجهزة الأخرى وتميرير إشارة إلى الأفرع الأخرى يتم عبر الجهاز الرئيسي.



شكل (٣-١) يوضح البنية النجمية الشجرية



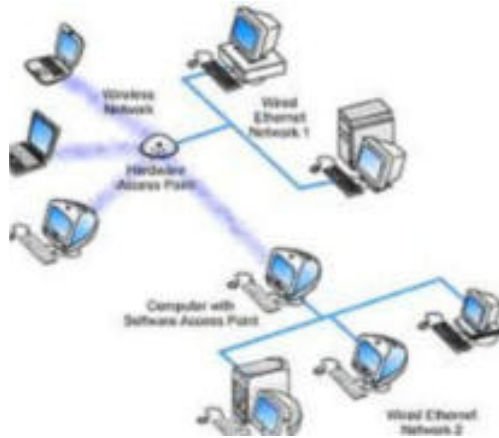


شكل (١-٤) يوضح شبكة الشجرة (Tree Topology)

#### ٤ - شبكة البث (Broadcast Network- Ethernet)

وهو من أكثر أنواع الشبكات المحلية شيوعاً وذلك بسبب فاعليته القصوى في إرسا قبال وتوريد الإشارات القليلة نسبياً، كما أن إمكانية عد الأجهزة وبمسافات أطـ عله مقبولاً لدى أكثر الشركا المؤسسات.

ويقوم مبدأ هذا النوع على توصيل كوابل خاصة تسمى (Coaxial Cable) يبلغ طول كل واحد منها ٢.٥ متراً- ببعضها البعض بواسطة وصلات خاصة يتم ربطها مع الأجهزة المختلفة والتي تسمى (Node) - بشرط عدم زيادة المسافة عن ٥٠٠ متر - و في حالة الزيادة يستخدم جهاز خاص يسمى (Repeater) والذي يربط مع الكوابل و يقوم باستقبال الإشارة الصادرة وإعادة بثها مرة أخرى وبهذه الحالة يتم توصيل الأجهزة لمسافة تصل إلى ١٥٠٠ متر بفاعلية جيدة.



شكل (٥-١) يوضح شبكة البث Ethernet.

ب) شبكة الحاسب المتوسطة (Metropolitan area network) (MAN)  
تمتد متوسطة كالمدن المذ غالبا ما تغطي مسافة قدرها من  
الى ١٠٠ كيلو متر، سرعتها محدودة ، و تدار من قبل هيئة عامة أو جهة  
حكومية ، مثل: شبكة الصراف الآلي وتدار من قبل مؤسسة النقد العربي  
السعودي .

Metropolitan area network (MAN)

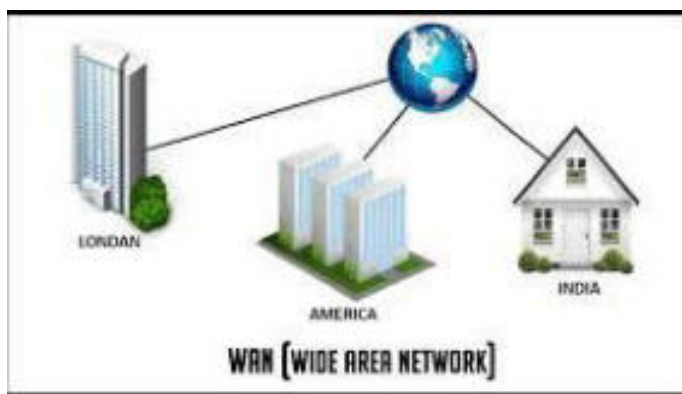


شكل (٦-١) يوضح شبكات الحاسب المتوسطة.

### ج) شبكة الحاسب الموسعة (WAN) Wide area network:

وهي تمتد لمنطقة كبيرة بين مجموعة الدول ، مثال: الشبكة العنكبوتية العالمية (World Wide web) ، وتدار في الغالب من قبل شركة الاتصالات الحكومية في البلاد المختلفة .

وتستخدم الشبكات واسعة المدى (Wide Area network) WAN لتغطية مناطق جغرافية واسعة قد تكون بين مدينتين أو حتى قارتين ، وليس هناك مسافات تمنع من ربط الأجهزة مع بعضها مهما كان عددها، فإذا توفرت خطوط الاتصال عبر الهاتف أو الأقمار الصناعية تصبح عملية ربط الأجهزة وإنشاء شبكة عملية ممكنة. وأكثر الأمثلة شيوعاً على هذه الشبكة هي الانترنت . تغطي معظم المنا على الكرة الأرضية وتسمح لأكثر ٢٠ جهاز من الاتصال ببعض وتبادل البيانات والمعلومات والملفات المختلفة بكافة أشكالها المرئية والمسموعة والمكتوبة.



شكل (٧-١) يوضح الشبكات واسعة المدى.

ومع تقدم العلم أصبح بالإمكان الربط بين شبكات الحاسب المحلية وشبكات النطاق الواسع لتشكل شبكة واحدة يمكن الاستفادة منها وكمثال على ذلك يمكن إنشاء شبكة في مختبر يحتوي على ٢٠ جهاز حاسب مرتبطة مع بعضها بشبكة محلية وربط الجهاز الرئيسي بشبكة نطاق واسع عن طريق المودم ثم السماح للأجهزة الأخرى بالاستفادة من خدمة الانترنت عن طريق الجهاز الرئيسي.

ثانيا : حسب علاقة الأجهزة مع بعضها داخل الشبكة : وتنقسم إلى :

#### أ) الخادم والعميل Client Server :

من أشهر الشبكات ، وأكثرها شيوعاً حول العالم ؛ نظراً لما تتميز به من مزايا عدة ومنها :

- ١- زية المعالجة للبيانات .
  - ٢- مركزية تخزينها للبيانات .
  - ٣- الاشتراك في مورد واحد مثل طابعة .
- وقد تكون شبكة الخادم والعميل شبكة محلية ، أو موسعة ، أو شبكة إنترنت .
- \* تحوي شبكة الخادم والعميل نوعين من الأجهزة ، هما :

#### \*النوع الأول : خادم (Server) :-

، وهو ( جهاز فائق القدرة على المعالجة والتخزين ، ويحتوي على نظام تشغيل خاص وبرمجيات خاصة ) ، ومن أمثلة نظم التشغيل التي تعمل على أجهزة الخادم : نظام Windows NT ، Windows Server ٢٠٠٣ .

## \*النوع الثاني : جهاز العميل (Client) :-

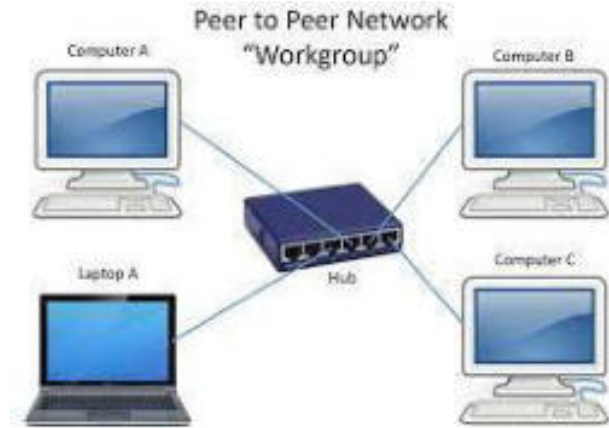
وهو عبارة عن ( حاسب شخصي وعليه نظام تشغيل شبكات)وهي الأنظمة التي تدعم خدمات العمل الشبكي ( ، مثل : Win XP ، Win me .



شكل (٨-١) يوضح شبكة من نوع الخادم-العميل

## ب- شبكات الند للند ( Peer To Peer ) :

ومن تسمية هذا النوع من الشبكات نجد أن علاقة الأجهزة بعضها ببعض متماثلة ، وقد يكون جهاز المستخدم خادم وعميل.



شكل (٩-١) يوضح شبكات الند للند.

ثالثا : حسب التقنية المستخدمة في وسائط النقل بين الأجهزة :

وتنقسم إلى قسمين :

أ- الشبكة السلكية :

تعتمد في الربط بين الأجهزة على أسلاك محسوسة ، وتنقسم الأسلاك إلى ثلاثة أنواع : ١- الكابلات الثنائية المجدولة Twisted Pair cables .

٢- الكابلات المحورية Coaxial cables .

٣- كابلات الليف البصري Fiber optic cables .

ب- الشبكة اللاسلكية :

تعتمد على الإرسال بالإشارات، وتنقسم الإشارات إلى :

١- إشارات الراديو ٢- الأشعة دون الحمراء

وتمثل الشبكات اللاسلكية المحلية تقنية واسعة الانتشار، نظراً لما تقدمه من دعم لجميع المميزات التي تقدمها الشبكات السلكية التقليدية، وخصوصاً مع سهولة استخدامها وأسعار نقاط الوصول (Access Point) المنخفضة، بالإضافة لدعم الشبكات اللاسلكية في معالجات الأجهزة المحمولة واتساع انتشار هذه التقنية، حيث لا يكاد يخلو منزل أو منشأة من نقاط الوصول للشبكات اللاسلكية.

### ماهية الشبكات اللاسلكية :-

لقد اكتسبت الشبكات اللاسلكية - التي تكتب بالإنجليزية اختصاراً (WLAN) - وأحياناً يطلق عليها اسم (Wi-Fi) انتشاراً لأسباب أهمها سهولة تركيبها و المرونة التي تمتاز بها، يضاف إلى ذلك رخص تكاليف إنشائها و صيانتها، و سهولة توسعتها عند الحاجة. تعود نقطة الانطلاق الحقيقة للشبكات المحلية اللا إلى العام ١٩٩٧م الذي ولادة مواصفات (IEEE ٨٠٢.١١) التي تعد أول مواصفات قياسية لهذا النوع من الشبكات، و كأى بداية كانت قدراتها محدودة من حيث قدرتها على تمرير المعلومات. كما أنها كانت تعمل في نطاق ترددي قدره ٤.٢ ميغاهرتز و هذا يجعلها عرضة للتداخل مع بعض الأجهزة التي تعمل في النطاق نفسه مثل بعض أجهزة المايكروويف و الهواتف المنزلية النقالة. و لتلافي هذه العيوب توالى صدور المواصفات القياسية .

### كيف تعمل الشبكة اللاسلكية؟

بعد إيصال الطاقة إلى نقطة الدخول إلى الشبكة والأجهزة المزودة ببطاقة الاتصال اللاسلكي ووضع الجميع في وضع التشغيل يحدث ما يلي:

١. ترسل نقطة الدخول إلى الشبكة نبضات إلكترونية على فترات منتظمة معلنة عن نفسها.

٢. تلتقط الأجهزة هذه النبضات التي تحوي في طياتها معلومات مهمة تساعد الأجهزة على الاستجابة وتهيئة نفسها للاتصال، ومن أهم هذه المعلومات ما يعرف باسم (Service Set Identifier) الذي يعرف اختصاراً باسم (SSID)، وهو ما يميز شبكة لاسلكية عن أخرى.

٣. كما تحوي النبضات المشار إليها القناة التي ستعمل عليها الشبكة اللاسلكية.

ولاحد سائل المتبادلة داخل اللاسلكية تشفر باستخدام نظام تشفير يعرف اختصاراً باسم (WEP)، ولكن نظام التشفير هذا يعاني من نقاط ضعف عدة يمكن للمهاجم النفاذ من خلالها و تهديد الشبكة اللاسلكية.

### أنماط الشبكات اللاسلكية

تعرف مجموعة معايير ٨٠٢.١١ نمطين أساسيين للشبكات اللاسلكية:

- الشبكات الخاصة
- شبكات البنية التحتية



لا بدّ من الإنتباه إلى أنّ بنية الشبكة قد لا تعكس هذه الأنماط مباشرةً وعلى الدوام. مثلاً، قد تعمل وصلةً لاسلكيةً بين نقطتين Point-to-Point ضمن النمط الخاص أو ضمن نمط البنية التحتية.

### ١. النمط الخاص (Ad hoc Mode (IBSS)

يعتبر النمط الخاص (والذي يعرف أيضاً بنمط الند للند (Peer-to-Peer) أحد أساليب الربط المباشر بين عملاء الشبكة اللاسلكية. إن السماح لعملاء الشبكة اللاسلكية بالعمل ضمن النمط الخاص يلغي الحاجة إلى استخدام أيّ نقاط ولوج مركزية. تستطيع جميع النقاط ضمن شبكة لاسلكية خاصة التواصل مباشرة مع النقاط الأخرى.

ينبغي إعداد بطاقات الشبكة اللاسلكية عند جميع عملاء الشبكة اللاسلكية الخا عمل ضمن النمط واستخدام نفس معرف مجم الخدمات SSID ورقم القناة "Channel Number".

تتألف الشبكة اللاسلكية الخاصة عادةً من مجموعة صغيرة من الأجهزة التي توضع على مسافة قريبة من بعضها البعض. ينخفض أداء الشبكة اللاسلكية كلما ازداد عدد النقاط الموجودة ضمنها. يتطلب ربط الشبكة اللاسلكية الخاصة بشبكة محلية سلكية أو بالإنترنت إعداد بوابة مخصصة لهذا الغرض.

كلمة "Ad hoc" لاتينية الأصل وتعني "لهذا الغرض" إلا أنّها غالباً ما تستخدم للتعبير عن الحلول أو الأحداث المرتجلة أو غير المعد لها.

تستخدم معايير ٨٠٢.١١ IEEE مصطلح (مجموعة الخدمات الأساسية المستقلة Independent Basic Service Set IBSS) للإشارة إلى النمط الخاص للشبكات اللاسلكية.

## ٢. نمط البنية التحتية (BSS) Infrastructure Mode

تحتوي الشبكات العاملة ضمن نمط البنية التحتية - خلافاً للشبكات الخاصة التي لا تتضمن عنصراً مركزياً - على عنصرٍ يقوم بمهمة التنسيق: نقطة وُلُجٍ أو محطة مركزية. يمكن لعملاء الشبكة اللاسلكية الوصول إلى الشبكة السلكية عبر نقطة الولوج فيما إذا كانت هذه النقطة موصولةً بالشبكة السلكية.

عند احتواء الشبكة على عدّة نقاط وُلُجٍ وعدّدٍ من العملاء ينبغي إعدادها جميعاً لاستخدام نفس المعرّف SSID. إذا ما رغبت في التأكد بأن شبكتك اللاسلكية تعمل باعتبارها القصوى عليك بإعداد جميع نقاط الولوج الموّضمن نفس الموقع الفيزيائي لاستخدام نفس القناة. يقوم العملاء باكتشاف (عبر مسح نطاق الترددات) القناة التي تستخدمها نقطة الولوج وبالتالي لا حاجة لهذه العملاء في معرفة رقم القناة مقدّماً.

تستخدم معايير ٨٠٢.١١ IEEE مصطلح (مجموعة الخدمات الأساسية Basic Service Set BSS) للإشارة إلى نمط البنية التحتية للشبكات اللاسلكية.

وتعتبر الشبكات اللاسلكية نظاماً مرناً لتبادل البيانات وتستخدم كامتداد أو كبديل للشبكة السلكية ، حيث تقوم هذه الشبكة ببث المعلومات عن طريق

تقنية ترددات أمواج الراديو (Frequency Radio) ، وهي بذلك تزيل الحاجة إلى الاتصالات السلكية وهكذا جمعت شبكة الاتصالات اللاسلكية بين توصيل البيانات وسهولة الوصول إلى المستخدم في أي مكان ؟

### مزايا الشبكات اللاسلكية

بطبيعة الحال توفر الشبكات اللاسلكية للمستخدم الكثير من الجهد والوقت بعكس الشبكات السلكية التي تسبب بعض العوائق في استعمالها، وتتمثل مميزات الشبكات اللاسلكية في مايلي:

-**المرونة:** للشبكات اللاسلكية فوائد أكثر من الشبكات السلكية و من بين هذه الفوائد المرونة، اذ تمر موجات الراديو عبر الجدران والحاسوب يمكن أن يكون مكان على نطاق الشد

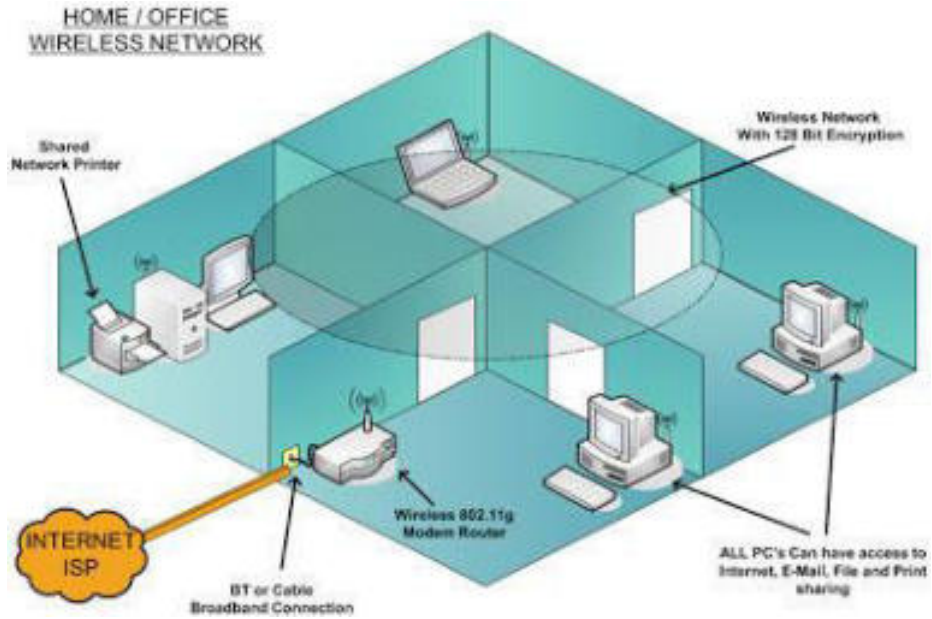
-**سهولة الاستخدام:** الشبكات اللاسلكية سهلة الاستخدام، اذ تحتاج فقط الى جهاز حاسوب نقال و حاسوب مكتبي مزود ببطاقة شبكة لاسلكية.



شكل (١٠-١) يوضح سهولة استخدام الشبكة اللاسلكية.

#### -التخطيط :

تحتا ات السلكية إلى تخط ق و كثرة الأجهزة يكلف في ع  
الصيانة، على عكس الشبكات اللاسلكية فهي أسهل من ذلك بكثير.



شكل (١١-١) يوضح أن الشبكات اللاسلكية لا تحتاج إلى تخطيط.

أ - لأجهزة :

في الشبكات اللاسلكية يمكن اخفاء الأجهزة بكل سهولة و هي مناسبة للأماكن التي من الصعب انشاء شبكات سلكية داخلها مثل المتاحف و البنايات القديمة.



شكل (١٢-١) يوضح الأجهزة المستخدمة في الشبكات اللاسلكية.

#### -الأسعار :

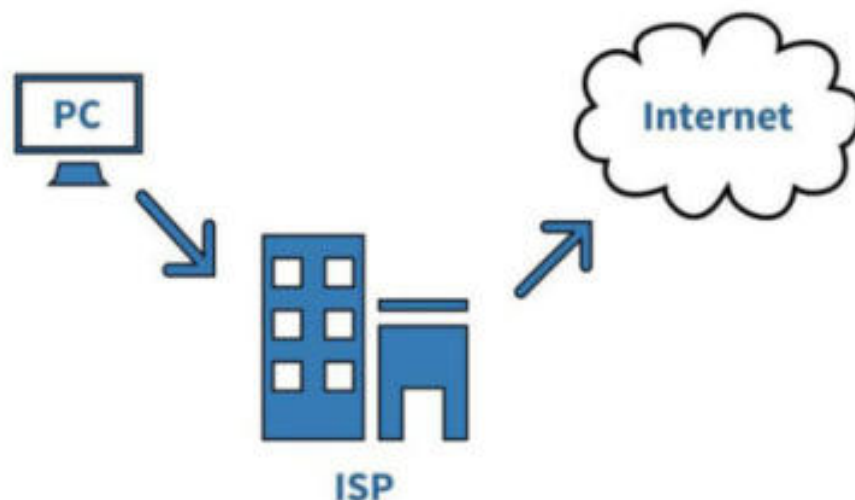
لقد عدات و أجهزة الشبكا لكية انخفاضا كبيرا في الأسعار ذلك نظرا للانتشار و الاقبال الكبير على هذه التقنية الرائعة اذ صارت تستخدم في العديد من البيوت.

## مصطلحات هامة

### ١- مزود خدمة الانترنت ISP

مزود خدمة الانترنت ISP اختصار الى "Internet Service Provider" وهو يوفر الوصول إلى شبكة الإنترنت. حيث في كل مرة تتصل بها بالإنترنت، يتم توجيه الاتصال عبر ISP .

في الماضي، قدمت مزودي خدمات الإنترنت ISPs الوصول إلى الإنترنت من خلال الطلب الهاتفي "أجهزة المودم". يعمل هذا النوع من الاتصال عبر خطوط الهاتف العادية واقتصر على سرعة ٥٦ كيلوبت في الثانية. في أواخر التسعينات بدأت مقدمي خدمات broadband تقدم نطاق العريض "هذا يشير إلى كمية نقل البيانات عالية السرعة حيث أن كابل واحد يمكن أن يحمل كمية كبيرة من البيانات دفعة واحدة" بشكل أسرع للوصول إلى الإنترنت عبر "DSL وهو الانترنت الحالي المتواجد لدى غالبية المستخدمين". بعض مقدمي خدمات الإنترنت الآن تقدم وصلات الألياف عالية السرعة، والتي توفر الوصول إلى الإنترنت من خلال كابلات الألياف الضوئية. للاتصال بمزود خدمة الانترنت ISP ، تحتاج إلى مودم وحساب نشط. عند توصيل المودم إلى الهاتف، فإنه يتصل مع ISP الخاص بك. و ISP يتحقق من حسابك ويعين المودم الخاص بك على عنوان IP واحد ولمرة واحدة عند كل اتصال.



شكل (١٣-١) يوضح الدور الذي يقوم به ISP.

يمكن دمج جهاز التوجيه الراوتر في نفس عنوان IP العام المعين من قبل .  
 (في المودم) لتوصيل أجهزة متعددة إلى الإنترنت. عند توصيل الأجهزة إلى  
 الراوتر ستشترك جميعاً في نفس عنوان IP العام المعين من قبل .

مزودي خدمات الإنترنت ISP تعمل كمراكز على شبكة الإنترنت لأنها غالباً  
 ما تكون مرتبطة مباشرة إلى الإنترنت العمود الفقري "يرتبط الإنترنت العمود  
 الفقري المحلي مع خطوط الشبكة الرئيسية التي بدورها تربط عدة شبكات في  
 المنطقة وغالباً هذا الربط يتم بواسطة كبلات الليف الضوئي المتواجده في  
 البحار.



## ٢-النطاق العريض Broadband

### ماهو النطاق العريض Broadband ؟

النطاق العريض أو الموجة العريضة Broadband هو وسيلة نقل عالية السرعة وعالية السعة يمكنها حمل إشارات من ناقلات شبكة مستقلة متعددة. ويتم ذلك على كبل واحد متحد المحور أو ليف بصري عن طريق إنشاء قنوات عرض نطاق مختلفة. يمكن أن تدعم تقنية النطاق العريض نطاقاً واسعاً من الترددات، يتم استخدامه لنقل البيانات والصوت والفيديو عبر مسافات طويلة قـت واحد.

السمتان المميزتان للنطاق العريض Broadband هما أنها عالية السرعة و تعمل على مدار الوقت. هذه الخصائص تميز النطاق العريض عن اتصالات الطلب الهاتفي الأقدم حيث يوفر النطاق العريض مرونة في الاستخدام أكثر من الاتصال الهاتفي فإنه يعمل على توصيل المنازل والشركات بالإنترنت وبالمجتمع العالمي للمستخدمين عبر الإنترنت.

## قدرات النطاق العريض Broadband

تقدم بعض الدوائر الحكومية تعريفات دقيقة للنطاق العريض تتضمن الحد الأدنى لسرعة التنزيل والتحميل ، مثل عدد معين من ميجابت في الثانية. وتعد إمكانات التنزيل والتحميل والاستخدام في النطاق العريض أكبر بكثير من الاتصال الهاتفي . سرعة النطاق العريض أيضا يجعل الألعاب عبر الإنترنت والخدمات التفاعلية ممكنة. يُحدد النطاق العريض الحد الأدنى من سرعات تنزيل بنحو ٢٥ Mbps والحد الأدنى من سرعات تحميل هي ٣Mbps على مر السنين ، غيرت لجنة الاتصالات الفيدرالية FCC سرعات النطاق العريض عدة مرات.

## أنواع النطاق العريض

تشمل أنواع النطاق العريض الخط المشترك الرقمي (DSL) ، مثل خط المشترك الرقمي غير المتماثل وخط المشترك الرقمي المتماثل، والأقمار الصناعية. يوفر DSL الوصول عريض النطاق من خلال البث اللاسلكي. تتوفر اتصالات DSL بسرعات مختلفة للشركات والمنازل. قد يكون النطاق العريض متاحًا أيضًا عبر مودم الكبل ، مما يعني أنه يمكن للمستخدمين الوصول إلى الإنترنت باستخدام نفس خدمة الكبل من مزودي

كبلات التلفزيون الخاصة "الستلايت" دون التدخل في استخدام التلفزيون. يمكن أن توفر كبلات الألياف سرعة عالية نقل الإنترنت. وتستخدم ألياف زجاجية شفافة رقيقة جدًا لنقل المعلومات كضوء. تتضمن إرسالات النطاق العريض اللاسلكي كلا من الهاتف الثابت والمتنقل "شبكات الجوال". توفر الاتصالات اللاسلكية الثابتة نطاقًا محدودًا من النطاق العريض داخل شبكة لاسلكية محلية (WLAN)، وغالبًا ما تستخدم في المنازل أو الشركات.

يمكن لمزودي خدمات الهاتف المحمول أن يوفرُوا النفاذ المتنقل إلى النطاق العريض الذي يمكن المستخدم من الوصول إلى الإنترنت في أي مكان تتوفر فيه متنقلة مماثلة. يأتي ذ خدمة النطاق العريض المتنقل الأقمار الصناعية التي تدور حول الأرض مثل شبكات الثريا Thuraya .

### ملخص:

يمكن للنطاق العريض عبر الأقمار الصناعية المساعدة في الوصول إلى النطاق العريض للأفراد والشركات في الأماكن النائية وهو ما يسمّى بالإنترنت الفضائي.

### ٣-الانترنت الفضائي

ما هو الانترنت الفضائي و كيف يعمل؟



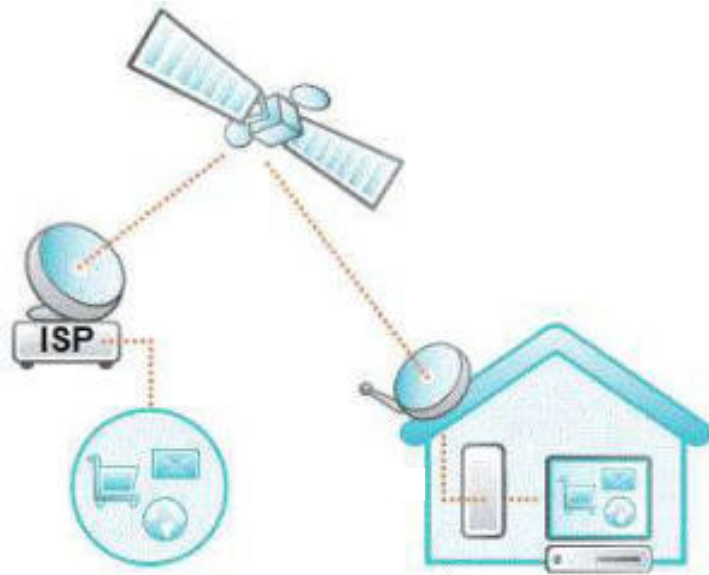
شكل (١٤-١) يوضح الإنترنت الفضائي.

الانترنت عبر الأقمار الصناعية "الانترنت الفضائي" هو اتصال لاسلكي ينطوي على ٣ أطباق "أقمار صناعية". واحد على المحور تابع لمزودي خدمات الإنترنت، و واحد في الفضاء، و واحد تابع لنا عن طريقه يتم الاتصال. بالإضافة إلى طبق الأقمار الصناعية أيضا نحتاج إلى مودم والكابلات "التوصيلات من وإلى الطبق إلى المودم".

### كيف يعمل الاتصال بالانترنت الفضائي ؟

مزود خدمة الانترنت ISP يرسل إشارة الإنترنت إلى الطبق في الفضاء، هذا الطبق يقوم بعكس الإشارة الى الطبق الموجود لديك. كل مرة نقوم فيها بطلب

الانترنت (صفحة ويب جديدة، وتحميل وإرسال البريد الإلكتروني، إلخ) هذا الطلب يذهب إلى الطبق الموجود في الفضاء ومن ثم إلى مركز ISP ، ثم يتم إرسال نتيجة الطلب عبر الفضاء، إلى الطبق الخاص بك ومن ثم إلى جهاز الكمبيوتر عن طريق المودم الخاص.



شكل (١٥-١) يوضح كيفية عمل الإنترنت الفضائي.

الطبق الهوائي يتلقى ويرسل الإشارات بسرعة تتراوح من ٥٠ الى ١٥٠ كيلوبت في الثانية. تأتي سرعة التحميل "download" بسرعات تتراوح من ١٥٠ كيلوبت في الثانية إلى أكثر من ١٢٠٠ كيلوبت في الثانية، وهذا يتوقف على عدة عوامل مثل قدرة الخادم "نوع الاشتراك" وأيضاً في أوقات الذروة والعمل لدى المشتركين قد تضعف السرعة بالإضافة الى العوامل المناخية التي تؤثر على الطبق الصناعي وتعيق ارسال واستقبال الإشارة.

**سلبيات هذا الانترنت:** ثمن الاشتراك يكون باهضاً نوعاً، حيث عليك أن تدفع حوالي \$ ١٠٠ شهرياً للحصول على سرعة ٢ ميجا بت في الثانية. بالإضافة الى عوامل الطقس التي تؤثر على جودة الانترنت. شركات الانترنت الفضائي تفرض قيود على عرض النطاق الترددي أي غالباً ما يكون هناك حد مسموح به من استهلاك البيانات وعند تجاوز هذا الحد سيعمل مزود خدمة الانترنت ISP على إبطاء الاتصال التابع لك ريثما يتم تجديد هذا الحد فيما بعد. الشبكات الافتراضية الخاصة VPN غير متوافقة مع الانترنت عبر الأقمار الصناعية.

**الإيجابيات :** الانترنت عبر الأقمار الصناعية أسرع من الاتصال الهاتفي

Up كثير. يمكن الاتصال ت الفضائي من أي مكان على الكرة الأرضية. لا يوجد حاجة إلى وجود خط هاتف للعمل.

### الملخص:

رغم أن الثمن باهضاً نوعاً ما، ولكن الانترنت الفضائي هو الخيار الأفضل للناس المتواجدة في المناطق الريفية حيث لا يوجد اتصال خط المشترك الرقمي "DSL" أو أنهم بحاجة الى الاتصال بالانترنت عن طريق الطلب الهاتفي Dial-Up وهذا الأخير له سلبيات كبيرة جداً مقارنة مع ايجابيته الوحيدة وهي إمكانية الاتصال من أي مكان يوجد فيه خط هاتف.

## ٤- معدل نقل البيانات Bandwidth

بالإنجليزية (Bandwidth): هي السعة التي يسمح بها لنظام ما لكي ينقل البيانات عبر اتصال ما وتقاس هذه الكمية بوحدة القياس البايت (كل فترة زمنية) كل شهر مثلا يسمح لك بالعدد كذا من البايتات.

المصطلح بالإنجليزية Bandwidth يستخدم بكثرة في علم الحاسوب لقياس معدل نقل البيانات في الشبكات وأجهزة المودم. كذلك بين أجهزة الحاسوب الداخلية مثل معدل نقل البيانات بين المعالج والذاكرة الرئيسية وبين المعالج والقرص الصلب.

## كيفية حساب معدل نقل البيانات؟

في أجهزة الاتصالات والشبكات يحسب معدل نقل البيانات بالبت لكل ثانية بت/ثانية. ولكن في العتاد الخاص بالحاسوب مثل الذاكرة وكروت الشاشة تحسب بالبايت لكل ثانية. للحصول على قيمة نقل البيانات بت/ثانية نضرب قيمة التردد بالميجاهيرتز (في عرض النطاق أو عرض الموجة لنحصل على القيمة بالميجابايت. الميجاهيرتز يساوي مليون نبضة في الثانية .

**عرض النطاق (Bandwidth)**

هي قيمة تستخدم لقياس كمية المعلومات المرسلّة أو المستقبلّة خلال فترة من الزمن ، وحدة Bandwidth عبارة عن عدد البتات المرسلّة أو المستقبلّة في الثانية الواحدة (Bits Per Second (Bps).

غالباً ما نشير الى Bandwidth بسرعة نقل البيانات أو سرعة جريان المعلومات على سبيل المثال قد تكون سرعة إرسال واستقبال المعلومات عبر بطاقة الشبكة، 10Mbps، 100Mbps أو 1000Mbps بينما تكون هذه السرعة تتراوح بين 33Kbps و 56Kbps بالنسبة لجهاز المودم.

ولحساب أقل زمن ممكن أن يستغرقه نقل ملف فإن الزمن يحسب من العلاقة:  
 $T = S / BW$ ، حيث S تدل على حجم الملف و BW تدل على سرعة نقل  
 الوسـد تخدم أو Bandwidth

تستغرق عملية إرسال قرص مرّن من البيانات (1.44 MB) عبر ISDN

$$T = 1.44 \text{ MB} / 128 \text{ KB/s} = 1.44 \times 10^6 \times 8 / 128 \times 10^3 / \text{s} = 90 \text{ s}$$

أي ما يعادل ٩٠ ثانية.

نستنتج من هذا المثال مدى أهمية عرض النطاق لأي وسيط اتصال، عندما يكون عرض النطاق كبير يمكننا هذا من إرسال ملفات ضخمة خلال فترة زمنية قصيرة.

ويدل زمن الإرسال T نظرياً على أقل زمن يستغرقه نقل الملف.



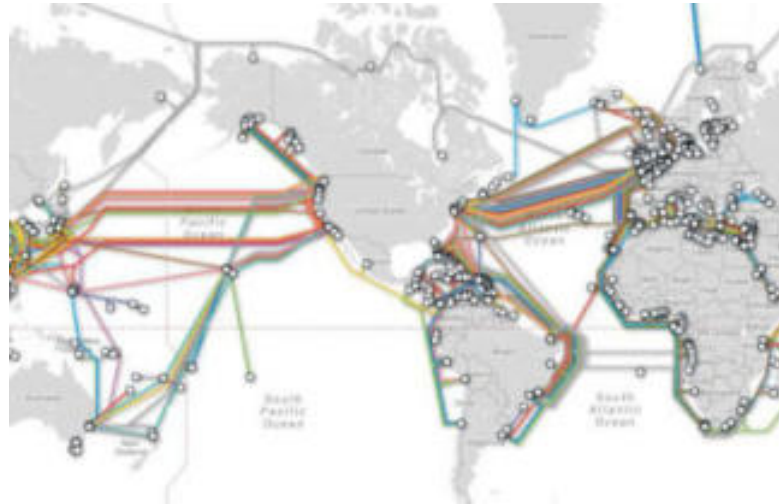
مثال على حساب أقل زمن من الممكن أن يستغرقه نقل ملف

لكن عملياً هناك عدة عوامل تجعل الزمن الذي تستغرقه عملية الإرسال أكبر من الزمن  $T$  ومن بين هذه العوامل:

- ١- نوع الأجهزة المستخدمة في ربط الشبكات.
  - ٢- نوع البيانات المرسل (نصوص، صور فيديو أو صوت).
  - ٣- الطبوغرافية المستخدمة.
  - ٤- عدد مستخدمي الشبكة (كلما ارتفع عدد المستخدمين قل الأداء).
  - ٥- إمكانيات جهاز الم
  - ٦- حالة وإمكانيات محطة العمل.
  - ٧- نوع البروتوكول المستخدم.
- كل هذه العوامل تؤثر على الزمن الذي تستغرقه عملية إرسال أو استقبال البيانات على الشبكة.

## ٥-العمود الفقري للإنترنت Backbone

### ماهو العمود الفقري Backbone للإنترنت؟



(١٦-١) يوضح مسارات الرئيسية بين الشبكات.

يشير العمود الفقري للإنترنت إلى أحد مسارات البيانات الرئيسية بين الشبكات الكبيرة والمتراصة استراتيجياً وأجهزة التوجيه الأساسية على الإنترنت. حيث يعد العمود الفقري لشبكة الإنترنت خط نقل بيانات عالي السرعة يوفر تسهيلات الربط الشبكي لمزودي خدمات الإنترنت الصغيرة نسبياً ولكن عالية السرعة في جميع أنحاء العالم. شبكات الإنترنت الأساسية هي أكبر اتصالات البيانات على شبكة الإنترنت. تتطلب اتصالات النطاق الترددي عالية السرعة والخوادم وأجهزة التوجيه عالية الأداء. الشبكات الأساسية هي مملوكة في المقام الأول من قبل الكيانات التجارية والتعليمية والحكومية والعسكرية لأنها توفر وسيلة

متسقة لمزودي خدمة الإنترنت (ISPs) للحفاظ على والحفاظ على المعلومات عبر الإنترنت بطريقة آمنة.

ومن بين أكبر الشركات التي تدير أجزاء مختلفة من العمود الفقري لشبكة الإنترنت UUNET و AT & T و GTE Corp. و Sprint Nextel Corp. وترتبط أجهزة التوجيه الخاصة بها بالوصلات عالية السرعة وتدعم خيارات نطاق مختلفة مثل T1 أو T3 أو OC1 أو OC3 أو OC48 .

### مميزات شبكة الانترنت الأساسية:

تتضمن بعض الميزات الرئيسية لشبكة الإنترنت الأساسية ما يلي: يكون مقدمو خدمات الإنترنت إما متصلين مباشرة بشبكاتهم الأساسية للطوارئ أو مع بعض مزود الإنترنت الأكبر حجماً ط بنيته الأساسية.

أول شبكة إنترنت أساسية كانت تسمى NSFNET . وقد تم تقديمه من مؤسسة العلوم الوطنية (NSF) في عام ١٩٨٧. وكان خط T1 يتكون من حوالي ١٧٠ شبكة أصغر تعمل بسرعة ١.٥٤٤ ميغابت في الثانية. كان العمود الفقري عبارة عن مزيج من خطوط الألياف البصرية لزيادة السعة.

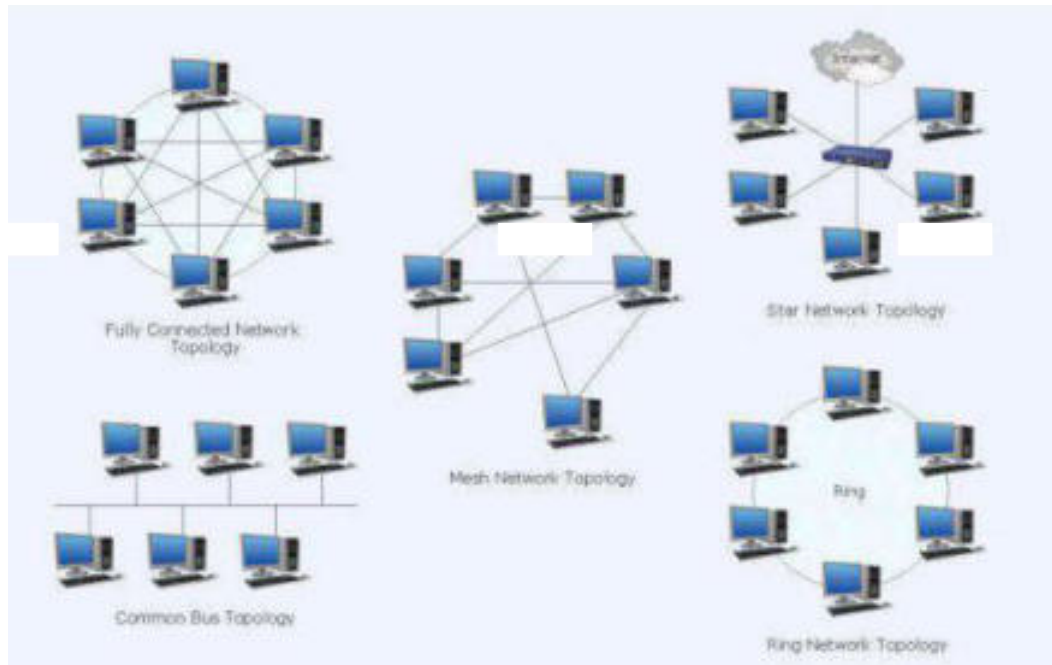
**الملخص:** يشير العمود الفقري المحلي إلى خطوط الشبكة الرئيسية التي تربط العديد من الشبكات المحلية ( LAN ) معاً. والنتيجة هي شبكة منطقة واسعة ( WAN ) مرتبطة بواسطة اتصال أساسي.



# الباب الثاني

## طبوغرافية الشبكة

### Network Topology



## أهداف الباب الثاني

بعد الانتهاء من دراسة هذا الباب ينبغي أن يكون الطالب قادراً على أن:

- ١- يُعرف الطبوغرافية.
- ٢- يميز بين الطبوغرافيات الأساسية للشبكات.
- ٣- يعدد مزايا وعيوب البنية الطبوغرافية الخطية.
- ٤- يبرر سبب وجود وصلة أو نهاية طرفية terminator على أطراف الكبل في حالة التوصيل Bus Topology.
- ٥- يعدد مزايا وعيوب البنية الطبوغرافية النجمية.
- ٦- يبرر السبب في أهمية جهاز المبدل Switch في البنية النجمية.
- ٧- يحدد متى تتوقف الشبكة النجمية عن العمل.
- ٨- يحدد كيف تعمل الشبكات النجمية.
- ٩- يعدد مزايا وعيوب البنية الطبوغرافية الحلقية.
- ١٠- يذكر الآلية المستخدمة في الشبكات الحلقية.
- ١١- يحدد كيف تعمل الشبكات الحلقية.
- ١٢- يحدد اسم الجهاز الذي يقوم كل جهاز في الشبكة الحلقية بدوره. يفرق بين التوصيل والحلقي.
- ١٤- يقارن بين الشبكات الخطية والنجمية والحلقية من حيث المزايا والعيوب والامكانيات ومتى تتوقف الشبكة بأكملها عن العمل.
- ١٥- يوضح الدور الذي يقوم به جهاز MAU في البنية النجمية الحلقية.
- ١٦- يعدد مزايا وعيوب البنية الطبوغرافية الشجرية.
- ١٧- يحدد متى تتوقف الشبكة الشجرية عن العمل.
- ١٨- يعدد مزايا وعيوب البنية الطبوغرافية التهجينية أو المختلطة.
- ١٩- يعدد مزايا وعيوب الشبكات المتداخلة.
- ٢٠- يبرر السبب في اتصال الأجهزة حتى لو انقطع الاتصال بينها في الشبكات المتداخلة.
- ٢١- يذكر المقصود بمنطقي التوجيه والتدفق.
- ٢٢- يفرق بين Redundancy و Fault Tolerance.
- ٢٣- يرسم الشكل الذي يوضح البنية الطبوغرافية الأساسية للشبكات.
- ٢٤- يحدد أي نوع من طبوغرافيات الشبكات يمكن استخدامه وتطبيقه في الشبكات اللاسلكية.
- ٢٥- يعدد أنواع طبوغرافيات الشبكات اللاسلكية.

٢٦- يفرق بين الشبكات اللاسلكية المتشابكة والشبكات السلكية المتشابكة.

( ٤٧ )

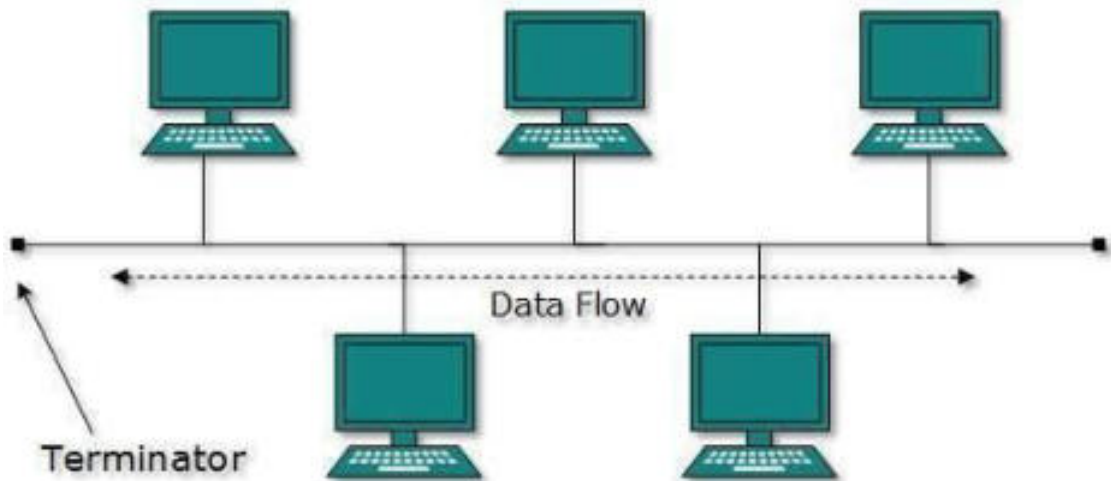
## طبوغرافية الشبكة Network Topology

يطلق على الكيفية التي تتم بها عملية توصيل الأجهزة معاً في شبكة اسم طبوغرافية الشبكات Network Topology.

هناك عدة تصميمات أساسية للشبكات وهي:

- ١- البنية الطبوغرافية الخطية Bus Topology.
- ٢- البنية الطبوغرافية الحلقية Ring Topology.
- ٣- البنية الطبوغرافية النجمية Star topology.
- ٤- البنية الطبوغرافية المختلطة Mesh Topology.
- ٥- لطبوغرافية الهجينيه Hybrid T y

أولاً: البنية الطبوغرافية الخطية:



شكل (٢-١) يوضح البنية الطبوغرافية الخطية.

إعداد د/ أميرة إبراهيم عبد الغني



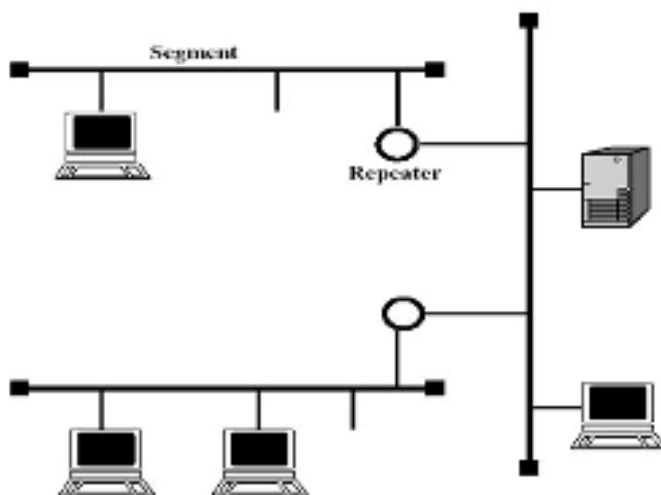
تستخدم طريقة التوصيل الخطي إذا كانت الشبكة المراد تكوينها:

- شبكة صغيرة أو بسيطة و يمكن حلها في أي وقت.
- التكلفة المخصصة لها منخفضة.

أي أنه إذا كان لديك ٤ أجهزة وتريد ربطهم معاً في شبكة بأقل تكلفة ممكنة فان طريقة التوصيل المختارة هي التوصيل الخطي، أنظمة Ethernet القديمة تستخدم البنية الطبوغرافية الخطية مع الكبلات المحورية (Coax) والتي تكون على الشكل المحوري السميك أو الرفيع.

### ومن مميزات طريقة التوصيل الخطي:

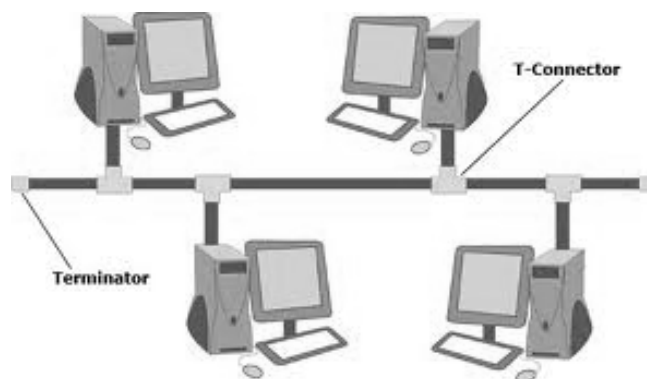
- ١- سهولة الاستخدام.
- ٢- طريقة عملية وبسيطة مع الشبكات الصغيرة.
- ٣- تحتاج الى أقل عدد من الكابلات ومن ثم فان التكلفة قليلة.
- ٤- ب وصيل كابل آخر يمكنه الشبكة، كما يمكن استخدام ج Repeater مقوي الإشارة حتى يتم مد الكابل لمسافات طويلة.



شكل (٢-٢) يوضح توسعة الشبكة الخطية باستخدام جهاز (المكرر Repeater).

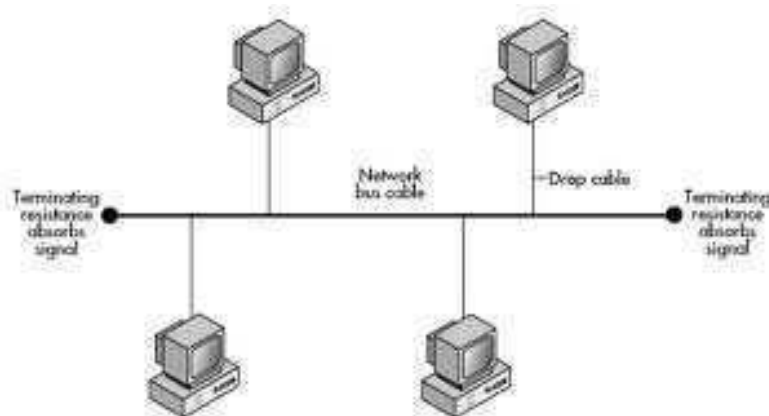
## عيوب طريقة التوصيل الخطي Bus topology

- ❖ في الشبكات الكبيرة والشبكات المزدحمة والتي يتم نقل كمية كبيرة من المعلومات بين الأجهزة، تصبح الطريقة الخطية غاية في البطء.
- ❖ نطاق التصادم فيها عالي ومن ثم يتم فقد جزء كبير من السرعة في هذه التصادمات.
- ❖ كل جهاز يتم توصيله في الشبكة يؤدي إلى ضعف الإشارة، وبالتالي عند توصيل عدد كبير من الأجهزة قد لا تصل المعلومات بطريقة صحيحة.
- ❖ ومن العوامل التي تؤثر على أداء الشبكة هي إمكانيات الأجهزة من حيث مكوناتها، عدد الأجهزة المتصلة بالشبكة، المسافة بين الأجهزة المتصلة بالشبكة وسر البيانات.
- ❖ عندما ترسل البيانات على الشبكة فإنها تنتقل من بداية الكابل إلى نهايته وتبقى الإشارة ترتد ذهاباً وإياباً على طول الكابل مما يمنع الأجهزة الأخرى من إرسال إشاراتها. لهذا يجب إيقاف هذه الإشارة التي أصبحت مشوشة وهذا بعد وصولها إلى عنوانها المطلوب أو الجهاز المستقبل.
- ❖ لإيقاف الإشارة ومنعها من الارتداد يستخدم مكون أو وصلة خاصة تسمى نهاية طرفية. يتم وضع وصلة على كل طرف من أطراف السلك، كما يظهر في الشكل التالي:



شكل (٢-٣) يوضح تثبيت النهايات الطرفية على طرفي الكبل

❖ احتمال وقوع الشبكة كبير في حالة انقطاع الكابل أو الوصلة الخاصة التي تصل بين الجهاز والآخر، عندما تقع وصلة أحد الأجهزة تتعطل الشبكة بأكملها.



شكل (٢-٤) يوضح عطل الشبكة نتيجة انقطاع أحد الأسلاك.

- ❖ من الصعب التعرف على سبب عطل الشبكة، حيث أنه أي عيب بالكابل في أي منطقة قد يؤدي إلى تعطيل الشبكة بأكملها.
- ❖ تعتبر معظم الشبكات الخطية عبارة عن كابل واحد مكون من سلك أو مجموعة أسلاك ولا توجد مقويات للإشارة بين الأجهزة Repeater، لذا تعتبر هذه الشبكة خاملة Passive Topology.

## ثانياً: البنية الطبوغرافية النجمية Star Topology

كل أجهزة الحاسوب الموصلة في الشبكة النجمية تتصل بوحدة توصيل مركزية يطلق عليها المجمع Hub قديماً والمبدل Switch حديثاً، فيصبح الشكل النهائي للشبكة على شكل نجمة Star، ولذا يطلق عليها اسم الشبكات النجمية.

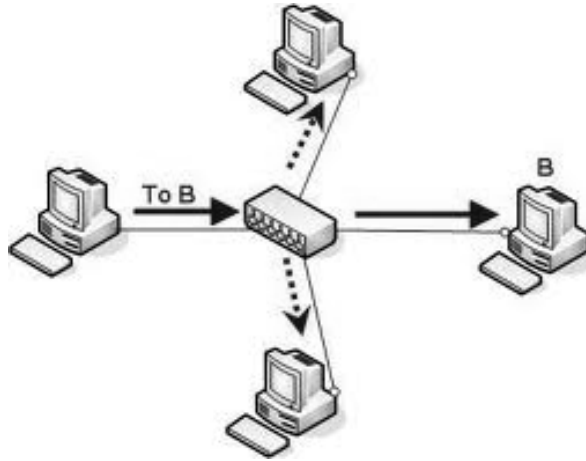
يعزل نظام التوصيل في المبدل كل سلك من أسلاك الشبكة عن الآخر وبالتالي إذا توقف جهاز ما أو انقطع السلك الذي يربطه بالمبدل فلن يتأثر إلا الجهاز الذي توقف أو انقطع سلكه بينما ستبقى باقي الأجهزة تعمل وتتبادل البيانات فيما بينها. ولكن إذا حدث وفشل المبدل فستتوقف الشبكة ككل عن العمل.



شكل (٥-٢) يوضح كيفية توصيل الأجهزة في الشبكات النجمية.

### كيف تعمل الشبكات النجمية How a star network works؟

- يرسل كل جهاز على الشبكة الإشارة إلى الوصلة المركزية (المجمع).

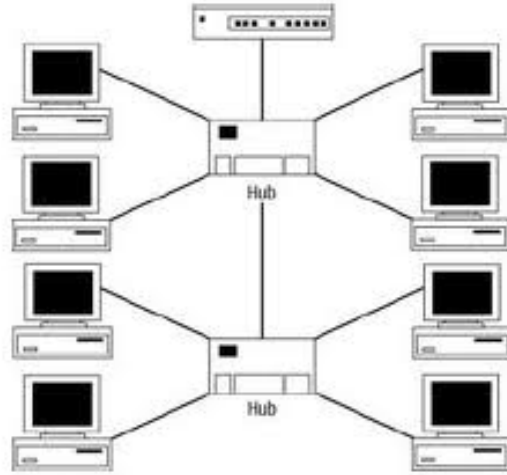


شكل (٦-٢) يوضح كيف يبث المجمع الإشارة الى جميع الأجهزة.

- يقوم جهاز hub إما إرسال الإشارة الى كل الأجهزة وتسمى هذه الشبكة بشبكة الإرسال النجمية Broadcast star network. أو إرسال الإشارة فقط إلى الجهاز المراد إرسال الرسالة له، وهذا النوع من معات يطلق عليه الم Swit، ويطلق على الشبكات Switched star networks تستخدم المبدل Switch اسم Switched star networks.

### مميزات طريقة التوصيل النجمية Star topology

- من السهل توسيع الشبكة من خلال إضافة أجهزة جديدة فكل ما نحتاج إليه هو كابل يتم توصيل أحد طرفيه بالجهاز والطرف الآخر بالمجمع Hub ويمكن توصيل مجمع آخر أو استخدام مجمع عدد منافذه أكبر.



شكل (٧-٢) يوضح توسيع الشبكة باستخدام أكثر من مجمع

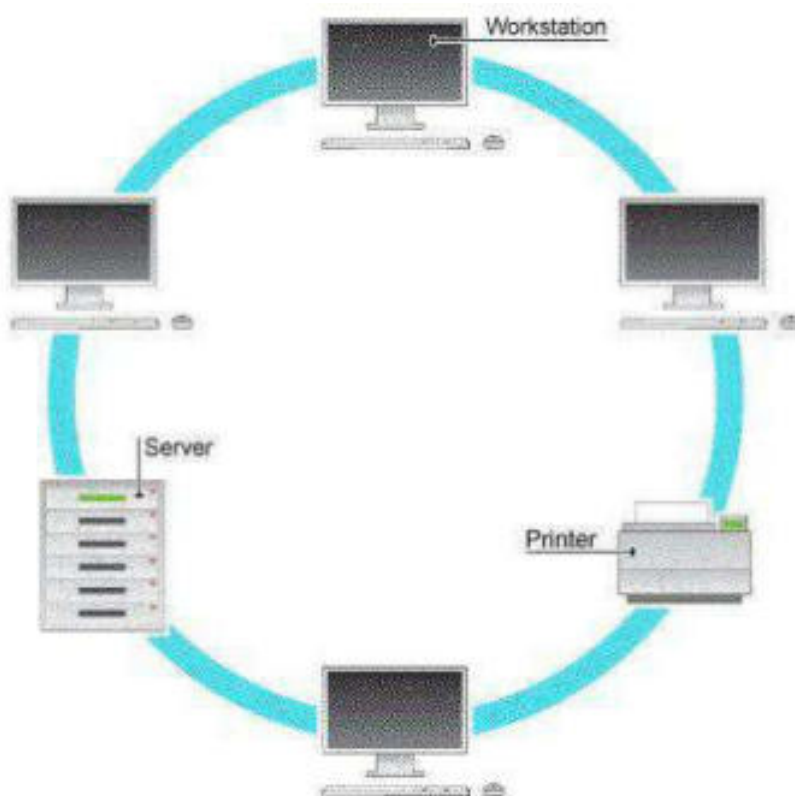
- من السهل معرفة الجهاز الذي تعطل بالشبكة بمجرد النظر إلى الوصلات الموجودة في المجمع Hub فكل وصلة سليمة لها Led لمبة بيان خاصة بها ، فإذا أضاءت كانت الوصلة سليمة. أما إذا فمأ هذا الضوء دل هذا ل الجهاز المتصل به.
- يمكن استخدام أكثر من نوع من أنواع الكابلات في الشبكة.

### عيوب طريقة التوصيل النجمية

- إذا تعطل المجمع Hub تعطلت الشبكة بأكملها.
- تحتاج إلى كابلات أكثر من الطريقة الخطية، وذلك لأن كل جهاز يمتد منه كابل إلى المجمع، بينما في التوصيل الخطي فهو كابل واحد يربط الأجهزة مع بعضها البعض.

### ثالثاً: البنية الطبوغرافية الحلقية Ring topology

ترتبط الأجهزة في الشبكات الحلقية Ring networks من خلال حلقة أو دائرة من السلك بدون نهايات. والشكل التالي يوضح كيفية ارتباط الأجهزة في الشبكات الحلقية.



شكل (٨-٢) يوضح ارتباط الأجهزة في الشبكات الحلقية

في الشبكات الحلقية يتم توصيل كل جهاز بالجهاز التالي له عن طريق كابل في شكل دائرة حتى يتم ربط طرفي نهايتي الكابل معاً لتصنع الدائرة أو الحلقة، كما هو موضح في الشكل السابق، وهذا هو الفرق بين الشبكات الحلقية والشبكات الخطية.

❖ في التوصيل الخطي يتم وضع نهايتين طرفيتين Terminators واحدة عند كل طرف ، أما في التوصيل الحلقي فيتم توصيل بداية الكابل بنهايته.

وهذه الطريقة لم تعد تستخدم بكثرة الآن، ولكن تم استبدالها بالوصلات النجمية الحلقية Star ring ، والتي يستخدم فيها المجمع ويتم توصيل الأجهزة بالمجمع من الخارج مثل الطريقة النجمية العادية ولكن داخل المجمع Hub يكون التوصيل على شكل حلقة.

❖ تستخدم الشبكات الحلقية في الشبكات عالية الأداء والتي تحتاج إلى وسط لنقل كمية كبيرة من المعلومات بسرعة عالية (High Bandwidth). مثل الصوت والصورة وأيضاً في الشبكات التي اج إلى أداء جيد مع هزة كبير وذلك لأنها شبكة نشد .Active network

### كيف تعمل الشبكات الحلقية؟

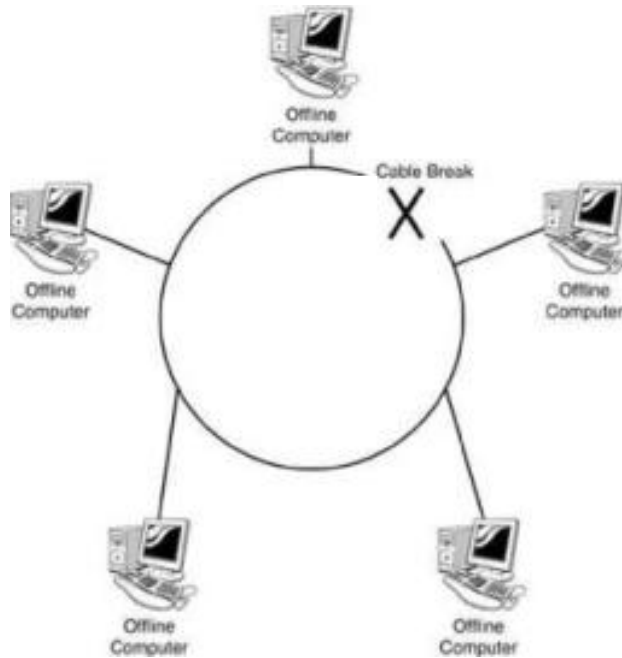
- تتصل الأجهزة مع بعضها البعض على شكل دائرة.
- كل حاسوب يقوم بالإرسال إلى الحاسوب الذي يليه.
- يأخذ الحاسوب البيانات ثم يعيد إرسالها مرة أخرى في اتجاه واحد وبترتيب واحد ولذلك فإن الشبكة التي تستخدم هذا النوع تكون نشطة Active، لأن إعادة إرسال الإشارة تؤدي إلى تقويتها. وهذا على



عكس ما يحدث في الطريقة الخطية مما يجعل الشبكات الخطية غير نشطة Passive.

### عيوب التوصيل الحلقي Ring topology

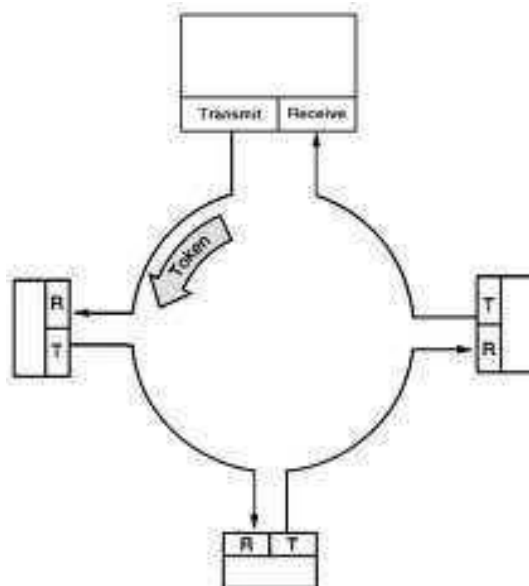
- سقوط أي جهاز وليس الكابل يؤثر على الشبكة ككل، وهذا يعني أن تعطل الجهاز نفسه يؤثر على الشبكة ككل لأن هذا يؤدي الى انقطاع الحلقة.



شكل (٩-٢) يوضح سقوط الشبكة عند انقطاع الكابل فقط.

- من الصعب اكتشاف العطل بها.
- إضافة او إزالة حاسوب يؤثر على الشبكة.

- يطلق على الآلية المستخدمة في إرسال البيانات على الشبكات الحلقية اسم Token Passing أو تمرير العلامة. لذلك فإن تكنولوجيا Token Ring تستخدم هذا النوع من الطوبوغرافية. انظر إلى الشكل التالي

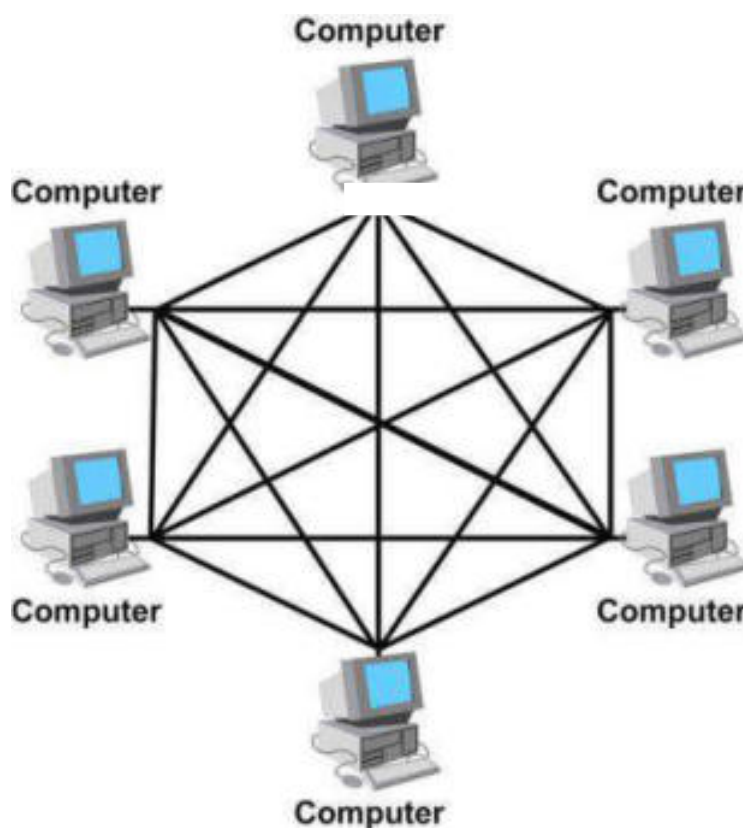


شكل (١٠-٢) يوضح كيف تمر الإشارة من جهاز إلى جهاز في الحلقة.

إن تصميم البنية النجمية التي تستخدمه الشبكات الحلقية يتيح قدرة الشبكة على العمل حتى في حالة فشل أحد الكبلات لأن MAU يحتوي على دائرة خاصة تفصل الأجهزة التي تفشل عن بقية الأجهزة، حيث تتصل الكبلات في الشبكات الحلقية بمجمع مركزي وتأخذ شكل نجمة. يستخدم هذا النوع من الشبكات نوعاً خاصاً من المجمعات يسمى وحدة الوصول متعدد المحطات (MAU) Multistation Access Unit حيث يستلم البيانات عبر أحد المنافذ ويرسلها عبر المنفذ الذي يليه. تستمر هذه العملية إلى أن ينقل MAU الإشارات إلى كل الأجهزة في الشبكة.

## رابعاً: الشبكات المتداخلة أو التوصيل النسيجي Mesh Topology

إن كلمة Mesh تعني خيوط الشبكة، فمن خلال الاسم يتضح أنها شبكة تتعاقد فيها الكابلات حتى تصبح شبيهة بخيوط الشبكة، و يوفر هيكل الشبكة المتداخلة الذي يشبه هيكل الإنترنت طريقتان مختلفتان لنقل وتبادل البيانات وهما: التوجيه والتدفق. عندما يتم توجيه البيانات، تستخدم الأجهزة المنطق لتحديد المسافة الأقصر من الجهاز المصدر إلى الجهاز الهدف، وعندما تتدفق البيانات، يتم إرسال المعلومة إلى كل الأجهزة داخل الشبكة دون الحاجة إلى منطق التوجيه.



شكل (١١-٢) يوضح Mesh Topology

## مميزات طريقة الشبكات المتداخلة Mesh Topology

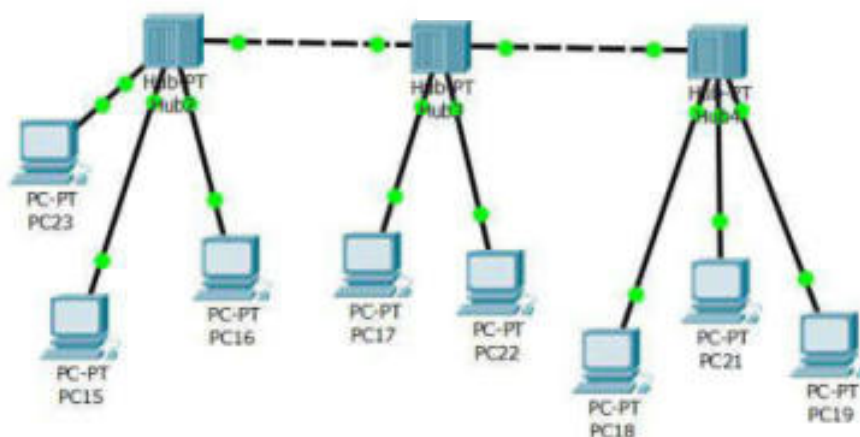
- الميزة الأساسية لهذا النوع من الشبكات هو تجنب تعطل الشبكة بانقطاع احد الوصلات أو بتعطل أحد الأجهزة وهو ما يطلق عليه Redundancy، فدرجة التعقيد في التداخل والترابط بين الأجهزة يجعلها أكثر مقاومة للفشل.
- من السهل تحمل الخطأ Fault tolerance بها فهي نوع التوصيل الوحيد الذي يوفر هذا. ففي حالة انقطاع الكابل بين حاسوبين فلن تتأثر الشبكة ولن يتأثر أي جهاز بما في ذلك الجهازين، حيث يمكنهما رؤية بعضهما من خلال بقية الوصلات، ولذا يستخدم هذا النوع في شبكة الانترنت.

### عيو ب شبكات المتداخلة :

- تستهلك هذه الطريقة العديد من الكابلات ولذا فإنها مكلفة
- صعوبة التركيب فتركيب كل هذه المسارات يتطلب مجهود كبير وخبرة واسعة.
- صعوبة الضبط difficult configuration ، حيث أنها تحتاج الى ضبط المسارات من كل جهاز لآخر.
- تكاليف الصيانة عالية.

### خامساً: طبوغرافية الشجرة Tree Topology

البنية الطبوغرافية الشجرية حصلت على اسمها من كيفية عمل العقدة المركزية كجذع للشبكة، بعقد ممتدة إلى الخارج تشبه الفروع . تقوم طوبولوجيا الشجرة بدمج كل من طوبولوجيا النجمة والطوبولوجيا الخطية لتشكيل شبكة هجينة. ومع أن كل عقدة Node في الطبوغرافية النجمية تكون متصلة مباشرة بجهاز المجمع أو المبدل المركزي، فإن بنية الشجرة تتخذ هرمية الأب-الطفل a parent-child في التوصيل بين العقد وبعضها.



شكل (١٢-٢) يوضح ارتباط الأجهزة على شكل هرمي.

تكون الشبكة على شكل هرمي، حيث تتصل الأجهزة في المستوى الأدنى بأجهزة أخرى في المستوى الأعلى منها وهي بدورها تتصل بأجهزة أخرى أعلى

منها لتنتهي بجهاز مركزي في قمة الشبكة. وتستخدم بنية الشجرة في شبكات النطاق الواسع نظراً لأن الهيكل التصميمي لها أكثر مرونة و أكثر قابلية للتوسع وذلك لدعم أجهزة كثيرة منتشرة.

### مميزات طبوغرافية الشجرة

الربط بين الأجهزة في الطبوغرافية النجمية مع الأجهزة في الطبوغرافية الخطية يسمح بإضافة أجهزة أخرى بسهولة وبهدف توسيع الشبكة.

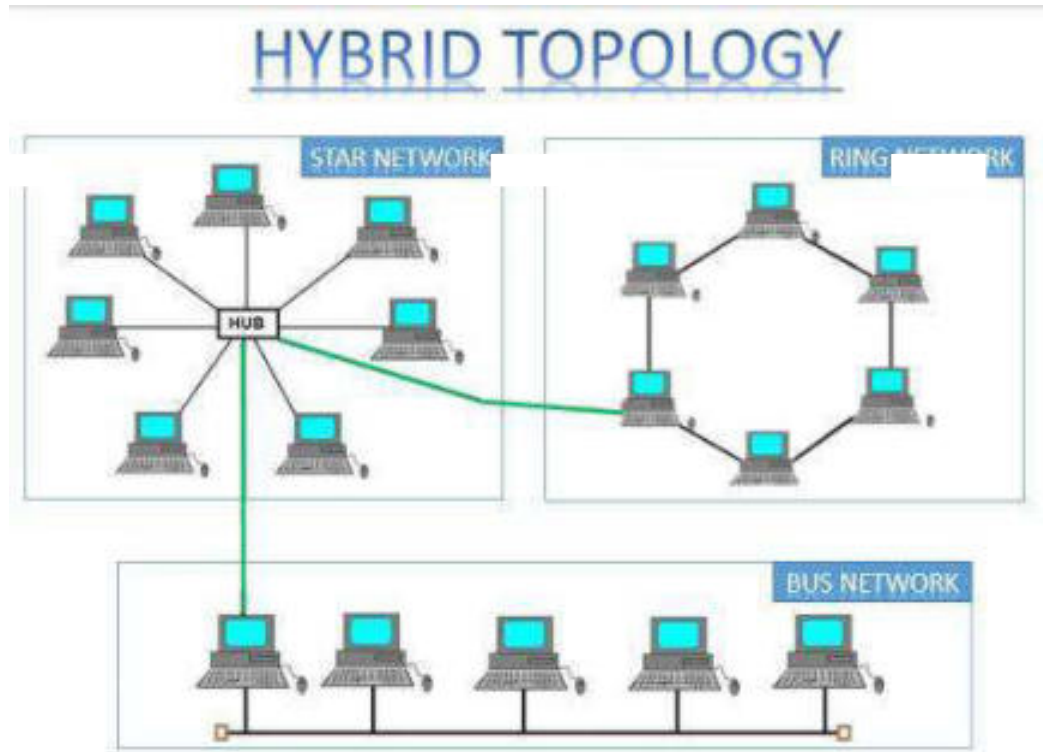
معالجة مشاكل أعطال الشبكة هي أيضاً عملية غير معقدة، لأن كل فرع من الفروع يمكن التعامل معه على حده وإصدار تقارير بتقويم الأداء.

### عيوب طبوغرافية الشجرة

كما هو الحال في الشبكة النجمية، تعتمد الشبكة بأكملها على حالة عقدة الجذر (الجهاز المركزي) الموجودة في بنية الشجرة. ربما يتعطل جهاز المبدل المركزي، في هذه الحالة تصبح جميع الفروع المختلفة غير متصلة، على الرغم من أن الاتصال بين الأجهزة داخل الفروع سيبقى ولكن بين الفروع وبعضها ينعدم الإتصال.

## سادساً: الشبكات التهجينية أو المختلطة Hybrid

تجمع الطوبولوجيا المختلطة بين هيكليين مختلفين أو أكثر من هياكل الطوبولوجيا - تعد طوبولوجيا الشجرة مثالاً جيداً على الطوبوغرافية المختلطة، حيث يتم دمج التصميم الخطي والنجمي. يتم العثور على الهياكل المختلطة بشكل شائع في الشركات الكبرى حيث يكون للإدارات الفردية طوبولوجيا شبكة مخصصة تتناسب مع احتياجاتهم والغرض من الشبكة.



شكل (١٣-٢) يوضح Hybrid topology.

## مميزات الطبوغرافية المختلطة

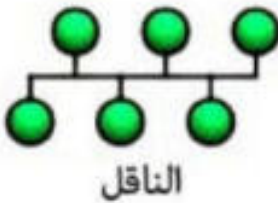
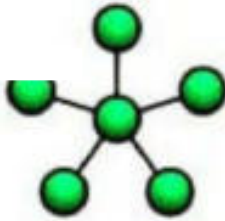

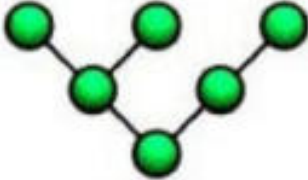
الميزة الرئيسية للهياكل المختلطة هي درجة المرونة التي توفرها ، حيث توجد قيود قليلة على بنية الشبكة نفسها.

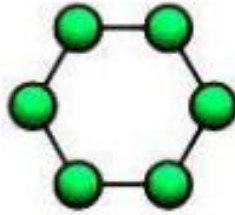
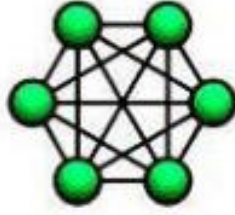
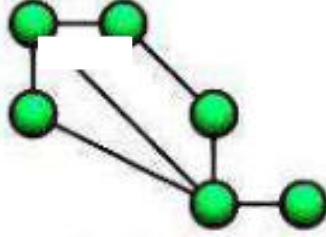
## عيوب الطبوغرافية المختلطة

كل نوع من طوبولوجيا الشبكة له عيوبه الخاصة ، وبما أن الشبكة معقدة ، فإن هذا يتطلب الخبرة والمعرفة من جانب المشرفين للحفاظ على أداء الشبكة على النحو الأمثل. كما أن التكلفة العالية يجب مراعاتها عند إنشاء طبوغرافية شبكة مختلطة.



## علاقة بنى الشبكات المختلفة بالبنى اللاسلكية

البنية	التمثيل البياني	العلاقة بالشبكات اللاسلكية
الناقل Bus	 <p>الناقل</p>	لا يمكن تطبيقها. نلاحظ لدى دراسة بنية الناقل بأن كل نقطة ترتبط بجميع النقاط الأخرى و موقع التقاء خط واحد مع الخطوط الأخرى غير موجود في حالة الشبكة اللاسلكية.
الذ	 <p>النجمية</p>	نعم، وهي البنية المعيار للشبكات اللاسلكية.
الخط Line	 <p>الخطية</p>	نعم، مع عنصرين أو أكثر. الخط بين نقطتين يمثل وصلة من نقطة إلى نقطة PTP .
الشجرة Tree	 <p>الشجرية</p>	نعم، تستخدم عادةً من قبل مزودي خدمات الإنترنت اللاسلكية.

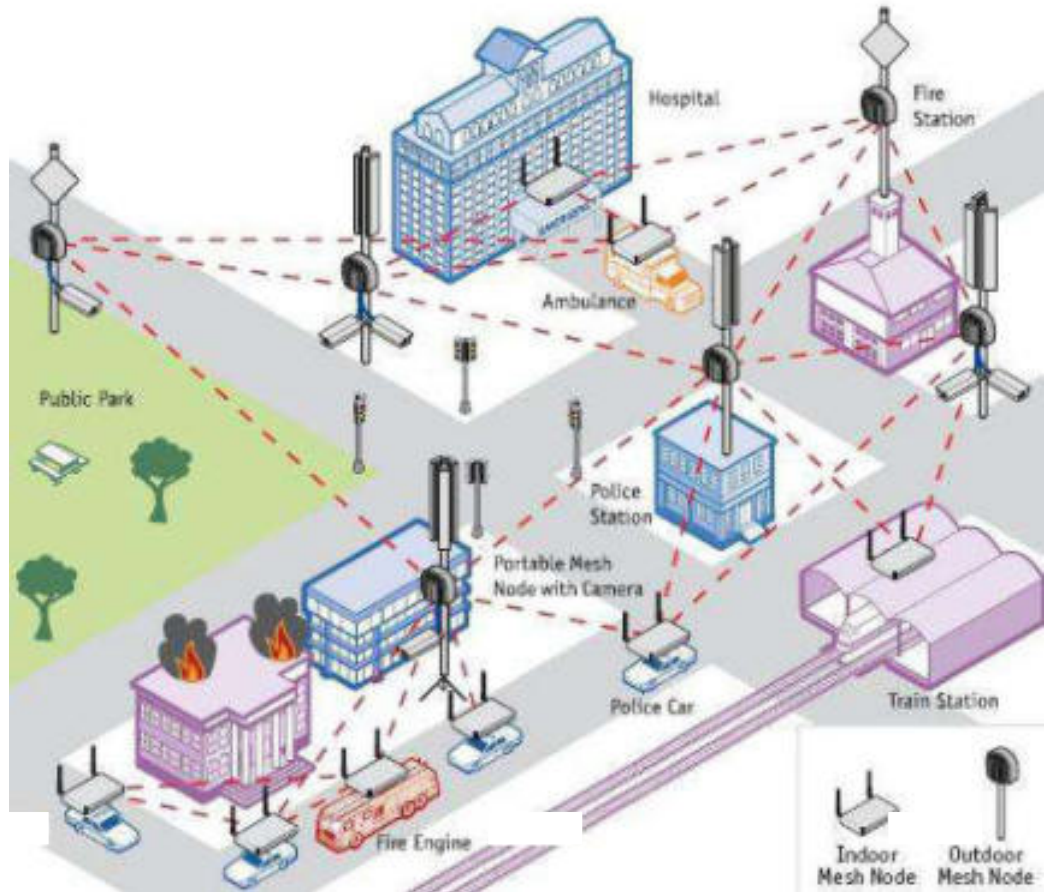
العلاقة بالشبكات اللاسلكية	التمثيل البياني	البنية
نعم، ممكنة إلا أنها نادرة الاستخدام.	 <p>الحلقية</p>	الحلقة Ring
نعم، إلا أنها على الأغلب معشقة جزئياً.	 <p>التعشيق الكامل</p>	الشبكات ذات التداخل الكامل Full Mesh
نعم.	 <p>التعشيق الجزئي</p>	١ المتداخلة جزئياً Partial Mesh

### مصطلحات هامة

## ١-الشبكات اللاسلكية المتشابكة Wireless Mesh Network (WMN)

الشبكات اللاسلكية المتشابكة (WMN) wireless mesh network هي شبكات اتصالات تتكون من نقاط لاسلكية منتشرة علي مساحة جغرافية كبيرة و الغرض منها توفير اتصال دائم بالإنترنت و ذلك عبر وجود نقاط دائمة تستطيع الدخول للشبكة منها في الحيز الجغرافي حيث تقوم كل نقطة فيها بالإرسال الي نقطة أخرى تالية لها و بعيدة عنها و تمثل كل نقطة في الشبكة النجمية المتشابكة كمكرر للإشارة Repeater لإرسالها الي نقاط بعيدة مغطية مساحة جغرافية لاسلكية يصعب مد أسلاك بها لوجود عوائق أو تضاريس جبلية أو مائية .

ترتب نقطة من نقاط الشبكات كية المتشابكة بأكثر من نقطة أ فإذا فشلت نقطة أو سقطت من الإتصال تقوم أخرى مجاورة لها بتغطيتها و العمل بدلا عنها أي ببساطة يتم ايجاد مسار بديل route كما يحدث في الإنترنت و هي بذلك تشبه أي شبكة سلكية متشابكة أخرى مثل الإنترنت و لكن الإتصال بين نقاطها يتم لاسلكيا و يتم ضمان اكثر من مسار بين نقاطها



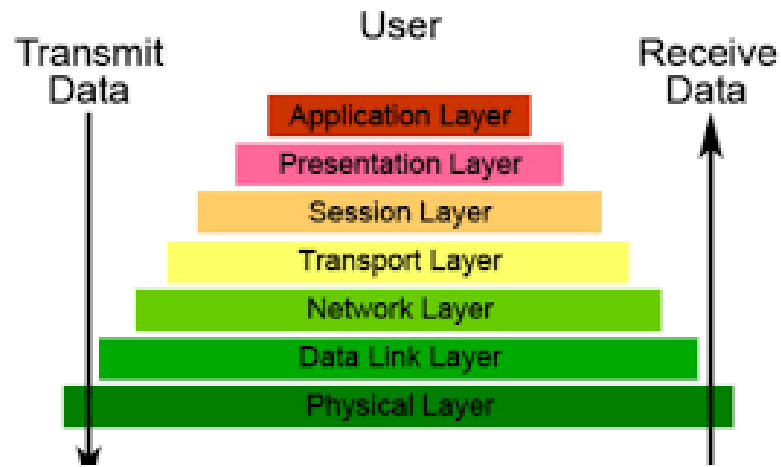
شكل (١٤-٢) يوضح مثال على الشبكات اللاسلكية المتشابهة.

و تعتمد كفاءة الشبكة علي حمل الدخول عليها و الشروط اللاسلكية للإتصال و كذلك أولوية المرور للبيانات و تختلف الشبكات اللاسلكية المتشابهة عن الشبكات اللاسلكية الأخرى في أنها تستطيع تغطية مساحة جغرافية كبيرة بدون الحاجة الي اتصال بعض أجزائها بشبكة سلكية.



# الباب الثالث

## النموذج المرجعي للاتصال بالانترنت



## أهداف الباب الثالث

بعد الانتهاء من دراسة هذا الباب ينبغي أن يكون الطالب قادراً على أن:

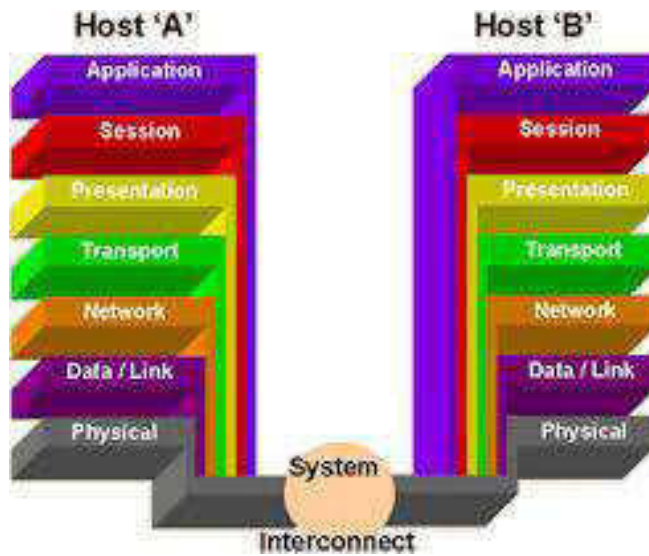
- ١- يُعرف النموذج المرجعي للانترنت.
- ٢- يميز بين المصطلحات التي تطلقها الطبقات على البيانات عند التغليف.
- ٣- يميز بين الطبقات التي تضيف ترويسة وتذييل والطبقات التي تضيف ترويسة فقط.
- ٤- يميز بين الطبقات التي لا تضيف ترويسة ولا تذييل.
- ٥- يبرر سبب وجود النموذج المرجعي للانترنت.
- ٦- يفرق بين ما يحدث أثناء عمليتي تغليف ونزع تغليف البيانات.
- ٧- يفرق بين ترويسة طبقة الشبكة وترويسة طبقة النقل.
- ٨- يفرق بين العناوين التي تتعامل معها طبقة ربط البيانات والعناوين التي تتعامل معها طبقة الشبكة.
- ٩- يفرق بين دور الطبقة الفيزيائية عند إرسال واستقبال البيانات.
- ١٠- يفرق بين الترميز الذي تستخدمه أنظمة Ethernet والترميز الذي تستخدمه أجهزة Token Ring.
- يوضح بالرسم عملية المخطط البياني Datagram.
- ١٢- يبرر السبب في أهمية طبقة ربط البيانات في الكشف عن الأخطاء.
- ١٣- يبرر السبب في أهمية طبقة الشبكة في عنونة وتوجيه البيانات.
- ١٤- يحدد البروتوكول الذي يستخدم في طبقة الشبكة.
- ١٥- يبرر السبب في أهمية بروتوكول الانترنت IP.
- ١٦- يعدد قواعد IP التي يجب الالتزام بها عند العنونة.
- ١٧- يبرر السبب في أهمية تفريع الشبكات.
- ١٨- يعطي مثال على عملية التفريع.
- ١٩- يستنتج عناوين الأجهزة على كل شبكة فرعية.
- ٢٠- يستنتج عناوين الأجهزة التي يمكن أن ترتبط مع بعضها البعض بدون راوتر.
- ٢١- يفرق بين العناوين من الفئة A والفئة B والفئة C.
- ٢٢- يقارن بين العناوين من الفئة A والفئة B والفئة C من حيث عدد الأجهزة وعدد الشبكات وقناع الشبكة الافتراضي.
- ٢٣- يوضح الدور الذي تقوم به طبقة النقل.
- ٢٤- يفرق بين بروتوكول TCP وبروتوكول UDP.

- == إعداد د/ أميرة إبراهيم عبد الغنى ==



## طبقات النموذج المرجعي

يتألف نموذج OSI المرجعي من سبع طبقات أو شرائح وهي من أعلى إلى أسفل: طبقة التطبيقات، طبقة التقديم، طبقة الجلسة، طبقة النقل، طبقة الشبكة، طبقة ربط البيانات و الطبقة الفيزيائية كما هو موضح في الشكل التالي:



شكل (٣-١) يوضح النموذج المرجعي للاتصال بالإنترنت.

## عملية تغليف البيانات

تتم عملية التغليف في الجهاز المرسل بينما تحدث العملية العكسية في الجهاز المستقبل، بعد عملية التغليف ، فإن كل طبقة تطلق مصطلحاً على البيانات لتعبر عن البيانات التي تم تغليفها.

## البيانات DATA

الطبقة العليا في نموذج TCP/IP والتي تدعى طبقة التطبيقات ( application layer) أو الطبقات ( التطبيقات، والتقديم و الجلسة) في نموذج OSI تقوم بعمل تدفق البيانات وتسليمه إلى طبقة النقل (transport layer).

الطبقات العليا لا تستخدم ترويسة أو تذييل مع البيانات. وتستخدم الطبقات العليا المصطلح بيانات Data بشكل شائع.

### القطعة Segment

تقوم طبقة النقل بتكسير البيانات المتدفقة التي يتم استلامها من الطبقات الأعلى إلى أجزاء صغيرة. ثم تقوم بإنشاء رأس لكل جزء من أجزاء البيانات. يشتمل الرأس على كل المعلو رورية عن هذا الجزء والذي ت إليه طبقة نقل البيانات في الجهاز المضيف البعيد لإستعادة تدفق البيانات مرة أخرى من خلال تجميع هذه الأجزاء. عندما يم الحاق جزء البيانات بالترويسة، يطلق على هذا الجزء اسم Segment، وعلى الفور بمجرد إنشاء Segments يتم تسليمها إلى طبقة الشبكة لإجراء معالجة مختلفة.

### الحزمة Packet

تقوم طبقة الشبكة بإنشاء رأس لكل segment قد استلمتها من طبقة النقل. وهذه الرأس تشتمل على معلومات مطلوبة للعنونة والتوجيه مثل عنوان الجهاز المصدر(المرسل) وعنوان الجهاز الهدف(المرسل إليه)، وبمجرد إضافة هذه

الرأس، يشار إلى segment بالحزمة packet. ويتم تسليم الحزم Packets إلى طبقة ربط البيانات.

يشار إلى المصطلح Packet في نموذج TCP/IP الأصلي بـ datagram. وكلا المصطلحين يشيران إلى حزمة البيانات data package. وهذه الحزمة تشتمل على ترويسة الشبكة و القطعة segment التي تم تغليفها.

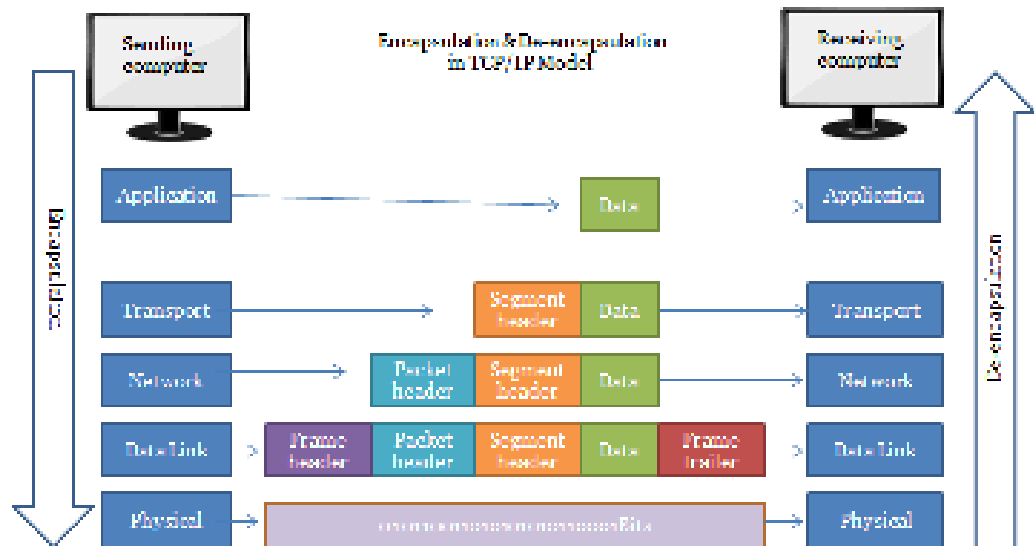
## الإطار Frame

تستلم طبقة ربط البيانات الحزم من طبقة الشبكة. خلافاً لما تقوم به كل من طبقة النقل وطبقة الشبكة من إنشاء رأس، فإنها أيضاً تنشئ تذييل مع الرأس لكل حزمة تم استلامها. يشتمل الرأس على المعلومات المطلوبة للتوجيه مثل عنوان المصدر وعنوان الوجهة. يشتمل التذييل على المعلومات المطلوبة لنقل الحزمة من المصدر إلى الوجهة. لفاسدة في المرحلة المبكرة لعملية التغليف de-encapsulation. بمجرد اضافة الرأس والتذييل بالحزمة، يمكن إطلاق الاسم frame وتعني الإطار عليها. ويتم تسليم الإطارات إلى الطبقة الفيزيائية.

## البتات Bits

تستلم الطبقة الفيزيائية الإطارات frames من طبقة ربط البيانات ثم تقوم بتحويلها إلى الصيغة تختلف باختلاف نوع الوسيط المستخدم في نقلها. على سبيل المثال، لو أن المضيف متصل من خلال كابل نحاسي، فإن الطبقة الفيزيائية ستقوم بتحويل الإطارات frames إلى فولتات. وإذا كان المضيف

متصل من خلال شبكة لاسلكية، فإن الطبقة الفيزيائية ستقوم بتحويل الإطارات frames إلى إشارات الراديو.



( ٢-٣ ) يوضح عملية تغليف البيانات في حالة الإرسال والاستقبال.

هذا يحدث خلال عملية الإرسال أما في الاستقبال فتحدث العملية العكسية: كما هو موضح في الشكل (٢-٣).

## عملية نزع التغليف De-encapsulation

عملية نزع التغليف De-encapsulation تحدث في الحاسوب المستقبل. في عملية فك التغليف، فإن الترويسة والتذييل اللذان تمت إضافتهما في عملية تغليف البيانات يتم إزالتها.

تتسلم الطبقة الفيزيائية الإشارات المشفرة من الوسيط وتقوم بتحويلها إلى إطارات وتسليمها إلى طبقة ربط البيانات.

تقوم طبقة ربط البيانات أولاً، بقراءة تذييل الإطار للتأكد من أن الإطار الذي تم استلامه بالشكل الصحيح. ثم تقوم بقراءة بقية الإطار فقط إذا كان الإطار صحيح.

إذا كان الإطار خالي من الأخطاء، فإنه يتم فحص عنوان الجهاز المرسل إليه لتحديد ما إذا كان وصل إلى وجهته الصحيحة أم لا.

إذا لم يكن الإطار مخصصاً له، فسيتم تجاهل هذا الإطار على الفور. أما إذا كان الإطار مخصصاً له، فسيتم إزالة الترويسة والتذييل من على الإطار، وعلا عندما يتم نزع الت والتذييل من الإطار، يصبح ket ويتم تسليم الحزم إلى بكة.

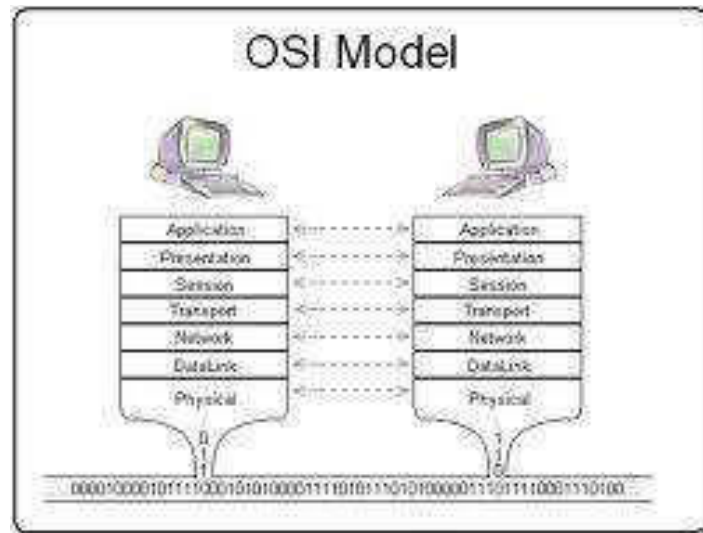
طبقة الشبكة تقوم بفحص عنوان الجهاز المستقبل في رأس كل حزمة packet. إذا كانت حزمة البيانات غير مخصصة له، فإن طبقة الشبكة سوف تتجاهل تلك الحزمة على الفور. وإذا كانت الحزمة مخصصة له، فستقوم بنزع الترويسة. وعلى الفور عند نزع الترويسة، ستتحول الحزمة packet إلى قطعة segment. يتم تسليم segments إلى طبقة النقل.

تقوم طبقة النقل باستلام القطع segments من طبقة الشبكة. ومن خلال ترويسات القطع segments تجمع طبقة الشبكة المعلومات الضرورية واعتماداً على هذه المعلومات تعيد ترتيب كل القطع في ترتيبها الصحيح. ثم، يتم نزع

ترويسة القطعة من كل القطع وتمثيلها بتدفق عادي للبيانات. ويتم تسليم تدفق البيانات إلى الطبقات العليا.

الطبقات العليا تقوم بترجمة تدفق البيانات إلى الصيغة التي يمكن أن يفهم بها التطبيق المستهدف.

وبذلك نحصل على بيانات التطبيق التي أرسلت من قبل الجهاز المصدر من خلال ذلك يبدو أن كل طبقة في جهاز الإرسال متصلة مع نظيرتها في جهاز الاستقبال عبر قناة وهمية، كما في الشكل التالي:



شكل (٣-٣) يوضح قنوات الاتصال الوهمية بين جهازين

## طبقات النموذج المرجعي OSI

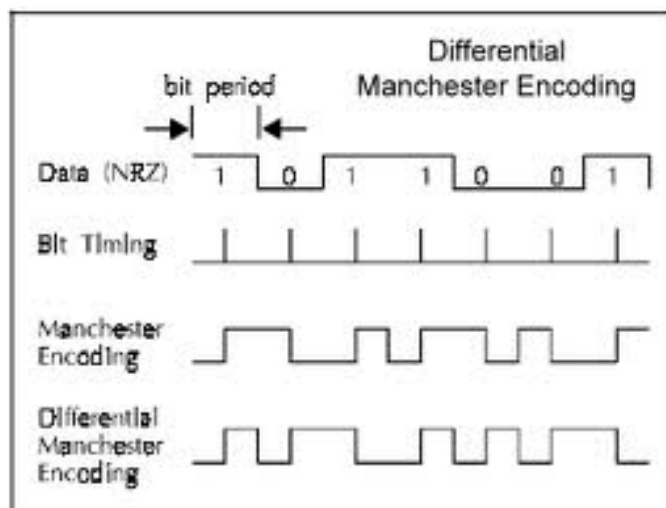
### أولاً: الطبقة الفيزيائية

تحدد هذه الطبقة كل ما يتعلق بالمكونات المادية اللازمة لتشبيك جهاز كمبيوتر على الشبكة كمحول الشبكة أو بطاقة الشبكة ونوع الأسلاك والوصلات المستخدمة كالأسلاك النحاسية (المحوري أو الزوج الملتوي) والألياف البصرية وأيضاً تحدد نوع الإشارة المولدة التي تمثل البيانات المرسله كالإشارات الكهربائية، الالكترومغناطيسية والضوئية.

في حالة الإرسال تخدم الطبقة الفيزيائية طبقة ربط البيانات التي تحدد نوع التكنلوجيا المستخدمة كبروتوكول Eth أو Token Ring.

بالنسبة للنبضات الالكترونية التي تمثل البيانات المرسله على الكبل، تستخدم أنظمة Ethernet نظام ترميز يسمى Manchester encoding، أما أنظمة Token Ring فتستخدم ترميزاً يسمى Differential Manchester ويبين الشكل التالي كلا النظامين.

في حالة الاستقبال تحول هذه الطبقة النبضات الالكترونية أو الالكترومغناطيسية أو الضوئية إلى بتات ثنائية لغرض معالجتها من قبل طبقة ربط البيانات.



شكل ( ٣-٤ ) يوضح الطبقة الفيزيائية في نقل البيانات

## ثانياً: طبقة ربط البيانات

### - الدور الذي تقوم به طبقة ربط البيانات

تحدد هذه الطبقة الأجهزة والمعدات اللازم شراؤها لبناء الشبكة، لأنه في هذه المرحلة يتم تحديد التكنولوجيا المستخدمة في الشبكة. ان طبقة ربط البيانات تضيف لبيانات طبقة الشبكة ترويسة وتذييل ثم تمرر الإطار إلى الطبقة الفيزيائية ومن بعد ترسل البيانات على الشبكة، ففي الترويسة توضع العناوين العتادية أو عناوين التحكم بالوصول للوسيط (MAC Address) للجهاز المرسل والمستقبل وهذا النوع من العناوين قد تم توليده من طرف طبقة الشبكة بواسطة عملية حل العناوين (ARP Address Resolution Protocol) ويمكننا هذا النوع من العناوين من الربط بين جهازين على نفس الشبكة المحلية.



بروتوكولات طبقة ربط البيانات

من البروتوكولات الشائعة الاستخدام في هذه الطبقة نذكر بروتوكول Ethernet، بروتوكول Token Ring أو بروتوكول PPP.

وتتخصص بروتوكولات طبقة ربط البيانات بالاتصالات مع أجهزة من نفس الشبكة المحلية. العنوان العتادي في الترويسة يشير دائماً إلى كمبيوتر على نفس الشبكة المحلية حتى ولو كان الجهاز النهائي المقصود الوصول إليه موجود على شبكة أخرى.

ويحتوي إطار بروتوكول طبقة ربط البيانات على رمز يحدد أي بروتوكول قد استخدم في طبقة الشبكة وفي الإطار أيضاً معلومات للكشف عن الأخطاء، هكذا مع بروتوكول طبقة ربط البيانات في الجهاز المستقبل م البروتوكول الذي استخدم في الإرسال، أما بالنسبة لكشف الأخطاء فالجهاز المرسل يؤدي عملية حسابية على محتوى بيانات رزمة الإطار ثم يرسل الناتج في تذييل الإطار وعند استقباله للبيانات يؤدي الجهاز المستقبل نفس العملية على محتوى البيانات المستقبلية ثم يقارن النتيجة المحصل عليها مع النتيجة المرسل، إذا كانت قيم النتائج متشابهة فيمرر بروتوكول طبقة ربط البيانات المعلومات إلى الطبقة العليا وفي حالة اختلاف النتائج فيرسل النظام المستقبل رسالة للنظام المرسل يطلب إعادة إرساله آخر الإطار.

### ثالثاً: طبقة الشبكة

تكون هذه الطبقة مسئولة عن الاتصالات بين الأجهزة الطرفية، والتي قد تكون على شبكات مختلفة، في حين أن طبقة ربط البيانات تعمل فقط للربط على الشبكة المحلية، بروتوكولات طبقة الشبكة مسئولة عن الرحلة الكاملة لرزم البيانات وهذا من الجهاز المصدر أو المرسل إلى الجهاز الهدف أو الوجهة النهائية، سواء كانت هذه الأجهزة على شبكة محلية جامعة أو شبكة موسعة.

في حالة الإرسال تضيف طبقة الشبكة لبيانات طبقة النقل ترويسة تتضمن مهام هذه المرحلة. من بين الحقول التي تتضمنها الترويسة حقل يدل على عنوان المصدر وآخر يدل على عنوان الوجهة النهائية للرسالة. عناوين IP هي عناوين لها ٣٢ بت تستخدمها أجهزة الكمبيوتر وبعض أنواع الطابعات بشكل فريد وهذا لغرض تمكين هذه الأخيرة من الاتصال وتبادل المعلومات على الشبكة.

طبقة الشبكة هي المسئولة عن التوجيه (Routing) وهذا لإعطاء البيانات إمكانية التنقل والوصول إلى وجهتها الأخيرة مهما كان حجم الشبكة كشبكة الانترنت مثلاً. في حالة التوجيه نشير للأجهزة المرسل والمستقبل للبيانات إلى أنها أنظمة طرفية، أما الموجهات فيشار إليها بأنها أنظمة انتقالية، ففي الأنظمة الطرفية تنتقل البيانات من أعلى إلى أسفل طبقة في الإرسال ومن أسفل إلى

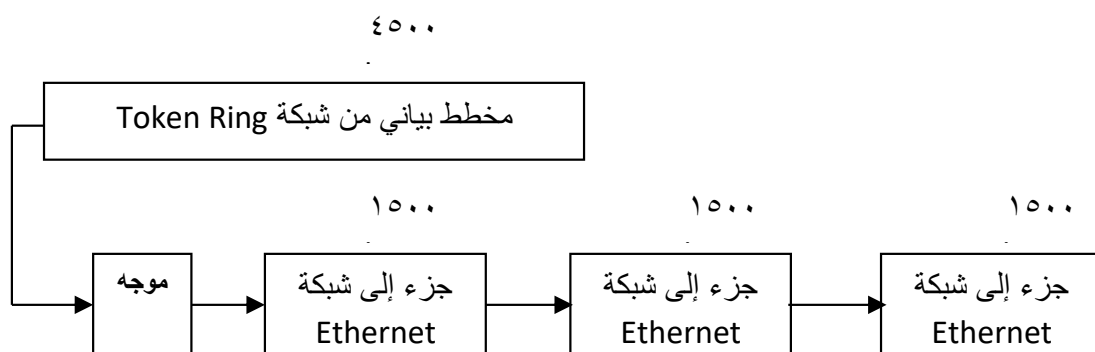
أعلى طبقة في الاستقبال، أما في الأنظمة الانتقالية فأقصى طبقة تصل إليها البيانات هي طبقة الشبكة.

تحتفظ الموجهات بمعلومات عن الشبكة ضمن جداول تحتوي على عناوين الموجهات اللازم المرور عليها حتى تصل البيانات إلى وجهتها النهائية.

### بروتوكولات طبقة الشبكة

من البروتوكولات الأكثر استخداماً لطبقة الشبكة بروتوكول الانترنت (Internet col). هناك لات أخرى كبروتوكول تبادل ا على الشبكات الجامعة (IPX) (Internetwork Packet Exchange) لشبكات Nvell Netware وبروتوكول Netbeui لشبكات Windows.

من المعلومات التي تتضمنها الترويسة هي عملية تجزئة المخطط البياني (Datagram) في حالة نقل البيانات على بروتوكولين مختلفين في طبقة ربط البيانات كالمرور من شبكة Token Ring إلى شبكة Ethernet وهذا لأن أقصى حجم لإطار يستطيع البروتوكول Token Ring نقله هو ٤٥٠٠ بايت بينما يكون هذا الحجم ١٥٠٠ بايت في حالة Ethernet .



شكل (٣-٥) يوضح عملية تجزئة المخطط البياني

### بروتوكول الانترنت IP

بروتوكول IP هو أحد أهم العناصر في طقم بروتوكولات TCP/IP لذلك من أي جهاز مو ي على أي جهاز مو بكة أن يكون له عنوان IP سواء كان محلية أو شبكة مو لانتترنت. وبما أن طبقة الشبكة (Network Layer) هي المسؤولة عن الاتصال بين جهازين مهما كان موقعهما وبما أن بروتوكول IP هو العمود الفقري لطبقة الشبكة. فالاستغناء عن هذا البروتوكول يؤدي الى عزل الجهاز عن الشبكة.

عناوين IP هي عبارة عن أرقام ثنائية طولها ٣٢ بت مقسمة الى أربع أجزاء بواسطة نقاط يحتوى كل جزء على ٨ بت، كل جزء من هذه الأجزاء له قيمة تتراوح بين صفر و ٢٥٥ يطلق على هذه الصيغة اسم التدوين الثنائي ذو النقاط (Dotted Binary Notation) لكي يسهل التعامل عملياً مع هذه السلاسل الثنائية ذات ٣٢ بت ويستخدم في بعض الحالات الأرقام العشرية بدلاً من الثنائية حينئذ تطلق على هذه الصيغة التدوين

العشري ذي النقاط (Dotted Decimal Notation)، تدل كل قيمة من أي جزء من الأجزاء الأربع على المكافئ العشري للقيمة الثنائية لذلك الجزء، فمثلاً:

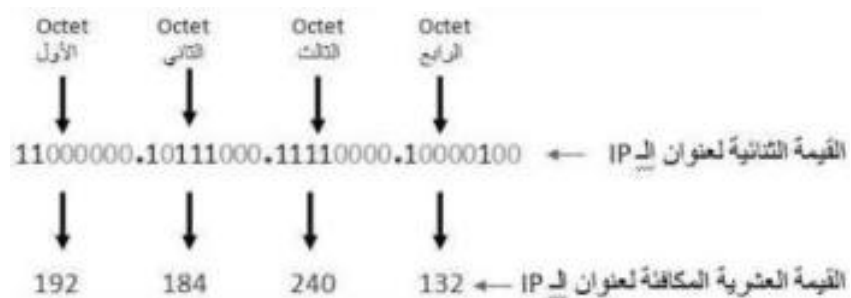
تدوين ثنائي ١١٠٠٠٠٠٠٠.١٠١١١٠٠٠.١١١١٠٠٠٠.١٠٠٠٠١٠٠

يكافئ

بالتدوين العشري

١٩٢.١٨٤.٢٤٠.١٣٢

يطلق على كل جزء من الأجزاء الأربع التي يتألف منها عنوان IP اسم Octet (ثمانية) أو مجموعة ٨ بت، كما هو موضح في الشكل التالي:



تحتوي بعض الأجهزة على عنوان IP واحد وفريد والبعض على أكثر من عنوان. بما أن كل محول شبكة يحتوي على عنوان، فقد يكون لبعض الأجهزة كالموجهات والتي تحتوي على بطاقتين شبكة على الأقل أكثر من عنوانين IP، عنوان IP لكل محول، وإذا كان الموجه موصل بالانترنت عبر المودم فيحتاج في الأخير هذا الجهاز الى عنوان IP ثالث على

الأقل. تعتبر عملية بناء، تعيين وتكوين عناوين IP جزءاً أساسياً في عملية إدارة وصيانة الشبكات.

من الضروري أن يكون لكل محول شبكة عنوان IP فريد، وإذا حصل وكان لجهازين نفس عنوان IP، فلن يستطيع كلا الجهازين الاتصال مع الشبكة. يتألف أي عنوان IP من جزأين وهما مميز الشبكة ومميز المضيف.

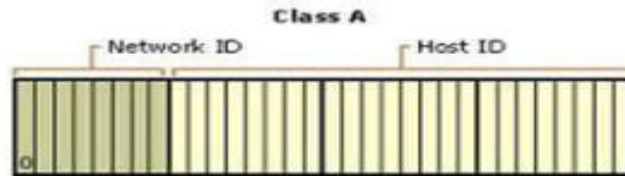
في حالة بناء شبكة محلية خاصة غير متصلة بالانترنت يمكن اختيار أي فئة وأي قيمة من العناوين المتاحة ولكن في حالة ربط شبكة محلية بالانترنت يتم تعيين مميزات الشبكة Network ID من قبل الجهة المانحة للأرقام المعينة على الانترنت IANA، وذلك لضمان عدم تكرار العناوين على ت حيث تسجل شركة ا يتم اعطاؤها مميز أو عنوان للشبكة وبعد ذلك يرجى الأمر لمدير الشبكة Administrator تعيين أرقام فريدة لمميزات المضيفات.

### فئات عناوين IP

يوجد خمس فئات مختلفة من عناوين IP لدعم الشبكات مختلفة الأحجام و هي الفئات A,B,C,D,E. الفئات الأساسية المستخدمة هي A,B,C أما الفئات D,E فهي مخصصة للبلاغات المتعددة (Multicasting) و أغراض تجارية، ونفرد بين الفئات في قيمة الثمانية بتات الأولى (Octet الأول).

## بالنسبة للفئة الأولى A:

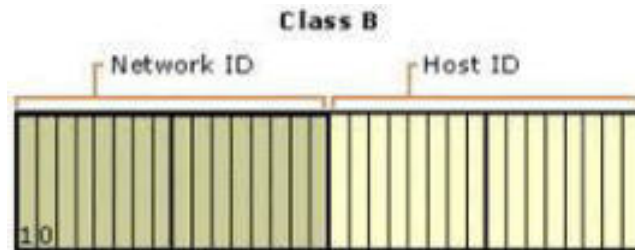
تبدأ الثمانية بتات الأولى بـ ٠ ومجالها يكون من ٠٠٠٠٠٠٠٠١ إلى ٠١١١١١١١ ما يعني عشرينياً من ١ إلى ١٢٧. ويظهر في الشكل التالي تنسيق لعنوان IP من الفئة A.



شكل (٦-٣) يوضح العنوان من الفئة A.

## بالنسبة للفئة B:

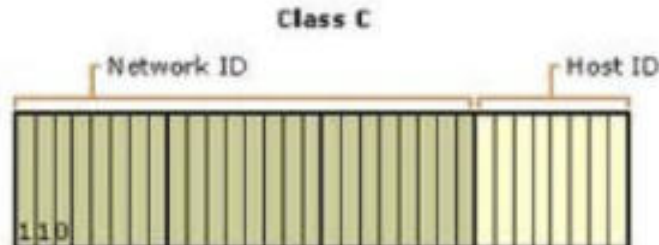
تبدأ العشرة بتات الأولى بـ ١٠ ويبرها يكون من ١٠٠٠٠٠٠٠٠ إلى ١٠١١١١١١١ ما يعني عشرينياً من ١٢٨ إلى ١٩١. ويظهر في الشكل التالي تنسيق لعنوان من فئة B.



شكل (٧-٣) يوضح العناوين من فئات B.

**بالنسبة للفئة C :**

فتبدأ الثمانية بتات الأولى بـ ١١٠ ومجال تغييرها يكون من ١١٠٠٠٠٠٠ إلى ١١٠١١١١١ ما يعادل عشرياً من ١٩٢ إلى ٢٢٣ ويظهر في الشكل التالي تنسيق لعنوان من فئة C.



شكل (٨-٣) يوضح العنوان من فئة C

**بالنسبة للفئة D:**

فتبدأ الثمانية بتات الأولى بـ ١١٠ ومجال تغييرها يكون من ١١١٠١١١١ إلى ١١١٠١١١١ (ن ٢٢٤ إلى ٢٣٩).

**بالنسبة للفئة E:**

فتبدأ الثمانية بتات الأولى بـ ١١١٠ ومجال تغييرها يكون من ١١١٠٠٠٠٠ إلى ١١١١٠١١١ (عشرياً من ٢٤٠ إلى ٢٤٧).

لذلك اذا كان لدينا عنوان IP فأول رقم من الأرقام الأربعة (Octet الأول) يدلنا على فئة العنوان، لكن كيف نتعرف على مميز الشبكة و مميز المضيف في عنوان ما؟

يوجد هناك علاقة بين مميز الشبكة في أي عنوان IP وفئة العنوان. إذا كان العنوان من فئة A فالثمانية بتات الأولى هي التي تميز الشبكة وباقي

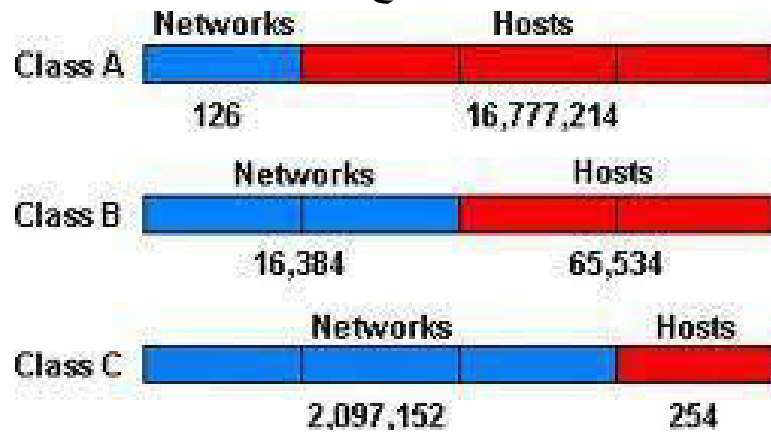


البتات يعنى ٢٤ تميز المضيف، اذا كان العنوان من فئة B، فمجموع الثمانية بتات الأولى مع الثمانية بتات الثانية يميز الشبكة و باقى البتات الست عشر تميز المضيف. أما اذا كان العنوان من فئة C فالثلاثة ثمانية بتات الأولى تميز الشبكة و الثمانية بتات المتبقية تميز المضيف. أى أن العنوان من فئة A يتقبل عدد كبير من المضيفات، و من فئة B عدد متوسط من المضيفات و من فئة C عدد صغير من المضيفات. فالشبكات من نوع A تكون ذات أحجام كبيرة. والشبكات من نوع C تكون شبكات ذات أحجام صغيرة. أما الشبكات من نوع B تكون شبكات متوسطة.

جدول (٣-١) يوضح فئات العناوين وعدد الأجهزة في كل فئة

فئة العنوان	من	إلى	عدد الشبكات	عدد الأجهزة في كل شبكة
A	١	١٢٦	١٢٦	١٦٧٧٧٢١٤
	١٢٨	٩١	١٦٣٨	٦٥٥٣٤
	١٩٢	٢٣	٢٠٩٧١	٢٥٤

فاجمالياً نستطيع أن نكون ١٢٦ شبكة من فئة A أو ١٦٣٨٤ شبكة من فئة B أو ٢٠٩٧١٥٢ شبكة من نوع C.



شكل (٣-٩) يوضح عدد الشبكات والأجهزة المتاحة لكل فئة من فئات العناوين.

## قواعد عناوين IP

يوجد بعض القواعد التي تستثني استخدام بعض القيم في بعض أجزاء العنوان IP وهي:

- ١- لا يمكن أن تكون قيم كل البتات في مميز الشبكة أصفاراً.
- ٢- لا يمكن أن تكون قيم كل البتات في مميز الشبكة أحاداً.
- ٣- لا يمكن أن تكون قيم كل البتات في مميز المضيف أصفاراً.
- ٤- لا يمكن أن تكون قيم كل البتات في مميز المضيف أحاداً.
- ٥- لا نستطيع استخدام قيمة ١٢٧ كميز أي شبكة لأنه محجوز لأغراض التشخيص.
- ٦- تستطيع كل شبكة من نوع A أن تتقبل ١٦٧٧٧٢١٤ مضيف أو جهاز، بالنسبة للشبكات من نوع B فبإمكانياتها استضافة ٦٥٥٣٤ جهازاً أما الشبكات من إنها لا تستطيع أن تتقب ٢٥ جهازاً فقط.

## أقنعة الشبكات الفرعية Subnet Masks

سوف نرى أن حصول أي جهاز على عنوان IP غير كاف لتمكين اتصاله مع أجهزة أخرى على الشبكة. حتى ولو كانت عناوين الأجهزة تنتمي لفئة واحدة من الفئات من المحتمل أن لا تتصل الأجهزة مع بعضها ولذلك من الضروري الأخذ بعين الاعتبار عامل من العوامل الأساسية في عملية بناء الشبكات والذي يدعى قناع التفرع Subnet Mask .

يحدد قناع الشبكة الفرعية أي البتات في عنوان IP تمثل مميز الشبكة وأياها تمثل مميز المضيف. فالأحاد تميز الشبكة والأصفار تميز المضيف.

### Network Masks

Class A: 255.0.0.0  
Class B: 255.255.0.0  
Class C: 255.255.255.0

	1 <sup>st</sup> Byte	2 <sup>nd</sup> Byte	3 <sup>rd</sup> Byte	4 <sup>th</sup> Byte
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

شكل (١٠-٣) يوضح أقنعة الشبكات.

### بالنسبة للعناوين من فئة A:

تكون القيمة الافتراضية لقناع الشبكة الفرعية تساوي: ٢٥٥,٠,٠,٠، ما يعادل ثنائياً: ١١١١١١١,٠٠٠٠٠٠٠٠,٠٠٠٠٠٠٠٠,٠٠٠٠٠٠٠٠. مما يدل أن الثمانية بتات الأولى والتي تتمثل بثمانية أحاد تميز الشبكة والأربعة وعشرون بتات المتبقية والتي تتمثل بأربعة وعشرين صفرًا تميز المضيف.

### بالنسبة للعناوين من فئة B:

تكون القيمة الافتراضية لقناع الشبكة الفرعية تساوي: ٢٥٥,٢٥٥,٠,٠، ما يعادل ثنائياً: ١١١١١١١,١١١١١١١,٠٠٠٠٠٠٠٠,٠٠٠٠٠٠٠٠. وهذا يعني أن الست عشرة بتات الأولى (أحاد) تميز الشبكة والست عشرة بتات المتبقية (أصفار) تميز المضيف (عنوان الجهاز في الشبكة).

## أما بالنسبة للعناوين من فئة C :

تكون القيمة الافتراضية لقناع الشبكة الفرعية تساوي: ٢٥٥.٢٥٥.٢٥٥.٠ والذي يعادل ثنائياً ١١١١١١١١.١١١١١١١١.١١١١١١١١.٠٠٠٠٠٠٠٠ مما يعني أن الأربعة والعشرين بتات الأولى (آحاد) تمثل عنوان الشبكة والثمانية بتات الأخيرة (أصفار) تمثل عنوان المضيف.

إذا كان لدينا عنوان من فئة A فانه من المستحيل تكوين شبكة محلية من خلاله تحتوي على أكثر من ستة عشر مليون مضيف أو جهاز، حتى إذا تم ذلك فستصبح عيوب الشبكة أكبر من مزاياها، و غالباً ما تظهر هذه العيوب في صعوبة إدارة و صيانة الشبكة، بالإضافة إلى تدهور في أداء الشبكة و الذي في ببطء عملية الات بين الأجهزة و هذا البطء ناتج عملية تبادل الرسائل كالبث أو التبريلغ (Broadcast). لذا من الضروري إجراء عملية تفريع للشبكة (Subnet)، لان هذه العملية تحسن من أداء الشبكة الذي يتمثل في ارتفاع سرعة إرسال و استقبال البيانات. لان نطاقات التصادم، تبادل الرسائل و البلاغات تصبح محددة بفرع من فروع الشبكة الذي تكون فيه عدد الأجهزة أقل بكثير من الشبكة الجامعة الغير مفرعة. و في حالة تفريع الشبكة يتكون عنوان IP من ثلاثة أجزاء و هي مميز الشبكة Net ID و مميز الشبكة الفرعية Subnet ID و مميز المضيف Host ID. ويوضح الشكل التالي تنسيق لعنوان IP قبل وبعد عملية التفريع.

### مثال عن قناع الشبكة الفرعية Subnet Mask

Class B address 190.52.0.0

Class B	Network	Network	Host	Host
---------	---------	---------	------	------

باستخدام القناع /24  
يمكن أن تصبح لدينا  
الشبكات الفرعية

Network	Network	Subnet	Host
---------	---------	--------	------

190.52.1.2  
190.52.2.2  
190.52.3.2

لكن بقيت موجهات الإنترنت *Internet* ترى جميع هذه  
الشبكات الفرعية على أنها الشبكة 192.52.0.0  
في حين أن الموجهات الداخلية المحلية تميز هذه الشبكات  
على أنها شبكات منفصلة.

شكل (١١-٣) يوضح عنوان من الفئة B قبل وبعد عملية التفريع

لكي تتمكن الأجهزة أن تتصل مع بعضها في نفس الشبكة الفرعية أو دون المرور عبر موجه (Router) فإنه من الضروري أن يكون لهذه الأجهزة نفس مميز الشبكة ونفس مميز الشبكة الفرعية. تؤدي عملية استخدام هذه الأقد تجزئة أي عنوان شب فئة A إلى عناوين من فئة B أو كذلك الأمر إذا أردنا تجزئة عنوان من فئة B إلى عناوين من فئة C.

**مثال:**

عنوان شبكة من فئة C بقيمة ١٩٤.٥٣.٦٩.٠ والذي نريد تقسيمه إلى شبكات فرعية. إذا استخدمنا ٣ بتات من البايث الرابع (آخر ثمانية بتات) لمميز الشبكة الفرعية فالخمس بتات المتبقية تكون مخصصة لمميز المضيف. وتكون قيمة قناع التفرع الخاصة بهذه الحالة كما يلي:

١١١١١١١١.١١١١١١١١.١١١١١١١١.١١١٠٠٠٠٠٠٠  
عشرياً القيمة التالية: ٢٢٤.٢٥٥.٢٥٥.٢٥٥ لأن ٢٢٤ هو المكافئ العشري  
للقيمة الثنائية ١١١٠٠٠٠٠٠ وهكذا يكون لدينا مميز الشبكة بطول ٣ بت  
ومميز المضيف بطول ٥ بت.

من خلال هذا نستطيع أن نستخلص أن عدد الاحتمالات أو الحالات التي  
نستطيع أن نحصل عليها من خلال ٣ بت هي ٨ أي  $2^3$  وتتمثل هذه القيم  
في: ١١١, ١١٠, ١٠١, ١٠٠, ٠١١, ٠١٠, ٠٠١, ٠٠٠

وكما ذكرنا في قواعد IP فإنه من غير الممكن أن تكون قيمة أي مميز شبكة  
كلها أصفار أو كلها آحاد فلذلك يمكن أن يأخذ مميز الشبكة الفرعية ذو ٣  
بتات دة من القيم الآتية: ٠١, ١١٠, ١٠١, ١٠٠, ٠١١

أما بالنسبة للخمس بتات التي تميز المضيف، فنستطيع من خلالها أن نحصل  
على عدد ٣٢ أي  $2^5$  من الاحتمالات والتي تتمثل في القيم  
التالية: ١١١١١, ١١١١٠, ..., ٠٠٠١١, ٠٠٠١٠, ٠٠٠٠١, ٠٠٠٠٠

هذا مع العلم بأنه غير ممكن لأي مميز مضيف أن يكون كله  
أصفار (٠٠٠٠٠) أو آحاد (١١١١١)، فلذلك يتبقى لنا ٣٠ قيمة تستطيع  
الأجهزة أن تتميز بها في أي شبكة فرعية والتي هي القيم العشرية التي تتراوح  
بين ١ (٠٠٠٠١) إلى ٣٠ (١١١١٠).

وهذا يعني عملياً أن استخدامنا لقناع تفرع ذي قيمة ٢٥٥.٢٥٥.٢٥٥.٢٢٤ يؤدي إلى إنشاء ستة شبكات فرعية تحتوي كل واحدة منها على ٣٠ مضيفاً.

المطلوب هو إيجاد عناوين الشبكات الفرعية التي نحصل عليها بعد ما اخترنا مميز المضيف كله أصفار. علماً أننا تعاملنا ثنائياً مع آخر ثمانية بتات وهذا لغرض التبسيط:

عنوان الشبكة الأولى: استخدام ٠٠١٠٠٠٠٠ يؤدي إلى ١٩٤.٥٣.٦٩.٣٢

عنوان الشبكة الثانية: استخدام ٠١٠٠٠٠٠٠ يؤدي إلى ١٩٤.٥٣.٦٩.٦٤

عنوان الشبكة الثالثة: استخدام ٠٠٠٠٠٠٠٠ يؤدي إلى ١٩٤.٥٣.٦٩.٩٦

عنوان الشبكة الرابعة: استخدام ١٠٠٠٠٠٠٠ يؤدي إلى ١٩٤.٥٣.٦٩.١٢٨

عنوان الشبكة الخامسة: استخدام ١٠١٠٠٠٠٠ يؤدي إلى ١٩٤.٥٣.٦٩.١٦٠

عنوان الشبكة السادسة: استخدام ١١٠٠٠٠٠٠ يؤدي إلى ١٩٤.٥٣.٦٩.١٩٢

لنرى الآن عناوين الأجهزة في كل من الشبكات الفرعية، الخمس بتات الخاصة بمميز المضيف والتي تتراوح ثنائياً بين ١١١١٠ و ٠٠٠٠١ وهذا بعد استخدامنا للقيم الممكن تقبلها في كل شبكة تكون عناوين الأجهزة في الشبكات الفرعية الستة كما يلي:

### في الشبكة الأولى

من ١٩٤.٥٣.٦٩.٣٣ إلى ١٩٤.٥٣.٦٩.٦٢

### في الشبكة الثانية

من ١٩٤.٥٣.٦٩.٦٥ إلى ١٩٤.٥٣.٦٩.٩٤

### في الشبكة الثالثة

من ١٩٤.٥٣.٦٩.٩٧ إلى ١٩٤.٥٣.٦٩.١٢٦

### في الشبكة الرابعة

من ١٩٤.٥٣.٦٩.١٢٩ إلى ١٩٤.٥٣.٦٩.١٥٨

### في الشبكة الخامسة

من ١٩٤.٥٣.٦٩.١٦١ إلى ١٩٤.٥٣.٦٩.١٩٠

### في الشبكة السادسة

من ١٩٤.٥٣.٦٩.١٩٣ إلى ١٩٤.٥٣.٦٩.٢٢٢



إذا أردنا الحصول على عناوين التبليغ في كل من الشبكات الفرعية فما علينا إلا أخذ مميز المضيف كله آحاد يعني ١١١١١. تكون عناوين التبليغ (Broadcast Addresses) لكل من الشبكات الفرعية كالآتي:

عنوان تبليغ الشبكة الأولى: ١٩٤.٥٣.٦٩.٦٣

عنوان تبليغ الشبكة الثانية: ١٩٤.٥٣.٦٩.٩٥

عنوان تبليغ الشبكة الثالثة: ١٩٤.٥٣.٦٩.١٢٧

عنوان تبليغ الشبكة الرابعة: ١٩٤.٥٣.٦٩.١٥٩

عنوان تبليغ الشبكة الخامسة: ١٩٤.٥٣.٦٩.١٩١

عنوان تبليغ الشبكة السادسة: ١٩٤.٥٣.٦٩.٢٢٣

فمن هذه النتائج نستطيع ستخلص عدة أشياء منها: عند الأجهزة التي تستطيع أن تتصل مع بعضها دون اللجوء إلى موجه، كالأجهزة التي تحمل العناوين التالية ١٩٤.٥٣.٦٩.٩٩ و ١٩٤.٥٣.٦٩.١٢٠.

العناوين غير الممكن استخدامها عندما نجزئ شبكة ذات عنوان ١٩٤.٥٣.٦٩.٠ بواسطة قناع ٢٥٥.٢٥٥.٢٥٥.٢٢٤ كالعنوان ١٩٤.٥٣.٦٩.٩٦ والذي يكون مخصصاً كعنوان شبكة فرعية والعنوان ١٩٤.٥٣.٦٩.١٥٩ الذي يكون بدوره محجوز كعنوان تبليغ لشبكة فرعية.

كل هذا يساعد في عملية إعطاء العناوين للأجهزة بصفة سليمة ودون الوقوع في خطأ.

## رابعاً: طبقة النقل

تتم طبقة النقل خدمات طبقة الشبكة فلذلك نلاحظ أن هناك انسجماً بين بروتوكولي هذه الطبقات وعلى سبيل المثال نذكر TCP/IP ، IP لطبقة الشبكة و TCP لطبقة النقل كذلك الوضع فيما يخص SPX/IPX ، IPX لطبقة الشبكة و SPX بروتوكول يخدم طبقة النقل.

### بروتوكولات طبقة النقل

في هذا النوع من الطبقات تنقسم البروتوكولات إلى نوعين، بعضها تقدم خدمات تعتمد الاتصال والأخرى عد اتصال. من البروتوكولات التي خدمات تعتمد على الاتصال بروتوكول TCP (بروتوكول التحكم في النقل)، أما بالنسبة للنوع الثاني عديمة الاتصال فمنها بروتوكول المخطط البياني للمستخدم UDP (User Datagram Protocol) ففي حالة TCP يكون تبادل الرسائل مسبق بين النظامين لتأسيس اتصال بينهما. يظهر هذا من خلال الترويسة التي يضيفها TCP للطبقات العليا والتي غالباً ما تكون ٢٠ بايت. أما فيما يخص UDP يكون طول الترويسة ٨ بايت وهذا لسبب كون TCP يقدم خدمات إضافية لا يستطيع أن يوفرها UDP.

## الخدمات التي يقدمها TCP

### ١- الإشعار باستلام الرزم (Packet Acknowledgment)

من خلال هذه الرسائل يستطيع النظام المرسل للبيانات أن يتواصل في عملية إرساله ومن خلال هذه العملية نرى موثوقية هذا النوع من البروتوكولات.

### ٢- تقطيع البيانات (Data Segmentation)

أي عملية على الشبكة تولد سلسلة من البيانات، وفي بعض الأحيان يكون حجم البيانات المتبادلة على الشبكة كبير مثل ما يحدث في عملية نقل الملفات أو الـ فيكون من غير المعقول سل أو يستقبل جهاز ما كميات من المعلومات دفعة واحدة، وهذا ما يعرض الشبكة لبطء ملحوظ لكون جهاز واحد يستخدم الشبكة والأجهزة الأخرى متوقفة.

والسبب الثاني يظهر عيوبه في حالة حدوث خطأ في الإرسال مما يسبب النظام المرسل من إعادة عملية الإرسال من جديد، لذلك نلاحظ أن عملية تقطيع البيانات تمكن كل الأجهزة بالتناوب على استخدام الشبكة (جهاز ما يرسل جزء ويعطي الفرصة لجهاز آخر).

وفي حالة حدوث خطأ في إعادة إرسال الجزء المعني بالأمر بدلاً من إعادة المحاولة لكل بيانات الملف.

## ٣- ترقيم وترتيب الأجزاء المرسل

عندما ترسل أجزاء ملف على الشبكة، هناك احتمال أن تصل هذه الأجزاء في ترتيب غير سليم لسبب اتخاذ الرزم لمسارات مختلفة، بعضها مزحومة والأخرى على مسافات بعيدة....الخ، فهذه الطبقة وبالأخص TCP هو الذي سيكون المسئول عن عملية ترتيب هذه الأجزاء وتجميعها.

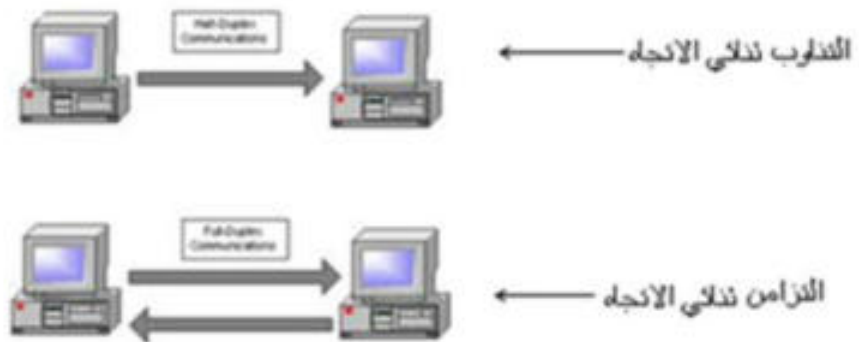
ويتميز TCP أيضاً بإمكانية توجيه التطبيقات إلى المنافذ اللازمة (Ports) في الجهاز المستقبل.

أما في بروتوكولات عديمة الاتصال مثل UDP يرسل النظام المرسل معلوماته ببساطة إلى النظام المستقبل دون علم إن كان هذا النظام جاهز لاستلام البيان إن كانت هذه البيانا ت، أو إن كانت وصلت بدون خلال استلامها من قبل الجهاز المستقبل. يستخدم هذا النوع من البروتوكولات في الحالات التي لا يتطلب فيها تبادل المعلومات ووصولها إلى وجهتها النهائية من المتطلبات الأساسية.

وكذلك لبروتوكول TCP في طبقة النقل إمكانية التحكم في جريان البيانات وكشف وتصحيح الأخطاء كما سيتم توضيح ذلك فيما بعد.

## خامساً: طبقة الجلسة

طبقة الجلسة هي المسؤولة عن تنظيم الحوار (Dialog Control) ما نعنيه بالحوار هو تبادل المعلومات بين نظامين على الشبكة، يحدث في هذه المرحلة اختيار الأسلوب الذي يستخدمه النظامان لتبادل الرسائل، من الأساليب الشائعة في أي عملية اتصالات نستطيع أن نذكر أسلوب التناوب ثنائي الاتجاه (Two Way Alternate) أو ما يعرف في بعض الحالات بـ (Half Duplex)، يكون في هذه الحالة تبادل المعلومات في اتجاهين يعني من الجهاز الأول إلى الجهاز الثاني ومن الثاني إلى الأول ولكن لا يسمح سوى لنظام واحد أن يرسل في نفس الوقت أما النظام الثاني فسيكون في حالة استقبال فقط، أما الأسلوب الآخر لتزامن ثنائي الاتجاه (Two Way Simultaneous) أو ما يعرف بـ (Full Duplex) في هذه الحالة يكون في إمكانية الجهازين الإرسال والاستقبال في نفس الوقت.



شكل (١٢-٣) يوضح كلاً من التزامن ثنائي الاتجاه و التناوب ثنائي الاتجاه.

**مهمة طبقة الجلسة:** مهمة هذه الطبقة هي التنظيم والتحكم في بدء الحوار، نقل البيانات وإنهاء الاتصال. ولهذه الطبقة إمكانية الاحتفاظ بعينه من آخر جزء مرسل حتى تتمكن من معرفة النقطة التي ابتداءً منها سوف تعاد عملية الإرسال وهذا في حالة عطل الشبكة ثم عودتها للعمل من جديد.

### سادساً: طبقة التقديم

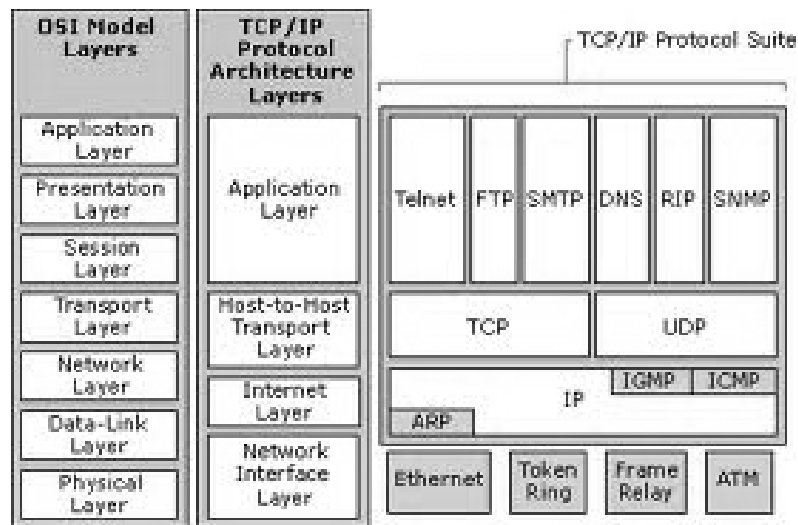
تقوم هذه الطبقة بترجمة الصيغة بين الأنظمة المختلفة، عندما يقوم المستخدم بأي عملية على الجهاز فهذه الطبقة هي التي تكون مسئولة عن ترجمة هذه العملية إلى لغة الكمبيوتر، ومن أنواع الترجمة التي نستطيع ذكرها هي عملية الترميز (Coding) لأي حرف مثلاً بمقابلته في شفرة ASCII ، عملية ضغط البيانات (Data Compressi) تمثل في آلية لتخفيض حجم البيا المرسل على الشبكة عن طريق إلغاء المعلومات المكررة، والغرض من هذه العملية هو إمكانية نقل البيانات بسرعة على الشبكة. وعملية تشفير البيانات (Data Encryption) التي تتمثل في آلية لحماية البيانات المرسله .

لكي تنتقل البيانات بأمان في الشبكة، كل هذه العمليات ممكنه في حالة الإرسال، أما في حالة الاستقبال عند استلام البيانات من طبقة الجلسة فستحدث العملية العكسية وهي فك التشفير (Decryption) وفك الضغط (Decompression) وترجمة الرموز ASCII إلى حروف يستطيع المستخدم استغلالها.

## سابعاً: طبقة التطبيق Application Layer

تقدم معظم بروتوكولات طبقة التطبيق خدمات تستخدمها البرامج للوصول إلى الشبكة. ومن التطبيقات الشائعة في الشبكات نذكر بروتوكول نقل الملفات FTP (File Transfer Protocol) وبروتوكول نقل البريد البسيط SMTP (Simple Mail Transfer Protocol) الذي يستخدم في تبادل الرسائل الإلكترونية (E-Mails).

نرى في الشكل التالي الطبقات السبع والبروتوكولات المستخدمة على مستوى كل طبقة.



شكل (١٣-٣) يوضح البروتوكولات على مستوى كل طبقة

## النموذج TCP/IP للاتصال بالانترنت

الطبقات الأربعة لبروتوكول TCP/IP التي تؤدي المهام المطلوبة في

نموذج OSI هي:

١- طبقة التطبيقات و الخدمات.

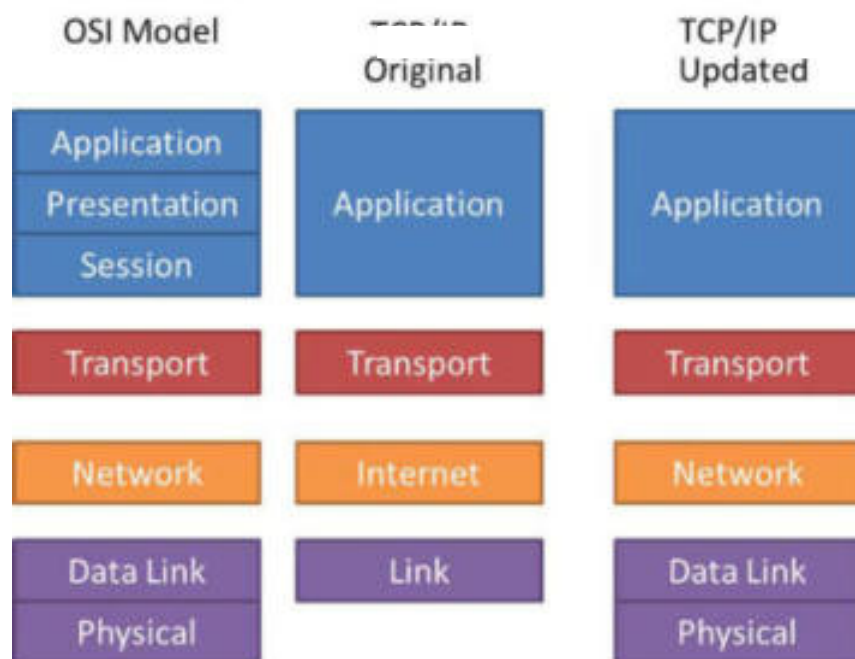
٢- طبقة النقل.

٣- طبقة الاتصال بالانترنت.

٤- طبقة الوصول الى الشبكة.

والشكل التالي يوضح الطبقات المكافئة لطبقات TCP/IP في نموذج

OSI المرجعي:



شكل (١٤-٣) يوضح الطبقات المكافئة لطبقات TCP/IP الأصلي وما تم تحديثه في

نموذج OSI المرجعي

إعداد د/ أميرة إبراهيم عبد الغني



## النموذج TCP/IP للاتصال بالانترنت

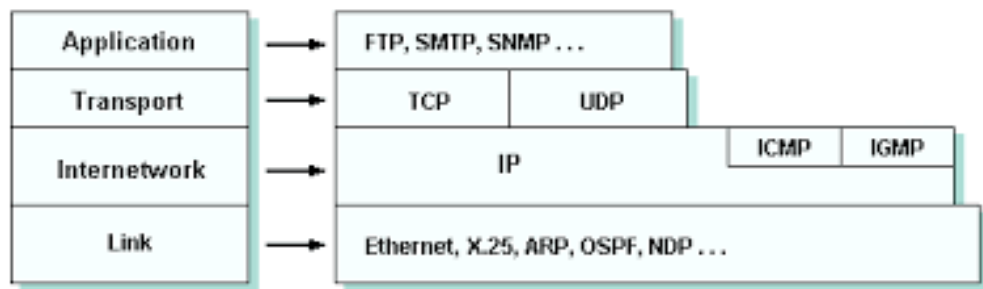
### أولاً: طبقة الوصول الى الشبكة

مهام طبقة الوصول الى الشبكة هي:

١- استخدام البروتوكولات اللازمة لإنشاء اطرار خاصة بالتكنولوجيا المستخدمة مثل بروتوكول Ethernet و بروتوكول Token Ring...الخ.

٢- تحويل البتات إلى اشارات كهربية أو الكترومغناطيسية أو ضوئية لغرض نقلها على الوسيط.

وتكافئ هذه الطبقة كلاً من طبقتي ربط البيانات والفيزيائية في نموذج OSI هذا أن مهمة هذه الـ طبقتين استخدام البروتوكولات اللازمة لإنشاء اطرار خاصة بالتكنولوجيا المستخدمة مثل بروتوكول Ethernet وبروتوكول Token Ring.....الخ.



شكل (١٥-٣) يوضح البروتوكولات على مستوى كل طبقة في TCP/IP.

ثانياً: طبقة الاتصال بالانترنت

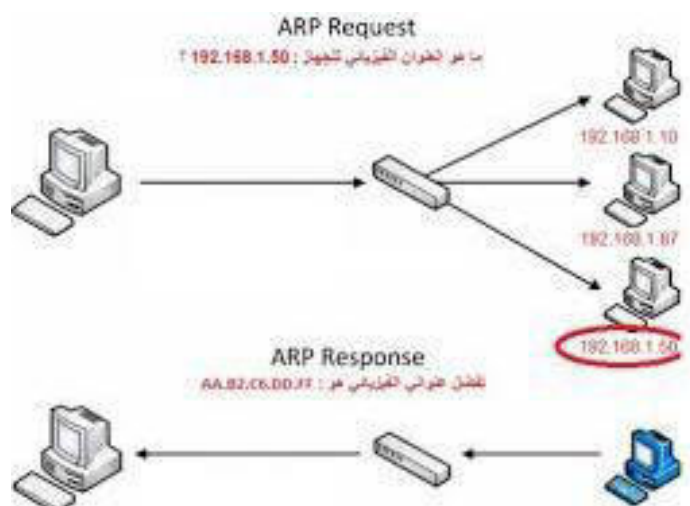
طبقة الاتصال بالانترنت هي المسؤولة عن امكانية الاتصال بين الأجهزة و من مهامها:

- ١- العنوان و التوجيه.
  - ٢- توفير المعلومات اللازمة الى طبقة الوصول الى الشبكة لكي تتمكن الأخيرة من ارسال اطاراتها على الشبكة .
  - ٣- توجيه البيانات على الشبكة الجامعة في حالة اذا كان الجهاز المستقبل على شبكة أخرى.
  - ٤- امكانية تبادل معلومات حول مشاكل أو أعطال الشبكة.
  - ٥- التبليغ المتعدد Multicasting و هذا بارسال معلومات معينة الى عدد هزة في نفس الوقت.
- وتستخدم طبقة الاتصال بالانترنت بروتوكول IP للعنوان وإرسال البيانات، لذا فان هذه الطبقة عديمة الاتصال وتكافئ طبقة الشبكة في نموذج OSI.

**بروتوكولات طبقة الاتصال بالانترنت**

### **بروتوكول حل العناوين ARP(Address Resolution Protocol**

دور بروتوكول حل العناوين ARP(Address Resolution هو تحويل عنوان IP لجهاز موجود على الشبكة المحلية إلى عنوانه العتادي الثابت و الفريد من نوعه. و هذا العنوان هو عنوان الواجهة إذا كان الجهازين على نفس الشبكة المحلية أو عنوان الموجه إذا كان الجهازان على شبكتين مختلفتين.



شكل (١٦-٣) يوضح عملية حل العناوين.

٢- بروتوكول RARP (Reverse Address Resolution Protocol): ومهمته هي تحويل أي عنوان عتادي إلى عنوان IP لإمكانية توصيل الجهاز بالشبكة.

يسند RA العنوان العتادي لا هذا لمخاطبة مزود العناوين CP لغرض إعطاء الجهاز عنوان IP وإمكانية توصيله بالشبكة.

٣- بروتوكول التحكم في رسائل الانترنت (ICMP): ومهمة بروتوكول ICMP Internet Control Message Protocol بروتوكول التحكم في رسائل الانترنت هي تبادل المعلومات حول مشاكل أو أعطال الشبكة.

٤- بروتوكول IGMP (Internet Group Management Protocol): ومهمته هي أنه بروتوكول ادارة مجموعات الانترنت و هو المسئول عن عملية التبليغ المتعدد Multicasting و هذا بارسال معلومات معينة الى عدد من الأجهزة في نفس الوقت.

## ثالثاً: طبقة النقل

تتولى طبقة النقل الخدمات اللازمة لتوفير اتصال موثوق بين الأجهزة، تكافئ هذه الطبقة طبقتي النقل و الجلسة في نموذج OSI الا أنها تحتوى على بعض أجزاء طبقات التقديم و التطبيقات في النموذج نفسه، و تحتوى هذه الطبقة على بروتوكولين و هما بروتوكول TCP و بروتوكول UDP.

### بروتوكولات طبقة النقل

#### ١ - بروتوكول TCP(Transmission Control Protocol)

بروتوكول TCP(Transmission Control Protocol) هو بروتوكول التد لنقل و يوفر خدمات تع الاتصال بين الأجهزة، و يعني هذا أنه لا تتم عملية تبادل البيانات بين الأجهزة الا في حالة اتصال مسبق بينها. و من مهمامه:

- ١- تجزئة و تجميع البيانات.
- ٢- الاشعار بالاستلام.
- ٣- تحديد المنافذ Ports.
- ٤- الكشف عن الأخطاء.
- ٥- ترقيم رزم البيانات.

## مهام بروتوكول TCP/IP

### ١ - تجزئة وتجميع البيانات:

لا يمكن لجهاز ما إرسال بياناته على الشبكة بصفة مستمرة لمدة من الزمن لأن هذا ينتج عيوب تؤدي إلى الانخفاض في أداء الشبكة. وتتمثل هذه العيوب في إجبار الأجهزة الأخرى على الانتظار وعدم الوصول إلى الشبكة حتى ينتهي الجهاز المرسل من تحويل كل بياناته.

وفي حالة حدوث خطأ خلال عملية الإرسال فمن الضروري إعادة محاولة إرسال كل البيانات مرة أخرى مما يسبب بطئاً ملحوظاً حتى على الجهاز المدبكة، فلذلك يستخدم بروتوكول TCP عملية تجزئة البيانات إلى لكي يكون هناك تناوب في استخدام الشبكة من قبل كل الأجهزة، وفي حالة حدوث خطأ ما يعيد الجهاز المرسل إرسال الجزء الخاص بالخطأ بدلاً من محاولة إرسال كل البيانات من جديد.

تحدث هذه العملية في حالة الاستعداد لعملية الإرسال، أما في حالة الاستقبال فتكون من مهام هذه الطبقة تجميع الرزم لغرض الحصول على بيانات تستغلها طبقة التطبيقات والخدمات.

## ٢ - الإشعار بالاستلام

في حالة استقبال رزمة من البيانات بدون خطأ يرسل الجهاز المستقبل للجهاز المرسل إشعار باستقبال واستلام مما يمكن الجهاز المرسل من متابعة إرساله للرزمة القادمة.

## ٣ - تحديد المنافذ Ports

من وظائف البروتوكول TCP إمكانية تمييز العملية التي ولدت البيانات الواردة من طبقة التطبيق. يحدد البروتوكول TCP أو UDP أرقام المنافذ التي من خلالها تعبر البيانات إلى مناطق معينة في ذاكرة الجهاز .

## ٤ - عن الأخطاء

من مهام طبقة النقل كشف الأخطاء التي بسببها يطلب من الجهاز المرسل إعادة محاولة إرساله لآخر رزمة من البيانات.

في حالة الإرسال يقوم النظام بإجراء عملية حسابية على إطار البيانات المرسل وترفق نتيجته العملية بذيل الإطار وعند استقبال البيانات يقوم النظام المستقبل بإجراء نفس العملية على البيانات المستقبلية. إذا كانت نتيجة العملية مطابقة للنتيجة المرفقة في ذيل الإطار يتابع النظام معالجته للبيانات، وفي حالة عدم مطابقة النتائج المرفقة والمحسوبة يقوم النظام بطلب إعادة إرسال البيانات مرة ثانية.

## ٥ - التحكم في الجريان

وتتحكم هذه الطبقة في جريان البيانات Flow Control و هذا توفيقاً مع ازدحام الشبكة، عدد المستخدمين وما إلى غير ذلك، غالباً ما يكون هذا التحكم عبارة عن رسائل مولدة من النظام المستقبل طالباً النظام المرسل من إسرار أو إبطاء عملية النقل.

## ٦ - ترقيم رزم البيانات

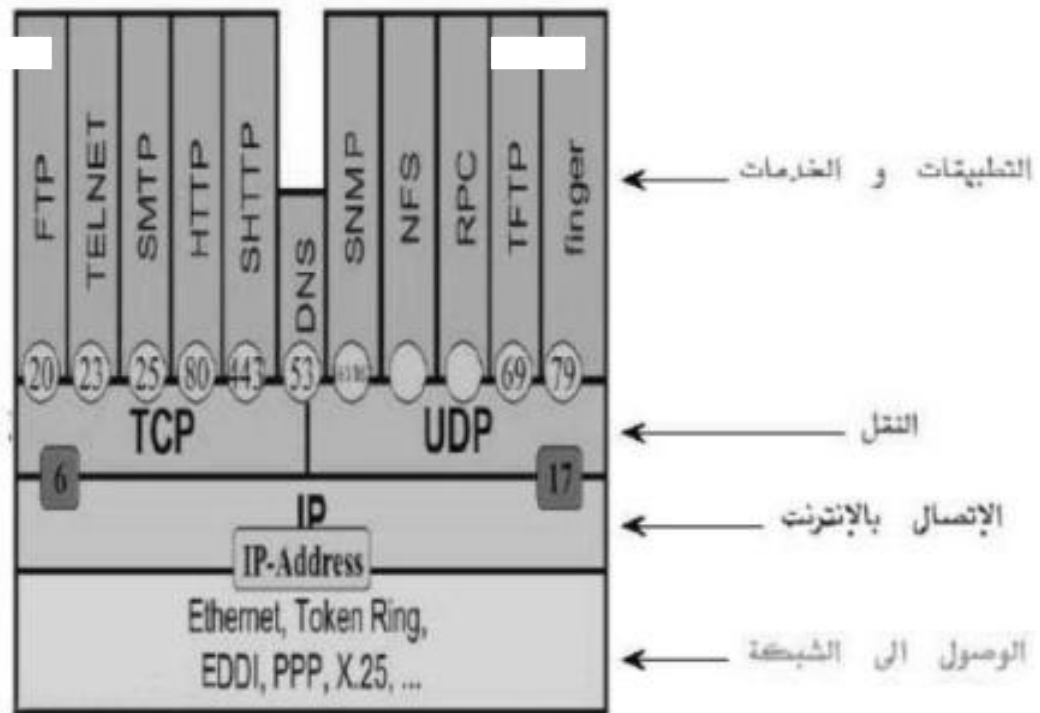
تتميز هذه الطبقة بترقيم الرزم في حالة الإرسال وترتيبها في حالة الاستقبال.

في يل الرزم (Pa witching) تسلك الرزم مسارات مختلفة طريقها من الجهاز المرسل إلى الجهاز المستقبل. غالباً ما تختار هذه الرزم المسارات الأقل ازدحاماً مما يسبب وصول الرزم إلى الوجهة في ترتيب غير سليم، لولا ترقيم الرزم في حالة الإرسال ما استطاع النظام ترتيبها في الاستقبال.

من خلال كل هذه المهام السابق ذكرها نلاحظ أن خدمات TCP معتمدة على الاتصال وموثوق بها لأن لديها إمكانية كشف الأخطاء أو الأعطال في أي اتصال.

## ٢ - بروتوكول المخطط البياني للمستخدم (User Datagram Protocol) UDP

مهمة بروتوكول المخطط البياني للمستخدم (User Datagram Protocol) هو بروتوكول بسيط عديم الاتصال ، يعنى أنه من غير الضروري اجراء اتصال مسبق قبل الشروع في تبادل البيانات لذلك فان هذا البروتوكول خالى من الوظائف التى تعتمد على الاتصال مثل الاشعار بالاستقبال و التحكم في جريان البيانات و كشف الأخطاء. و لقد صمم هذا البروتوكول للتطبيقات التى لا تحتاج الى الخدمات و المهام الموفرة في الحالات المعتمدة على الاتصال، فعندما نقوم بارسال بواسطة UDP فليس هناك ضمان أن البيانات تصل الى وجهتها بدون أخطاء.



شكل (٣-١٧) يوضح المنافذ المستخدمة في حالة TCP و UDP.



## رابعاً: طبقة التطبيقات و الخدمات

تتميز هذه الطبقة بخدمات تتمثل بروتوكولات عالية المستوى و التي يتمثل الغرض تصميمها هو الاستفادة من البروتوكولات منخفضة المستوى كبروتوكولات TCP و UDP. و تستفيد تطبيقات هذه الطبقة من مميزات البروتوكولات TCP و UDP لتوفير عدة خدمات بعضها موثوقة و قائمة على الاتصال والبعض الآخر غير موثوقة و مقطوعة الاتصال.

### ١- بروتوكول نقل الملفات (FTP(File Transfer Protocol)

يعتبر بروتوكول FTP من أشهر البروتوكولات المستخدمة لنقل الملفات بين أنظم TC، و يصنف FTP ن البروتوكولات التي تعد تطبيقا حد ذاتها و ليس مجرد بروتوكول فعمل FTP يستطيع أن يستعرض بنية فهارس أحد الأجهزة التي يتصل معها و اختيار الملفات التي يريد تحميلها. و هو يستخدم منفذين بدلا من منفذ واحد.

### ٢- بروتوكول HTTP(Hyper Text Transfer Protocol)

HTTP هو بروتوكول نقل النصوص الفائقة هو البروتوكول المستخدم من قبل ملقمات و عملاء الويب لتبادل الملفات. إذا أراد جهاز (عميل) استعراض صفحة ويب يقوم مستعرض الويب بفتح اتصال TCP مع ملقم الويب Web

( Server ) ، بعدها يرد الملقم بإرسال ذلك الملف الذي يعرضه المستعرض كصفحة رئيسية تتضمن النصوص و الصور .

### ٣- بروتوكول نقل البريد البسيط STMP (Simple Mail Transfer Protocol)

SMTP هو البروتوكول الذي تستخدمه ملقمات البريد الإلكتروني لإرسال الرسائل إلى بعضها عبر شبكة الإنترنت. عندما يريد ماقم بريدي إرسال بريد إلكتروني يقوم البروتوكول بفتح اتصال مع الملقم الثاني و من خلاله يحقق الطلب المرغوب.

### ٤- ل مكتب البريد POP٣ (Post Office Protocol)

POP٣ هو أحد البروتوكولات التي يستخدمها عملاء البريد الإلكتروني للحصول على رسائلها من ملقم البريد الإلكتروني. يفتح POP٣ اتصال عبر المنفذ ١١٠ من ناحيته و المنفذ ٢٥ من ناحية الملقم.

### ما هو نظام أسماء النطاقات DNS(Domain Name System)?

تستفيد أنظمة TCP/IP من خدمات DNS لحل أسماء المضيفات على الإنترنت و تحويلها إلى عناوين IP التي تحتاجها للاتصال.

## ٦- بروتوكول التكوين الديناميكي للمضيف DHCP ( Dynamic Host Configuration protocol )

DHCP هو البروتوكول الذي تستخدمه محطات العمل (المضيفات) لطلب اعدادات تكوين TCP/IP من ملقم DHCP. و غالبا ما تكون وظيفته هي اعطاء عناوين IP لمضيفات بصفة ديناميكية أو متغيرة. و هذا على عكس ضبط IP للمضيف بصفة ساكنة أو ثابتة.

## ٧- بروتوكول الإدارة البسيطة للشبكات SNMP ( Simple Network Management Protocol )

بروتوكول الإدارة البسيطة للـ Simple Network Management Protocol (SNMP) هو بروتوكول مهمته جمع معلومات حول مختلف مكونات الشبكة ، و يعتمد هذا البروتوكول على برامج بعيدة تسمى ممثلين (Agents) التي تجمع المعلومات و ترسلها إلى مؤازر (Console) مركزي لإدارة الشبكة باستخدام رسائل SNMP.

## أوامر فحص الإنترنت

## ١ - الأمر PING

يمكن التحكم في حجم الرزم و عدد المحاولات باستخدام الأمر Ping ويتم ذلك عن طريق كتابة السطر التالي من سطر الأوامر:

حجم الرزم

```
Ping -l 1470 -n 9 192,168,162,39
Pinging 192,168,162,39 with 1470 bytes of data:
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
Reply from 192,168,162,39: bytes=1470 time=10ms TTL=128
```

عدد المحاولات

Ping statistics for 192,168,162,39:

Packets : Sent=9, Received =9, Lost=0 (%loss),

Approximate round trip times in milli-seconds:

Minimum =0 ms, Maximum=10 ms, Average=1 ms

## ٢- الأمر Traceroute

Traceroute هو أحد أشكال البرنامج Ping ، فهو يعرض المسار الذي تسلكه الرزم في طريقها الى وجهتها، علماً بأن المسار يتغير عبر الشبكة من دقيقة الى أخرى لذا فان البرنامج Traceroute يعرض قائمة بالمسارات المتاحة حالياً للوصول الى وجهه معينة و يستخدم هذا البرنامج echo request و echo reply من بروتوكول ICMP.

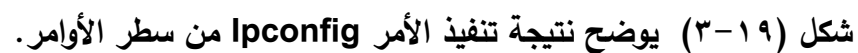
و الشكل التالي يوضح نتيجة تنفيذ هذا الأمر

```
Tracing route to IS~SERV2000[10.61.10.3]
Over a maximum of 30 hops:
  0 < 10ms < 10ms NETS      2,168,162,1
  1 < 10ms < 10ms IS~SERV2000[10.61.10.3]
Trace complete.
```

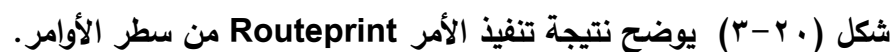
شكل (١٨-٣) يعرض نتيجة تنفيذ الأمر Tracert الذي يعرض المسار إلى الوجهة .

## ٣- الأمر Ipconfig من سطر الأوامر

عند تنفيذ الأمر Ipconfig من سطر الأوامر يعرض النظام قائمة شاملة ببيانات التكوين لمحطة عمل عادية لجهاز .



يعر الأمر جدول توجيه الرا .Routing Ta





# الباب الرابع

## عناصر الشبكات





## أهداف الباب الرابع

بعد الانتهاء من دراسة هذا الباب ينبغي أن يكون الطالب قادراً على أن:

- ١- يحدد الدور الذي يقوم به المودم.
- ٢- يميز بين أنواع المودم المختلفة.
- ٣- يفرق بين المودم التناظري والرقمي.
- ٤- يُعرف بطاقة الشبكة.
- ٥- يميز فتحة التوسعة التي يتم تركيب بطاقة الشبكة عليها.
- ٦- يبرر سبب أهمية بطاقة الشبكة عند الربط بين الأجهزة.
- ٧- يعدد وظائف بطاقة الشبكة.
- ٨- يُعرف طلب المقاطعة.
- ٩- يحدد دور عنوان المنفذ المدخل/المخرج.
- ١٠- يحدد دور قناة الوصول المباشر للذاكرة.
- ١١- يحدد دور عنوان الذاكرة الرئيسية.
- ١٢- يفرق بين معايير الواجهات لمشغلات الشبكة.
- ١٣- يُعرف NDIS.
- يعدد مميزات DIS
- ١٥- يُعرف المجمعات.
- ١٦- يحدد الدور الذي تقوم به المجمعات.
- ١٧- يحدد كيف يتم الربط بين المجمعات.
- ١٨- يبرر السبب في أن المنافذ العادية للمجمع تحتوي على دوائر عبور.
- ١٩- يبرر السبب في أن منفذ الربط التوسعي للمجمع لا يحتوي على دوائر عبور.
- ٢٠- يُعرف الجسور.
- ٢١- يبرر السبب في أهمية الجسور.
- ٢٢- يُعرف المبدل.
- ٢٣- يفرق بين المجمع والمبدل.
- ٢٤- يعطي مثال على الفرق بين المجمع والمبدل في تخصيص عرض النطاق.
- ٢٥- يعدد مزايا المبدل.
- ٢٦- يعدد عيوب المبدلات.
- ٢٧- يوضح بالرسم كيف يوجه المبدل البيانات إلى وجهتها.

- ٢٨- يُعرف الموجهات.
- ٢٩- يوضح بالرسم كيفية توجيه البيانات باستخدام الموجهات.
- ٣٠- يعدد مزايا الموجهات.
- ٣١- يذكر مكونات الشبكات اللاسلكية.
- ٣٢- يبرر أهمية بطاقة الاتصال اللاسلكي.
- ٣٣- يُعرف نقطة الوصول إلى الشبكة.
- ٣٤- يبرر السبب في أهمية نقطة الوصول إلى الشبكة.

## ١ - اتصال أجهزة الحاسب

- يمكن توصيل أجهزة الحاسب بطرق مختلفة منها:

❖ استخدام المودم



شكل (١-٤) يوضح كارت الفاكس Fax Modem

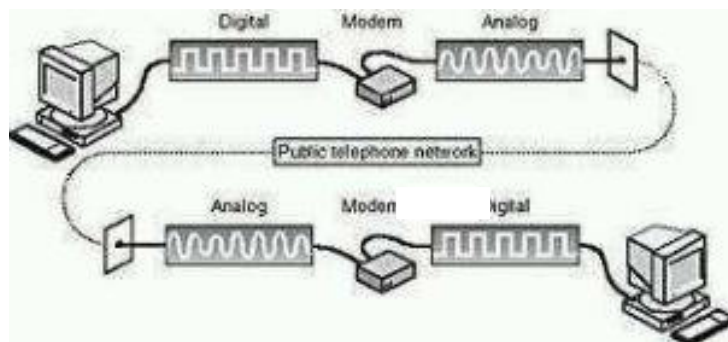
❖ خدام كارت الشبكة



شكل (٢-٤) يوضح كارت الشبكة Ethernet Card

## أولاً: المودم

تستطيع أجهزة الحاسب باستخدام المودم Modem أن تتحاور وتتبادل المعلومات عبر خطوط الهاتف. فالمودم يقوم بتحويل البيانات الرقمية إلى نبضات تناظرية لنقلها عبر خط الهاتف. بحيث يتقبل المودم المرسل البيانات الرقمية الثنائية من الحاسب ثم يقوم بتحويلها إلى إشارات تناظرية يمكن إرسالها عبر خطوط الهاتف. ويقوم المودم في الجهاز المستقبل بترجمة الإشارات التناظرية إلى بيانات رقمية ثنائية يستطيع الحاسب التعامل معها.



شكل (٣-٤) يوضح كيف يقوم المودم بتحويل الإشارات من رقمية إلى تناظرية والعكس.

**استخدامات المودم :-** ١- تبادل الملفات ورسائل البريد الإلكتروني مع الأجهزة الأخرى في الشبكة. ٢- استقبال وإرسال الفاكسات باستخدام أحد البرامج الخاصة. ٣- التحدث مع الآخرين عبر الهاتف ( إذا كان المودم يدعم خاصية الصوت). ٤- استخدامه كنظام رسائل صوتية (إذا كان المودم يدعم خاصية الصوت). ٥- الاتصال بالإنترنت من أجل الحصول على المعلومات.

## أنواع أجهزة المودم

١- مودم داخلي (Internal) يتم تركيبه في فتحات التوسعة على اللوحة الأم Motherboard.



شكل (٤-٤) مودم داخلي

٢- مودم خارجي (External) وهو عبارة عن جهاز مستقل خارجي.



شكل (٤-٥) مودم خارجي

## أنواع المودم من حيث المعالج

أ- يقوم المودم بترجمة الإشارات الصوتية إلى معلومة بواسطة المعالج الخاص بالمودم وتسمى (Hardware Modem).  
الميزة: قدرته على العمل مع جميع أنظمة التشغيل، ولاحتوائه على معالجه الخاص فانه يعمل بشكل أسرع .

**العيوب:** غلاء سعره وعدم توافره بكثرة في الأسواق.

ب- يقوم المودم بترجمة الإشارات الصوتية إلى معلومة بواسطة معالج الحاسب الآلي وتسمى (Win MODEM).

**الميزة:** رخص سعره وتوافره بكثرة في للأسواق.

**العيوب:**

١- عدم قدرته على العمل مع نظام التشغيل DOS.

٢- استغلاله لجزء كبير من معالج الحاسب الآلي مما يؤدي الى بطء الجهاز.

٣- عند استخدام شبكة مكونة من أكثر من جهاز للمشاركة في استخدام واحد للانترنت Internet Sharing.

### أنواع المودم من حيث الصوت

أ- المقدرة على استخدام الحاسب الآلي للتحدث إلى شخص آخر من خلال الانترنت أو استغلال الحاسب كجهاز هاتف أو جهاز تسجيل المكالمات التليفونية، وتسمى مودمات الصوت/الفاكس/البيانات، وتسمى ( VOICE VIEW ).

**الميزة:** عند عدم وجود كارت صوت في الجهاز أو عندما يكون كارت الصوت لا يتمتع بميزة استقبال وإرسال الصوت في نفس الوقت "Full Duplex".

إعداد د/ أميرة إبراهيم عبد الغني

العيوب: ١- لا تستطيع التعامل مع الأصوات الموجودة في الألعاب أو الاستماع إلى التسجيلات الصوتية.

٢- عند عدم وجود كارت صوت يحتوي على خاصية "Full Duplex" لن تحتاج إلى ميزة الصوت في المودم. بل يمكن لهذه الميزة في بعض الأحيان أن تسبب تضارباً ما بين المودم وكارت الصوت.

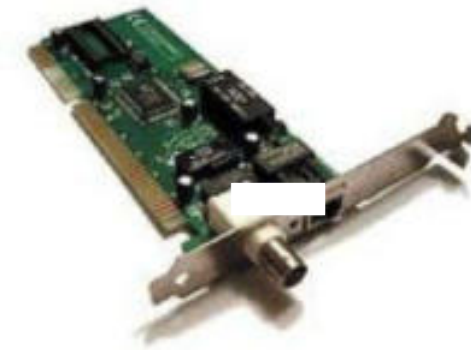
### أنواع المودم من ناحية السرعة

أ- المودم التناظري "Analog": تقاس سرعة المودم بالكيلوبت بالثانية. والبايت يحت ٨ بت والكيلوبت تحت ١٠٠٠ بت. وعليه فإن المودم كان يعمل بسرعة ٥٦ كيلوبت بالثانية فإنه سيقوم بنقل ٧٠٠٠ بايت بالثانية. وأحدث أنواع المودم غير الرقمي هي المستخدمة مع خطوط الهاتف العادية، تسمى ٧.٩٠.

ب- المودم الرقمي "Digital": وهو يستخدم تقنية الاتصال بالموجة الرقمية العريضة، وهناك أنواع من الاتصالات الرقمية العريضة أشهرها ISDN أو DSL . وسرعة هذا النوع تفوق سرعة الاتصال التناظري بأكثر من عشرة أضعاف وتبدأ من ١.٥ ميجابت في الثانية وأعلى وذلك حسب سعة الخط الذي تم الاشتراك به.

## ثانياً: بطاقة الشبكة

بطاقة الشبكة هي المكون الذي يربط الكمبيوتر بالشبكة ويمكنه من الاتصال بالشبكة، ويطلق عليها أيضاً اسم محول الشبكة، LAN Adapter أو NIC. تعتبر بطاقة الشبكة الواجهة التي تصل بين جهاز الكمبيوتر وسلك الشبكة وبدونها لا تستطيع الأجهزة الاتصال فيما بينها من خلال الشبكة. تتركب بطاقة الشبكة في فتحة توسعة فارغة (Expansion slot) في الجهاز وتثبت في الشق الذي من الممكن أن يكون إما من النوع ISA أو PCI أو PCMCIA.



شكل (٦-٤) بطاقة شبكة من نوع ISA



شكل (٧-٤) بطاقة شبكة من نوع PCI





شكل (٨-٤) بطاقة شبكة من نوع PCMCIA تستخدم في الأجهزة المحمولة.

بطاقة الشبكة بالتشارك مع برنامج تشغيلها مسئولة عن القيام بمعظم بروتوكولات طبقة ربط البيانات والطبقة الفيزيائية. تتضمن بعض محولات الشبكة أكثر من وصلة كبل مما يتيح إمكانية التوصيل مع أكثر من نوع من كبل الشبكة.



شكل (٩-٤) يوضح بطاقة شبكة بها ثلاثة أنواع من الوصلات RJ٤٥، BNC، AUI.

## وظائف بطاقة الشبكة

يتلخص دور بطاقة الشبكة في الوظائف التالية:

### ١ - تغليف البيانات

في هذه المرحلة تحضر بطاقة الشبكة البيانات لبثها على الشبكة. عندما تستقبل البطاقة البيانات التي يولدها بروتوكول طبقة الشبكة تقوم ببناء إطار حول هذه البيانات تحضيراً لإرسالها. أما في حالة الاستقبال فيقرأ محول الشبكة محتويات الأطر الواردة ويمرر البيانات إلى بروتوكول طبقة الشبكة.

### ٢ - تحويل الإشارات والبتات

ل بطاقة الشبكة الإطال من بتات ثنائية إلى إشارة تتنا مع نوع الكبل المستخدم. غالباً ما يكون نوع الإشارة المرسله عبارة عن نبضات كهربية في حالة استخدام الأسلاك النحاسية أو إشارات ضوئية في حالة استخدام الألياف البصرية وإشارات الكترومغناطيسية في حالة استخدام تقنية إرسال لاسلكية. أما في حالة الاستقبال فتحول بطاقة الشبكة أي نوع من الإشارات التي تستلمها من كبل الشبكة إلى بيانات ثنائية تمثل إطار البيانات.

### ٣ - إرسال واستقبال البيانات

من وظائف محول الشبكة هو إرسال الإشارات من النوع المناسب عبر الشبكة واستلام الإشارات الواردة في حالة الاستقبال. تتم عملية الاستلام هذه

بتفحص بطاقة الشبكة لعنوان وجهة رزم البيانات. في حالة توافق عنوان الوجهة مع العنوان المادي لبطاقة الشبكة، تلتقط البطاقة البيانات وتمررها إلى الطبقات العليا، أما في حالة عدم توافق العناوين فتتجاهل البطاقة رزم البيانات.

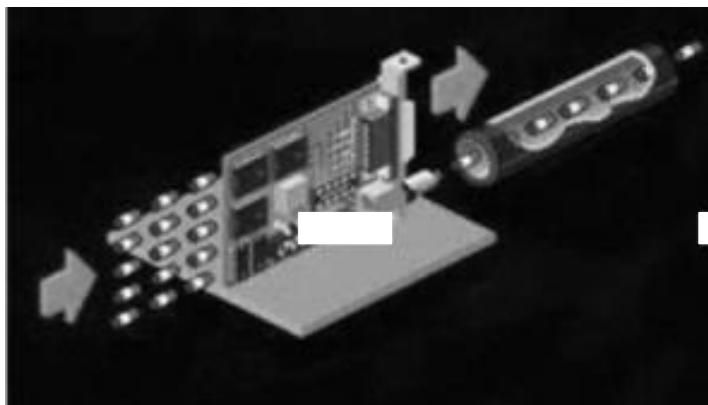
#### ٤ - التخزين المؤقت

غالباً ما تكون سرعة نقل البيانات من ذاكرة الجهاز إلى البطاقة أكبر من سرعة نقل البيانات من البطاقة إلى كبل الشبكة. لهذا يجب تخزين (Buffering) جزء من البيانات مؤقتاً على ذاكرة البطاقة إلى أن تتمكن البطاقة من بثها إلى السلك. أما في حالة استقبال البيانات فتمكن هذه العملية من لبيانات التي تصل من بكة إلى أن يصبح لدينا إطار وجاهز للمعالجة من قبل طبقة ربط البيانات.

#### ٥ - التحويل التوازي / التوالي

تنتقل البيانات في الكمبيوتر في ممرات تسمى نواقل باستخدام هذه الممرات يتمكن الناقل من نقل كمية كبيرة من البيانات في نفس الوقت. وتوجد نواقل قادرة على نقل ٨ بتات من البيانات في الوقت الواحد وتوجد أيضاً نواقل قادرة على نقل ١٦ بت أو ٣٢ بت أو ٦٤ بت في المرة الواحدة. تنتقل البيانات

في هذه الحالة بشكل متواز (Parallel). أما سلك الشبكة فيستطيع حمل بت واحد من البيانات في المرة الواحدة ويطلق على هذا البث المتسلسل ( Serial Transmission) وبطاقة الشبكة هي المسؤولة عن تحويل البيانات من الجريان بشكل متوازي على ناقل البيانات داخل الجهاز إلى الجريان بشكل متسلسل على كبل الشبكة، هذا ما يحدث في حالة الإرسال، أما في حالة الاستقبال فتقوم البطاقة بالتحويل من الشكل المتسلسل للبيانات إلى الشكل المتوازي.



شكل (١٠-٤) يوضح التحويل من التوازي الى التوالي عبر بطاقة الشبكة.

## ٦- التحكم بالوصول إلى الوسيط MAC(Media Access Control)

بطاقة الشبكة هي المسؤولة عن تنفيذ آلية التحكم بالوصول إلى الوسيط أو MAC التي يستخدمها بروتوكول طبقة ربط البيانات. وكمثال لهذا النوع من الآليات نذكر آلية (Ethernet) CSMA/CD و آلية Token Passing (Token Ring).

## تركيب بطاقة الشبكة

تعتبر بطاقة الشبكة من أهم مكونات الشبكات، فهي الواجهة بين ناقل البيانات الداخلي (Internal Bus) للجهاز وكبل الشبكة. ناقل البيانات هو المسئول عن نقل البيانات بين المعالج أو ذاكرة الجهاز وذاكرة البطاقة أو المخزن المؤقت.

يوجد أربعة أنواع لتصميم ناقل البيانات وهي:

١-ISA (Industry Standard Architecture).

٢-MCA (Micro Channel Architecture).

٣-EISA (Extended Industry Standard Architecture).

٤-PCI (Peripheral Component Interconnect).

ر تصميم PCI الأسرع تطوراً ويتميز بوظيفة Plug and Play أو ركب وشغل، وهي مواصفات تسمح بالإعداد التلقائي للأجهزة والبطاقات بمجرد تركيبها. ولتحقيق ذلك لابد أن يكون BIOS الجهاز ونظام التشغيل وبطاقة الشبكة متوافقين مع Plug and Play.

للقيام بعملية التركيب الفعلي لبطاقة الشبكة يجب إتباع الخطوات التالية:

١- إزالة سلك الكمبيوتر من قابس الكهرباء.

٢- مسك الغطاء المعدني للجهاز لتفريغ شحنات الكهرباء الساكنة ثم إزالة الغطاء.

٣- تركيب البطاقة بحذر في منفذ فارغ متوافق معها.

٤- تركيب غطاء الجهاز وتوصيل سلك الكمبيوتر إلى قابس الجهاز.

٥- توصيل سلك الشبكة بالبطاقة.

## إعدادات وتكوين بطاقة الشبكة

إذا كانت البطاقة أو نظام التشغيل لا يدعمان مواصفات Plug and

Play فلا بد من إعداد البطاقة يدوياً. تعني هذه الإعدادات ضبط موارد معينة

والتي تتمثل فيما يلي:

### ١- طلب المقاطعة IRQ

اطعة هي عبارة عن إجهها البطاقة إلى المعالج طالبة

جزءاً من اهتمامه، وعندها يتوقف المعالج عن القيام بمهامه مؤقتاً إلى أن يتم معالجة المقاطعة ثم يعود لمتابعة معالجة مهامه.

يجب على كل جهاز أن يستخدم خط طلب مقاطعة مختلف عن

الآخر، وتكون هذه الخطوط مرقمة من ١ إلى ١٤ ويكون البعض منها مخصصاً لبعض المكونات الطرفية.

في كثير من الأحيان تستخدم بطاقة الشبكة خط طلب المقاطعة IRQ٣

أو IRQ٥ ومن الممكن استخدام أي خط مقاطعة غير مشغول.



شكل (١١-٤) يوضح تغيير إعدادات طلب المقاطعة

## ٢- المنفذ المدخل/المخرج Base I/O Port Ad

يقوم هذا العنوان بتحديد قناة يتم تدفق المعلومات من خلالها بين بطاقة الشبكة والمعالج (Processor).

يظهر هذا المنفذ للمعالج كعنوان مكتوب بالنظام الست عشري. من الضروري أن يكون لكل جهاز رقم منفذ مختلف عن الآخر. عناوين المنافذ التي غالباً ما تستخدم لبطاقة الشبكة هي من ٣٠٠ إلى ٣٠٤ أو من ٣١٠ إلى ٣١٤ ومن الممكن استخدام أي رقم منفذ غير مشغول.

### ٣- قناة الوصول المباشر للذاكرة(DMA) Direct Memory Access

DMA هي قناة تنقل البيانات بين بطاقة الشبكة وذاكرة الكمبيوتر دون أي تدخل من المعالج، يجب تخصيص قناة منفصلة للبطاقة مختلفة عن باقي الأجهزة.

### ٤- عنوان الذاكرة الرئيسية Base Memory Address

يمثل عنوان الذاكرة الرئيسية موقع محدد في ذاكرة الجهاز RAM تستخدمه بطاقة الشبكة للتخزين المؤقت للبيانات المرسل والمستقبل. غالباً ما يكون العنوان المستخدم من قبل بطاقة الشبكة D٨٠٠٠. ومن الممكن استخدام أي عنوان غير محجوز من قبل جهاز آخر.

### تنصيب برنامج تشغيل محول الشبكة Network Driver

مشغل البطاقة هو البرنامج الذي يسمح لنظام تشغيل الكمبيوتر بالعمل والتخاطب مع بطاقة الشبكة ومن خلال هذا المشغل يتم التخاطب بين نظام التشغيل والبطاقة.

هناك عدة شركات مصنعة لبطاقات الشبكة وبالتالي فهناك احتمال أن يكون لكل بطاقة خواص مختلفة وسيكون من الصعب عملياً تزويد جميع أجهزة



الكمبيوتر بالبرامج اللازمة للعمل مع كل نوع من أنواع بطاقة الشبكة. ولحل هذه المشكلة فإن كل شركة تزود بطاقتها ببرنامج للتشغيل.

يقوم مشغل البطاقة بتوفير اتصال بين بطاقة الشبكة وبين موجه برمجي Network Redirector الذي يحتوي على جزء من برنامج التشبيك المدمج مع نظام التشغيل والتي مهمته هي استقبال طلبات على الجهاز وتحويلها للجهاز المطلوب.

تعمل مشغلات بطاقة الشبكة من خلال الطبقة الفرعية MAC لطبقة ربط البيانات في نموذج OSI. تستخدم كل بطاقة بروتوكولاً معيناً للاتصال عبر الشبكة وحيث أن أنظمة التشغيل المختلفة تدعم بروتوكولات مختلفة فإن على بطاقة أن بدورها أن تدعم بروتوكولات متعددة ومختلفة.

تكون مشغلات الشبكة متوافقة مع أحد معايير الواجهات التالية:

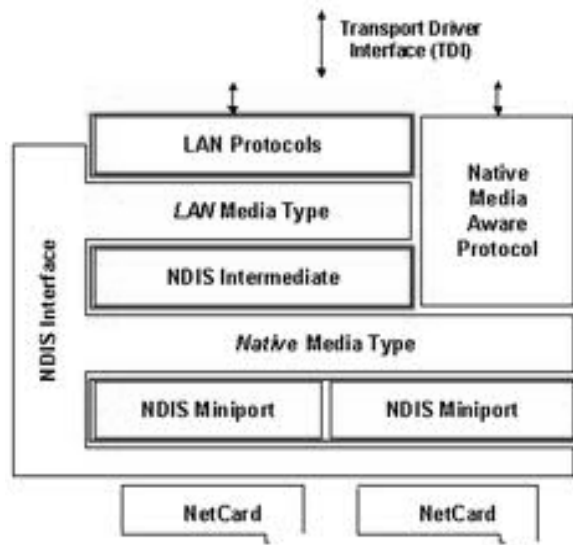
١ – Network Driver Interface Specification (NDIS).

٢ – Open Data Link Interface (ODI).

برنامج تشبيك نظم تشغيل Microsoft متوافق مع NDIS، بينما أنظمة Novell Netware فهي متوافقة مع ODI، يقوم NDIS بعزل بطاقة الشبكة عن تفاصيل البروتوكولات المختلفة المستخدمة وعزل البروتوكولات عن الأنواع المختلفة لبطاقات الشبكة.

من خلال هذه الواجهات أصبح من غير الضروري كتابة مشغلات خاصة لكل بروتوكول أو نظام تشغيل بل يكفي كتابة مشغلات متوافقة مع NDIS أو ODI، وهكذا أصبح المستخدمون قادرين على الاتصال عبر شبكات تستخدم بروتوكولات مختلفة باستخدام بطاقة شبكة وحيدة ومشغل شبكة وحيد متوافق مع أحد الواجهتين. ومن مميزات NDIS أنها تدعم أكثر من معالج على نفس الجهاز وتستطيع التعامل مع عدة اتصالات شبكية وبروتوكولات نقل في نفس الوقت، وللتخلي عن كتابة مشغلات خاصة متوافقة مع كل بروتوكول أو نظام تشغيل، تم تطوير واجهة مشغل الشبكة Network Interface Driver.

تكون واجهة NDIS مسؤولة عن إرسال واستقبال البيانات، إدارة بطاقة الشبكة بما يتناسب مع نظام التشغيل، تشغيل نظام I/O في بطاقة الشبكة وتلقي طلبات المقامها وإعلام نظام التشغيل بالبيانات أو الانتهاء من إرسال



شكل (١٢-٤) يوضح واجهة NDIS

### ثالثاً: المجمعات HUBS

المجمع هو جهاز يربط الحاسبات في بنية نجميه أو حلقيه، وتحتوي المجمعات الصغيرة على أربعة منافذ وتستخدم في الشبكات الصغيرة على أربعة منافذ وتستخدم في الشبكات الصغيرة كالشبكات المنزلية أما المجمعات الكبيرة فتحتوي على أكثر من ٢٤ منفذ.



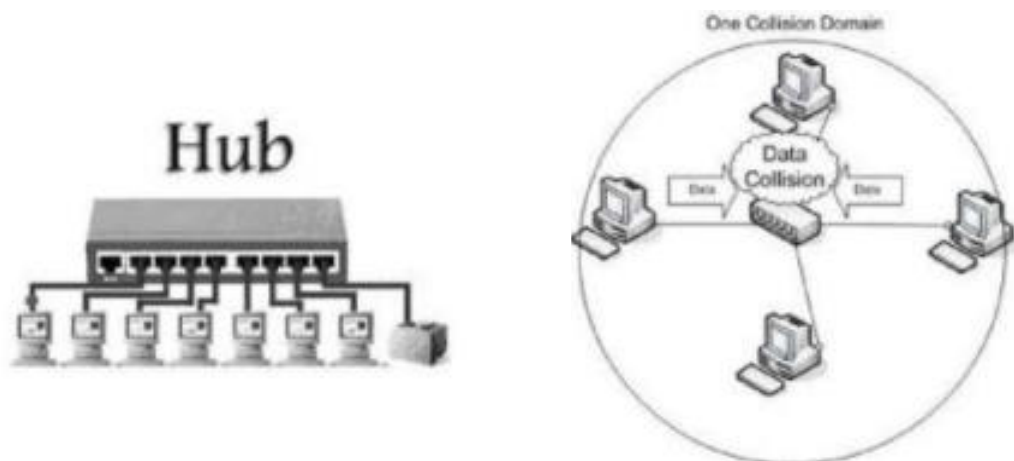
شكل (١٣-٤) يوضح مجمع صغير ذو أربعة منافذ



شكل (١٤-٤) يوضح مجمع ذو أربعة وعشرون منفذاً.

تدخل الإشارة المرسله من أحد الأجهزة إلى أحد منافذ المجمع عندئذ يقوم المجمع بتضخيم الإشارة الكهربائية لتقويتها وبنها على باقي المنافذ ليلتقطها جهاز استقبال واحد وهذا بعد التحقق من أنها مرسله إليه. ولذلك يطلق على

المجمع اسم المكرر متعدد المنافذ Multiport Repeater. من عيوب المجمعات أنها تنشئ نطاق تصادم تتشارك فيه كل الأجهزة مما يقلل من أداء الشبكة.

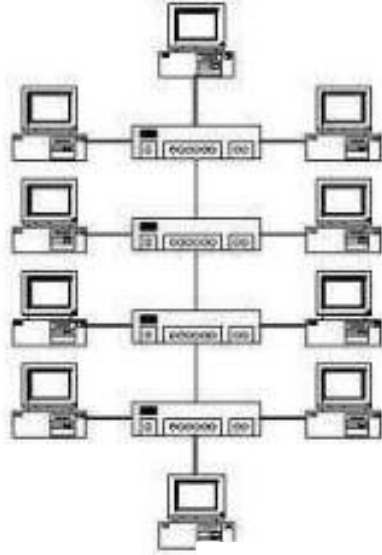


شكل (١٥-٤) يوضح وظيفة المجمع بالشبكات

يمكننا تثبيت مجمع في مكان ما من تمديد الطول الأقصى لكبل UTP من ١٠٠ متر إلى ٢٠٠ متر. وإضافة مجمع ثاني يمكننا من الربط بين جهازين تفرق بينهما مسافة ٣٠٠ متر، كلما أضفنا مجمع مددنا أقصى مسافة مسموح بها بمقدار مائة متر.

هكذا نرى كيف يحقق المجمع إمكانية توسيع الشبكة محلياً. وبما أن التوصيل والتضخيم مضمون فيكون الاتصال وتبادل البيانات ممكن. تعمل مجمعات شبكات Ethernet على الطبقة الفيزيائية في نموذج OSI ، يلتقط المجمع الإشارة من أحد الأسلاك ثم يضخمها ويرسلها إلى باقي الأسلاك. يعني هذا أن

المجمع يستلم الإشارات الكهربائية الموجودة على الكبل يكبرها ويرسلها إلى كل المنافذ الأخرى دون أن يكون له العلم إلى أي جهاز هذه الإشارات موجهة.



شكل (١٦-٤) يوضح إمكانية توسيع الشبكة باستخدام أكثر من مجمع

### ربط المجمعات

يمكننا توصيل مجمع بمجمع ثاني من الزيادة في عدد الأجهزة الموصلة بالشبكة، ويتطلب نمو أي شبكة إضافة مجمع إلى الشبكة. تحتوي المجمعات على منفذ إضافي يسمى منفذ الربط التوسعي (Uplink Port) والذي يستخدم خصيصاً للربط بين مع مجمع آخر وليس لجهاز كمبيوتر لأن طريقة توصيل هذا المنفذ تختلف عن طريقة توصيل المنافذ الأخرى.

يحتوي المجمع في المنافذ العادية على دوائر عبور ( Crossover Circuits ) دور هذه الدوائر هو توصيل أسلاك الإرسال في كبل UTP من جهاز ما إلى أسلاك الاستقبال للأجهزة الأخرى.

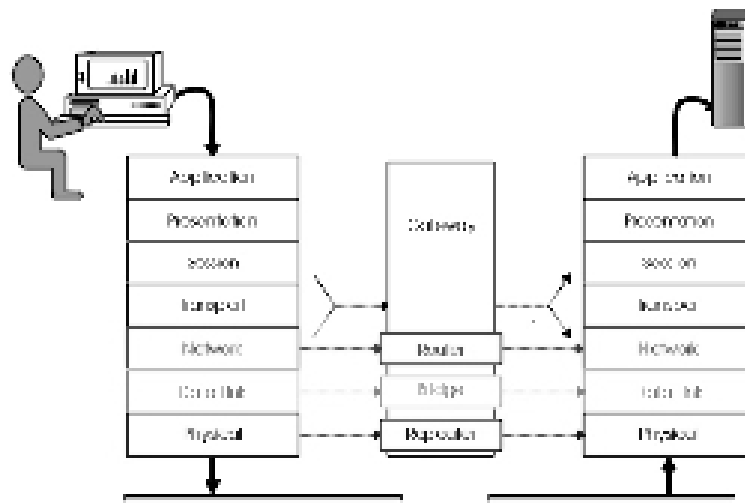
أما منفذ الربط التوسعي فهو المنفذ الوحيد الذي لا يحتوي على دائرة عبور فلذلك ربط المنفذ التوسعي للمجمع الأول بمنفذ عادي من المجمع الثاني يمكن الأجهزة المربوطة مع المجمع الأول من الاتصال مع الأجهزة المربوطة مع المجمع الثاني لأننا نستخدم في هذه الحالة دائرة عبور المجمع الثاني، وإذا ربطنا المنفذ التوسعي للمجمع الأول مع المنفذ التوسعي للمجمع الثاني فأسلاك إرسال الأجهزة المربوطة بالمجمع الأول تكون متصلة بأسلاك إرسال الأجهزة المربوطة مع المجمع الثاني مما يؤدي إلى اتصال الأجهزة مع بعضها لأن منفذ الربط التوسعي للمجمعين لا يحتويان على دوائر عبور.

### رابعاً: الجسور Bridges

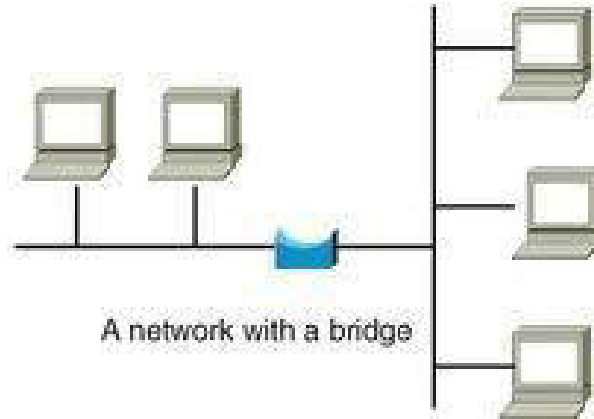
الجسر هو جهاز ذو منفذين يستخدم للربط بين شبكتين محليتين أو لتجزئة شبكة محلية إلى جزأين. غالباً ما يستخدم الجسر لتقسيم شبكة محلية ضخمة تعاني من التصادمات، ففي هذه الحالة إذا أراد جهازان موجودان على الجزء الأول الاتصال ببعضهما فسيبقى نطاق تبادل الرسائل والبيانات متعلق بالجزء الأول من الشبكة المجزئة وسوف لا يكون هناك تأثير على الجزء الثاني مما يؤدي إلى نقص في التصادمات وبالتالي زيادة في أداء الشبكة ككل. لا

تستطيع البيانات العبور من الجزء الأول إلى الجزء الثاني إلا في حالة رغبة اتصال جهاز من الجزء الأول بجهاز من الجزء الثاني. يبنى القرار في إبقاء أو توجيه رزم البيانات بالنظر إلى العنوان المادي أو الفيزيائي لجهاز الوجهة أو المستقبل، مما يعني أن الجسر يعمل على مستوى طبقة ربط البيانات في نموذج OSI المرجعي.

ويبين الشكل التالي عدد من الأجهزة موصلة بمجمع مركزي ونطاق التصادم الناتج في هذه الشبكة، حيث تدخل البيانات إلى الجسر عبر أحد منافذه فيقرأ الجسر عنوان الوجهة أو الجهاز المقصود للاتصال به ثم يقرر بتوليد رزمة البيانات على المنفذ الثاني في حالة وجود جهاز الوجهة على الجزء الثاني من الشبكات. اهل هذه الرزمة في كان عنوان الوجهة هو جهاز م في نفس الجزء مع الجهاز الذي قام بتوليد الرزمة أو الكمبيوتر المرسل.



شكل (١٧-٤) يوضح أن الجسر يعمل على طبقة ربط البيانات.

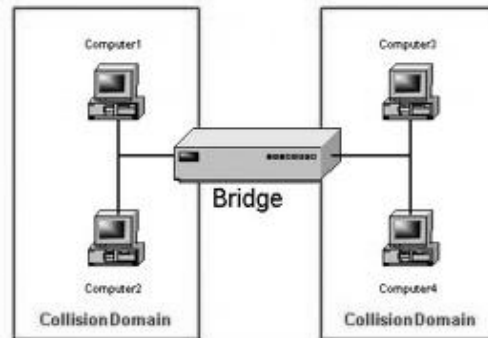


شكل (١٨-٤) يوضح كيف يقلل الجسر من حركة النقل.

وهكذا نرى أن الجسر يقلل من حوالي نصف حركة النقل على كل جزء مما يزيد في سرعة الشبكة.

مزايا الجسور هو تقسيم التصادم (main Collision)

مما يقلل من احتمال وقوع تصادم حين يرغب جهازان إرسال رزم البيانات في نفس الوقت.



شكل (١٩-٤) يوضح كيف يقوم الجسر بتقسيم نطاق التصادم.



الشبكات التي تستفيد من فصل نطاقي التصادم هي على وجه الخصوص شبكات إترنت Ethernet لأن في هذا النوع من شبكات التصادم أمراً طبيعياً وجزءاً متوقعاً من عمل الشبكة.

من عيوب الجسور أنها تثبت الإشارات إلى كل من جزأي الشبكة في حالة التبليغ (Broadcasting) لأن عملية البث تحدث على مستوى طبقة الشبكة وإمكانات الجسور لا تستطيع أن تفوق طبقة ربط البيانات. يؤدي الجسر إلى تقسيم الشبكة إلى نطاقي تصادم مختلفين. إلا أن هذين الجزأين يظلان جزء من نفس نطاق البث أو البلاغ (Broadcast Domain)، وهذا منطقي لأن تجزئة الشبكة بواسطة جسر يؤدي إلى بقاء جزئي الشبكة كشبكة محلي .

### خامساً: المبدلات Switches

المبدل هو جهاز يربط الأجهزة مع بعضها في بنية نجميه. يعمل المبدل على مستوى طبقة ربط البيانات، فهو يشبه المجمع فيما يخص الشكل وعدد المنافذ ويشبه الجسر في الوظيفة، لذلك نستطيع أن نقول أن المبدل هو عبارة عن جسر متعدد المنافذ.



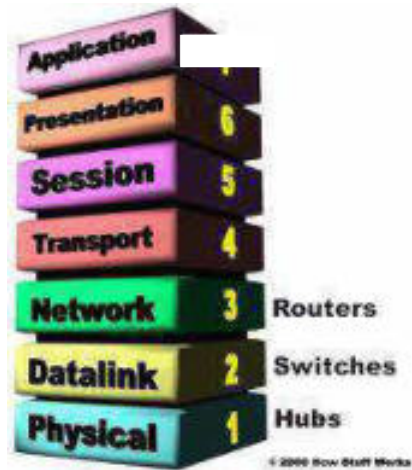
شكل (٢٠-٤) يوضح مبدل ذو ١٦ منفذ.



شكل (٢١-٤) يوضح مبدل ذو ٢٤ منفذ.



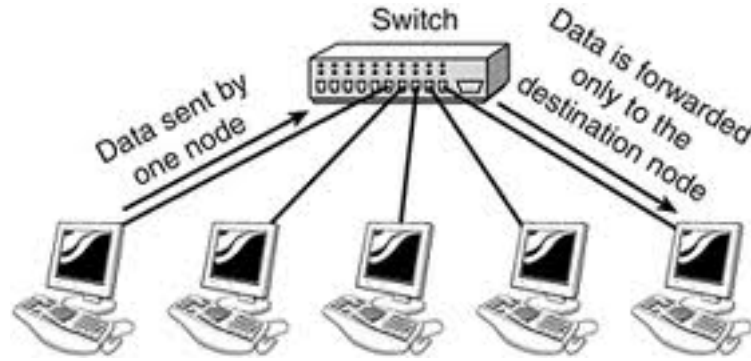
شكل (٢٢-٤) يوضح مبدل ذو ٤٨ منفذ.



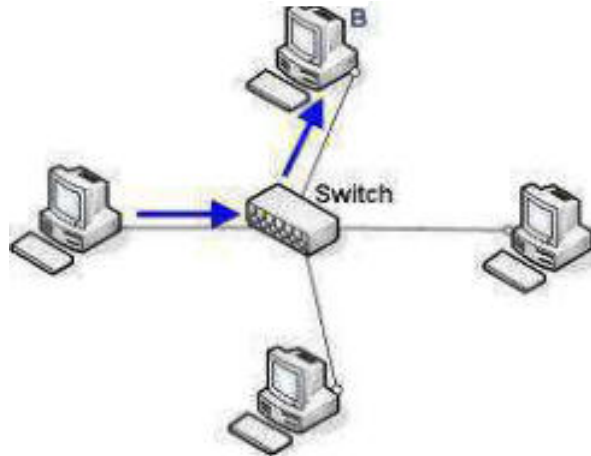
شكل (٢٣-٤) يوضح أن المبدل يعمل على مستوى طبقة ربط البيانات

الفرق بين المجمع والمبدل هو أن المجمع يوجه كل الرزم الواردة إلى كل المنافذ، أما المبدل فانه يوجه الرزمة فقط إلى المنفذ الموصل بجهاز

الوجهة أو المستقبل. عندما يريد جهاز الاتصال بجهاز آخر يقرأ المبدل البيانات الموجودة في ترويسة الإطار وبالضبط العنوان المادي للجهاز المستقبل، ثم يخصص المبدل قناة مادية بين الجهازين. تحدث هذه العملية لأي جهاز يرغب في الاتصال مع جهاز آخر وفي نفس الوقت، وهكذا تأخذ كل رزمة مساراً مخصصاً لها من الجهاز المصدر إلى الوجهة.



شكل (٢٤-٤) يوضح كيف يوجه المبدل البيانات إلى وجهتها.



شكل (٢٥-٤) يوضح كيف يوجه المبدل البيانات إلى وجهتها.

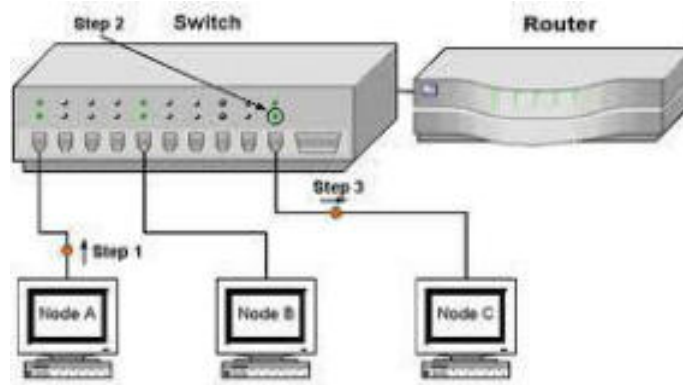
بما أن كل جهاز يستطيع أن يكون بحوزته قناة خاصة تربطه بالجهاز الذي يرغب في الوصول إليه فهذا يعني أن الشبكة تكون خالية من التصادم

والازدحام. الشيء الآخر الذي يزيد من أداء الشبكة عند استخدام المبدلات هو تخصيص كامل النطاق الترددي أو عرض النطاق (Bandwidth) لكل زوج من الأجهزة المتصلة مع بعضها.

### مثال:

إذا كانت هناك شبكة من نوع اترنت مكونة من ٥٠ جهاز ويستخدم فيها كل جهاز بطاقة شبكة ذات سرعة ١٠٠Mbps. يؤدي ربط الأجهزة بمجموعات إلى تبادل البيانات بين الأجهزة بسرعة حركة نقل تعادل ٢Mbps أما استخدام المبدلات فيؤدي إلى نقل البيانات بسرعة ١٠٠Mbps لأنه في الحالة الأخيرة يكون مخصص لكل جهاز قناة عرضها ١٠٠Mbps تربطه مع أي جهاز آخر.

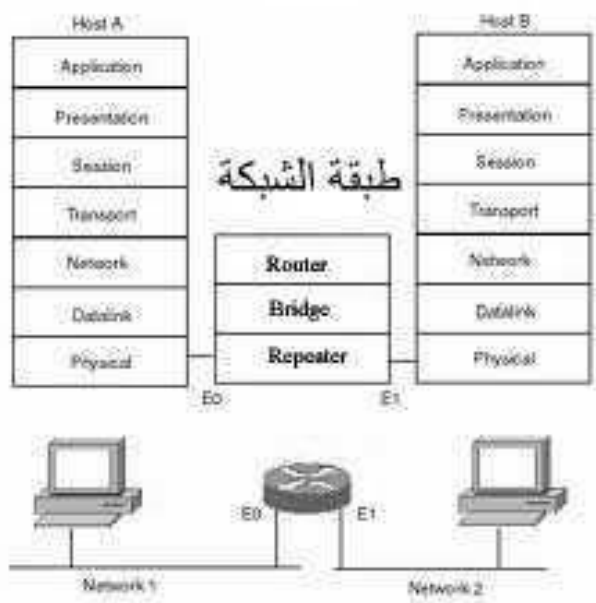
**ومن عيوب المبدلات أنها تنقل كل رسائل التبليغ إلى كل الأجهزة على الشبكة.**



شكل (٢٦-٤) يوضح تخصيص قناة لكل جهاز باستخدام switch.

## سادساً: الموجهات Routers

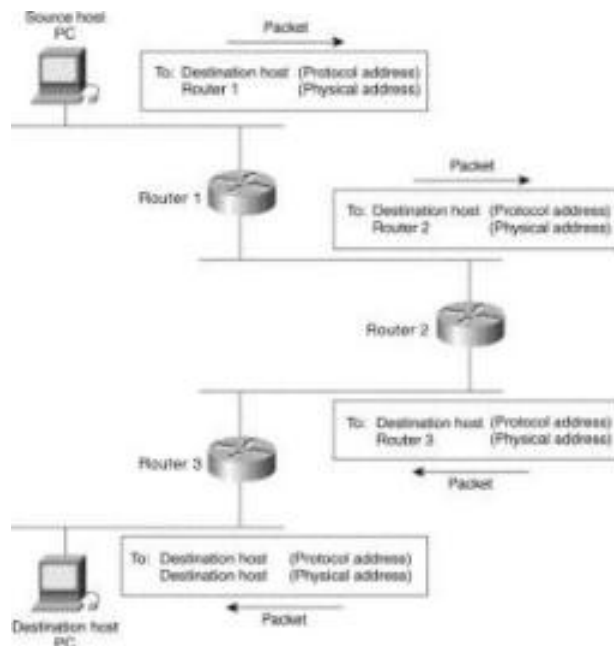
يعتبر الموجه من الأجهزة التي تربط بين شبكتين محليتين مختلفتين. بما أن الشبكات المختلفة تتميز باختلاف عناوينها فإن الموجه يحقق هدفه مستعيناً بالمعلومات التي ينشئها بروتوكول IP مما يعني أن الموجه يعمل على طبقة الشبكة في نموذج OSI المرجعي، وهذا يدل على أنه طالما تكون هناك شبكات محلية تستخدم نفس بروتوكول طبقة الشبكة فإنه من الممكن أن تربط مع بعضها بواسطة موجه حتى ولو استخدمت هذه الشبكات المحلية بروتوكولات أو تكنولوجيات مختلفة على مستوى طبقة ربط البيانات. يعني هذا أنه بإمكان الموجه الربط بين شبكة اترنت Ethernet وشبكة Token Ring. يكون ربط الموجهات مع بعضها ما يسمى بالشبكة الجامعة (Internetwork).



شكل (٢٧-٤) يوضح أن الموجه يعمل على طبقة الشبكة.

عندما يريد جهاز موجود على الشبكة المحلية الاتصال بجهاز على شبكة محلية أخرى يرسل بياناته إلى موجه الشبكة المحلية الذي بدوره يرسل البيانات إلى الشبكة المحلية المقصودة والتي قد تكون موصلة مباشرة بالموجه في حالة ما كان جهاز الوجهة على هذه الشبكة أو إلى موجه آخر في حالة ما إذا كان الجهاز مربوطاً على شبكة أخرى ويعيد الموجه الثاني نفس العملية التي قام بها الموجه الأول يعني إرسال البيانات إلى جهاز آخر مشبوك على شبكته أو توجيهها إلى موجه آخر وهكذا تستمر العملية إلى أن تصل البيانات إلى وجهتها الأخيرة.

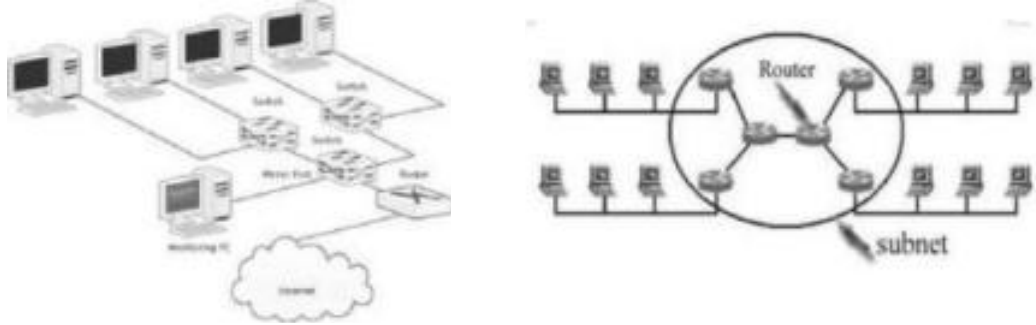
إن شبكة الانترنت نموذج شبكة جامعة تتكون من عدد كبير من الشبكات موصلة مع بعضها بواسطة موجهات.



شكل (٢٨-٤) يوضح كيفية توجيه البيانات باستخدام الموجه.

## طريقة عمل الموجهات

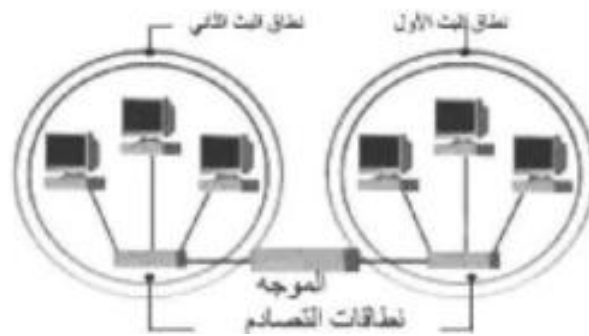
عندما تصل البيانات إلى الموجه وتدخل عبر أحد بطاقاته تتابع البيانات طريقها للأعلى حتى تصل إلى طبقة الشبكة، حينئذ تتم إزالة إطار طبقة ربط البيانات وبعدها يمرر الموجه البيانات للأسفل لكن هذه المرة عبر بطاقة شبكة ثانية التي تقوم بتغليف البيانات بإطار جديد ثم إرسالها على الشبكة المحلية الثانية.



شكل (٢٩-٤) يوضح استخدام الموجه في الربط بين أكثر من شبكة

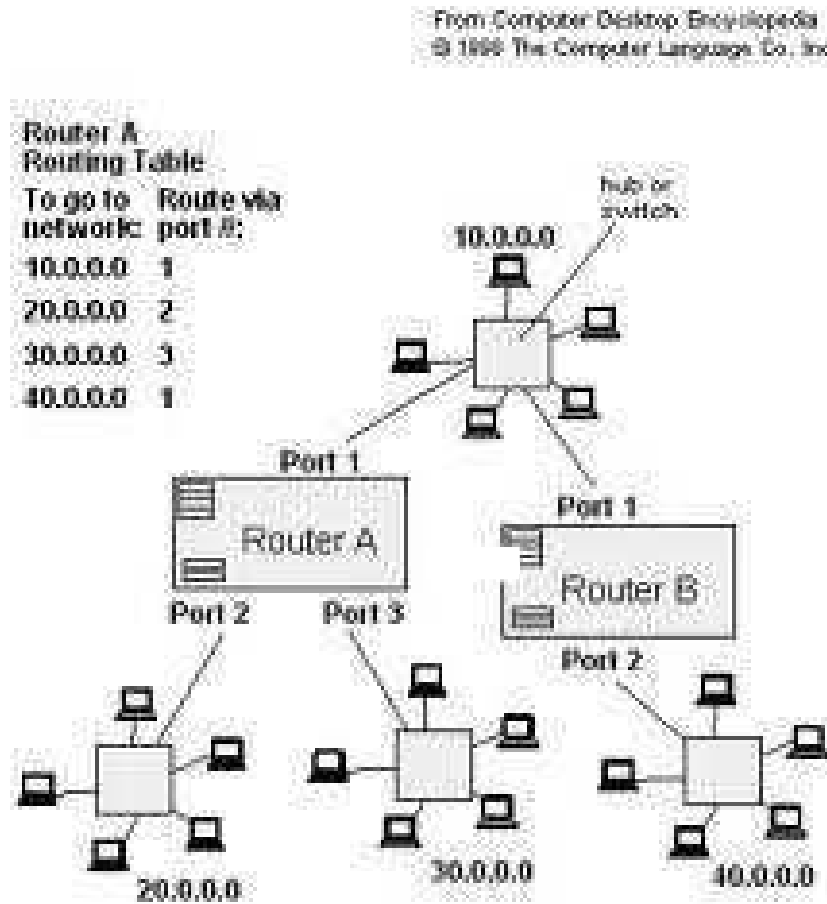
## مزايا الموجهات :

من مزايا الموجهات أنها تجزيء نطاق البث بمعنى أنها لا توجه رسائل التبليغ المرسل من قبل جهاز ما إلى شبكة أخرى إنما تتركها على نفس الشبكة التي يوجد عليها الجهاز المولد للبلاغ.



شكل (٣٠-٤) يوضح كيف يعزل الموجه نطاقات التصادم والتبليغ.

يتضمن الموجه جداول تسمى جداول التوجيه والتي تحتوي على معلومات عن الشبكة المحيطة به. ومن خلال هذه الجداول يقرر الموجه بإرسال رزمة البيانات إلى جهاز متصل بالشبكة المجاورة له أو إرسالها إلى موجه آخر.



شكل (٣١-٤) يوضح كيف يقوم الموجه بعمل جدول توجيه



## مكونات الشبكة اللاسلكية

إن الشبكة المحلية اللاسلكية هي ببساطة تتألف من مكونين هما:

### ١. بطاقة الاتصال اللاسلكي:-

تثبت هذه البطاقة في الحاسوب أو أي جهاز نرغب أن يكون عضوا في الشبكة اللاسلكية كالطابعات مثلاً، وكما مر معنا فإن معظم الحواسيب المحمولة تأتي مزودة بهذه البطاقة من مصنعها، أما الحواسيب المحمولة غير المزودة بالبطاقة أو الأجهزة الأخرى فلا بد من تزويدها بها لتكون قادرة على الاتصال، و في الشكل رقم (٣٢-٤) أحد أنواع كروت الاتصال اللاسلكي الذي يمكن استخدامه في الحواسيب المحمولة.



شكل (٣٢-٤) : بطاقة الاتصال اللاسلكي

ودور بطاقة الاتصال تمرير البيانات جيئة و ذهاباً بين الحاسوب و الشبكة اللاسلكية، فهي نقطة الوصل بين الطرفين.

### ٢. نقطة الدخول إلى الشبكة:

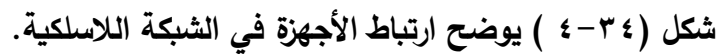
وهذه تسمى (Access Point) و هي عبارة عن جهاز صغير به هوائي صغير كما في الشكل (٣٣-٤) ، و يبث الجهاز الموجات الكهرومغناطيسية

لنقل البيانات بين نقطة الدخول و الأجهزة المزودة ببطاقات الاتصال بالشبكة اللاسلكية السابق ذكرها في الفقرة السابقة، و يعمل هذه النقطة مع الأجهزة يتألف لدينا شبكة لاسلكية .



شكل ( ٣٣-٤ ) يوضح نقطة الدخول إلى الشبكة.

وفي معظم الأحيان نرغب في أن نربط الشبكة اللاسلكية بشبكة المعلومات الأم في المنشأة، أو بشبكة الإنترنت، و يتحقق هذا بربط نقطة الدخول بالشبكة الأم أو شبكة الانترنت، و بهذا يمكن لكل جهاز في الشبكة اللاسلكية الاتصال بالشبكة الأم أو الدخول إلى شبكة الإنترنت كما يمكن للمستخدمين في الشبكة الأم أو شبكة الإنترنت الوصول إلى الأجهزة التي تؤلف الشبكة اللاسلكية.



A diagram illustrating a mobile ad hoc network topology. It shows three mobile devices: two laptops at the top and a mobile phone at the bottom. The devices are interconnected by lightning bolt symbols, representing wireless communication links. The topology is a triangle, with each device connected to the other two, forming a mesh network.

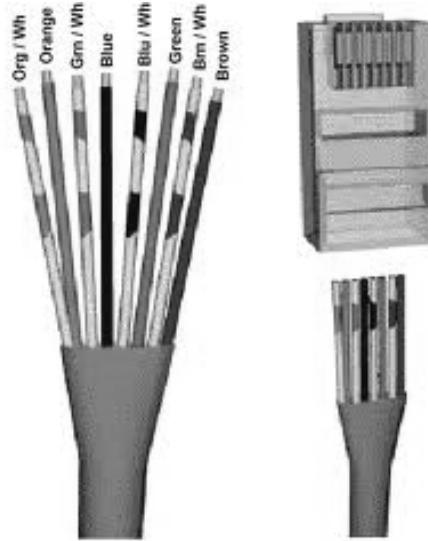
شكل (٣٥-٤) شبكة لاسلكية بسيطة (بدون نقطة دخول)



## الباب الخامس

### وسائط الاتصال في الشبكات

### (كابلات الشبكة)



## أهداف الباب الخامس

بعد الانتهاء من دراسة هذا الباب ينبغي أن يكون الطالب قادراً على أن:

- ١- يُعرف وسيط الاتصال داخل الشبكة.
- ٢- يفرق بين وسائط الاتصال داخل الشبكة.
- ٣- يُعدد خواص الأوساط.
- ٤- يعدد الصور التي توجد عليها الوسائط السلوكية.
- ٥- يعدد الموجات التي تنتقل من خلالها الشبكات اللاسلكية.
- ٦- يبرر سبب أهمية بطاقة الشبكة عند الربط بين الأجهزة.
- ٧- يحدد العوامل التي تساعد على اختيار نوع الوسيط.
- ٨- يوضح مكونات الكابل المحوري بالرسم.
- ٩- يذكر أنواع الكبلات المحورية.
- ١٠- يفرق بين Base ٢ ، Base ٥ ، Base ١٠.
- ١١- يعدد استخدامات كبل الزوج الملتوي.
- ١٢- يبرر السبب في جدولة الأسلاك.
- ١٣- يبرر السبب في تصنيف كبلات STP.
- ١٤- يطبق معايير توصيف UTP عند تجهيز الكبل.
- ١٥- ينشئ وصلة عبور في الكبل (Cross over).
- ١٦- يبرر سبب أهمية كبل العبور.
- ١٧- يذكر مكونات الليف البصري.
- ١٨- يعدد مزايا الليف البصري.
- ١٩- يعدد عيوب الكبلات النحاسية.
- ٢٠- يعدد أنواع الألياف البصرية.
- ٢١- يوضح ما تدل عليه أو ما يمكن الكشف عنه باستخدام أجهزة اختبار الكبلات.
- ٢٢- يحدد الدور الذي يقوم به جهاز توليد الإشارة والتقاطها.
- ٢٣- يحدد الدور الذي يقوم به جهاز اختبار مخطط الأسلاك.
- ٢٤- يحدد الدور الذي يقوم به جهاز اختبار الكبلات متعدد الوظائف.

## وسائط الاتصال في الشبكات (كابلات الشبكة)

وسط الاتصال داخل الشبكات Network Media الذي يتحقق انتقال البيانات فيه إما أن يكون:

### ١ - سلكياً (Using Cable) على صورة أسلاك موصلة مثل:

- الكابلات المحورية Coaxile.
- الكابلات المجدولة Twisted Pair.
- كابلات الألياف الضوئية Fiber Optic.

### ٢ - Wireless بانتشار في طبقات الجو المختلفة مثل

- الموجات تحت الحمراء Infra red.
- الموجات متناهية القصر Microwave.
- موجات الراديو Radio.

كل وسط Media يستطيع تحقيق مجموعة من الخواص تناسب أنواع محددة من الشبكات. ولاختيار أفضل وسط يناسب الشبكة التي تصممها ينبغي معرفة خواص الأوساط ومقارنتها بالعوامل التالية:

- التكلفة Cost.
- التركيب Installation.

- السعة Capacity.
- التضاؤل Attenuation.
- التداخل مع الموجات الكهرومغناطيسية Electro Magnetic Interference (EMI).

## ١ - التكلفة:

التكلفة عليها عامل كبير في تحديد نوع الوسط المستخدم فإذا كانت التكلفة المفترضة للشبكة كبيرة فيمكن اختيار نوع وسط غالي وسريع، أما إذا كانت التكلفة قليلة، فينبغي مراعاة الموازنة بين السرعة المطلوبة و التكلفة المفترضة، حتي لا يتم اختيار كابلات لا تحقق الاتصال المطلوب، فكابلات الألياف الضوئية Fiber Optic cabl رعات عالية جداً وثنها مرتفع ب ولكن قد لا تحتاج الشبكة التي تصممها هذه السرعة العالية وبالتالي فإن اختيار هذا النوع يعد إهداراً للأموال.

## ٢ - التركيب Installation :

هناك أنواع من الكابلات سهلة التركيب مثل الكابلات المحورية Coaxile Cables والكابلات المجدولة Twisted Pair، فإذا كانت الشبكة صغيرة وبتكلفة قليلة ولا تحتاج لخبراء في تركيبها فلن تحتاج هذه الشبكة الى كابلات



الألياف الضوئية Fiber Optic Cables ، والتي تحتاج لشركات متخصصة وعالية الأجر لتوصيلها.

### ٣- السعة Capacity :

سعة النطاق (سرعة نقل المعلومات) Bandwidth Capacity or Transmission Speed ، وتقاس سعة الوسط Medium Capacity بما يسمى سعة النطاق Band Width(BW) أو عرض النطاق أو سرعة نقل المعلومات Transmission Speed ، وتقاس هذه السرعة بالمليون بت على الثانية.

### ٤- عدد الأجهزة المراد توصيلها Node Capacity :

كل نظام كابلات يحدده عدد معين من الأجهزة يمكن توصيله بدون إضافة أجهزة لتقوية الإشارة إضافية وغالية.

### ٥- التضاؤل Attenuation:

عند نقل المعلومات من جهاز لآخر فإنها تنتقل على صورة إشارات كهرومغناطيسية Electromagnetic Signals وهذه الإشارات تضعف قوتها

أثناء الاتصال فيما يعرف بالتضاؤل Attenuation، فمع بعد المسافة يحدث تسرب وتضاؤل Degradation حتى تصل إشارة ضعيفة وتحمل الكثير من الأخطاء.

- يجب مراعاة الحد الأقصى لطول الكابل بين الجهاز والآخر لتجنب التضاؤل.
- يتناسب التضاؤل Attenuation تناسباً عكسياً مع طول الكابل  
High Attenuation=Short distance

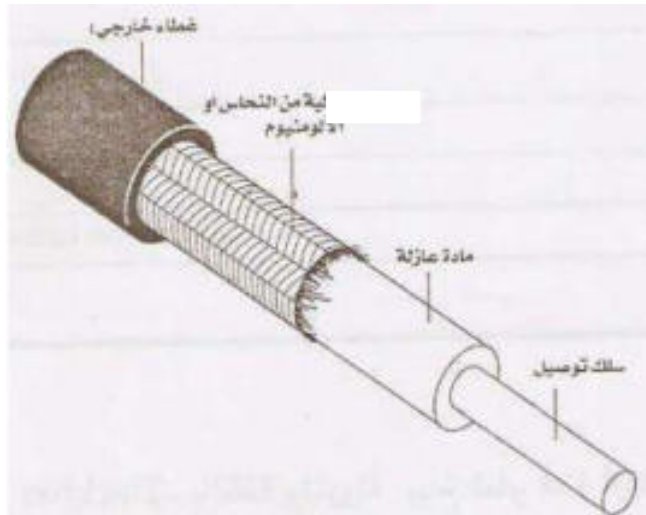
## ٦- التداخل مع الموجات الكهرومغناطيسية Electro Magnetic Interference (EMI)

هنا الأوساط تتأثر بالمواد كهرومغناطيسية المحيطة مما يـ على تشويش الإشارة المتنقلة.

- EMI هو عبارة عن المجال الكهرومغناطيسي الذي ينشأ بسبب وجود مجال كهربائي وهي العامل الوحيد الذي يتأثر بالكهرباء لأن التضاؤل Attenuation يتأثر بطول الكابل.
- ينتج التداخل بسبب الضوضاء المحيطة بالوسط.
- الأوساط التي لها (EMI) عالية فإنها غير آمنة ويمكن التصنت وتتبع المعلومات من الخارج لذا لا يمكن استخدامها إذا كانت الشبكة تحتاج إلى سرية في نقل المعلومات.

## أولاً: الكابلات المحورية Coaxial cables

- يحتوي الكابل المحوري على ناقلين من نحاس موضوعين واحداً داخل الآخر ضمن نفس الغمد. مهمة الناقل الداخلي هي نقل الإشارات الكهربائية التي تمثل البيانات المتبادلة بين أجهزة الحاسب في الشبكة. أما مهمة الناقل الثاني والذي يأتي على شكل شبكة من أسلاك نحاسية فإنه يعمل كقطب أرضي للسلك. يوجد بين الناقلين طبقة عازلة داخلية. يغلف غمد خارجي عازل كلاً من الناقلين والطبقة العازلة الداخلية.



شكل (٥-١) يوضح الكابل المحوري.

يوجد نوعان من الأسلاك المحورية وهي السلك المحوري المرن والذي يسمى RG٥٨ والسلك المحوري السميك والمعروف باسم RG٨. يعتبر RG٨

أكثر سماكة من RG٥٨ ويستخدم RGA وصلة من نوع N. أما RG٥٨ فيستخدم وصلة من نوع BNC. ويبين الشكل التالي أنواع الوصلات المستخدمة مع الكابلات المحورية.



شكل (٥-٢) يوضح وصلات من نوع BNC والمستخدمات مع الكابلات المحورية



شكل (٥-٣) وصلة من نوع BNC-T

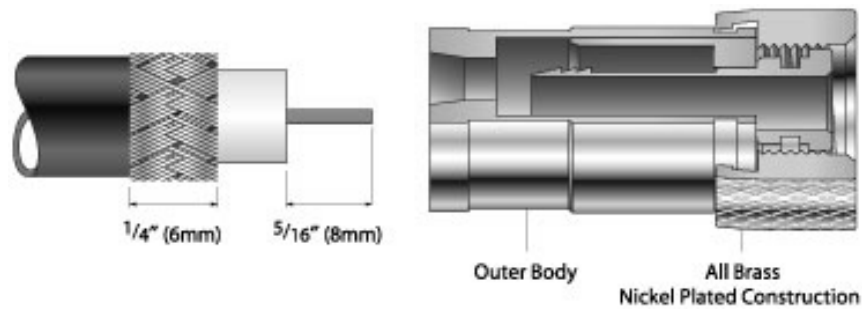
يعرف هذين النوعين من الأسلاك المحورية أيضاً باسم Base٢ ١٠ للسلك المرن أو Thin Ethernet و Base٥ ١٠ بالنسبة للسلك الثخين أو Thick Ethernet.

علماً بأنه في حالة Base٢ ١٠ أقصى طول يتحمله أي جزء دون استخدام مكرر للإشارة هو ٢٠٠ متر (١٨٥ متر بالتحديد) وبالنسبة لـ Base٥ ١٠ يبلغ أقصى طول لأي قطعة من الكبل ٥٠٠ متر.

وغالباً ما يستخدم هذا النوع من الكبلات في البنية الطبوغرافية الخطية. ومن عيوب الكابلات المحورية : الحجم وقلة المرونة التي تزيد في صعوبة تركيبها وصيانتها.

### تجهيز الكبل المحوري

تتم عملية تجهيز الكبل المحوري الرقيق بتركيب وصلات من نوع BNC على أطراف كل قطعة من القطع المستخدمة لربط العدد اللازم من الأجهزة في الشب لا تشبيك ٢٠ جهاز ف الخطية يستلزم استخدام ١٩ ق من الكبلات لا يتجاوز طول الواحدة منها مترين و تكون كل واحدة منها مزودة بوصلتين BNC . توصل كل قطعة الى أحد أذرع وصلة BNC T من كلا الجهازين المتجاورين و هكذا الى أن توصل كل الأجهزة. يتم بعد ذلك تركيب وصلة من نوع النهاية الطرفية BNC Terminator على أول و آخر جهاز في البنية الخطية.





شكل (٤-٥) يوضح الأداة المستخدمة في تجهيز الكبلات المحورية

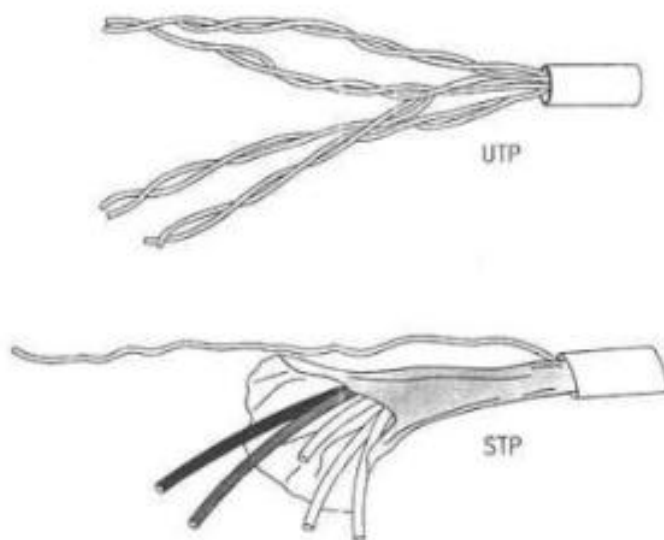
و دور النهاية الطرفية BNC Terminator التي تتركب على أول وآخر جهاز في البنية الخطية هو امتصاص الإشارة لتحرير الكبل وإعطاء فرصة لجهاز آخر بياناته. يتقبل هذا ١ من الشبكات ٣٠ جهاز على الأ موزعة على جزء أقصى طوله ١٨٥ متر، أقل مسافة مسموحة بين أي جهازين متجاورين هي نصف متر.

تعتبر عملية تثبيت وصلة من نوع BNC على أية قطعة من الكبل المحوري من العمليات الأساسية لتجهيز هذا النوع من الكبلات.

## ثانياً: كبل الزوج الملتوي أو المجدول Twisted Pairs

تستخدم معظم الشبكات المحلية كابلات الزوج الملتوي غير المعزول (Unshielded Twisted Pair) UTP ، ويوجد أيضاً الزوج الملتوي المعزول (Shield Twisted Pair) STP والمستخدم خصيصاً في الأماكن المعرضة للإشعاع الكهرومغناطيسي ولمصادر أخرى من التشويش.

تقلل الجدولة من تأثير الأسلاك على بعضها وقت نقلها للإشارات الكهربائية المتمثلة في البيانات المتبادلة بين أجهزة الشبكة، وللجدولة أيضاً دور في المقاومة للتشويش الخارجي.



شكل (٥-٥) يوضح كلاً من كبلات UTP و STP.

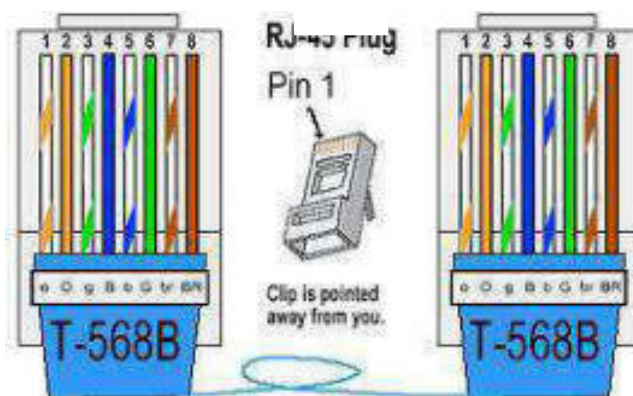
## تصنيف كابلات STP

تحتوي كابلات STP على طبقة رقيقة أو شبكة عازلة دورها حماية البيانات أو الإشارات من الإشعاع الكهرومغناطيسي في الأماكن القريبة من الأجهزة الكهربائية، وفي هذه الحالات يفضل استخدام STP بدلاً من UTP.

أنواع STP هي A1 الذي يستخدم للوصلات الطويلة و A7 الذي يستخدم للوصلات القصيرة.

## معايير توصيل أسلاك UTP و STP

يستخدم في الشبكات معياران لتوصيل كابلات UTP و STP بالوصلات وهما ٥٦٨A و ٥٦٨B. ويبين الشكل التالي ألوان الأسلاك وأرقام التماسات المقابلة لها في كل واحد من هذين المعيارين.



شكل (٥-٦) يوضح معايير توصيل الأسلاك في كابلات UTP

نلاحظ أنه في كلا المعيارين تحتفظ الأزواج الزرقاء والبنية بأماكنها، أما الأزواج البرتقالية والخضراء فانها تستبدل أماكن بعضها، يعني أن الزوج البرتقالي يحل محل الزوج الأخضر والعكس.

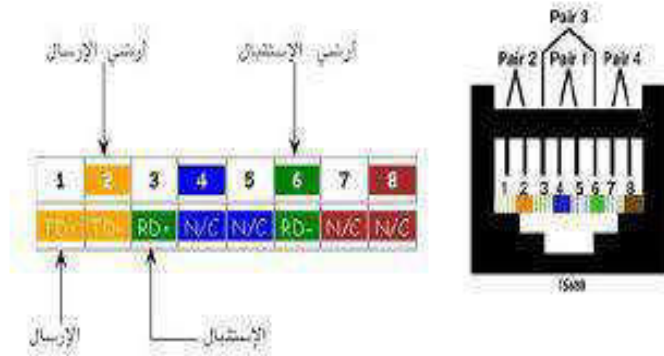


إن المعيارين ٥٦٨A و ٥٦٨B متكافئان في العمل. من الضروري أن نختار أحد المعيارين بحيث يكون ثابت على كل الوصلات. نحتفظ به خلال كل عملية التوصيل. أي لا نستطيع استخدام معيارين مختلفين في نفس الشبكة.

في أغلب الحالات نستخدم أربعة أسلاك من ضمن الثمانية، اثنان للإرسال واثنان للاستقبال ويوضح الشكل التالي الأطراف المستخدمة للإرسال والأطراف المستخدمة للاستقبال في حالة المعيار ٥٦٨A.

إن المعيارين ٥٦٨A و ٥٦٨B متكافئان في العمل. من الضروري أن نختار أحد المعيارين بحيث يكون ثابت على كل الوصلات. نحتفظ به خلال كل عملية التوصيل. أي لا نستطيع استخدام معيارين مختلفين في نفس الشبكة.

في أغلب الحالات نستخدم أربعة أسلاك من ضمن الثمانية، اثنان للإرسال واثنان للاستقبال ويوضح الشكل التالي الأطراف المستخدمة للإرسال والأطراف المستخدمة للاستقبال في حالة المعيار ٥٦٨A.



شكل (٥-٧) يوضح التوصيلات في حالة المعيار ٥٦٨B.

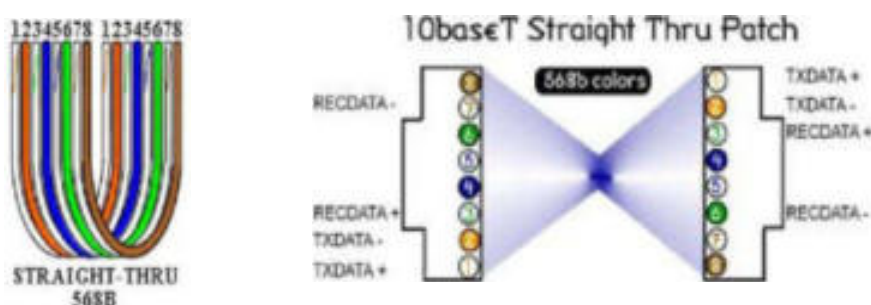
أسباب كثيرة جعلت من الزوج الملتوي يحل محل السلك المحوري وهي: مرونة الزوج الملتوي ، عدد أسلاكه، سعره ، وسهولة تركيبه وصيانته.

## تجهيز كابل UTP

يتضمن كبل UTP ثمانية أسلاك منفصلة، تضم مع بعضها في أربعة أزواج ملتوية، يثبت على طرفي الكبل وصلة من نوع RJ٤٥ والتي تتضمن ثمانية تماسات ناقلة موصلة بالأسلاك الثمانية في الكبل. عندما نوصل الكبل الجاهز ببطاقة الشبكة تتلامس تماسات الوصلة من نوع ذكر من جانب الكبل بتماسات الوصلة من نوع أنثى من جانب بطاقة الشبكة فتشكل دائرة كهربية.

تستخدم شبكات Ethernet المعيارية من نوع ١٠BaseT و ١٠BaseTX أربعة أسلاك من الأسلاك الثمانية في كبل UTP، أما الشبكات من نوع ١٠Base٤ فإنها تستخدم الأسلاك الثمانية.

في وصيل جهاز كمبيوتر مع مركزي فإننا نستخدم الوصل المستقيمة (Cable thru) ، ويعني هذا توصيل كل سلك مع نفس التماس في الوصلتين. تماسات الإرسال في طرف من الكبل تتصل مع تماسات الإرسال في الطرف الآخر وتماسات الاستقبال في الطرف الأول تتصل مع تماسات الاستقبال في الطرف الثاني.

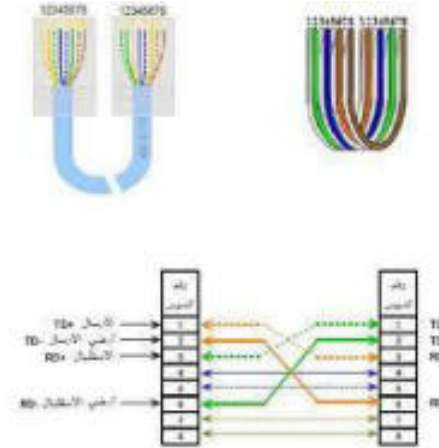


شكل (٨-٥) يوضح كيفية توصيل الأسلاك في المعيار T٥٦٨B

نلاحظ انه من غير الممكن توصيل جهازين مباشرة بواسطة وصلة مستقيمة، وفي مثل هذه الحالة المجمع المركزي هو الذي يضمن دائرة العبور لإمكانية تبادل المعلومات بين الجهازين.

من الممكن توصيل جهازين مباشرة وهذا بإنشاء وصلة عبور ( crossover cable ) في الكبل. في هذه الحالة نربط سلكي الإرسال بسلكي الاستقبال المقابلين لهما. نوصل التماس TD+ على كل طرف مع التماس RD+ في الطرف الآخر. بشكل مشابه، نوصل التماسين TD- مع التماسين RD-، تمكن هذه الطريقة من إرسال بيانات من جهاز وإمكانية استقبالها على جهاز آخر. لا نستطيع استخدام كبل عبور لتوصيل جهاز كمبيوتر بمجمع مركزي، لأن دائرة عبور المجمع تلغي دائرة عبور الكبل وتصبح أسلاك الإرسال مقابلة لأسد رسال في الجهاز الثالث ، يلغي عملية تبادل البيانات الجهازين.

نلاحظ في الشكل التالي كيف تتم عملية توصيل الأسلاك بتماسات الوصلتين RJ45 لإنجاز كبل عبور (Crossover Cable).



شكل (٩-٥) يوضح كيفية توصيل الأسلاك في كابل العبور (Crossover Cable).

**عملية تركيب الوصلات RJ٤٥:**

تسمى عملية توصيل أطراف الكبل غير الجاهز بالوصلات بعملية الكبس، أهم جزء في عملية كبس الأسلاك هي وضع الأسلاك على التماسات الصحيحة المقابلة لها. الأسلاك في كبل UTP تتخذ الألوان البرتقالي، الأخضر، الأزرق و البني.

**عملية تثبيت الوصلات:**

تتطلب عملية تثبيت الوصلات RJ٤٥ بكبل UTP استخدام أداة خاصة تسمى لاوية Crimper وتتضمن اللاوية مجموعة من اللقم اللولبية تمكن من عصر جزئي وصلة RJ٤٥ مع بعضهما وبداخلهما الأسلاك. ويبين الشكل التالي الأدوات المستخدمة في تأريج الكبلات.



شكل (٥-١٠) يوضح الأدوات المستخدمة في تجهيز كبل UTP



شكل (٥-١١) يوضح الموصل Connector

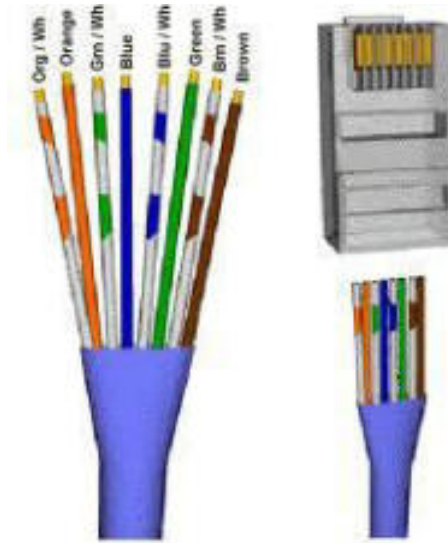
وتتألف عملية تثبيت وصلات RJ٤٥ من الخطوات التالية:

### ١- تجريد قليل من العازل عن الكابل



شكل (١٢-٥) يوضح كيفية تجريد العازل.

### ٢- ترتيب الأسلاك حسب المعيار الذي اخترنا استخدامه:



شكل (١٣-٥) يوضح كيفية ترتيب الألوان في كابل UTP.

### ٣- قص الأسلاك لتسهيل وضعها في الوصلة



شكل (١٤-٥) يوضح كيفية قص الأسلاك

### ٤- وضع الأسلاك داخل الوصلة



شكل (١٥-٥) يوضح الأسلاك بداخل الوصلة

### ٤- وضع الوصلة مع الأسلاك في المكان المخصص في اللاوية



شكل (١٦-٥) يوضح وضع الوصلة مع الأسلاك في المأخذ المخصص

٦- الضغط بقابض اللاوية لعصر الأسلاك وإمكانية التماسها بالتماسات. إعادة الخطوات من ١ إلى ٦ بالنسبة للطرف الثاني من الكبل. وهكذا نكون قد ثبتنا ك الثمانية في نفس ويكون الكبل جاهزاً لتوصيل الكمبيوتر إلى المجمع. من الأفضل اختبار الكبل قبل استخدامه، وهذا بواسطة أجهزة خاصة لاختبار الكبلات.



شكل (١٧-٥) يوضح كبل ذو وصلة مستقيمة جاهز للاستخدام

### ثالثاً: الألياف البصرية

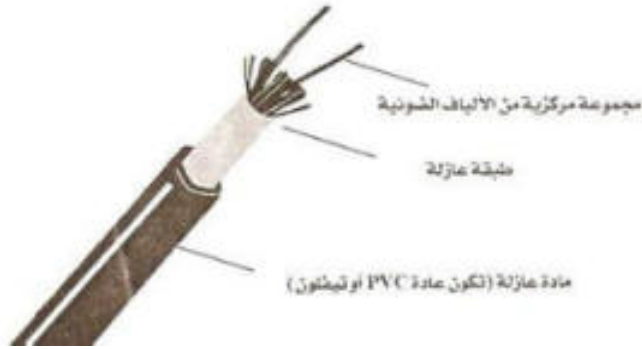
يتكون الليف البصري من ناقل زجاجي أو بلاستيكي. تكون الإشارات أو البيانات المرسلّة عبر الألياف البصرية عبارة عن نبضات ضوئية لذلك فإن الألياف البصرية غير حساسة للتشويش الكهرومغناطيسي الذي يؤثر بسهولة على الكابلات التي تعتمد على الأسلاك النحاسية.

من عيوب النواقل النحاسية هو ضعف الإشارة المرسلّة مع المسافة أو طول الكبل. تصبح الإشارة غير مقروءة بعد ١٠٠ متر في حالة UTP وبعد ٥٠٠ متر في حالة Base٥٠.

سبة للألياف البصرية ممكن امتداد الكبل إلى طول كيلو ن انخفاض ملحوظ في أو قدرة الإشارة مما يجعل هذا من النواقل ملائم لربط الأنظمة البعيدة عن بعضها.

يتألف الليف البصري من ناقل من زجاج أو بلاستيك والذي دوره نقل البيانات التي تكون في هذه الحالة عبارة عن نبضات ضوئية. يحيط بهذا الناقل طبقة عاكسة والتي دورها إبقاء النبضات الضوئية تتعكس إلى داخل الناقل الزجاجي بدلاً من مغادرته. يوجد حول الطبقة العاكسة فاصل بلاستيكي، يليها طبقة داعمة من الكيفر وغمد خارجي واق.

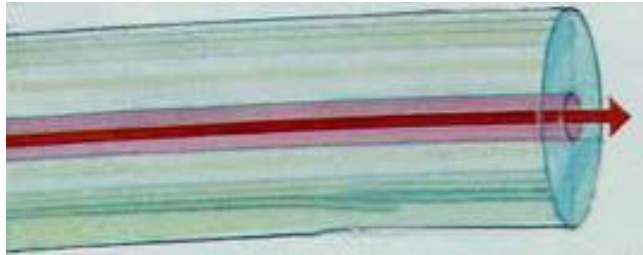




شكل (٥-١٨) يوضح الليف البصري.

### أنواع الألياف البصرية

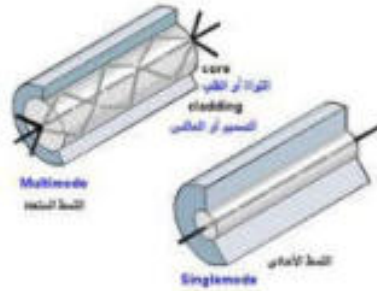
هناك نوعان من كبلات الليف البصري وهما أحادي النمط (Single mode) متعدد الأنماط (Multimode). يتميز أحادي النمط بقيمة ميكرون (مليون من المتر) لقطر الناقل وبقيمة ١٢٥ ميكرون لسماكة الناقل مع الطبقة العاكسة. ويستخدم هذا النوع من الكبل شعاع ليزر أحادي طول الموجه كمصدر لنقل النبضات وبإستطاعته حمل الإشارات إلى مسافات طويلة جداً.



شكل (٥-١٩) يوضح الليف البصري أحادي النمط

أما متعدد الأنماط فيتميز بناقل قطره ٦٢.٥ ميكرون وبسماكة الناقل مع الطبقة العاكسة تساوي ١٢٥ ميكرون. يستخدم هذا النوع من الليف البصري

ثنائياً قاذفاً للضوء LED كمنبع أو إشارة ضوئية حاملة للبيانات المرسلة. يمتد هذا النوع من الكبلات لمسافات أقل طول من ناظرتها في أحادي النمط.



شكل (٢٠-٥) يوضح الفرق بين النمط الأحادي والمتعدد في الألياف البصرية

#### رابعاً: أجهزة اختبار الكبلات

أجهزة الكبلات هي أجهزة الكبلات. هناك عدة أشياء تجعل الكبل غير صالح للاستخدام. زيادة على انكسار الكبل هناك أسباب كثيرة تجعل الكبل غير صالح، مثل توصيل التماسات على الطرفين بشكل غير صحيح، أو تمرير كبل يعمل بشكل صحيح بجوار محرك كهربائي، أو المسافة بين جهاز الكمبيوتر والمجمع طويلة. كل هذه الحالات تجعل الكبل غير صالح للاستخدام.

تستطيع أجهزة اختبار الكبلات الدلالة على:

- ١- طول الكبل.
- ٢- انكسار في أحد أسلاك الكبل.

٣- تحديد السلك المنكسر

٤- تلامس الأسلاك.

٥- الترتيب الغير سليم للأسلاك مثل (الزوج المقسوم).

٦- قدرة الاشعاع الكهرومغناطيسي.

## ١- جهاز توليد الاشارة و التقاطها

يستخدم هذا النوع من الأجهزة في حالة التمديد الداخلي للكبلات و بالأخص عندما نريد وضع علامات على الكبلات لمعرفة الى أين موصل الطرف الثاني من الكبل. ولتحقيق ذلك نستخدم أداتي توليد الاشارة والتقاطها.



شكل (٢١-٥) يوضح أداتي توليد الإشارة والتقاطها

أداة توليد الاشارة هي جهاز يوصل مع الكبل من أحد الطرفين ثم يرسل إشارة عبر أسلاك الكبل وأداة التقاط الاشارة هي جهاز منفصل مزود بمجس قادر على الكشف على الاشارة وهذا بلامسة إما الناقل أو العازل الخارجي للكبل. عندما يلتقط الجهاز الاشارة يصدر نغمة معناها أن الطرف الثاني للكبل هو الموصل بالطرف الذي موصل بأداة توليد الإشارة.

لذا عندما يكون لدينا عدد كبير من الكبلات يمكننا هذه الأدوات من معرفة الكبل الخاص بوصلة معينة.



إذا نسينا أن نضع علامات على الكبلات خلال عملية التمديد الداخلي، نستطيع من خلال توصيل الأداة الأولى إلى المأخذ الجداري وتمرير المجس على كل واحد من الكبلات من طرف لوحة الوصل، من العثور على الكبل الصحيح.

شكل (٢٢-٥) يوضح إمكانية العثور على الكبل المعني بالأمر

وهكذا بإمكاننا تمييز كبل معين بين حزمة من الكبلات. لجها والتقاط الإشارة عدة أخرى كاختبار وصلات الأسد الثمانية المستقلة داخل كبل UTP وهذا باستخدام لاقطات فك التماسح. وهذا يمكننا من الكشف على الدوائر المفتوحة (غياب النغمة) ودوائر القصر (عندما نلتقط الإشارة على أكثر من سلك).

## ٢-جهاز اختبار مخطط الأسلاك Wire Map Tester

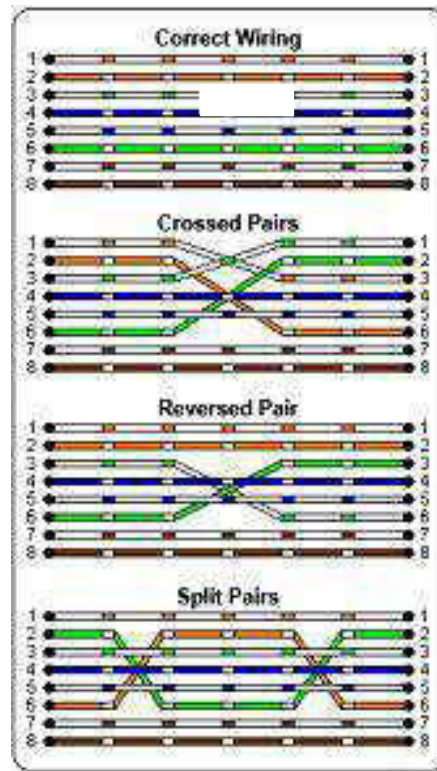
مبدأ هذا الجهاز هو نفس مبدأ أداتي توليد الإشارة والتقاطها، والفرق بينهما أن جهاز اختبار مخطط الأسلاك يفحص كل الأسلاك في كبل UTP دفعة واحدة.

يتألف هذا الجهاز من قطعتين تثبت كل واحدة منهما على أحد طرفي الكبل. تقوم القطعة الأولى بإرسال الاشارات وتقوم الثانية بالتقاط الإشارات



شكل (٢٣-٥) يوضح أجهزة اختبار الكبلات

من امكانيات هذا الجهاز أيضاً الكشف عن الأسلاك المقلوبة، الدوائر المفتوحة و حالات القصر، ويظهر في الشكل التالي حالة زوج مقسوم، زوج مقلوب وتوصيل صحيح.



شكل (٢٤-٥) يوضح توصيل صحيح، زوج معكوس، مقلوب، وزوج مقسوم.

الشيء الذي لا يستطيع جهاز اختبار مخطط الأسلاك الكشف عنه هو حالة الزوج المقسوم Split Pairs، الزوج المقسوم هو خطأ توصيل يتم فيه وصل الأسلاك بالتماسات الخاطئة على طرفي الكبل بنفس الطريقة تماماً.

يوصل كل تماس بشكل مباشر مع التماس المقابل له على الطرف الآخر، يكون سلك من كلا الزوجين موصلاً وكأنه بشكل زوج مثلاً الأزرق و الأبيض/برتقالي موصلان بالتماسات ٤و٥ والأبيض/أزرق والبرتقالي موصلان بالتماسات ٣و٦. فيبدو الوصلة صحيحة لجهاز اختبار مخطط الأسلاك. لكن الأسلاك التي تحمل الإشارات تشكل زوجاً خاطئاً. في حالة الزوج المقسوم قد يتشكل زوج من السلكين المرسل والمستقبل والزوج الآخر من سلكي الأرضي. حينئذ يزداد التشويش الجانبي (NEXT) إلى حد كبير مما يؤثر سلبياً على الات

تبدو الأمور عادية بالنسبة لجهاز اختبار مخطط الأسلاك الذي لا يتمكن من اكتشاف هذا الخلل لذلك يحتاج الأمر إلى أجهزة أكثر تطوراً والتي زيادة عن اختبارها لمخطط الأسلاك تقيس مقدار التشويش الصادر عن هذا الخلل. من بين الأجهزة التي تمكن من الكشف عن هذا النوع من المشاكل جهاز اختبار الكبلات متعدد الوظائف.

### ٣- جهاز اختبار الكبلات متعدد الوظائف

يتميز جهاز اختبار الكبلات متعدد الوظائف بكثرة العمليات الاختبارية التي يؤديها على الكبلات.



أجهزة (٢٥-٥) يوضح أجهزة اختبار الكبلات متعددة الوظائف

بإمكاننا برمجة هذا الجهاز بإدخال قيم معيارية خاصة بكل اختبار نريد أن نؤديه. بعد توصيل الكبل على الجهاز، نضغط على زر فيقوم الجهاز بعرض قائمة من معدلات النجاح والفشل خاصة باختبارات مختلفة.

## من التي يقوم بها ج تبار الكبلات متعدد الوظائف

### ١ - قياس طول الكبل

يتحقق هذا النوع من العمليات عند استخدام مبدأ قياس زمن ارتداد الإشارة. لهذا يرسل الجهاز نبضة عبر الكبل ويقيس الوقت الذي تستغرقه هذه النبضة لترتد أو تنعكس من الطرف الثاني. تنتقل الإشارة في الكبل بسرعة تتراوح بين ٥٩٪ و ٦٥٪ من سرعة الضوء، يطلق على هذه السرعة اسم السرعة الدنيا للإشارة (Nominal velocity of Propagation) NVP والتي غالباً ما تكون معينة من قبل الشركة المصنعة للكبل.

بعد برمجة قيمة NVP على الجهاز، يستطيع الجهاز أن يدلنا على طول الكبل باستخدام المعادلة التالية:

الطول =  $(T \times NVP) / 2$ ، حيث T هو زمن ذهاب وإياب اشارة على طول الكبل. فباستخدامنا هذه الطريقة نتمكن من تحديد مكان القطع في الكبل بدقة.

## ٢ - قياس التلاشي

التلاشي هو ضعف الإشارة عندما تنتقل على الكبل. فيقوم الجهاز بمقارنة قوة الإشارة على الطرف الثاني للكبل بقوتها على الطرف الأول يعني عند الإرسال. يكون مقدار التلاشي يساوي قوة الإشارة عند الاستقبال مقسومة على قوتها عند الإرسال تمكننا قيمة مقدار التلاشي من معرفة ما إذا كان ممكن استخدام هذه القطعة من الكبل لأنية وصول معينة.

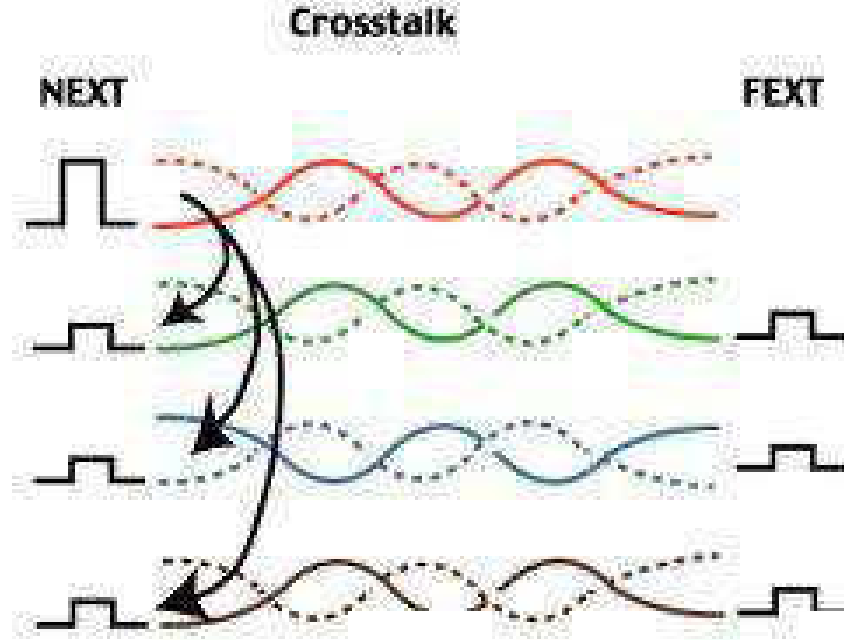
## ٣- قياس التشويش الجانبي على الطرف القريب NEXT ( Near End Crosstalk ):

لفهم ماذا يعني التشويش الجانبي على الطرف القريب NEXT ( Near End Crosstalk )، افترض أنك تتكلم في التليفون، ففي العادة وأنت تتكلم تستطيع أن تسمع الشخص على الطرف الثاني، وفي نفس الوقت تسمع صوتك عبر السماعه.

أما إذا تضخم صوتك حتى يصبح أعلى من صوت الشخص الثاني، بعبارة أخرى يعني NEXT انتشار وانتقال كمية كبيرة من الاشارة المرسله إلى الزوج المستقبل مما يؤثر على البيانات المستقبله ويجعلها غير مفهومه من قبل الجهاز الموصل للزوج المستقبل.



تكون عملية اختبار التشويش الجانبي على الطرف القريب عن طريق إرسال إشارة عبر أحد أسلاك الكبل ثم قياس قوة الإشارة المنتقلة إلى بقية الأسلاك بالقرب من الطرف المرسل للإشارة.



شكل (٢٦-٥) يوضح التشويش الجانبي على الطرف القريب NEXT والبعيد FEXT.

#### ٤- قياس تأخير الانتشار

يقوم الجهاز في هذه الحالة بحساب الزمن الذي تستغرقه الإشارة للانتقال من أحد طرفي الكبل الى الطرف الثاني.



# الباب السادس

## تقنيات الشبكات و تكوين شبكة محلية



## أهداف الباب السادس

بعد الانتهاء من دراسة هذا الباب ينبغي أن يكون الطالب قادراً على أن:

- ١- يُعرف تقنيات الشبكات.
- ٢- يفرق بين أشهر تقنيات الشبكات.
- ٣- يذكر اسم الآلية التي تعمل بها شبكات الانترنت.
- ٤- يُعرف شبكات BaseT ١٠.
- ٥- يُعرف شبكات Base٢ ١٠.
- ٦- يُعرف شبكات Base٥ ١٠.
- ٧- يُعرف شبكات BaseF ١٠.
- ٨- يعدد قواعد توصيل الكبلات المحورية.
- ٩- يُعرف شبكات BaseX ١٠٠ Fast Ethernet.
- ١٠- يُعرف شبكات BaseT٤ ١٠.
- ١١- يُعرف شبكات BaseTX ١٠.
- ١٢- يُعرف شبكات BaseFX ١٠.
- ١٣- يفرق بين شبكات الانترنت التي تستخدم كبلات UTP وتلك التي خدّم الألياف البصرية.
- ١٤- يُعرف تقنية Token Ring.
- ١٥- يبرر السبب في عدم انتشار Token Ring.
- ١٦- يحدد الأجهزة المستخدمة في Token Ring.
- ١٧- يوضح الدور الذي يقوم به جهاز MAU في شبكات Token Ring.
- ١٨- يذكر نوع الكبل الذي يستخدم لربط جهازين MAU.
- ١٩- يذكر الآلية المستخدمة للوصول إلى وسيط الانتقال في شبكات Token Ring.
- ٢٠- يقوم باعداد جهاز الحاسوب للاتصال.
- ٢١- يعنون ويرقم الأجهزة.
- ٢٢- يُعرف الشبكة المخصصة Ad hoc.
- ٢٣- يعدد مميزات الشبكة المخصصة.
- ٢٤- يذكر كيفية اعداد الشبكة المخصصة.
- ٢٥- ينشئ مستخدمين محليين على الأجهزة.
- ٢٦- يشارك الملفات والأجهزة.
- ٢٧- يشغل Network Discovery.

- ٢٨- يبرر السبب في أهمية تشغيل **Network Discovery**.
- ٢٩- يجهز قرصاً كاملاً للمشاركة.
- ٣٠- يعطي صلاحيات لكل مستخدم على الشبكة عند مشاركة مجلد.
- ٣١- يحدد متى يمكن إزالة الحماية بكلمة المرور.
- ٣٢- يدرك كيفية التغلب على مشكلات مشاركة الملفات.
- ٣٣- يقوم بتخينة قرص أو مجلد مشترك.
- ٣٤- يشارك الطابعة.
- ٣٥- يتصل بطابعة تمت مشاركتها.

## تقنيات الشبكات المحلية

يطلق على بروتوكولات طبقة ربط البيانات اسم تقنيات الشبكات ويحدد هذا النوع من البروتوكولات المكونات المادية المستخدمة على مستوى الطبقة الفيزيائية مما يعني أنه المسؤول عن آلية التحكم في الوصول الى وسيط الاتصال Media Access Control . و من أشهر تقنيات الشبكات المحلية Ethernet,Token Ring.

### أولاً: الاثرنت Ethernet

يعتبر بروتوكول Ethernet من أشهر البروتوكولات التي تعمل على طبقة ربط البيانات في الشبكات المحلية (LANs). كان في البداية اترنت محتر على كات التي هي Interox و Intel Equipment Corporation والمعروف باسم Dix Ethernet والذي كان يستخدم السلك المحوري السميك أو RG٨ في الشبكات ذات سرعة ١٠Mbps التي يمتد طول الكبل فيها إلى ٥٠٠ متر والتي تدعى أيضاً شبكات Base٥١٠. ظهر بعدها Dix Ethernet II الذي سمح بإمكانية استخدام السلك المحوري المرن أو RG٥٨ في الشبكات ذات سرعة ١٠Mbps والذي يمتد فيها طول الكبل إلى ٢٠٠ متر. يطلق على هذا النوع من الشبكات اسم شبكات Base٢١٠. ما يدعى حالياً بـ Ethernet هو في الحقيقة مجموعة IEEE٨٠٢,٣ التي تشبه معيار Ethernet والتي تعمل بآلية CSMA/CD (Carrier Sense Multiple Access With Collision Detection) أو ما يعني الوصول المتعدد الحساس للناقل مع كشف التصادمات.

لنرى الآن مواصفات المكونات المستخدمة على مستوى الطبقة الفيزيائية والتي تتمثل في أنواع الكبلات، البنية الطبوغرافية، الأطوال القصوى للكابلات وعدد المكررات التي يستحسن استخدامها في الشبكة لتجنب تأثيرات ضعف الإشارة والتشويش والتصادمات. نستطيع أن نلخص مواصفات الطبقة الفيزيائية لبعض الحالات في Ethernet في الجدول التالي:

جدول (٦-١) يوضح مواصفات الطبقة الفيزيائية في Ethernet

رمز التقنية المستخدمة	البنية الطبوغرافية	نوع الكبل المستخدم	سرعة تبادل البيانات (Mbps)	أقصى طول للكبل (في كل جزء متر)
Base ٢ ١٠	خطية	محوري RG٥٨	١٠	١٨٥
Base ٥ ١٠	خطية	محوري RG٨	١٠	٥٠٠
T ١	نجمية	Catego	١٠	١٠٠
Base FL ١٠	نجمية	ليف بصري متعدد الأنماط	١٠	٢٠٠٠
Base TX ١٠٠	نجمية	Category ٥ UTP	١٠٠	١٠٠
Base T٤ ١٠٠	نجمية	Category ٣ UTP	١٠٠	١٠٠
Base FX ١٠٠	نجمية	ليف بصري متعدد الأنماط ٦٢.٥/١٢٥	١٠٠	٤١٢
Base LX ١٠٠٠	نجمية	ليف بصري وحيد النمط ٩/١٢٥	١٠٠٠	٥٠٠٠
Base SX ١٠٠٠	نجمية	ليف بصري متعدد الأنماط ٦٢.٥/١٢٥	١٠٠٠	٢٢٠
Base SX ١٠٠٠	نجمية	ليف متعدد ٢٠٠MHZ	١٠٠٠	٢٧٥

رمز التقنية المستخدمة	البنية الطبوغرافية	نوع الكبل المستخدم	سرعة تبادل البيانات (Mbps)	أقصى طول للكبل في كل جزء (متر)
Base L ١٠٠٠	نجمية	ليف بصري وحيد النمط ٩/١٢٥	١٠٠٠	١٠٠٠٠
Base ZX ١٠٠٠	نجمية	ليف بصري وحيد النمط ٩/١٢٥	١٠٠٠	١٠٠٠٠
Base CX ١٠٠٠	نجمية	سلك نحاسي معزول (١٥٠Ω)	١٠٠٠	٢٥
Base T ١٠٠٠	نجمية	CAT٥,٥E,UTP	١٠٠٠	١٠٠

كانت IEEE ٨٠٢,٣ تستخدم السلك المحوري المرن والسميك بالإضافة إلى اختيار الزوج الملتوي غير المعزول UTP. ويرمز لنوع الشبكات التي يستخدم فيها UTP باسم BaseT ١٠.

نستد الجدول أن هناك حالتين دم فيهما السلك المحوري مع شب Ethernet وهما Base ٢ و Base ١٠ و Base ٥. في الحالة الأولى يكون الطول الكامل للناقل من أحد الأطراف إلى الطرف الآخر ١٨٥ متر. أما في الحالة الثانية فيبلغ أقصى طول للجزء ٥٠٠ متر.

في كلا الحالتين لا تتعدى السرعة ١٠ Mbps لذلك يستحسن استخدام UTP لأنه أرخص، أسرع وسهل التنصيب والصيانة.

لنرى الآن ما تعنيه بعض المصطلحات الموجودة في الجدول والخاصة بالمعيار Ethernet و Fast Ethernet و سنتكلم هنا بما يخص المعيار Ethernet:



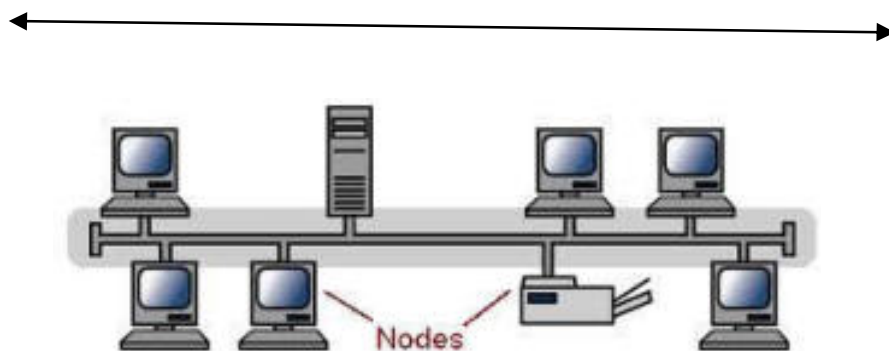
**BaseT :١٠**

١٠ تعني أن السرعة ١٠Mb/s ، Base هي النطاق الأساسي لنقل الإشارة و T هو السلك الملتوي (Twisted Pair) سواء كان معزول أو غير معزول.

**Base ٢ :١٠**

يدل ١٠ على السرعة ١٠Mb/s ، Base هي النطاق الأساسي لإرسال الإشارة و يدل ٢ على أقصى طول للكبل الذي لا يمكن أن يتجاوز ٢٠٠ متر (٢ مضروب في ١٠٠). بمعنى آخر يشير هذا المصطلح ( ١٠ Base ٢ ) إلى شبكة سرعة نقل البيانات فيها ١٠ ميجابت في الثانية تستعمل إرسال الإشارة في نطاقها الأساسي وطول أي قسم من الكبل فيها لا يتجاوز ٢٠٠ متر وغالباً ما يكون هذا النوع من الحالات خاص بالسلك المد رن (Thin Coax). موضح في الشكل التالي:

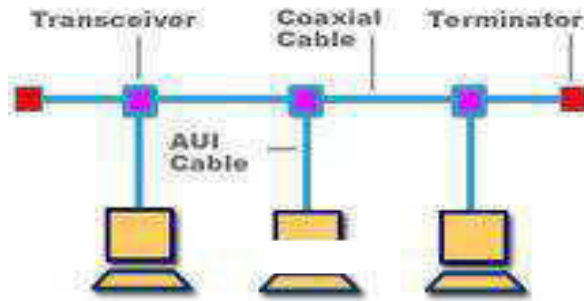
١٨٥ متر



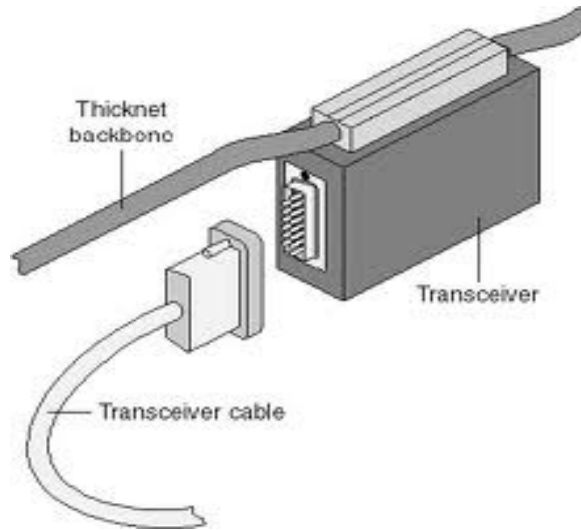
شكل (١-٦) يوضح مميزات تقنية Base ٢ :١٠

## ٥ Base ١٠ :

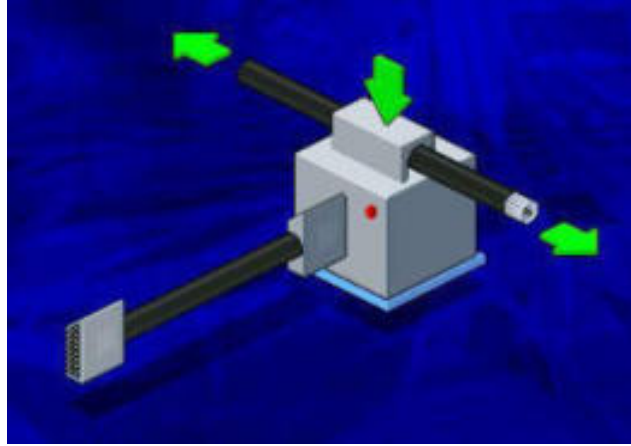
١٠Mb/s هي سرعة نقل البيانات، Base تعني الإشارة المرسلة في نطاقها الأساسي، ٥ تعني أن طول السلك المحوري المستخدم لا يتجاوز ٥٠٠ متر، وغالباً ما يستخدم في هذه الحالات السلك المحوري الثخين (Thick Coax). يستلزم في هذه الحالة استخدام جهاز من نوع Transceiver وهذا لإمكانية توصيل السلك المحوري السميك إلى وصلة AUI (Attachment Unit Interface) لبطاقة الشبكة ويوضح الشكل التالي كيف يتم هذا التوصيل.



شكل (٦-٢) يوضح شبكات ٥ Base ١٠



شكل (٦-٣) يوضح كيفية توصيل جهاز Transceiver



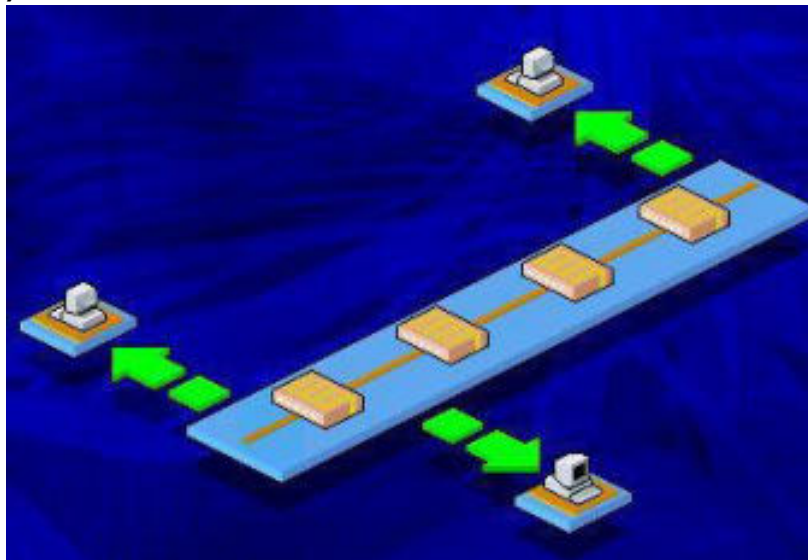
شكل (٦-٤) يوضح Transceiver في شبكات Base ٥ ١٠ وهو يصل بين السلك المحوري التخزين و Transceiver cable.

#### : ١٠ Base F

و تعني نقل البيانات بسرعة ١٠ ميجا بايت في الثانية في نطاق أساسي للإشعاع نوع السلك المست هذه الحالة هو من الألياف البصرية (Optical Fibers).

#### قواعد لتوصيل الكبلات المحورية

يوجد قوانين تحدد عدد المكررات والأجزاء الممكن استخدامها على الشبكة المحلية الواحدة. يتمثل هذا بالقاعدة ٣-٤-٥ والتي تنص أنه يمكن أن تتضمن شبكة واحدة حتى ٥ أجزاء أو قطع من الكابلات موصولة بأربع مكررات بحيث لا يزيد عدد القطع التي تحتوي على أجهزة مشبوكة فيها عن ثلاثة.



شكل (٥-٦) يوضح قاعدة ٣-٤-٥.

بالنسبة للسلك المحوري وفي حالة ٢ Base ١٠ من الممكن أن يكون في شبكة واحدة ٥ أجزاء موصلة حسب القاعدة المذكورة سالفاً والموضحة في الشكل الذي من خلاله يمكن لهذا النوع من الشبكات أن تمتد حتى ٩٢٥ (١٨٥×٥) متر. أما في حالة الشبكات ٥ Base ١٠ فمن الممكن أن تمتد هذه المسافة حتى ٢٥٠٠ (٥×٥٠٠) متر.

### ثانياً: المعيار ١٠٠ Base x Fast Ethernet

يستخدم اترنت السريع Fast Ethernet آلية CSMA/CD للوصول إلى وسيط الاتصال وينقسم المعيار ١٠٠ Base x fast Ethernet إلى ثلاثة أنواع هي:

#### ١٠٠ Base T٤:

السرعة ١٠٠Mbps، مستخدماً الأزواج الأربعة من الأسلاك UTP التابع لفئة Cat٣, Cat٤, Cat٥.

**Base Tx :١٠٠**

تستخدم هذه التقنية زوجين من أسلاك UTP Cat٥ أو كبلات من نوع STP. تكون فيها سرعة نقل البيانات ١٠٠Mbp/s.

**Base Fx :١٠٠**

تستخدم هذه التكنولوجيا سلكين واحد للإرسال والثاني للإستقبال من الألياف البصرية أي تنتقل البيانات بسرعة ١٠٠Mbp/s

**شبكات Ethernet التي تستخدم كبلات UTP:**

في معظم الحالات تستخدم الطبقة الفيزيائية في Ethernet الطبوغرافية النجمية أين توصل الأجهزة بنقطة واحدة تسمى مكرراً متعدد المنافذ أو مجمعاً (Hub). ومن أشهر الأسلاك المستخدمة في هذه البنية هي أسلاك الزو غير المعزول UTP تركيبها وصيانتها والتي تتراوح سرعة نقل البيانات من ١٠Mbps إلى ١٠٠٠Mbps. أقصى طول لقطعة الكبل الرابط بين الكمبيوتر والمجمع هي ١٠٠متر. لذا تستطيع أن تكون الأجهزة موزعة على دائرة قطرها ٢٠٠متر.

نلاحظ أنه في كلا الحالتين ١٠٠BaseTX و ١٠٠BaseT٤ تستخدم سلك UTP وتكون فيهما سرعة نقل البيانات ١٠٠Mbps. والفرق بينهما أن ١٠٠BaseTX تستخدم زوج للإرسال وزوج للإستقبال مع نوعية UTP Cat٥ و ١٠٠BaseT٤ تستخدم ٤ أزواج، زوجين للإرسال وزوجين للإستقبال من UTP Cat٣ مع إمكانية الإرسال والاستقبال في نفس الوقت.

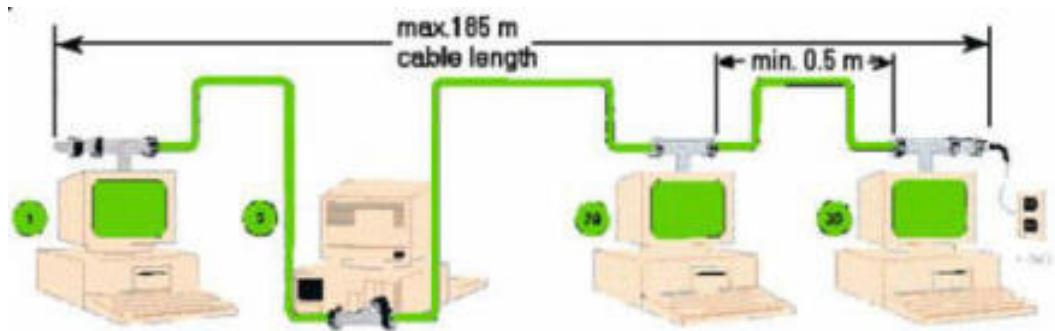
## شبكات Ethernet التي تستخدم الألياف البصرية:

نلاحظ أن معظم حالات Gigabit Ethernet يعني Ethernet بسرعة ١٠٠٠Mbps تستخدم الليف البصري.

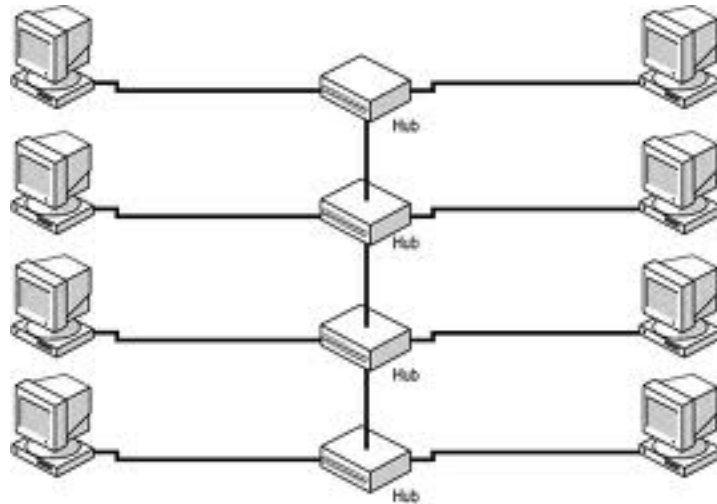
عند استخدام الليف البصري وحيد النمط غالباً ما تكون أطوال الكبل المسموح تركيبها كبيرة فمثلاً في حالة Base Zx ١٠٠٠ نستطيع أن نوصل أجهزة بعيدة عن بعضها بمسافات تصل إلى ١٠٠ كيلو متر.

## قواعد توصيل كبلات UTP :-

يمكننا في شبكات ١٠BaseT ربط أربع مجموعات مكررة مع بعضها باستخدام منافذ الربط التوسعي (Uplink Ports) وتوصيل الأجهزة إلى هذه المجموعات مع ١ القاعدة ٣-٤-٥ طالما البيانات بين أبعد جهازين عبر من أربع مجموعات يظل تصميم الشبكة صحيحاً ويكون الامتداد الأقصى للشبكة ٥٠٠ متر.



شكل (٦-٦) يوضح قاعدة ٣-٤-٥ في شبكات ١٠BaseT



شكل (٦-٧) يوضح إمكانية ربط أربعة مجموعات.

أما في حالة Fast Ethernet فهناك إمكانية استخدام نوعين من المجموعات Class I و Class II. وتربط مجموعات Class I قطع كبلات مختلفة كالليف البص UT بينما تربط مجمع Class قطع كبلات من نفس الذ

## تقنية Token Ring

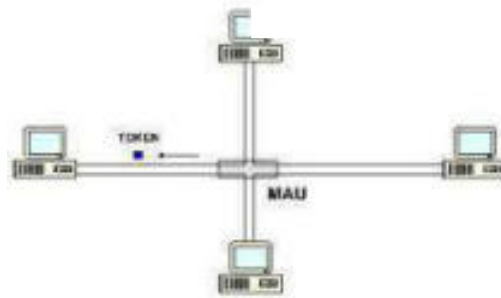
Token Ring هو بروتوكول يعمل على مستوى طبقة ربط البيانات. فهو الذي يزود الطبقة الفيزيائية بالمعلومات المراد إرسالها. بما أن هذا البروتوكول مختلف تماماً عن بروتوكول اترنت فهذا يعني أنه هو الذي يحدد المكونات المادية اللازم استخدامها على مستوى هاتين الطبقتين. بروتوكول Token Ring معروف أيضاً بتسمية IEEE 802.5.

كانت في البداية سرعة هذا النوع من الشبكات 4Mbps؛ وأصبحت فيما بعد 16Mbps. من مزايا Token Ring أنه لا يعاني من التصادمات مما يزيد من فعاليته نسبياً.

لم يرى هذا البروتوكول انتشاراً مثل Ethernet بسبب أسعار أجهزته التي غالباً ما تعادل أضعاف أسعار الأجهزة المستخدمة في Ethernet.

### أولاً: الأجهزة المستخدمة في شبكات Token Ring

تستخدم شبكات Token Ring البنية الطبوغرافية الحلقية حيث توصل كل الأجهزة بواسطة أسلاك إلى نقطة واحدة تدعى وحدة الوصول متعدد المحطات (Multistation Access Unit) MAU. والتي تقابل المجمع في شبكات Ethernet.



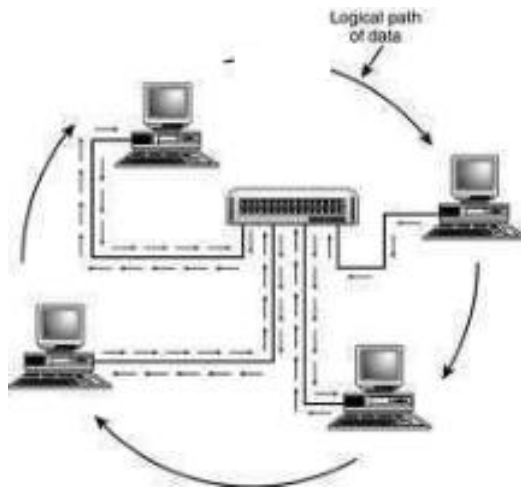
شكل (٨-٦) يوضح توصيل الأجهزة إلى MAU في تقنية Token Ring

عندما ننظر إلى التوصيلات الخارجية بين الأجهزة و MAU تبدو لنا الكبلات وكأنها تشبه البنية النجمية. وحدة الوصول المتعدد MAU هي التي تحول الأشياء لتعمل فيزيائياً على حلقة بدلاً من نجمة. عندما تصل البيانات إلى MAU فإنه يوجهها إلى المنفذ الذي يليه بدلاً من إرسالها إلى كل المنافذ و



هكذا تتمكن البيانات من الانتقال من جهاز الى جهاز ثاني الى أن تصل مرة ثانية الى الجهاز المولد لهذه البيانات.

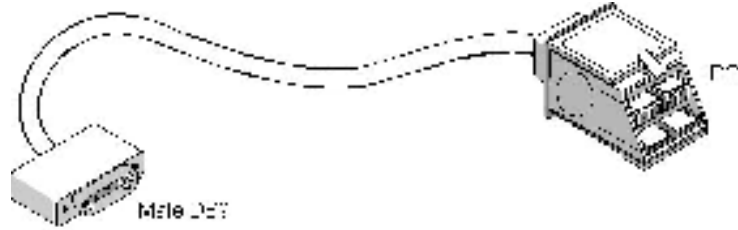
عندما يريد جهاز إرسال بيانات إلى جهاز آخر فإنه يمرر البيانات إلى MAU الذي يمررها إلى الجهاز الثاني في الحلقة والذي بدوره يقرأ عنوان الوجهة في ترويسة الإطار. إذا كان العنوان المادي للجهاز يوافق عنوان الوجهة يستلم الجهاز المعلومات ويمررها إلى الطبقات العليا في كدسة البروتوكولات. أما إذا كان العنوانين مختلفين فيمرر الجهاز الثاني البيانات إلى MAU الذي يمررها إلى الجهاز الثالث وهكذا إلى أن تصل المعلومات إلى هدفها. والشكل التالي يبين كيف يحول MAU منطقياً النجمة إلى حلقة.



شكل (٩-٦) يوضح استقبال MAU الإشارة من جهاز وتمريرها إلى الجهاز الثاني مكوناً حلقة

لربط أجهزة الكمبيوتر بـ MAU كانت في البداية Token Ring تستخدم كبلات خاصة مع وصلات مثبتة عليها. الوصلة التي تقع من جهة MAU هي

لقمة تدعى IDC، والوصلة التي تشبك ببطاقة الشبكة هي من نوع DB٩ ذكر ويطلق على هذا النوع من الكبلات اسم كبل فصّي (Lobe Cable) كما هو في الشكل التالي.



شكل (١٠-٦) يوضح الكبل الفصّي.

لربط جهازين MAU تستخدم كبلات يتصل معها وصلتا IDE من الطرفين وهذا ما يسمى بكبلات خطوية (Patch Cable).

أما معظم شبكات Ring To تستخدم كبل UTP من ٥ C مع وصلات من RJ في طرفيه. هذا يعني أيضاً منافذ MAU هي نفس الوصلات الموجودة على بطاقة الشبكة مما يؤدي إلى تبسيط في عملية توصيل الأجهزة في الشبكة وصيانتها. حوّلت تقنية استخدام UTP امتداد طول الكبل الفصّي من ٣٠٠ متر إلى ١٥٠ متراً وعدد الأجهزة في كل شبكة من ٢٦٠ إلى ٧٢ محطة عمل.

### ثانياً: آلية الوصول إلى وسيط الاتصال في Token Ring

تعمل شبكات Token Ring بآلية تسمى Token Passing والتي تلعب نفس الدور التي تلعبه آلية CSMA/CD في Ethernet، و تمنح هذه الآلية لكل

نظام على الشبكة فرصة متساوية لإرسال بياناته دون حدوث تصادمات لذلك فان هذه الآلية فعالة بطبيعتها.

تعمل آلية Token Ring بمبدأ تمرير رزمة خاصة بطول ٣ بايت تسمى علامة أو Token والتي غايتها تعيين النظام المسموح له استخدام الشبكة.

تبقى هذه العلامة تدور ضمن الحلقة من نظام إلى آخر. عندما يريد أحد الأجهزة إرسال بياناته، عليه أن ينتظر وصول العلامة إليه قبل البدء في الإرسال.

عندما يستحوذ جهاز ما على العلامة يدخل في وضع الإرسال بتغيير بت في العلامة لتصبح علامة الشبكة مشغولة (Network Busy) والتي تدل على باقي ة أن الشبكة قيد الاستع

بعدها مباشرة يبدأ الجهاز بإرسال بياناته إلى MAU ثم إلى كل جهاز بدوره في الحلقة. بعد ما يلتقط جهاز الوجهة البيانات تستمر البيانات في تنقلها في الحلقة إلى أن تصل ثانياً إلى جهاز المصدر والذي تكون له مسؤولية تجريد الشبكة من الرزمة لكي لا تبقى البيانات تدور بشكل لا نهائي.

بعدها يرسل الجهاز علامة الشبكة حرة (Network Free) لكي يستطيع جهاز آخر من التقاطها والبدء في عملية إرسال بياناته على الشبكة.

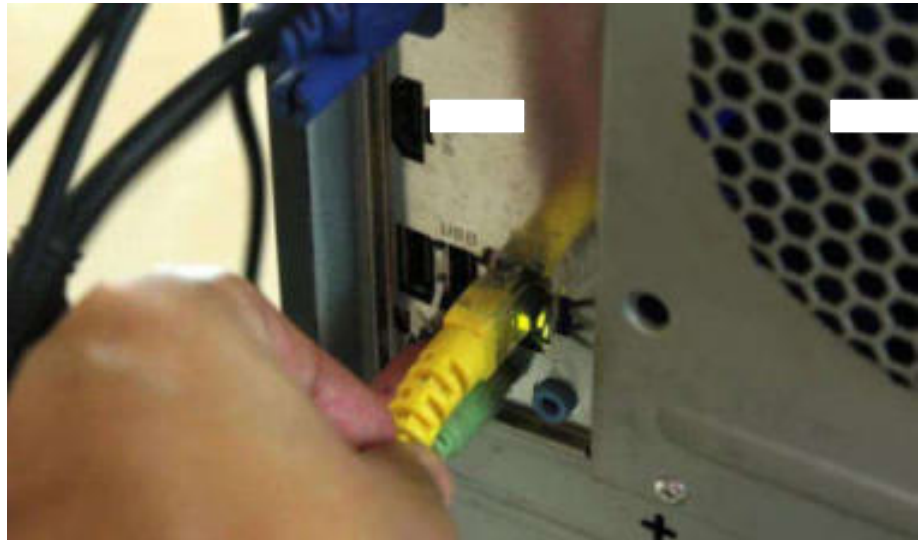
## إعداد الحاسوب للإتصال بشبكة محلية

كيف يمكنك إعداد حاسوبك للإتصال شبكة محلية Local Network Area؟

من المفترض أنه من المستحيل أن تجد مجال عمل ليس لديه شبكة محلية في المكان. اذا كنت تعمل في مكتب ستحتاج الى اعداد جهازك الشخصي وربطه بالشبكة المحلية حتى تتمكن من الإتصال بالإنترنت.

## خطوات إعداد جهازك للإتصال بالشبكة:

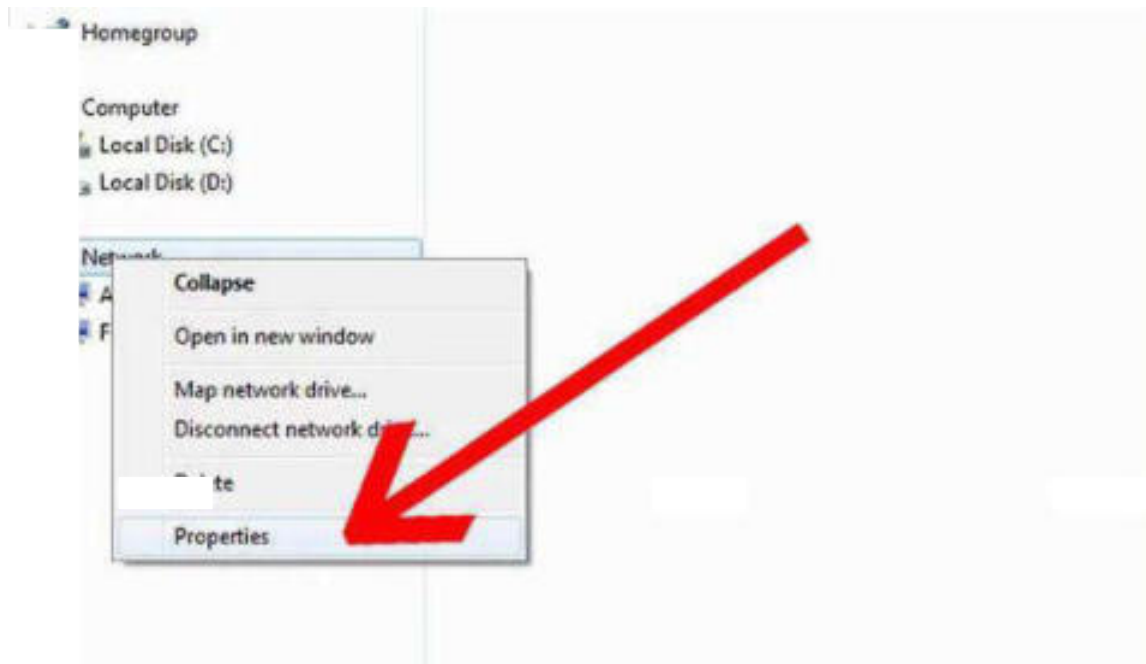
١- قم بتوصيل RJ-٤٥ إلى منفذ شبكة الإترنت في حاسوبك.



شكل (١١-٦) يوضح توصيل كابل الشبكة في المنفذ الخاص به خلف الجهاز.

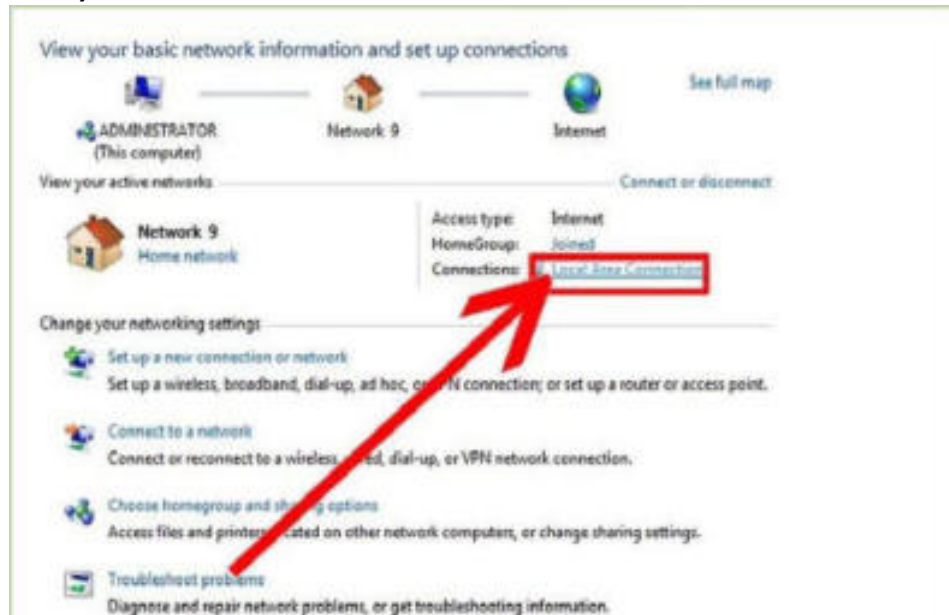
٢- اضغط بالزر الأيمن على أيقونة 'My Network Places' الموجودة على سطح المكتب desktop ومن القائمة المنسدلة اضغط على خصائص Properties.

أو بدلاً من ذلك، اضغط على زر البدء 'Start' من شريط المهام taskbar ثم اضغط بالزر الأيمن على الخيار 'My Network Places' من القائمة المنسدلة. ومن القائمة التي تظهر اختر خصائص 'Properties'.



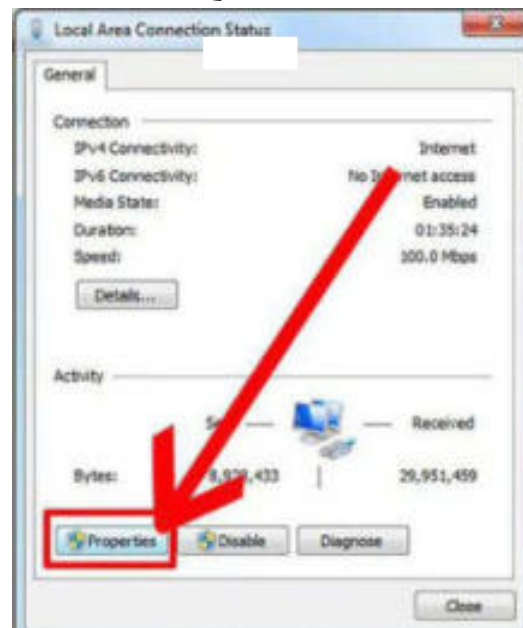
شكل (١٢-٦) يوضح اختيار الأمر Properties من القائمة المختصرة.

٣- اضغط بالزر الأيمن على 'Local Area Connection' في النافذة الجديدة التي تظهر ( تحت LAN أو الجزء المخصص لـ (High-Speed internet).



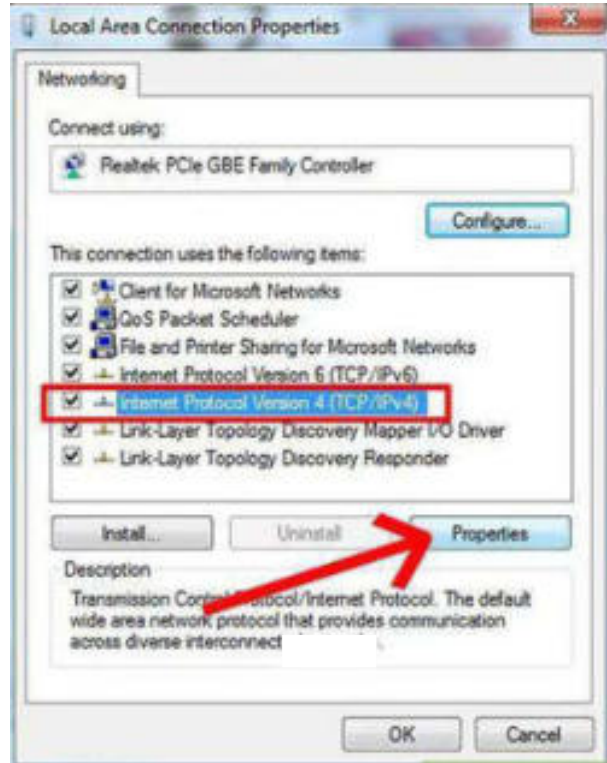
شكل (١٣-٦) يوضح اختيار Local area connection من النافذة.

٤- اضغط على خصائص من المربع الحواري الذي يظهر.



شكل (١٤-٦) يوضح الضغط على زر خصائص من نافذة Local Area Connection

- ٥- تحرك بشرط التمرير واختار 'Internet Protocol (TCP/IP)' ثم اضغط على خصائص 'Properties' في المربع الحوار Local Area Connection والذي يظهر تحت مربع connection.



شكل (١٥-٦) يوضح اختيار بروتوكول الإنترنت ثم خصائص Properties.

- ٦- لكي يتم ضبط الإعدادات بطريقة أوتوماتيكية، اختار 'Obtain an IP Address Automatically' على الرغم من ذلك، فإنه حتى تتمكن من استخدام هذا الخيار، فإنه لابد أن يكون لديك DHCP server والذي سيعمل على تحديد وإدارة عنوان IP للتأكد من عدم وجود تعارض مع الأجهزة الأخرى.



شكل (١٦-٦) يوضح اختيار تحديد بروتوكول الإنترنت أوتوماتيكياً دون تدخل.

٧- قم بربط حاسوبك إلى الشبكة يدوياً، إذا كان جهاز المودم modem الخاص بك غير متصل وهذا من ضمن الخيارات التي تم ذكرها أعلى. اضغط على الخيار 'Use the following IP Address' استخدم عنوان IP التالي.

إعداد د/ أميرة إبراهيم عبد الغني





شكل (١٧-٦) يوضح الاختيار الذي يسمح بضبط IP يدوياً.

- قم بادخال عنوان IP الذي ستستخدمه. انه من المهم أن تستشير مدير الشبكة في عنوان IP الذي يمكنك استخدامه وذلك حتى تتجنب

تعارض جهازك مع الأجهزة الأخرى الموجودة على الشبكة، والذي يحدث عندما يكون لجهازين نفس عنوان IP.



شكل (١٨-٦) يوضح المكان الذي يكتب به IP يدوياً.

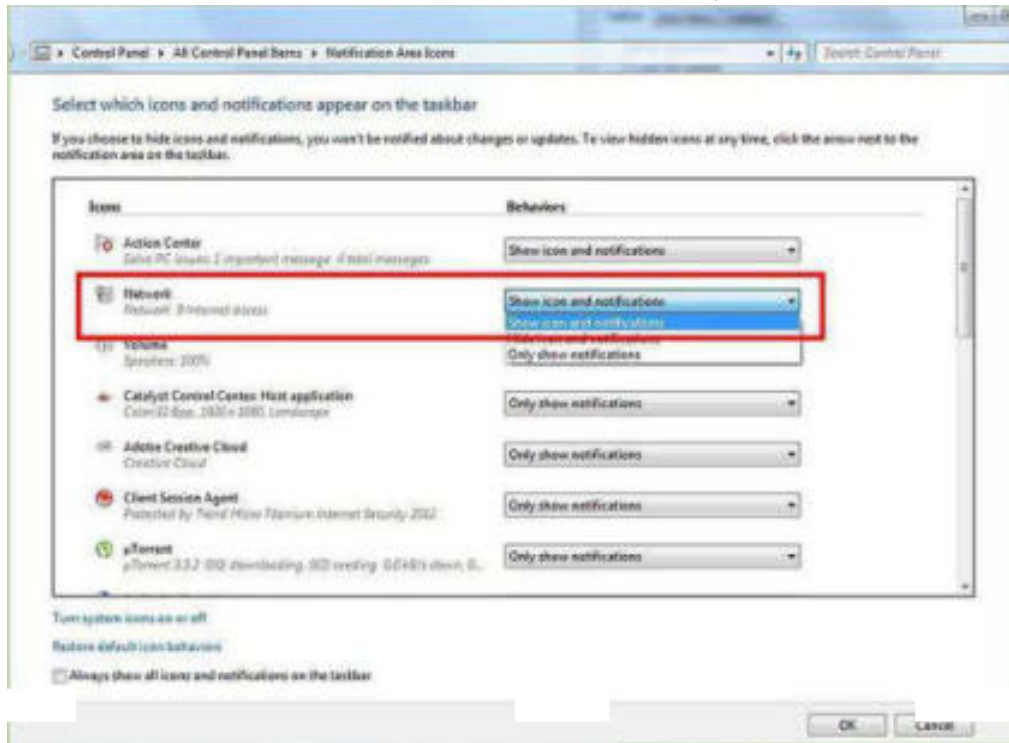
قم بادخال قناع الشبكة Subnet Mask و Default gateway. ويستخدم قناع الشبكة لتحديد مستوى الشبكة بينما يحدد default gateway الإتصال بجهاز الراوتر router.



شكل (١٩-٦) يوضح المكان الذي يكتب به قناع الشبكة الفرعية وعنوان الراوتر يدوياً. كيف يمكنك ترقيم وعنونة الأجهزة؟

عنونة الأجهزة على الشبكة تتم بإعطاء عنوان IP خاص ومنفرد بكل جهاز على الشبكة. تتكون عناوين IP من ٤ خانات مفصولة بنقاط تحتوي كل واحدة منها على رقم يتراوح بين ٠ و ٢٥٤ مع بعض الحالات الإستثنائية ، لنفترض أننا اخترنا شبكة خاصة من نوع C ويكون فيها عنوان الشبكة ١٩٢.١٦٨.١٠٠.٠ تكون الثلاث خانات الأولى ١٩٢.١٦٨.١٠٠ مشتركة لكل الأجهزة وتكون الخانة الرابعة أي رقم بين ١ و ٢٥٤. - يقوم النظام باختيار قناع الشبكة الفرعية بصفة افتراضية ومناسبة للعنوان IP المختار.

٨- حدد الخيار 'Show icon in notification area when connected' أي اظهر أيقونة الشبكة في حالة الإتصال.



شكل (٢٠-٦) يوضح اختيار إظهار أيقونة الشبكة في حالة الإتصال.

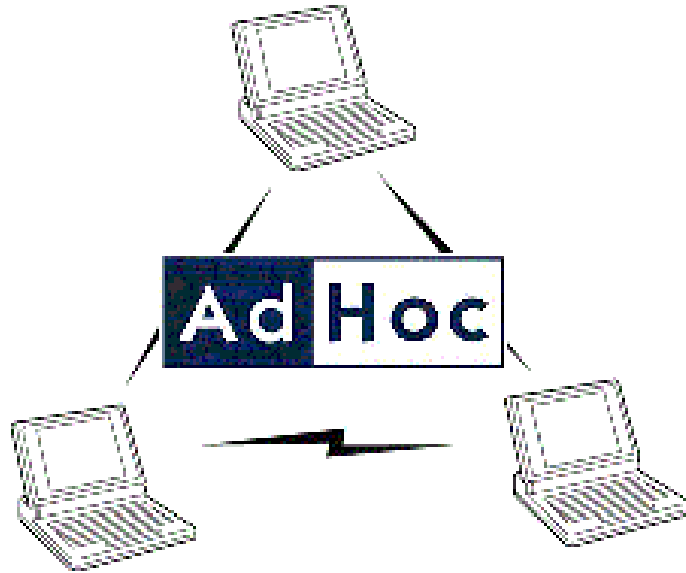
٩- اضغط على زر "OK". هذا سيمكنك من التعرف على ما إذا كان هناك إتصال بالشبكة المحلية أم لا.



شكل (٢١-٦) يوضح ظهور أيقونة الشبكة في شريط المهام.

## كيف يمكنك إعداد شبكة مخصصة Ad Hoc Network؟

### ماهي الشبكة المخصصة Ad Hoc Network ؟



شكل (٢٢-٦) يوضح الشبكة المخصصة.

الشبكة المخصصة أو Ad Hoc Network هي شبكة تعمل على انشاء اتصال مباشر بين الاجهزة المتصلة بدون الحاجة الى خادم أو راوتر للتنسيق بين الاجهزة المتصلة Ad Hoc Network. تقوم بعمل اتصال مؤقت بين حاسوب الى اخر، حيث تستطيع انشاء اتصال لاسلكي مباشر الى حاسوب اخر دون الحاجة للاتصال بشبكة Wi-Fi أو نقطة وصول. على سبيل المثال، إذا كنت بحاجة إلى نقل ملف إلى جهاز اخر، فيمكنك إنشاء شبكة مخصصة بين الكمبيوتر الخاص بك وجهاز الكمبيوتر الاخر لنقل الملف. قد يتم ذلك

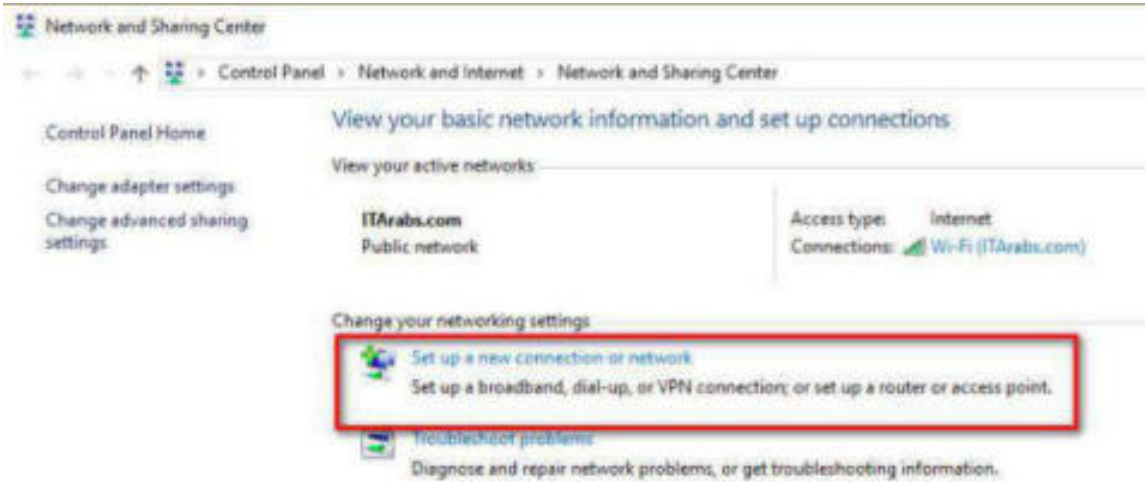
باستخدام كبل إيثرنت "الكبل السلكي" أو من خلال استخدام بطاقات الكمبيوتر اللاسلكية للاتصال.

### مميزات الشبكة المخصصة Ad Hoc Network

من مميزات الشبكة المخصصة Ad Hoc Network الشبكات المخصصة مفيدة عندما تحتاج إلى مشاركة الملفات أو غيرها مباشرة مع كمبيوتر آخر في حال لا يوجد شبكة واي فاي أو كابل إيثرنت. يمكن توصيل أكثر من جهاز كمبيوتر بالشبكة المخصصة، طالما أن جميع بطاقات مهئية وتتصل بنفس اسم الشبكة المخصصة (SSID) والأجهزة يجب أن تكون بمسافة ضمن ١٠٠ متر من بعضها البعض. إذا كنت الشخص الذي يقوم بإعداد الشبكة المخصصة، عند الاتصال من الشبكة ١ قطع اتصال جميع المستخدم الآخرين. يمكنك استخدام شبكة لاسلكية مخصصة لمشاركة اتصال الإنترنت بالكمبيوتر مع كمبيوتر آخر.

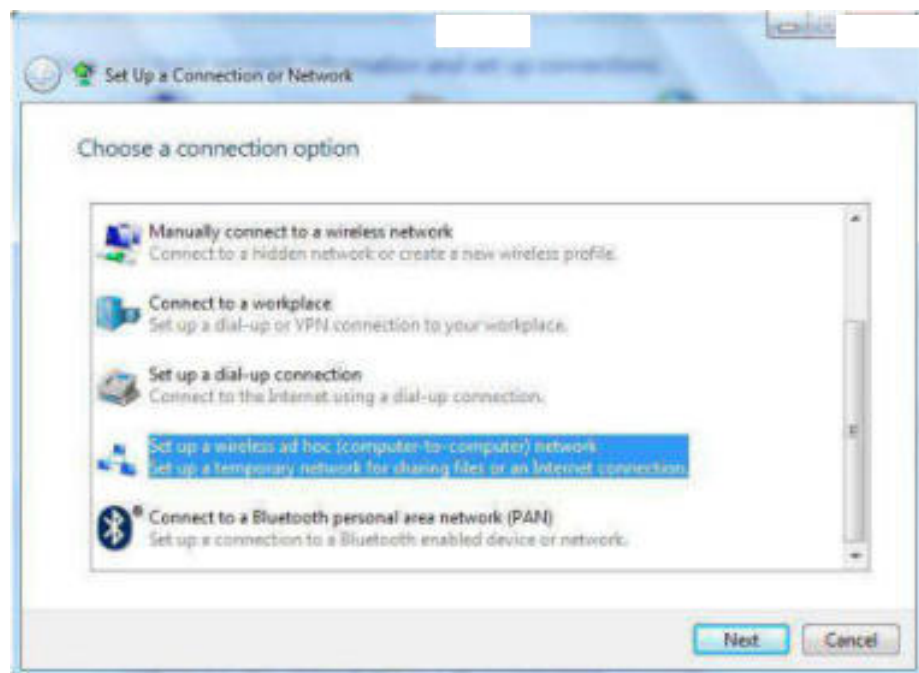
### كيفية اعداد الشبكة المخصصة على ويندوز ٧

أولاً، افتح مركز الشبكة والمشاركة "Network and Sharing Center" من لوحة التحكم. انقر على "إعداد اتصال أو شبكة جديدة".



شكل (٦-٢٣) يوضح اختيار **Set up a new connection** من **Network and Sharing Center**

ثانياً، قم باختيار اعداد شبكة مخصصة "setup a wireless Ad hoc"



شكل (٦-٢٤) يوضح اختيار اعداد شبكة مخصصة Ad hoc.



سترى نافذة جديدة تخبرك بالأشياء التي يمكنك القيام بها على من خلال اعداد شبكة لاسلكية مخصصة. انقر على التالي. الان حان الوقت لإعداد الشبكة. أولاً، اكتب اسم الشبكة ثم حدد نوع الأمان الذي تريد استخدامه. الأفضل استخدام WPA2 ، حيث أنه يوفر تشفير أفضل و من الصعب فك تشفير هذا النوع من التشفير.



شكل (٢٥-٦) يوضح اختيار بروتوكول التشفير WPA2.

اكتب كلمة المرور التي تريد استخدامها، وفي حالة رغبتك في استخدام هذه الشبكة في مرة أخرى، حدد المربع الذي يقول "حفظ هذه الشبكة". عند الانتهاء، انقر على التالي لتصبح الشبكة جاهزة للاستخدام. لمشاركة الانترنت



بين الاجهزة انتقل إلى محول اللاسلكي الخاص بالشبكة التي تم انشاءها "wireless adapter" وانقر بزر الماوس الأيمن عليه "خصائص" وبعد ذلك إلى علامة التبويب "مشاركة" وحدد "السماح لمستخدمي الشبكة الأخرى للاتصال بالانترنت من خلال هذا الكمبيوتر".



شكل (٢٦-٦) يوضح نافذة المشاركة والسماح للمستخدمين الآخرين بالمشاركة.

## كيفية اعداد الشبكة المخصصة على ويندوز ٨ و ويندوز ١٠

للاسف في هذا النظام لا يوجد واجهة للاعداد كما هو الحال في ويندوز ٧، ولكن يمكن الاستعانة بطريقة لاعداد الاتصال.

**أولاً:** قم بالتوجه على قائمة ابدأ، اضغط على القائمة بالزر الأيمن للفأرة وقم بفتح موجه الاوامر Command prompt وتشغيله كمسؤول Command Prompt admin أو في ويندوز ١٠ ستجده بالاسم Windows PowerShell admin.

**ثانياً:** قم بنسخ هذا الكود وادخاله مع مراعاة تغيير اسم الشبكة وكلمة المرور الى `tsh wlan set hostednetwork mode=allow` `ssid=<اسم الشبكة>` `key=<كلمة المرور>` `netsh wlan start hostednetwork` هذه الشبكة وهنا يجب كتابة الامر في موجه الأوامر اذا كنت تريد تفعيل مشاركة الانترنت قم بتنفيذ خطوات التفعيل في الاعلى فهي مشابهة تماماً في حال اردت انهاء الاتصال قم بكتابة الامر `netsh wlan stop hostednetwork` في موجه الأوامر.

**الملخص:** الشبكة المخصصة ad hoc هي اتصال شبكة مؤقتة تم إنشاؤها لغرض معين (مثل نقل البيانات من جهاز كمبيوتر إلى آخر).

وعليك باتباع الخطوات التالية والتي تساعدك على اتمام عملية الإعداد في ويندوز ١٠:

- اضغط بالزر الأيمن على زر start.
- اختار **Command Prompt (Admin)** أو في ويندوز ١٠ ستجده بالاسم **Windows PowerShell admin**.
- إذا طلب منك **User Account Control** ، اضغط
- تظهر نافذة موجه الأوامر **Command Prompt** على الشاشة.
- اكتب الأمر التالي الذي سيقوم بفحص الدعم الافتراضي لواجهة الشبكة، **"netsh wlan show drivers"**.
- الآن إذا ظهرت لك الرسالة **No** عليك تحديث محول الشبكة.
- أما إذا أعطتك الشبكة المضيفة **Hosted Network** الإجابة **Yes** فان هذا يعني تطيع الاستمرار كواجه مدعمة للافتراضية.
- اكتب الأمر التالي لإعداد الإتصال المخصص اللاسلكي **ad hoc**،  
**"netsh wlan set hostednetwork mode=allow ssid=**  
**key="**
- استبدل الآن علامات الترميز بالإدخالات التي تريدها.
- في مكان "اسم الشبكة" **"network name"**، أدخل اسم الشبكة الذي تريده وبدلاً من "كلمة المرور" **"pass key"** ، أدخل كلمة المرور الذي يجب ألا تقل عن ٨ أحرف.
- بعد إعداد الشبكة المستضافة ، تحتاج إلى بدء تشغيلها.
- وللقيام بذلك ، اكتب الأمر التالي **"netsh wlan start hostednetwork"**

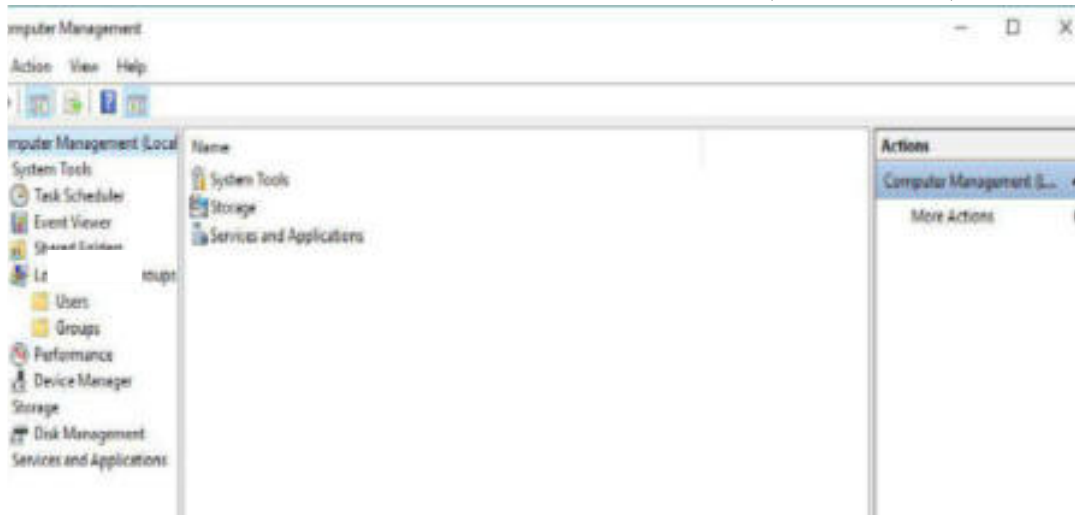
- افتح الآن لوحة تحكم Windows ١٠ Control Panel.
- اختر مركز الشبكة والمشاركة Network and Sharing Center .
- في الجزء الأيمن من نافذة Network and Sharing Center ، انقر فوق الرابط تغيير إعدادات محول الشبكة **Change Adapter Settings**، سيفتح هذا اتصالات الشبكة **Network Connections**.
- أو اتصال Wi-Fi الذي تم إنشاؤه مؤخرًا ، هنا تحتاج إلى تشغيل "مشاركة اتصال الإنترنت" **Internet Connection Sharing** ، وللقيام بذلك ، انقر بزر الماوس الأيمن على جهاز الاتصال بالإنترنت المتصل حاليًا بالإنترنت.
- انتقل إلى المشاركة.
- حدد مربع الاختيار الذي يطلب منك **Allow other network computers to connect through this computer's Internet connection** وتعني السماح لمستخدمي الشبكة الآخرين بالاتصال من خلال اتصال الإنترنت الخاص بهذا الكمبيوتر.
- ثم استخدم القائمة المنسدلة وحدد الشبكة المخصصة **ad hoc** التي تم إنشاؤها مؤخرًا.
- يمكنك الحصول على عنوان IP الخاص بالاتصال المخصص الذي تم إنشاؤه مؤخرًا عن طريق النقر المزدوج فوق خصائص TCP / IPv4.
- ضمن علامة تبويب الشبكات Networking tab.
- يمكنك الآن توصيل أي من أجهزتك التي تدعم Wi-Fi بجهاز Windows ١٠ الخاص بك.

## كيف يمكنك إنشاء مستخدمين محليين على الأجهزة؟

نقوم في هذه المرحلة بإنشاء مستخدمين محليين وهذا لتمكينهم من استخدام واستغلال موارد الشبكة.

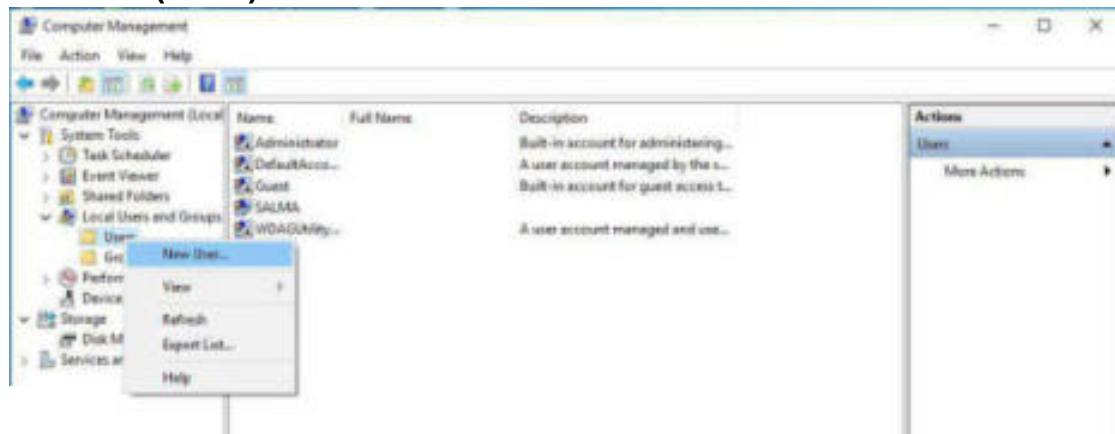
وتتلخص هذه العملية في الخطوات التالية:

- انقر بالزر الأيمن على أيقونة This PC.
- اختيار إدارة manage من القائمة المختصرة.
- ستظهر لك نافذة إدارة الحاسوب Computer Management كما هو موضح في الشكل التالي:



شكل (٢٧-٦) يوضح نافذة إدارة الحاسوب Computer Management.

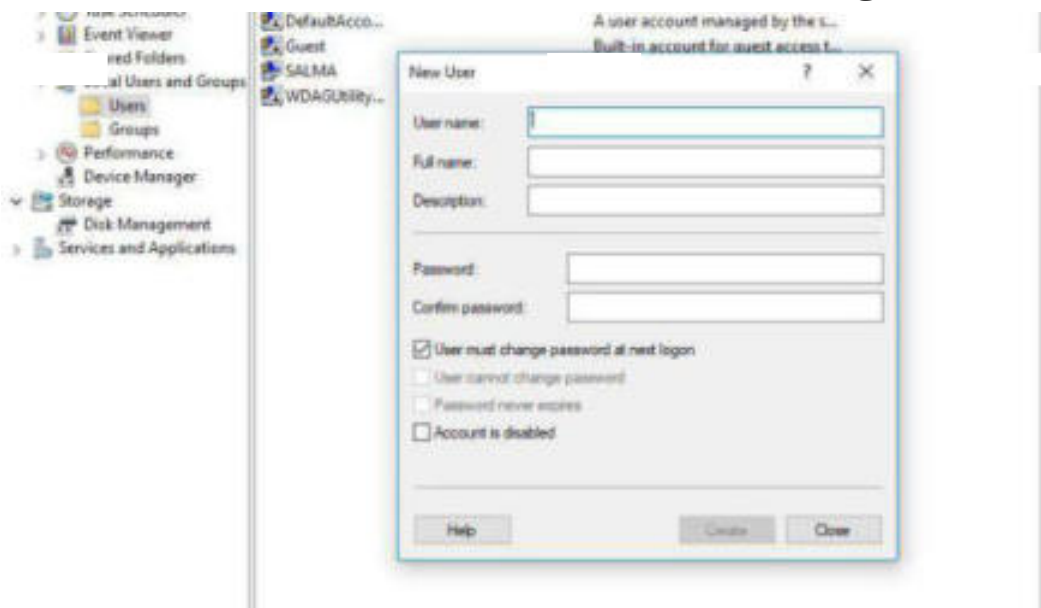
- انقر على العلامة التي بجوار مجلد (المستخدمون المحليون) والمجموعات المحلية Local users and Groups.
- انقر بالزر الأيمن على مجلد (المستخدمون) Users في جهة اليسار واختيار مستخدم جديد من القائمة كما يتضح من الشكل التالي:



شكل (٦-٢٨) يوضح اختيار User ثم New user.

- في مربع حوار مستخدم جديد قم بإدخال اسم المستخدم User name، كلمة المرور Password و تأكيد كلمة المرور Confirm Password.

- اضغط على إنشاء Create.



شكل (٦-٢٩) يوضح نافذة New user والتي تطلب بيانات المستخدم الجديد.

كرر هذه الخطوات لكل مستخدم جديد محلي تعطيه صلاحيات استخدام الجهاز والشبكة.

إعداد د/ أميرة إبراهيم عبد الغني

## مشاركة الملفات والأجهزة

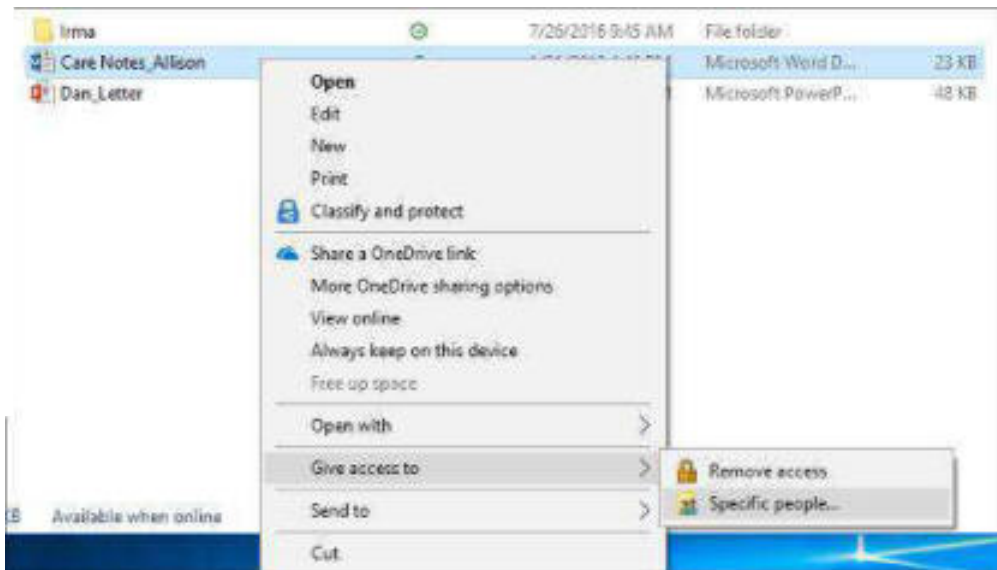
### أولاً: مشاركة الملفات:

هي عملية تحضير الملفات بطريقة تسمح بتوفيرها لمستخدمين آخرين للاطلاع عليها أو استخدامها على جهاز حاسوب آخر، أو تحميلها على الشبكة. يتيح نظام التشغيل Windows ١٠ مشاركة الملفات والمجلدات لحواسيب أخرى موصولة بالشبكة ذاتها.

### مشاركة الملفات عبر الشبكة في نظام النوافذ ١٠

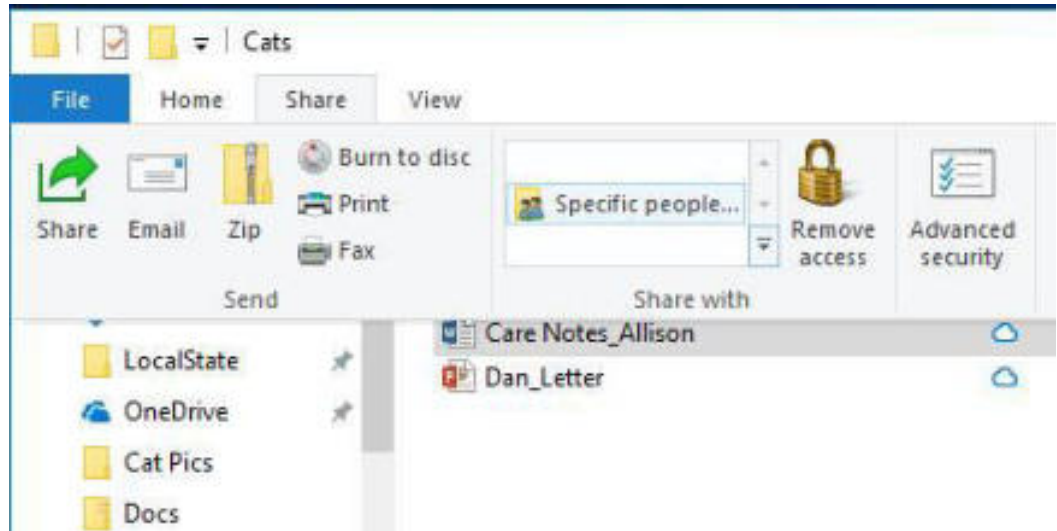
لمشاركة ملف أو مجلد في مستكشف الملف، قم بآداء أيا مما يلي:

١. اضغط بالزر الأيمن على الملف، واختار > Give access to Specific people.



شكل (٣٠-٦) يوضح اختيار > Give access to Specific people.

٢. حدد الملف، اختار التبويب Share في أعلى نافذة مستكشف الملف File Explorer، ثم في الجزء الخاص بالمشاركة مع Share with، اختار Specific people.



شكل ٦) يوضح تحديد المل Share with Specific peop

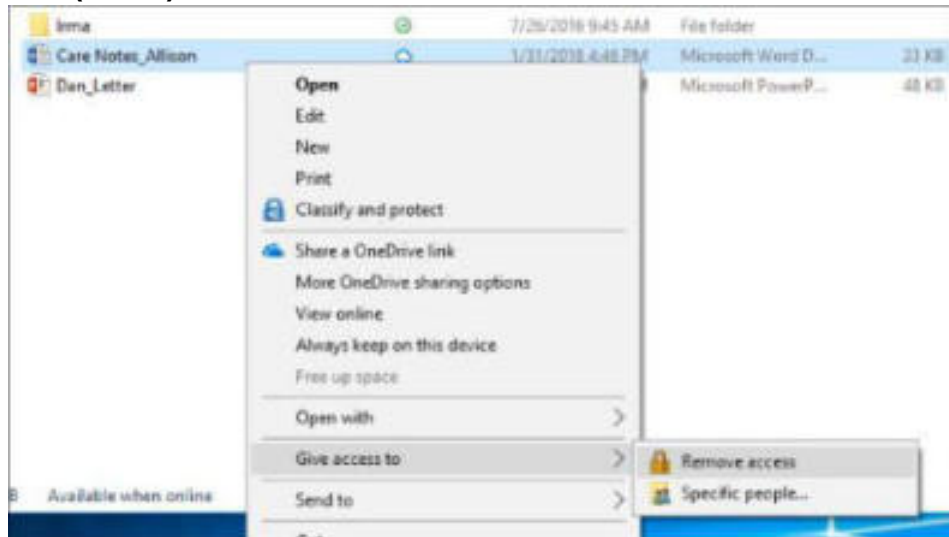
إذا قمت بتحديد العديد من الملفات في نفس الوقت، يمكنك مشاركتهم بنفس الطريقة. ويمكن المشاركة أيضاً في المجلدات، وكل الملفات الموجودة بها سيتم مشاركتها.

### كيف يمكنك إيقاف عملية مشاركة الملفات والمجلدات؟

لإيقاف المشاركة في مستكشف الملف File Explorer، قم بآداء واحدة مما يلي:

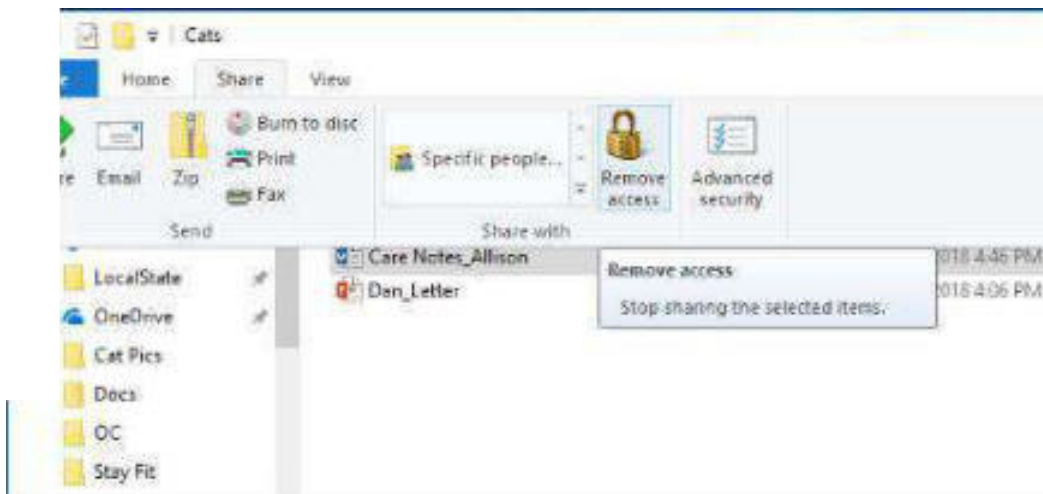
- ١- اضغط بالزر الأيمن على الملف أو المجلد، ثم اختار Give access to > Remove access.





شكل (٦-٣٢) يوضح اختيار Remove Access من القائمة الفرعية.

٢- حدد الملف أو المجلد، اختار التبويب مشاركة Share في أعلى نافذة  
كشف الملف xplorer ، ثم في الجزء المخصص للمش  
Share w اختار ازالة الوصول Remove access.



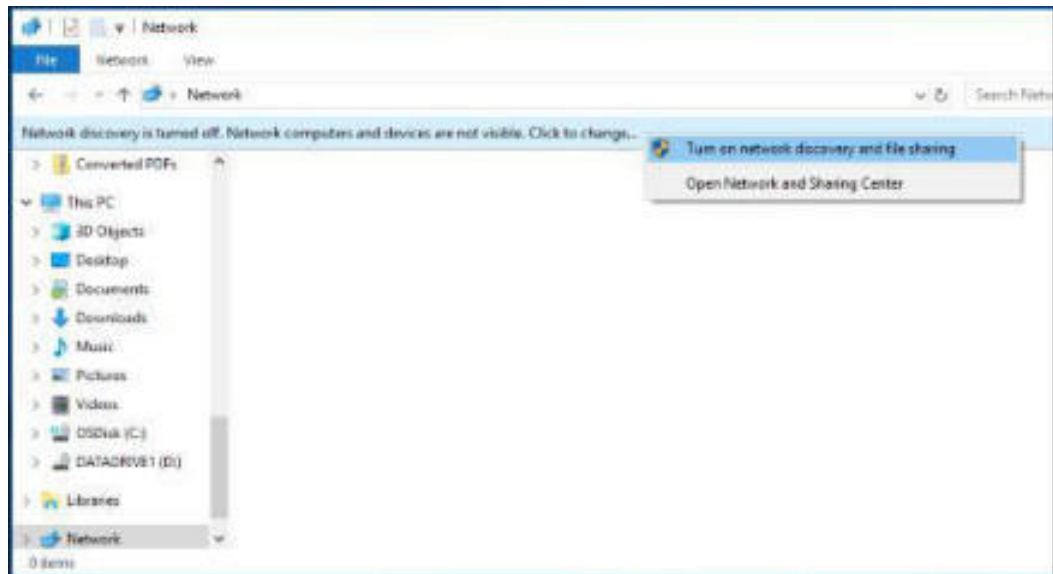
شكل (٦-٣٣) يوضح اختيار Remove access من الجزء المخصص للمشاركة.

إعداد د/ أميرة إبراهيم عبد الغني

لماذا يظهر في مستكشف الملف File Explorer خيار لإيقاف المشاركة "Stop sharing" او منع الوصول "Remove access" للملفات التي لم يتم مشاركتها عبر الشبكة؟ مستكشف الملف يعرض الخيار "Remove access" والذي يحل محل "Stop sharing" في الإصدارات القديمة من ويندوز (١٠) لكل الملفات، حتى التي لم يتم مشاركتها عبر الشبكة.

### كيف يمكنك تشغيل Network discovery؟

عندما تفتح مستكشف الملف File Explorer، اذهب إلى Network، وسترى رسالة الخطأ التالية ("Network discovery is turned off....") ، ستحتاج إلى تشغيل Network discovery لترى الأجهزة التي تقوم بمشاركة ملفات عبر الشبكة. ولتشغيله، اضغط بالزر الأيمن على الشعار Network discovery is turned off، ثم اختار Turn on network discovery and file sharing . and fil ing

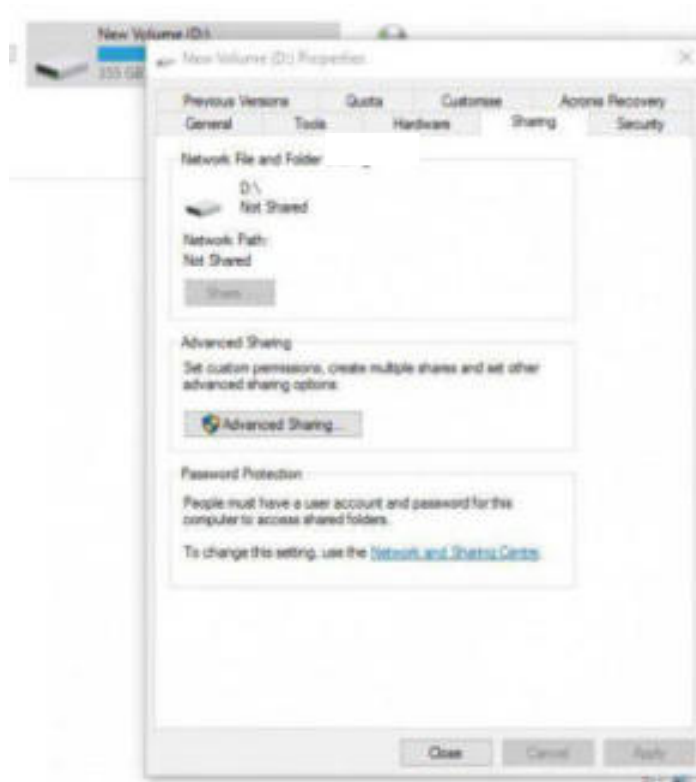


شكل (٣٤-٦) يوضح كيفية تشغيل Network discovery.

## إعداد قرص كامل للمشاركة في ويندوز ١٠

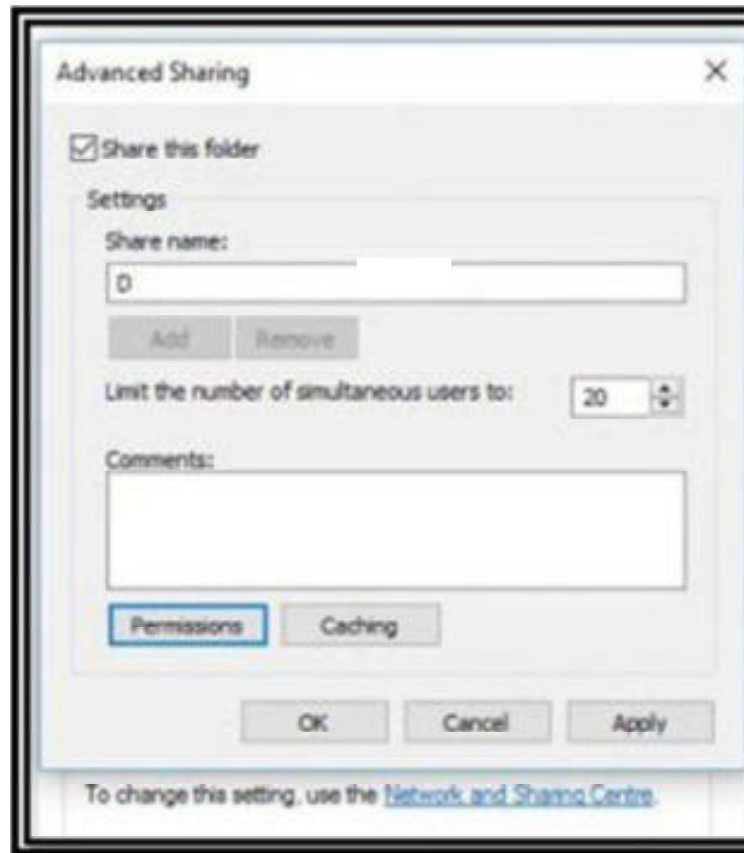
إذا كان إعداد القرص أو المجلد يسمح بمشاركته، يمكن لأي مستخدم على الشبكة التعامل معه إذ لا يتطلب ذلك سماحاً للمستخدم أو أي كلمة سر.

**مشاركة القرص الصلب:** كما رأيت سابقاً في عملية مشاركة المجلد، فإنه يمكنك أداء نفس الإجراءات على كل المجلدات في المشغل أو فقط بعض المجلدات المحددة. ومع ذلك، ماذا لو كنت ترغب في وصول كل شخص وكل جهاز في الشبكة المنزلية إلى مشغل الأقراص بأكمله؟ إبدأ بالضغط بالزر الأيمن على القرص، ثم اضغط على الخيار خصائص Properties يلي ذلك Sharing tab.



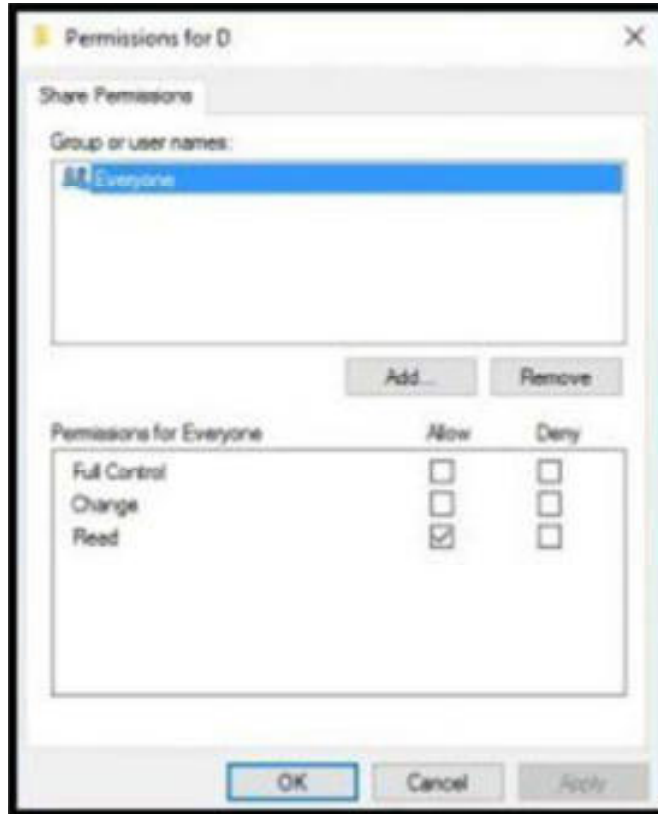
شكل (٣٥-٦) يوضح خصائص القرص الصلب.

ويكمن الاختلاف في أن زر المشاركة 'Share...' يكون باهت، لذلك ستحتاج إلى الضغط على زر 'Advanced Sharing...' والذي يوجد أسفل الجزء المخصص للمشاركة المتقدمة Advanced Sharing. ولكن، قبل أن تضغط على الزر اقرأ في دقيقة العبارة الموجودة أسفل الجزء المخصص للحماية بكلمة السر Password Protection ، وهذا يذكرك بأنه للوصول إلى المشاركة تحتاج إلى حساب account على الحاسوب الذي توجد به المشاركة وستحتاج إلى كتابة كلمة السر password للوصول إلى الحاسوب. اضغط على زر 'Advanced Sharing...' للاستمرار في مشاركة القرص.



شكل (٣٦-٦) يوضح نافذة Advanced sharing لتحديد اسم المشاركة.

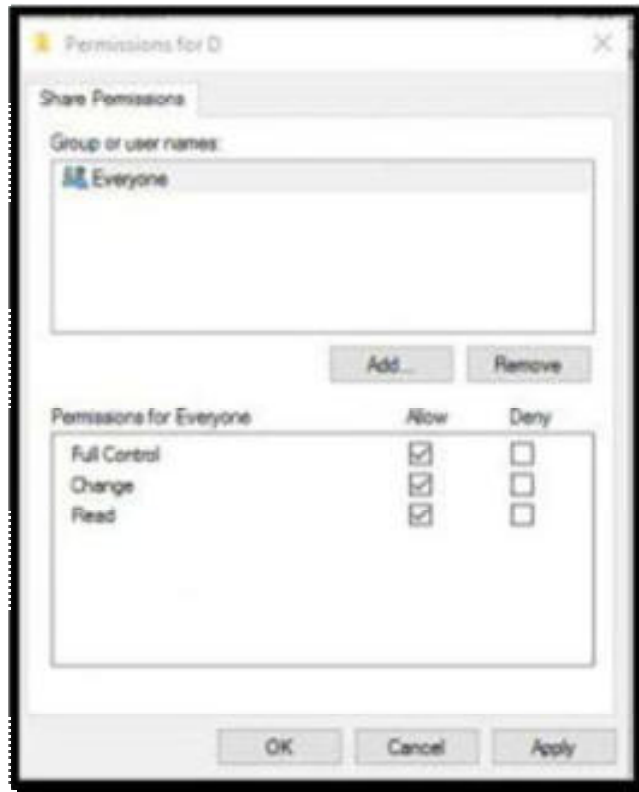
في النافذة الجديدة التي تظهر اضغط ببساطة لتحديد المربع بجوار 'share this folder' ثم قم بإعطاء اسم لمشاركة القرص share name - ولتكن D . وقبل الضغط على زر 'OK' ، اضغط على زر 'Permissions' أسفل الجزء المخصص للتعليقات Comments.



شكل (٣٧-٦) يوضح تحديد الصلاحيات للمستخدمين.

لكي تسمح لكل شخص على شبكتك المنزلية بالقراءة والكتابة والوصول إلى المشاركة، فانك ستحتاج إلى التأكد من أن مربع السماح بالتحكم الكامل Full Control قد تم تحديده أسفل العمود المخصص للسماح Allow إلى المستخدم Everyone أي كل الأشخاص. وبهذا سيتمكن كل جهاز على الشبكة من

الوصول إلى محتويات القرص والقراءة والكتابة دون أي قيود. عندما تكون جاهزاً، اضغط على زر موافق 'OK' ثم يلي ذلك الضغط على زر موافق 'OK' مرة أخرى في النافذة المفتوحة و الخاصة بـ Advanced Sharing.



شكل (٦-٣٨) يوضح إعطاء كل الصلاحيات لكل مستخدم على الشبكة.

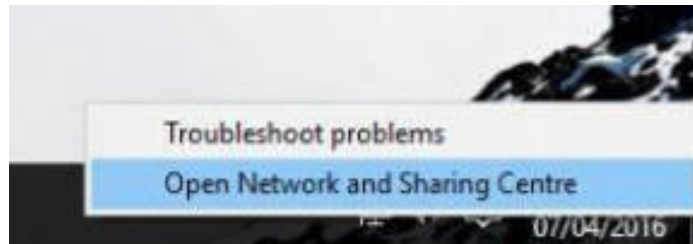
وبهذا تكون قد انتهت عملية مشاركة القرص. وللوصول إليه من حاسوب آخر أو جهاز ستحتاج إلى كتابة مسار المشاركة، والذي هو في المثال هنا WindowsD. إذا أعدت تسميتها يترجم المسار إلى \متبوعة باسم الجهاز ثم اسم المشاركة على الشبكة التي تمت فيها المشاركة. ومع ذلك عند الوصول

إلى المشاركة ستحتاج إلى كتابة اسم المستخدم username وكلمة المرور password، والذي قد يمثل عقبة في الوصول.

### إزالة الحماية بكلمة المرور Remove the password protection

ليس من الأمان ، بل الكثير يرفض فكرة ازالة الحماية بكلمة المرور . ولكن هنا أتاولها من وجهة أن الشبكة منزلية آمنة، حيث يمكنك الوصول إلى كل الموارد التي تمت مشاركتها على الشبكة المنزلية. وإلا، فإنني أوافقك على الإحتفاظ بالحماية بكلمة المرور.

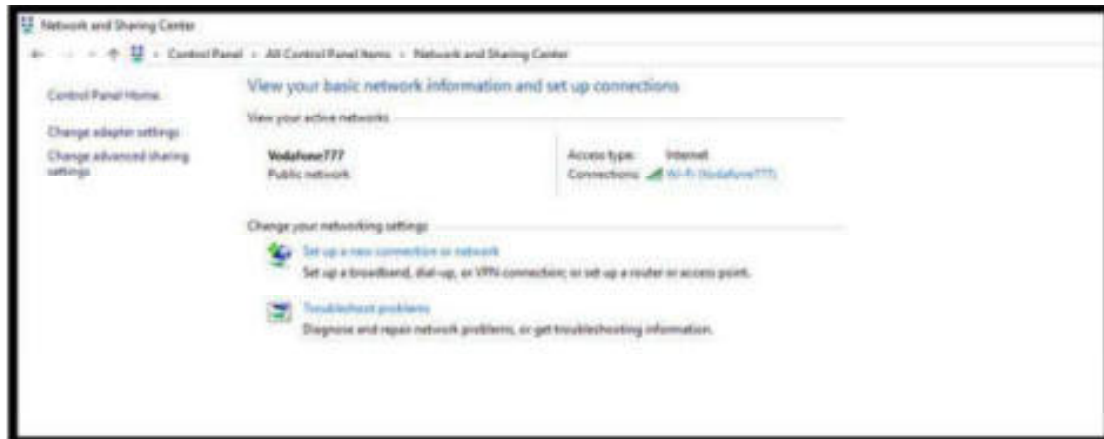
العبارة التي رأيتها في الجزء المخصص للحماية باستخدام كلمة المرور Password Protection عند مشاركة القرص تذكرك أن نظام التشغيل ويندوز ١٠ الآن يطلب تلقائياً اسم المستخدم وكلمة المرور للوصول لكل مورد ستم ٤ .



شكل (٣٩-٦) يوضح اختيار Open Network and Sharing Center

من القائمة المختصرة التي تظهر عند الضغط على أيقونة الشبكة.

لإزالة الخاصية اضغط بالزر الأيمن على أيقونة الشبكة المتصلة الموجودة في شريط المهام ثم اضغط على Open Network and Sharing Centre .



شكل (٦-٤٠) يوضح نافذة Network and Sharing Centre.  
في النافذة المفتوحة مؤخراً Network and Sharing Centre، اضغط على الرابط 'Change advanced sharing settings' على الجانب الأيسر من النافذة.



شكل (٦-٤١) يوضح نافذة Advanced Sharing settings.

إعداد د/ أميرة إبراهيم عبد الغني



مرر إلى أن تصل إلى الجزء الخاص بـ All Networks، حتى تصل إلى الأسفل ستلاحظ جزء يدعى Password-protected sharing، لإزالة خيار كلمة السر من عملية الوصول للمشاركة، اضغط بسهولة على زر الخيار بجوار 'Turn off password-protected sharing'.

عندما تنتهي من إجراء التعديلات اضغط على زر 'Save Changes' الموجود في أسفل النافذة ثم قم باغلاق نافذة Network and Sharing Centre.

### كيف يمكنك التغلب على مشكلات مشاركة الملفات والمجلدات؟

للتغلب على المشكلات التي تواجهك أثناء مشاركة الملفات أو المجلدات، تتبع الذ التالية على كل الأجه ستتم من خلالها عملية مش الملف

- حدث نظام التشغيل ويندوز ١٠.
- تأكد من أن الحواسيب على نفس الشبكة. على سبيل المثال، اذا كانت أجهزة الحواسيب تتصل بالانترنت من خلال راوتر لاسلكي، تأكد من أنها جميعاً تتصل من خلال نفس الراوتر.
- اذا كانت الشبكة لاسلكية Wi-Fi، قم بضبطها إلى Private.
- قم بتنفيذ network discovery and file and printer sharing، وعدم تفعيل حماية المشاركة من خلال كلمة سر password protected sharing.

١- اضغط على زر Start ثم اختار > Network Settings  
Internet ، وعلى الجانب الأيمن، اختار خيارات المشاركة  
Sharing options.

٢- أسفل كلمة Private، حدد Turn on Network discovery and  
٣- Turn on file and printer sharing، أسفل All Networks،  
حدد Turn off password protected sharing.

• اجعل خدمات المشاركة تبدأ تلقائياً automatically.

١- اضغط على مفتاح شعار الويندوز + Windows R.  
٢- في المربع الحواري Run، اكتب services. MSc، ثم اضغط على  
زر OK.

٣- اضغط بالزر الأيمن على كل من الخدمات التالية، واختار خصائص  
Property، اذا لم تكن شغليها، اضغط على Start، و  
Startup type، حدد Automatic:

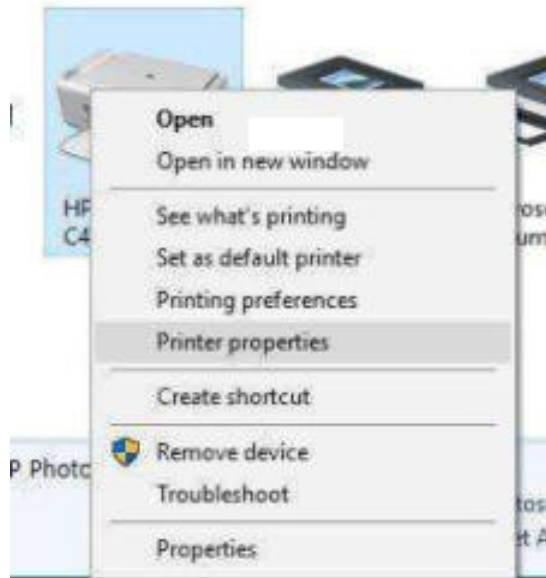
- Function Discovery Provider Host.
- Function Discovery Resource publication.
- SSDP Discovery.
- UPnP Device Host.

### تخبة قرص أو مجلد مشترك

ماذا لو أردت أن تحصر استخدام مجلد على الشبكة بعدد من المستخدمين؟  
الحل هو إنشاء hidden share من خلال إضافة علامة ('\$') في نهاية  
share name ، وبذلك ينحصر استخدام الملف بالمستخدمين الذين يعرفون  
. share name

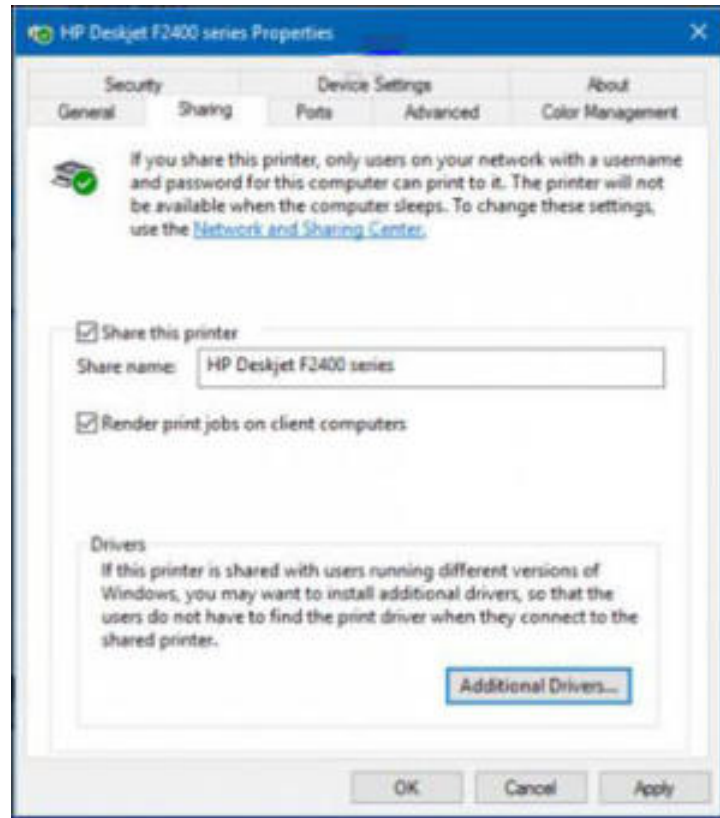
## مشاركة طابعة عبر الشبكة في ويندوز ١٠

في نظام ويندوز ١٠، يمكنك استخدام طابعة، بعد توصيلها بجهاز حاسوب واحد، والطباعة من حاسوب آخر. وذلك من خلال مشاركة الطابعة عبر الشبكة. قبل أن تقوم بمشاركة الطابعة، لابد أن تقوم بتعريفها أولاً، كما يجب أن تكون موصلة وتم تشغيلها. قم بالضغط على **Start > Settings > Devices**، ثم قم بفتح رابط الأجهزة والطابعات **Devices and Printers**. اضغط بالزر الأيمن على الطابعة، ثم اختار خصائص الطابعة **Printer properties**.



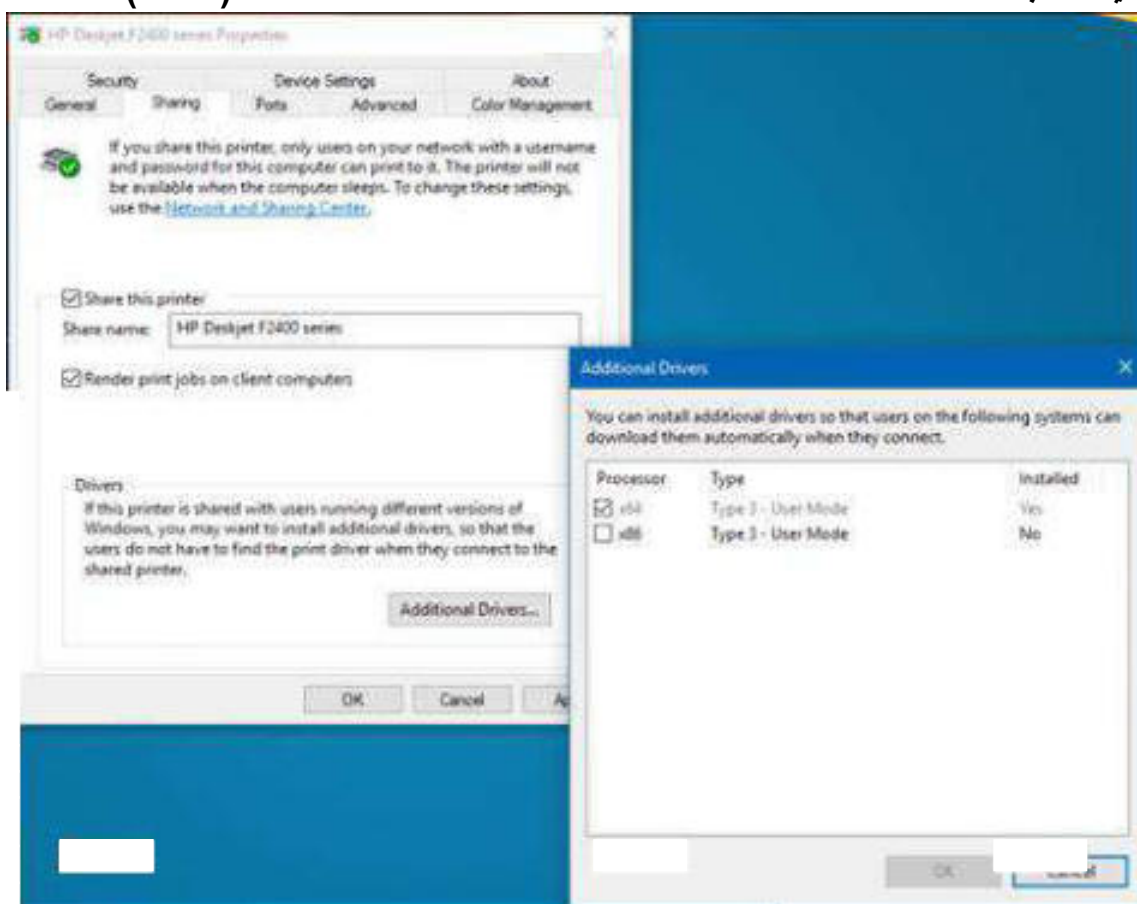
شكل (٤٢-٦) يوضح اختيار خصائص الطابعة من القائمة المختصرة.

- حدد تبويب المشاركة **Sharing tab**، ثم حدد الاختيار **share this printer**



شكل (٤٣-٦) يوضح خصائص مشاركة الطابعة.

إذا كنت تشارك الطابعة بين العديد من الأجهزة التي تختلف في بيئات النوافذ ٣٢ أو ٦٤ بت، ينبغي تفعيل الخيار "Render print jobs on client computers"، فهذا سيجعل المستخدمين يتمكنون من تثبيت الطابعة عندما يتصلون عبر الشبكة.

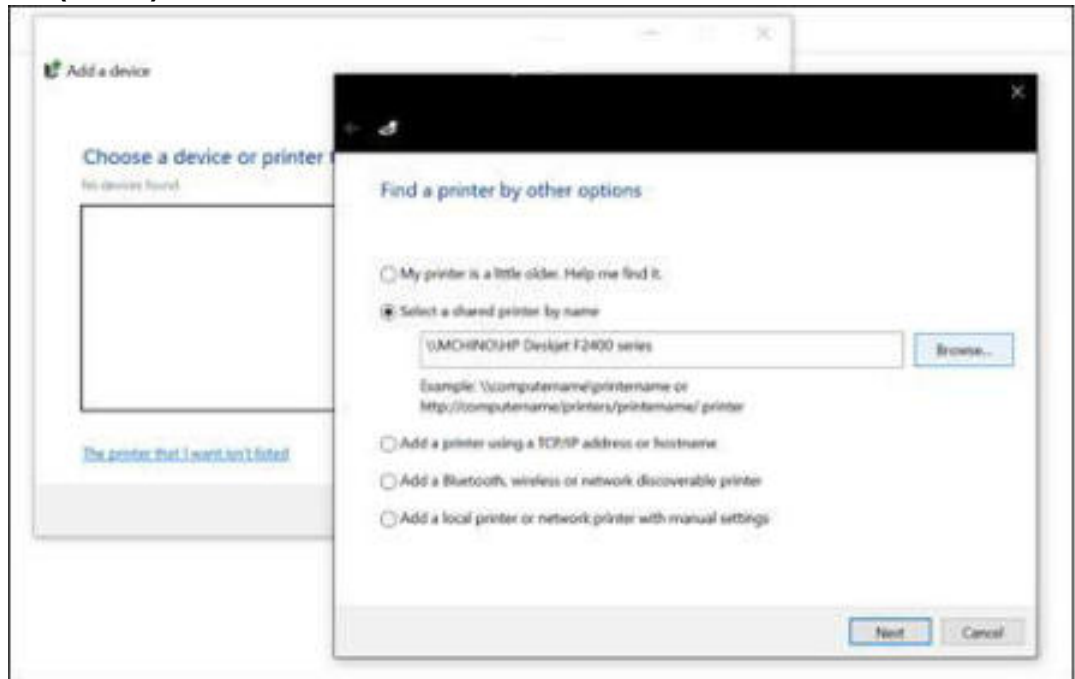


شكل (٤٤-٦) يوضح تفعيل الخيار "Render print jobs on client computers"

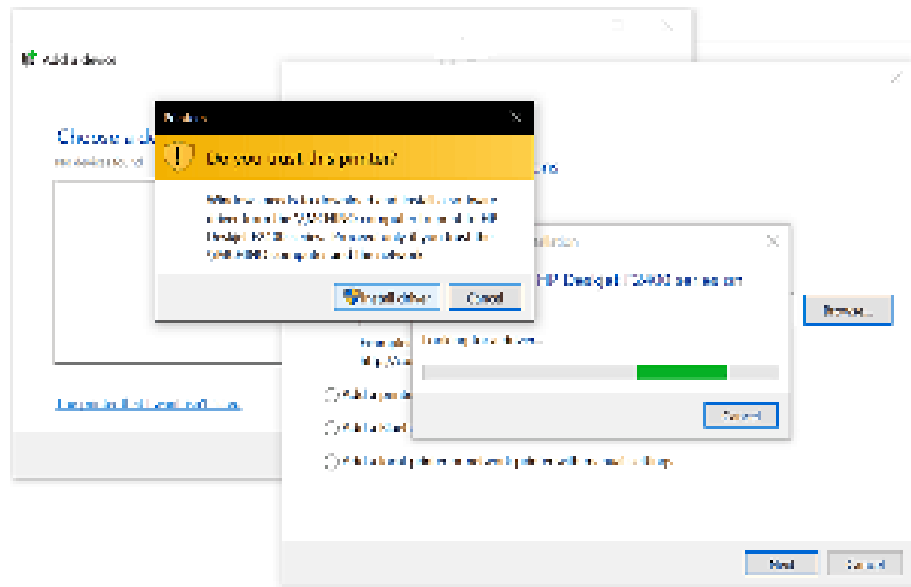
## الإتصال بطابعة تمت مشاركتها في ويندوز ١٠

بعد إعداد الطابعة التي سيتم مشاركتها، يمكنك الإتصال بها من خلال طرق متعددة. الطريقة الأولى تكون من خلال Devices and Printer. اضغط على زر إضافة طابعة Add Printer ، ثم اضغط على الرابط، *The printer that I want isn't listed* ، ثم اختار *shared printer by name* ثم استعرض الطابعات على الشبكة ثم اضغط فتح.

إعداد د/ أميرة إبراهيم عبد الغني



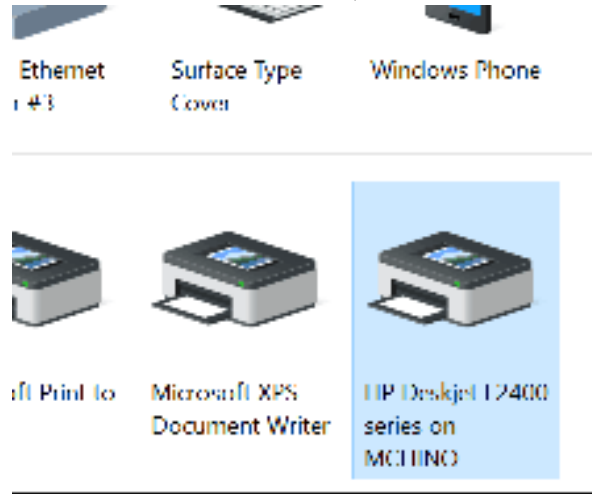
شكل (٦-٤٥) يوضح الإتصال بطابعة قد تمت مشاركتها عبر الشبكة.  
سيطلب الأمر إعداد المشغل ، اضغط على زر Next كي يتم اكتمال عملية  
إعدادة.



شكل (٦-٤٦) يوضح إعداد الطابعة التي يمكن مشاركتها عبر الشبكة.

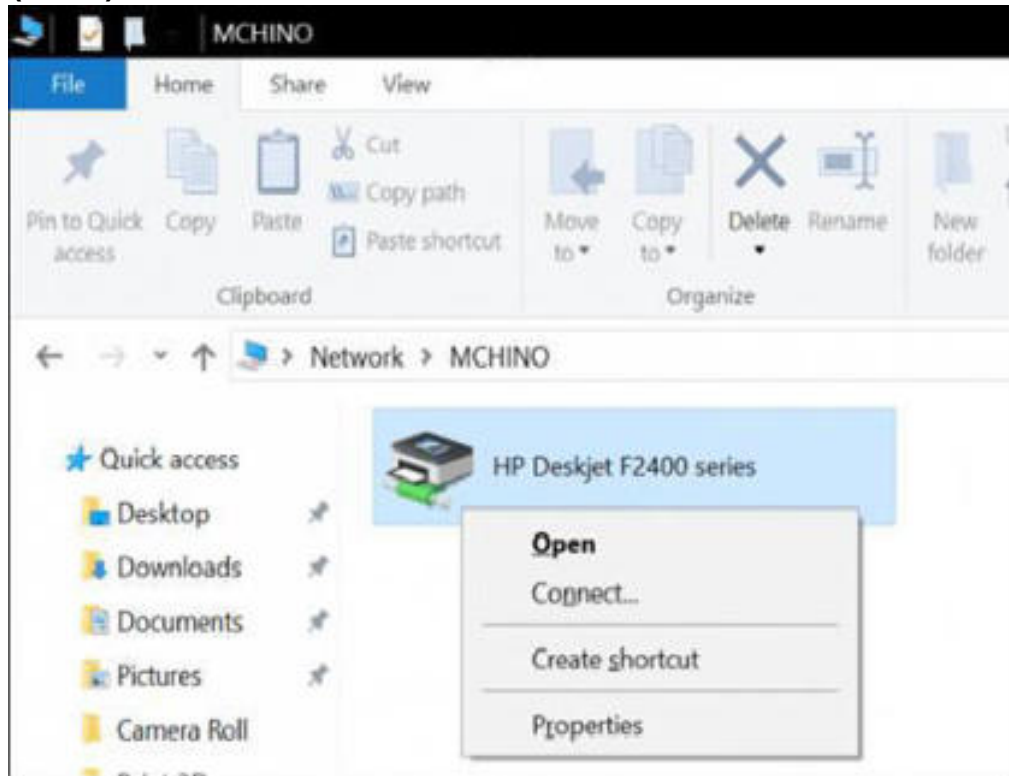
إعداد د/ أميرة إبراهيم عبد الغني

وبهذا ستظهر الطابعة في Devices and printers كجهاز محلي local device (كطابعة من الطابعات التي تم تعريفها من قبل وتوصيلها بالجهاز).



شكل (٤٧-٦) يوضح ظهور الطابعة في نافذة طابعات وأجهزة الجهاز.

أما الأخرى التي يمكنك م ال بطابعة عبر الشبكة فتكون خلال File Explorer . افتح مجلد الشبكة Network، استعرض الحاسوب الذي يشتمل على الطابعة التي تمت مشاركتها، اضغط عليها بالزر الأيمن ثم اضغط اتصال Connect.



شك ( يوضح اختيار الإتصال التي تمت مشاركتها من خلال مستك الملف.

## الملخص

مشاركة الطابعة في نظام ويندوز ١٠ من خلال الشبكة يجعل العديد من الأجهزة تتمكن من الطابعة على نفس الطابعة. وهذا يسمح لك بطباعة الملفات والوثائق بدون مراسلتها بين الأجهزة.





# الباب السابع

## أمن شبكات الحاسوب

### Computer Networks Security





## أهداف الباب السابع

بعد الانتهاء من دراسة هذا الباب ينبغي أن يكون الطالب قادراً على أن:

- ١- يُحدد نقاط ضعف الشبكات اللاسلكية.
- ٢- يُحدد إجراءات الأمن المتبعة لتحقيق الأمن في الشبكات اللاسلكية.
- ٣- يضبط اسم المستخدم وكلمة المرور على الراوتر.
- ٤- يفرق بين السماح بالاتصال بالراوتر عن طريق الواي فاي (بطريقة لاسلكية) وبين الاتصال عن طريق كبل الشبكة المحلية.
- ٥- يذكر المقصود بالتحكم بالوصول.
- ٦- يُعرف اسم الشبكة SSID.
- ٧- يبرر السبب في عدم تسمية الشبكة باسم يدل على شخصيتك أو مكانك.
- ٨- يبرر أهمية عدم تفعيل بث اسم الشبكة Hide SSID Broadcast.
- ٩- يبرر السبب في عدم استخدام التسمية الافتراضية.
- ١٠- يُعرف التشفير.
- ١١- يُعرف ماذا يعني بدون تشفير Open.
- ١٢- يُعرف الخصوصية المكافئة للشبكات اللاسلكية WEP.
- ١٣- يفرق بين WEP، WPA٢.
- ١٤- يفرق بين Brute force attack، Dictionary attack.
- ١٥- يُعرف اعدادات شبكة محمية WPS.
- ١٦- يبرر السبب في تعطيل WPS.
- ١٧- يُعرف MAC Filtering.
- ١٨- يُبرر السبب في أن يكون على علم دائماً بالعناوين التي يريد لها الوصول إلى الشبكة.
- ١٩- يُعرف شبكات الهندسة الاجتماعية.
- ٢٠- يحدد كيفية مراقبة ما يحدث داخل الشبكة اللاسلكية.
- ٢١- يُعرف اختراق الأجهزة.
- ٢٢- يُعرف جدران الحماية.
- ٢٣- يحدد أنواع جدران الحماية.
- ٢٤- يُعرف تقنية NAT.
- ٢٥- يوضح الدور الذي تقوم به تقنية NAT في حماية الشبكات اللاسلكية.
- ٢٦- يُعرف المقصود بالتحديث التلقائي.

- ٢٧- يقوم بضبط خيار التحديث التلقائي.
- ٢٨- يُفرق بين بروتوكولات التشفير للشبكات اللاسلكية.
- ٢٩- يعدد عيوب WEP.
- ٣٠- يعدد عيوب WPA.
- ٣١- يُبرر السبب في استخدام بروتوكول WPA٢.
- ٣٢- يعدد شروط تسمية الشبكات اللاسلكية.
- ٣٣- يذكر كيفية حماية الشبكات اللاسلكية.

## أمن الشبكات اللاسلكية

### مقدمة

انتشرت تقنية الـ WIFI بشكل كبير لأنها مناسبة وسهلة الاستخدام بشكل اكبر من الاسلاك ولكن تلك السهولة تأتي مع سهولة التجسس واختراق تلك الموجات بشكل اسهل من اختراق الشبكات السلكية وللأسف تقوم الشركات المصنعة للأجهزة الموجهة والتي تعرف "بالراوتر (Router)" بتجاهل العديد من اعدادات وسائل الحماية لجعل الامر اكثر سهولة للمستخدم علي حساب الأمان. أفضل طريقة لتأمين الشبكات اللاسلكية هي بعدم استخدامها اطلاقاً والاعتماد علي الشبكات السلكية ولكن هذا الحل غير واقعي بالمرّة لما تقدمه الشبكات اللاسلكية من سهولة وراحة وسرعة لكن حقيقة الامر هو أن الشبكات ووسائل الات سلكية ستظل دائماً أقـ قارنة مع نظيرتها السلكية ولذلك المستحيل - حتي الآن - ان تكون اي شبكة لاسلكية آمنة بنسبة مائة بالمائة لكن مع بعض الإعدادات والإستخدام الصحيح يمكن ان تضع عوائق كبيرة امام من يحاول اختراق الشبكة.

### نقاط ضعف الشبكات اللاسلكية

للشبكات المحلية اللاسلكية عدد كبير من المزايا مما يضيفي عليها جاذبية يصعب مقاومتها، و لن نجاوز الحقيقة إذا قلنا أن هذه الجاذبية هي وراء كثير من نقاط الضعف التي يعاني منها هذا النوع من الشبكات، و نقاط ضعف الشبكات اللاسلكية متعددة، و يمكن إجمال أهمها في الآتي:

١. بسبب سهولة تركيب و تشغيل الشبكات اللاسلكية فإن كثيرا ممن ينصب و يشغل هذه الشبكات هم من الأشخاص الذين ليس لهم دراية كافية بأمن المعلومات، و بالتالي فإنهم - في كثير من الأحيان - لا يعرفون كيف يهيئون الإعدادات - خاصة المتعلقة بأمن الشبكة - بشكل صحيح فيتركون ثغرات أمنية كبيرة في الشبكات اللاسلكية التي أقاموها. ومن أمثلة ذلك ترك قيمة (SSID) الأصلية دون تغيير مما يسهل على المهاجم الاشتراك في الشبكة اللاسلكية.

٢. وضع نقاط الدخول إلى الشبكة في أماكن مفتوحة مثل الممرات و القاعات، أي أنه بإمكان أي شخص أخذها من موقعها و العبث بإعداداتها بما يسهل عليه شن الهجمات ثم إعادتها في مكانها الأصلي.

٣. سهولة تعرضها للهجمات المؤدية إلى تعطيل الخدمة (Denial of Service) الذي يجعل أعضاء الشبكة اللاسلكية غير قادرين على تبادل المعلومات بينهم، هذا النوع من الهجمات يعتبر من أخطر ما تتعرض له الشبكات اللاسلكية لاعتبارات أهمها:

(أ) أن الشبكات اللاسلكية تعتمد على نطاق ترددي ضمن الطيف الكهرومغناطيسي لنقل البيانات، و يمكن بسهولة التشويش على ذلك النطاق الترددي لتوفر الأجهزة اللازمة للتشويش و رخص ثمنها.

(ب) وفقا لما جاء في نسخة عام ٢٠٠٤م من التقرير المشترك الذي يصدره في الولايات المتحدة الأمريكية كل من معهد أمن الحاسوب و مكتب التحقيقات الفدرالي فإن هجمات تعطيل الخدمة تبوأ المركز الأول -

مشاركة مع الهجمات باستخدام البرامج السيئة - من حيث حجم الأضرار الذي تنزله، و هذا يدل على أن عددا كبيرا من المهاجمين صاروا يعتمدون هذا النوع من الهجمات.

(ج) هناك ثغرات في تصميم البروتوكول الذي يدير عملية انضمام الأعضاء إلى الشبكة، وقد مر معنا أنه أثناء تأسيس الاتصال بين نقطة الدخول و الأجهزة الراغبة في الاتصال بالشبكة ترسل نقطة الدخول نبضات إلكترونية على فترات منتظمة معلنة عن نفسها، وأن هذه النبضات تحوي في طياتها معلومات مهمة تساعد الأجهزة على الاستجابة و تهيئة نفسها للاتصال. و تستمر نقطة الدخول إلى الشبكة في إرسال هذه النبضات طيلة فترة عملها للمحافظة على الاتصال بين الشبكة. و لكن الم الرسائل التي تحملها هذه النبض تبث دون أي نوع من الحماية فليس هناك ما يدل بشكل قطعي على هوية من أرسلها، و بالتالي فإنه يمكن للمهاجم إرسال نبضات مزورة تحمل هوية نقطة الدخول الحقيقية، و يحمل تلك النبضات رسالة تطلب من جميع الأجهزة المرتبطة بالشبكة إنهاء الاتصال، و هذا يقطع عمل الشبكة و يعطل الخدمة.

٤. أيضا بسبب طريقة عمل الشبكات اللاسلكية واعتمادها على الطيف الكهرومغناطيسي فإنها عرضة بشكل خطير للتصنّت إذ توجد أجهزة خاصة يمكن للمهاجم استخدامها لبث نداءات لاسلكية، و بسبب طبيعة



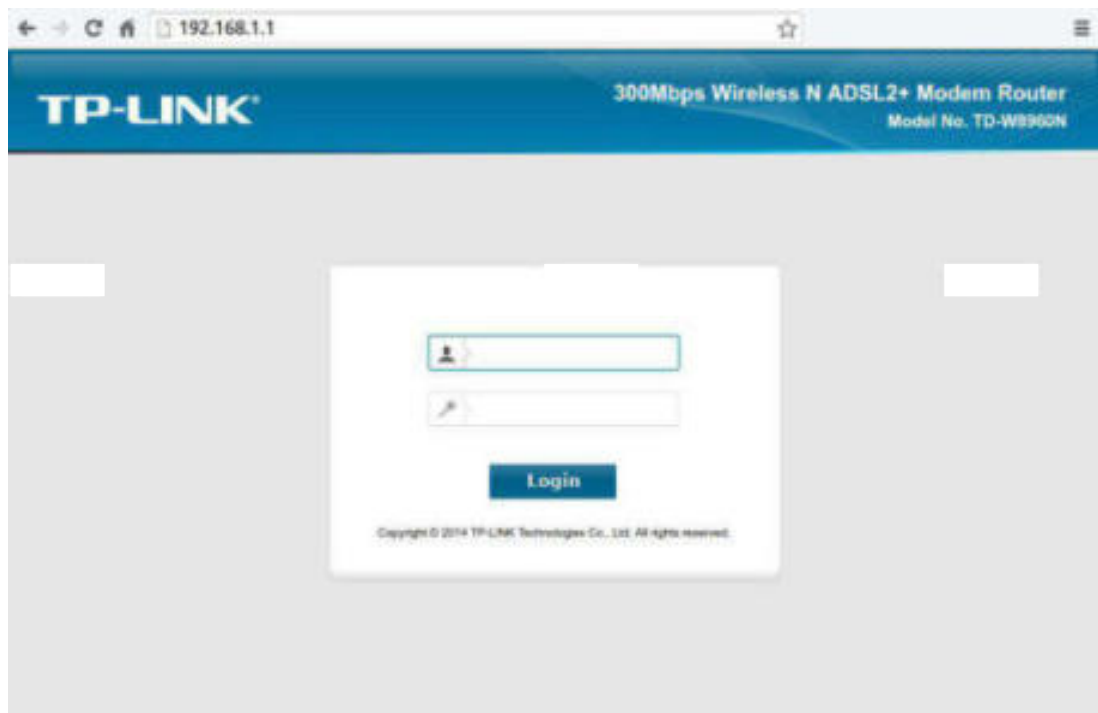
عملها فإن نقطة الدخول إلى الشبكة تستجيب لهذه النداءات مما يكشف وجود الشبكة اللاسلكية و عندها يقوم المهاجم باستخدام أجهزة أخرى لالتقاط الرسائل المتبادلة داخل تلك الشبكة.

## الإجراءات المتبعة لتحقيق الأمن في الشبكات اللاسلكية

### أولاً: الراوتر

نقطة البداية هي جهاز الراوتر "Router" وفي الحقيقة تتكون أجهزة الراوتر المنزلية من ٣ أجهزة مدمجة معا لتسهيل الأمور علي المستخدم المنزلي. فتلك الأجهزة عادة تتكون من "المودم" + "الراوتر" + "نقطة اتصال لاسلكية" ولكن للتبسيط، سأقوم بالإشارة له بالراوتر. هو الجهاز الذي يوجه حزم البيانات بين الشبكات ، لذلك يعتبر البوابة بين العالم الخارجي والشبكة المنزلية وبالتالي يجب افر به جدار حماية ضد ات التي قد تأتي من شبكة الانترنت وفي الحقيقة ان اغلب اجهزة الراوتر الحديثة تقوم بذلك الامر بشكل فعال الي حد ما بالنسبة للأجهزة الموجهة للاستخدام المنزلي. تبدأ **الخطوة الاولى** بشراء جهاز راوتر جيد يوفر اساليب الحماية المطلوبة وايضا يكون خالي من عيوب اونقط اختراق في نظام تشغيله. يمكنك ان تبحث عن كل المعلومات اللازمة عن طريق شبكة الانترنت قبل الشراء او البحث عن عيوب (إذا وجدت) في الجهاز الذي تمتلكه. جملة بحث مثل "TD-W٨٩٧٠ vulnerability" كفيلة بإمدادك بالمعلومات الكافية عن تلك العيوب وإذا كان هناك تحديث للجهاز. تأتي **الخطوة التالية** في كيفية الاتصال بجهاز الراوتر نفسه لتغيير تلك الإعدادات والتحكم في الجهاز بشكل عام وسنقسمهم بشكل عام الي طريقتين وهما "Local Access" و "Remote Access" الاتصال المحلي او "Local

"Access" يعني الاتصال بجهاز الراوتر من داخل الشبكة المحلية (الشبكة المنزلية) سواء عن طريق كابل الشبكة المحلية "LAN Cables" او عن طريق تكنولوجيا الواي فاي "WiFi" وذلك يكون عامة عن طريق ادخال عنوان بروتوكول الانترنت المحلي "Local Internet Protocol Address" لجهاز الراوتر في المتصفح. غالبا ما يكون العنوان "192.168.1.1" او "192.186.1.254" وذلك يعتمد علي الجهاز نفسه ويمكن من معرفة ذلك عن طريق دليل المستخدم او عن طريق البحث علي شبكة الانترنت.



شكل (١-٧) يوضح الدخول على صفحة الراوتر التي تطلب اسم المستخدم وكلمة المرور.

توفر بعض الاجهزة خيار عدم السماح بالاتصال بالراوتر عن طريق الواي فاي (بطريقة لاسلكية) وتسمح فقط بالاتصال عن طريق كابل الشبكة المحلية

إعداد د/ أميرة إبراهيم عبد الغني

ويفضل تفعيل ذلك الخيار إذا امكن لأنه يحد من طريقة الاتصال بالراوتر الي الطريقة المادية الاكثر أماناً ولكنه ايضا قد يكون غير ملائم إذا كنت لا تملك جهاز كومبيوتر ثابت يمكن توصيله بشكل دائم بجهاز الراوتر ولا تحب ان تقوم بالبحث عن كابل شبكة محلية لايصال الكومبيوتر المحمول كلما اردت الوصول الي الراوتر اوتريد الاتصال بالراوتر عن طريق جهاز لوجي "Tablet" او عن طريق هاتفك الذكي. الاتصال عن بعد او "Remote Access" يعني الاتصال بالراوتر عن بعد من خارج الشبكة المحلية وهو خيار يسمح للمستخدم المنزلي ان يطلب المساعدة من الشركة الموفرة للانترنت او اي شخص اخر بتعديل او ضبط الاعدادات الخاصة بالراوتر عن بعد وهي خاصية يجب ان تكون غير مفعلة الا عند الحاجة.

## ثانياً كم في الوصول

بعد الاتصال بالراوتر تجد الصفحة التي تطلب اسم مستخدم وكلمة المرور وإذا كان الجهاز جديد او لم تقم بتغيرهما سابقاً فإن اسم المستخدم وكلمة المرور سيكونان علي الوضع الافتراضي "Router Default Password" وغالبا ما يكونان "admin" أو سيأتي مع الجهاز ورقة تحدد اسم المستخدم وكلمة المرور وبالطبع في دليل المستخدم. بعد الدخول يجب عليك ان تغيرهما الي شئ اخر -بعض الاجهزة قد لا تسمح لك بتغير اسم المستخدم ولكن ان امكن فعليك بتغييره من "admin" الي اي شئ اخر تريده- واستخدام كلمة مرور قوية لا يعرفها غيرك.



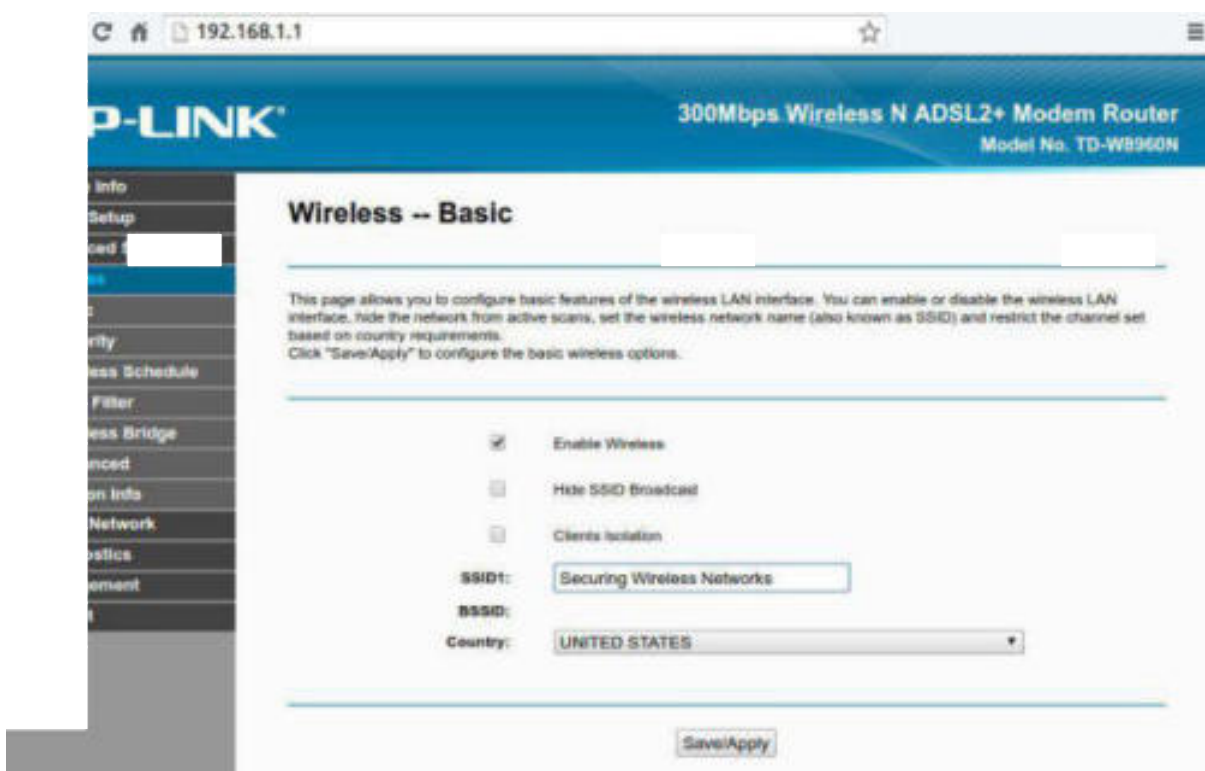
شكل (٢-٧) يوضح اعدادات التحكم بالوصول في الراوتر.

قد يختلف تصميم وتختلف المسميات من راوتر لآخر لكن يمكن ان تكتشف مكان كل شئ في وقت بسيط وبالطبع البحث في دليل المستخدم اوشبكة الانترنت. تأكد من تغير كلمات المرور الخاصة بكل اسماء المستخدمين ("admin" بالطبع ولكن ايضا "support" و "user" مثلا ان وجد او تعطيلهم اومسحهم ان امكن (وايضا التأكد من تعطيل خيارات الاتصال عن بعد "Remote Access" وتفعيلهم فقط في حالة استخدامهم، مع العلم انه عند استخدام تلك الخاصية يجب استخدام عنوان بروتوكول الانترنت الخارجي وليس المحلي "External Internet Protocol Address" .

إعداد د/ أميرة إبراهيم عبد الغني

## ثالثاً: إسم الشبكة SSID

تسمية الشبكة باسم يدل علي شخصيتك أو مكانك يعتبر امر سئ امنيا لما يوفره لمن يبحث عن معلومات لاختراق الشبكة. فاسم الشبكة يوفر معلومات أولية قد تقود الي معرفة كلمة المرور الخاصة بالشبكة اللاسلكية خصوصا إذا كان من يريد اختراق الشبكة شخص يعرفك كالجيران للاتصال بشبكة الانترنت أو إذا كنت هدف محدد لمن يريد اختراق الشبكة لاسباب اكثر خطورة. الاسم المبهم قد يساعد علي وضع بعض العقبات في طريق المهاجم .



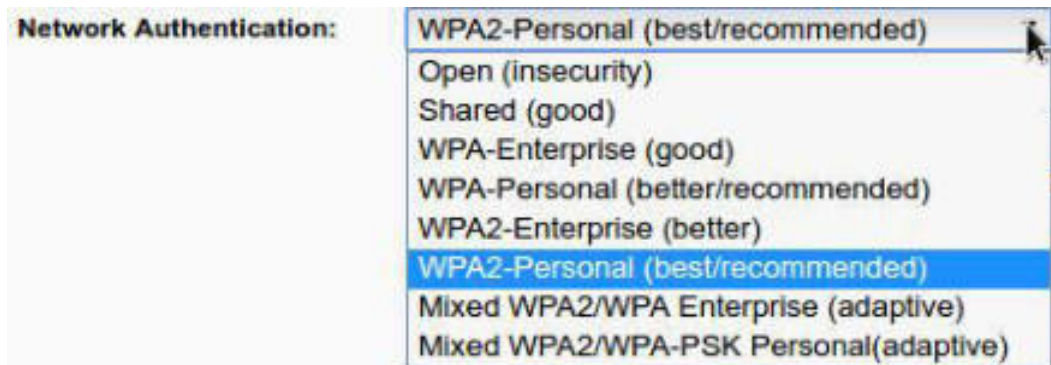
شكل (٣-٧) يوضح كيفية تغيير اسم الشبكة SSID.

يمكنك ايضا تفعيل خاصية عدم بث اسم الشبكة "Hide SSID Broadcast" فلا تظهر كالعادة في قائمة الشبكات اللاسلكية عند البحث وللاتصال بالشبكة يجب ان يتم ادخال كلمة المرور بالإضافة الي اسم الشبكة وذلك يوفر طبقة حماية اخري خصوصا ضد من لا يمتلكون خبرة كافية. تكون هذه الخطوة الاضافية مطلوبة فقط عند الاتصال بالشبكة أول مرة ويكون الامر تلقائيا بعد ذلك كالعادة. قد لا تدعم بعض الاجهزة امكانية الاتصال بشبكة مخفية خصوصا الاجهزة القديمة نسبيا ولكن اغلب الاجهزة وانظمة التشغيل الحالية تدعم تلك الخاصية. يمكن بسهولة اكتشاف وجود شبكة لاسلكية مخفية وعدم بث اسم الشبكة قد يقيك من هجمات الهواة.

التسمية الافتراضية قد تكون مشكلة ايضا لانها تتيح التعرف علي نوع ونموذج الراوتر بطريقة سهلة) يمكن تحديد نوع الراوتر عن طريق الـ "MAC (s" A بما يتيح البحث عن معروفة مرتبطة بنموذج الراوتر الإعدادات الافتراضية من الشركات الموفرة لخدمة الإنترنت. عزل الاجهزة أو "Clients Isolation" هي خاصية اخري قد تتوافر في بعض اجهزة الراوتر وهي تفصل الاجهزة المتصلة بالشبكة اللاسلكية عن بعضها وعن الاجهزة الاخري المتصلة عن طريق كابل الشبكة المحلية وذلك يعني ان الاجهزة المتصلة بالشبكة اللاسلكية لا يمكنها التفاعل مع بعضها أو مع اي اجهزة اخري علي الشبكة ولا تستطيع الا الوصول الي شبكة الانترنت وفي ذلك أمان اكبر للشبكة لذا من الافضل ان تكون مفعلة إذا كنت لا تحتاج ان تتفاعل الاجهزة مع بعضها.

## رابعاً: التشفير

تظل مشكلة الشبكات اللاسلكية الكبرى هي اهمال البعض الجزء الخاص بالتشفير أو كلمة المرور الخاصة بالشبكة اللاسلكية بشكل أو بآخر. والمقصود هنا ليس تشفير الشبكة كليا ولكن طريقة تشفير عملية المصادقة بين الاجهزة والشبكة بمعنى تشفير عملية اثبات ان الجهاز الذي يحاول الاتصال بالشبكة هو جهاز مسموح له بالاتصال عن طريق كلمة سر ولا يستطيع احد قد يكون بمراقبة الشبكة من التصنت علي تلك العملية وبالتالي معرفة كلمة السر التي تتبادل بين الاجهزة والشبكة او جهاز الراوتر. البعض قد يترك الشبكة بدون كلمة سر نهائيا. البعض قد يختار كلمة سر ضعيفة أو طريقة تشفير يعتقد انها قد تحميه وهي في حقيقة الامر لا تقدم الا حماية زائفة. يجب ان تكون الشبكة اللاسلكية مشفرة ومحمية بكلمة سر تحت اي ظرف حتي إذا كنت تريد ان تشار الآخرين. يجب ان انواع التشفير التي تختارها ولا وببساطة، فإن استخدام بروتوكول "WPA2 – Personal" هو أفضل اختيار وكل الإختيارات الأخرى ماهي إلا دعما لأنظمة قديمة قد لا تدعم البروتوكول الحديث نسبيا.



شكل (٤-٧) يوضح ضبط بروتوكولات الشبكة اللاسلكية على WPA2.

## بدون تشفير "Open"

إذا تركت الشبكة متاحة لأي شخص كان وذلك يتنافي مع كل خطوات الحماية التي أشرحها هنا. حتي وإن كنت تريد مشاركة الشبكة مع الغير فإن من الأفضل ان تقوم بإستخدام كلمة سر وطريقة تشفير قوية ومن ثم اعطاء كلمة السر لمن تسمح لهم بالاتصال بالشبكة وقد يوفر لك جهاز الراوتر خيار تفعيل شبكة لاسلكية أخرى خاصة بالزوار تكون منفصلة عن شبكتك اللاسلكية الرئيسية.

## الخصوصية المكافئة للشبكات السلكية WEP

قد يوحي الاسم انها افضل الطرق لحماية الخصوصية ولكن "Wired Equivalent Privacy" يمكن فك شفرتها في غضون دقائق ان لم يكن أقل. توجد من البرامج التي تقو بطريقة تكاد تكون تلقائية ويست استخدامها اي شخص حتي وان لم يكن شخص محترف أو حتي غير تقني أشهرهم "Aircrack-ng" جدير بالذكر ان اغلب الإعدادات الافتراضية لاجهزة الراوتر تستخدم تلك الخوارزمية بدون ايضاح انها ضعيفة ويمكن كسرها بسهولة.

```
[00:03:53] Tested 454246 keys (got 76164 IVs)

key depth byte(s)
0 0/ 1 40(104352) 80(88328) 28(88864) 55(85584) 14(85248) 50(88960) A1(84960) 32(84480) 5E(84480) 8A(84480) F2(84480)
1 0/ 1 8F(103984) 94(87940) 90(85584) 83(84736) D3(84480) 20(84128) F1(84224) 15(83456) C7(83280) FC(83200) 85(82688)
2 0/ 1 68(104352) 7E(87888) 28(88784) AE(86528) F8(85504) 52(84960) 79(84480) 6A(84224) 49(83968) 79(83968) 84(83712)
3 0/ 1 61(104248) 8F(87808) 4C(87296) 56(86272) 96(85760) 6F(85504) 1D(85584) 32(85584) 56(84480) 9A(84480) 85(84480)
4 0/ 1 8D(86232) 48(87040) A8(86784) 4E(86272) 76(85760) FF(85680) 4B(84512) 98(84000) EC(84736) 81(84480) 73(84224)
5 0/ 1 85(83184) 79(86016) F2(85248) DC(84224) 4D(83456) 51(83520) 4C(83280) 24(82544) 2A(82944) 45(82688) 5E(82688)
6 0/ 1 04(86512) C1(88576) 74(88320) 3F(88784) 21(88672) 86(88784) 16(88784) 88(88784) 53(84480) C5(84224) CC(84224)
7 0/ 7 0A(87888) 32(85584) 4A(85248) AC(85248) CC(85248) 89(84960) 6C(84736) FE(84736) 88(84480) 4F(84224) 38(83712)
8 0/ 1 64(88948) F9(89580) A8(88328) F1(87296) 99(86528) 80(84224) 88(84128) 8F(84224) 71(83968) D8(83968) 53(83712)
9 0/ 3 11(88832) 1D(87040) 8F(87040) 3A(85760) DC(85760) 89(84736) 51(84480) 18(84224) 46(84224) 80(84224) D6(84224)
10 0/ 1 8E(87296) 8D(87040) C2(86528) 99(84960) 9D(84736) E4(84480) 7A(84224) CA(84224) E3(83968) 1E(83712) A2(83712)
11 5/ 1 8F(85584) 12(84960) 4E(84960) 88(84960) 9A(84224) 4C(83968) 22(83712) C9(83712) 62(83456) 1C(83456) C1(83456)
12 0/ 1 77(89188) 98(89084) 6A(85348) 3F(84820) 74(82892) F2(82956) 91(82548) 85(82584) 56(82288) F0(82196) F1(82098)

KEY FOUND! [ 8D:6F:98:61:8D:65:64:61:64:65:6C:78:77 ] (ASCII: mohamed@l3w)
hit withDecrypted correctly: 100%
```

شكل (٥-٧) يوضح اختراق بروتوكول WEP وفك شفرتها.

إعداد د/ أميرة إبراهيم عبد الغني



## بروتوكول WPA و WPA٢

بعد اكتشاف ضعف الخصوصية المكافئة للشبكات السلكية أو "WEP" قامت المؤسسة التي تطور تكنولوجيا الواي فاي والمسماة بـ "Wi-Fi Alliance" بتطوير بروتوكول "WPA" ليكون بديلا عن "WEP" لتأمين الشبكات اللاسلكية وفي نفس الوقت يمهّد الطريق لحين تطوير بروتوكول "WPA٢" الأكثر قوة لذلك ينصح دائما استخدام "WPA٢" الذي يعتبر الطريقة الوحيد الآمنة نسبيا لتأمين الشبكات اللاسلكية والذي صمم ليحل مكان "WEP" و "WPA". تظل طرق التشفير الأخرى "WEP" و "WPA" متاحة كخيار في أجهزة الراوتر حتي تتيح للأجهزة القديمة أو البرامج القديمة ان تتصل بسهولة بالشبكة، ولكن أغلبية الأجهزة والبرامج التشغيلية الآن تدعم "WPA٢" الأقوي والأف كمن تعتمد قوة كلا الب ين علي قوة كلمة السر المست بمعذ قام المستخدم باختيار ول "WPA٢" القوي واستخدام السر "apple" مثلا فان اي شخص يستطيع باستخدام نفس حزمة البرامج السابقة "Aircrack-ng" ان يكسر التشفير ويحصل علي كلمة السر. ببساطة، يعتمد بروتوكول "WPA٢" علي معيار تشفير يسمى "AES" و الذي بالتالي يعتمد علي خوارزمية تقوم بتبديل (تشفير) كلمة السر أو النص الي رموز أو حروف ليست لها معني لا يمكن استخدام اي خوارزمية اخري لإعادتها الي النص أو كلمة السر الاصلية فمثلا تقوم بتحويل "apple" الي "٢" fsGsNtyFu٨Y١٦fWGLMxMA== لذلك ان استطاع احد الوصول الي النص المشفر لن يستطيع استخدامه لأنه بلا معني ولا يمكن اعادته إلي النص الاصيل، ولكن يمكن استخدام نفس خوارزمية التشفير لتشفير كلمات

```

[00:03:36] 143376 keys tested (677.97 k/s)

KEY FOUND! [ weakpassword ]

Master Key      : 5E 68 AF 88 2E 88 68 6E 17 D5 BF 39 9C 2D 2E 58
                  87 68 78 83 [REDACTED] 0A 47 80 F8 A4 BE CF D3 [REDACTED]

Transient Key   : CF C7 6B 56 F3 DE F0 5D 31 76 64 E3 CC C0 58 E1
                  8B 4F F8 6C AA 2D 26 D1 D5 3C 83 B8 EF A0 5F 5C
                  97 97 85 2C C5 91 67 CA 62 6D C7 2C 98 94 7C E1
                  2B 9B A0 AD E5 B4 76 82 B1 06 74 38 AE 75 81 4D

Please provide the following:

EYBOG HWVC      : 21 23 21 34 V0 00 30 B8 00 00 0C DC 00 D0 B0 43
                  0A B8 V1 3C E3 E0 E0 1A 25 20 10 00 01 C1 5E C1
                  05 33 0E 83 3E 0E 50 82 08 C0 40 E2 13 02 E0 50
                  00 B4 22 00 V1 20 1E C0 E4 50 05 04 25 0E 0E C0
Transient Key    : 04 83 7E 1D 11 40 C0 E5 81 E0 00 18 00 0B E0 50
                  21 35 D8 E5 02 44 10 B4 E4 30 0E 10 B8 3B 42 00
Weak Key         : 0B 0C D3 V0 2E V4 E3 B8 E0 B4 E1 1A 2E 5E D0 53

Please provide: [ ]:~>

[00:13:52] 405141 keys tested (210.23 k/s)

```

شكل (٦-٧) يوضح الطريقتان المستخدمتان لكسر كلمة المرور.

== إعداد د/ أميرة إبراهيم عبد الغنى ==

كما تري فان كلا الطريقتين الاكثر استخداما يعتمدان علي قوة جهاز المهاجم وعلي قوة كلمة السر التي تستخدمها. فان كنت تستخدم كلمة سر ذات معني أو كلمة سر تحتوي علي حروف أو ارقام قصيرة حتي وان كانت بلا معني يمكن كسرها مع بعض الوقت والمجهود لذلك ينصح باستخدام كلمات سر ليس لها معني وتحتوي علي عدد كبير من الاحرف والارقام والرموز مثل "LttSw۲F٤٤dEO٠" و "bwpFW٩٣Fm۲٠BN" و "H٠٣٨٢OBe٣٠" بحيث يصعب وجودها في قاموس كلمات وفي حالة هجوم "Brute-force" تأخذ وقت طويل جدا يصل الي دهور. بالتالي فان كسر بروتوكول "WPA" و "WPA٢" يعتمد علي قوة كلمة السر المستخدمة بالإضافة الي درجة التزام المهاجم بالوصول الي كلمة السر وإمكانياته من برامج، اجهزة، وقواميس للوصول اليها وفي الغالب ان لم يكن المستخدم المنزلي أو الشبكة اللاسلكية هد ، فان المهاجم سريعا اب بالملل وسينتقل في الغالب محاولة إختراق شبكة اخري اكثر سهولة. إذا كان جهاز الراوتر يوفر لك خيار اختيار طريقة التشفير، اختر "AES" ولا تقم بإختيار "AES + TKIP" معتقدا انها تقدم حماية أقوى.

### سادساً: إعدادات شبكة محمية Wi-Fi Protected Setup

أو "WPS" اختصاراً، هو معيار تم اضافته حديثاً نوعاً ما لييسط عملية اتصال الاجهزة الجديدة بالشبكة بدون ادخال كلمات السر المعقدة والطويلة (والأمنة) بعدة طرق قد تتوفر بعضها أو جميعها بجهاز الراوتر ولكن تعتمد كلها علي "PIN" أو رقم تعريف شخصي يتم تبادله بين جهاز الراوتر والجهاز الذي يريد الاتصال بالشبكة. إذا كان هذا المعيار مفعلاً، وبغض النظر إذا كنت تستخدم

بروتوكول "WPA٢" وكلمة سر قوية، فإن الشبكة يمكن اختراقها بسهولة في فترة قد لا تزيد عن يومين كحد اقصى وفي بعض الحالات، في بضع دقائق باستخدام برامج (أو عدة برامج معا) لا تتطلب معرفة تقنية مثل "Reaver" "WPS" للأسف، تأتي معظم اجهزة الراوتر الحديثة بهذا المعيار مفعّل ويجب علي المستخدم المنزلي عدم الاعتماد عليه تماما وتعطيله لما يحمله من مخاطر.



شكل (٧-٧) يوضح إلغاء تفعيل WPS.

## MAC Filtering

الـ "MAC" هو اختصار لـ "Media Access Control" وهو عبارة عن عنوان أو قيمة فريدة ترتبط ببطاقة الشبكات سواء كان لاسلكية أو سلكية ،لا توجد بطاقتين تستخدم نفس العنوان أو القيمة لذلك يمكن استخدامهم لمنع اجهزة معينة من الاتصال بالشبكة اللاسلكية أو الافضل من ذلك، السماح لاجهزة معينة فقط الاتصال بالشبكة اللاسلكية ومنع كل الاجهزة الاخرى. ليست طريقة أمنة بالكامل فهناك طريق تمكن اي شخص من تغيير (أو بالاصح

محاكاة) اي عنوان يريد، ولكنها طبقة اخري من الحماية لزيادة صعوبة عملية الاختراق. لتفعيل تلك الخاصية، يجب ان تكون علي علم بالعناوين التي تريد السماح لها بالوصول الي الشبكة (أو منعها) وطريقة معرفتهم تختلف من نظام تشغيل الي اخر لذلك من الاسهل ان تبحث عن الطريقة الخاصة بنظام التشغيل الذي تستخدمه مثل Windows ١٠ أو يمكنك معرفة العناوين المتصلة حالية بالشبكة عن طريق جهاز الراوتر من خلال البحث عن "Devices Info" أو "DHCP" أو البحث عن طريق الانترنت عن الطريقة لمعرفة الاجهزة المتصلة بالشبكة الخاصة بجهاز الراوتر الذي تمتلكه مثل : TD-W8960N بعد ذلك يمكنك ببساطة إضافة العناوين وتفعيل الـ "MAC Filtering" سواء بالسماح للعناوين المضافة بالاتصال بالشبكة أو منعهم.



شكل (٨-٧) يوضح كيفية ضبط العناوين التي تريد السماح لها بالوصول الي الشبكة (أو منعها) من خلال الراوتر.

## المخاطر

ربما تعتقد انه لا ضرر إذا كان هناك شخص آخر علي الشبكة اللاسلكية ولربما تعتقد انك تشارك الآخرين وتساعدهم علي الوصول الي شبكة الانترنت ولكن الحقيقة قد تكون مخيفة لاقصي درجة. يمكن ببساطة ان يعيث شخص ما باعدادات الشبكة من اجل المتعة وكل ما سيسببه هو بعض الازعاج. شخص اخر قد يستخدم شبكتك للوصول الي الانترنت للتصفح أو التحميل، مما سيؤثر علي السرعة وسعة التحميل. ربما قد يكون الشخص يستعمل الانترنت لاغراض غير قانونية أو غير اخلاقية فيستخدم شبكتك لاختفاء هويته ومكانه ولربما تقع انت في مشاكل قانونية بالنيابة عنه. لكن كل ما سبق لا يعد بخطورة شخص قد تكون نواياه اكثر خبثا، فاي شخص يستطيع الوصول الي شبكتك لية عن طريق الشبكة ة وبعض المعرفة التي تتراوح م البسي عقدة، يمكنه ان يري تفعل، يسمع كل ما تقول، ويست الوصول الي تفاصيل خصوصياتك التي قد تعتقد انها بأمان.

## الهندسة الاجتماعية

الهندسة الاجتماعية هي فن التلاعب النفسي للأشخاص بهدف الوصول الي معلومات سرية أو الاحتيال والنصب وهي ليست سهلة لانها تعتمد في الاساس علي ثقة من يقوم بالهجوم بنفسه وشخصيته، لكن جزء كبير منها يتعلق بما يمكنه الوصول اليه من معلومات لاستخدامها للوصول الي اهدافه. في معظم الاحيان، يقوم الاشخاص باستخدام ارقام هواتفهم ككلمة سر للشبكة وبعد ان

يقوم المهاجم من كسر كلمة السر) إذا كان التشفير المستخدم WEP مثلا ( يحصل علي رقم الهاتف الذي يستطيع وبكل سهولة معرفة المزيد عن صاحبه باستخدام خدمة مثل truecaller أو بالبحث في مواقع موفرين الخطوط عن الفاتورة الخاصة بالرقم ليصل الي معلومات اكثر.

شكل (٧-٩) يوضح الوصول إلى بيانات من خلال الفاتورة الخاصة بالمستخدم.

في بعض الاحيان الاخرى، تحتوي اعدادات الراوتر نفسها علي رقم الهاتف المرتبط بمزود خدمة الانترنت في صورة اسم المستخدم أو بالذهاب الي صفحة الحساب الخاصة بالمستخدمة فور دخوله علي موقع الانترنت الخاص بالشركة المزودة للانترنت مما قد يتيح للمهاجم -بالإضافة الي المعلومات- التلاعب باشتراك الانترنت الخاص بك.

وفي اغلب الاحيان، يمكن الوصول بعد ذلك الي حسابات صاحب الشبكة الاجتماعية لجمع المزيد من المعلومات وبسبب ان نسبة من الاشخاص يستخدمون نفس كلمة المرور لمعظم حساباتهم، قد يستطيع تسجيل الدخول والسيطرة عليها.

يست خص المهاجم بعد ذلك ام كل ما يملك من معلومات ان بالاحتيال عليك أو علي الآخرين، انتحال شخصيتك، أو ابتزازك. بالرغم من قلة حدوث تلك الهجمات في العالم العربي، ولكنها تظل مخاطرة كبيرة.

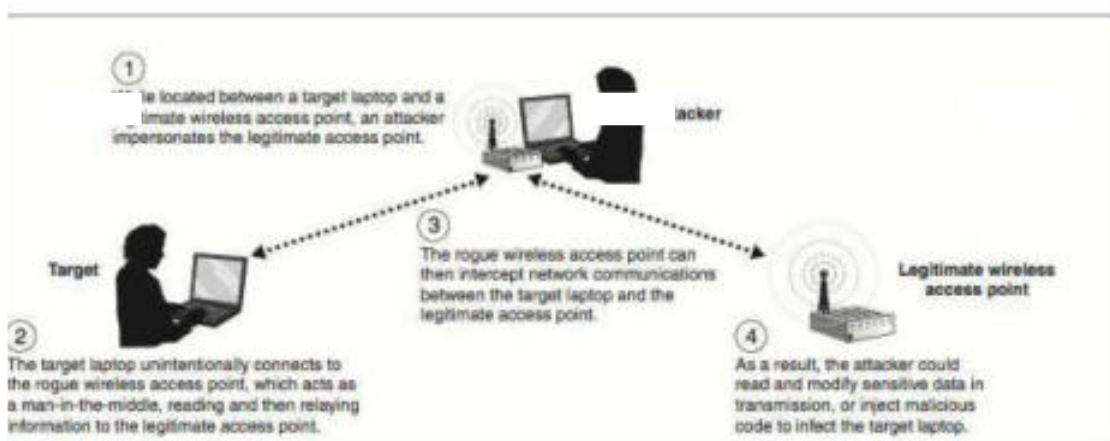
### مراقبة الشبكة

يستطيع اي شخص علي الشبكة اللاسلكية ان يقوم بمراقبة كل ما يحدث بداخل الشبكة بعدة طرق قد تكون اشهرها واقواها MITM أو Man in the Middle وكما يوحي الاسم ببساطة، هي طريقة هجوم تعتمد علي ان يقوم المهاجم بوضع نفسه في المنتصف بين الجهاز الهدف كجهاز كومبيوتر أو هاتف ذكي، وبين نقطة الاتصال اللاسلكية (الراوتر) وبالتالي يستطيع ان يري كل ما يمر بينهم من كلمات سر، صور، محادثات، المواقع التي تقوم بزيارتها، أو اي



بيانات أو أنشطة أخرى تقوم بها على شبكة الانترنت. يستطيع أيضا ان يعيد توجيهك الى مواقع أخرى شبيهة بالمواقع التي تقوم بزيارتها يكون هو المتحكم بها فيحصل على كلمات السر إذا قمت بادخالها أو يخدعك لتحميل برامج خبيثة ليتحكم في جهازك فيما يعرف بـ Spoofing attack .

كانت تلك الطرق أكثر سهولة فيما مضى، ولكن مع ازدياد تلك الهجمات وتطور مجال أمن المعلومات، تقوم معظم المواقع والبرامج بتشفير البيانات المتناقلة بينها وبين الأجهزة وتقوم باكتشاف بعض من طرق تلك الهجمات، ولكن بالطبع تطورت أيضا الأدوات التي تستطيع التحايل على كل تلك الاجراءات.



شكل (١٠-٧) يوضح دور Man in the Middle في مراقبة الشبكة واكتشاف الهجمات.

## اختراق الأجهزة

قد تبدو كلمة اختراق كبيرة نوعا ما هنا. في أغلب الاحيان، يستطيع المهاجم الوصول الي بعض الاجهزة المتصلة بالشبكة بدون "اختراقها" وذلك بسبب انها تكون بسهولة متاحة للجميع علي الشبكة المحلية أو بسبب تركها علي الاعدادات الافتراضية فيسهل تسجيل الدخول اليها مثل اجهزة التخزين المتصلة بالشبكة "Network-Attached storage" أو "NAS" اختصارا. أو ربما يحتوي جهاز الراوتر الخاص بك علي مدخل USB لتوصيل قرص صلب خارجي أو "USB flash drive" لتستطيع الوصول اليهم عن طريق الشبكة. أو ربما تمتلك كاميرا مراقبة منزلية لم تقم بتغيير اعدادتها الافتراضية وتغير كلمات المرور مما يتيح لاي شخص بالوصول اليها ومشاهدة بثها. ومع انتشار الاج صلة بالانترنت وتركها عدادات الافتراضية، تصبح الاله السهل بل وقد تكون بوابة لشبكتك المحلية بدون اختراق ال نفسه. ثم نأتي الي المشكلة الاكبر والتي نستطيع هنا استخدام كلمة اختراق في مكانها، فبعض الجهد يستطيع المهاجم ان يخترق الاجهزة المتصلة بالشبكة عن طريق بعض الثغرات التي تكون معروفة ولكن لم يتم تحديث تلك الاجهزة لسدها أو قد تكون ثغرات غير معروفة وبالتالي ليس لها تحديث أو "patch" يسد تلك الثغرة وهي ما تعرف باسم "zero day vulnerability" وفي العادة تكون تلك الثغرات الغير معروفة مرتبطة بمجموعات أو اشخاص متطورين وعلي معرفة واسعة بما يفعلون. اما الثغرات المعروفة والتي يصدر لها تحديث لسدها في كثير من الاحيان يهمل المستخدم المنزلي عملية التحديث لقلة معرفته أو عدم اهتمامه. جهاز الراوتر يصدر له بعض التحديثات من حين الي

آخر. اجهزة الكمبيوتر بانظمتها المختلفة يصدر لها تحديثات دورية واخري فورية حين اكتشاف ثغرة أو مشكلة تتعلق بالأمان وكذلك ايضا الهواتف الذكية (بسبب كثرة الهواتف الذكية المنتجة خصوصا التي تعتمد علي نظام التشغيل اندرويد لا تقوم الشركات المصنعة لها باصدار التحديثات اللازمة وبالتالي تترك المستخدم عرضة للخطر.

## حماية شبكات المعلومات Network Protection

هل يمكن تفادي المخاطر التي تواجه شبكات المعلومات؟ نعم  
ما هي الوسائل التي يمكن عن طريقها تجنب حدوث مثل هذه المشاكل  
والاختراقات في شبكات المعلومات التي تخصنا؟

### أولاً: جدران الحماية Firewalls

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين، وتختلف جدران الحماية حسب احتياجات المستخدم، فإذا استدعت الحاجة إلى وضع جدار الحماية على عقدة منفردة عاملة على شبكة واحدة فإن جدار الحماية الشخصي هو الخيار المناسب، وفي حالة وجود حركة مرور داخلية وخارجية من عدد من الشبكات، فيتم استخدام مصافي لجدار الحماية في الشبكة لتصفية جميع الحركة المرورية، علماً بأن الكثير من الشبكات والخوادم تأتي مع نظام جدار حماية افتراضي، ولكن ينبغي

التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراً على ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

وفي بعض الأحيان تقوم بعض شبكات المعلومات بوضع جدران حماية لعزل شبكتها الداخلية عن شبكة الإنترنت، ولا يكون هذا العزل كلياً بالطبع حتى يمكن للمستخدمين الاستفادة من بعض خدمات الإنترنت وفي نفس الوقت منع المخربين من الدخول إلى الشبكة الداخلية أو اختراق أمن وسرية المعلومات على الشبكة.

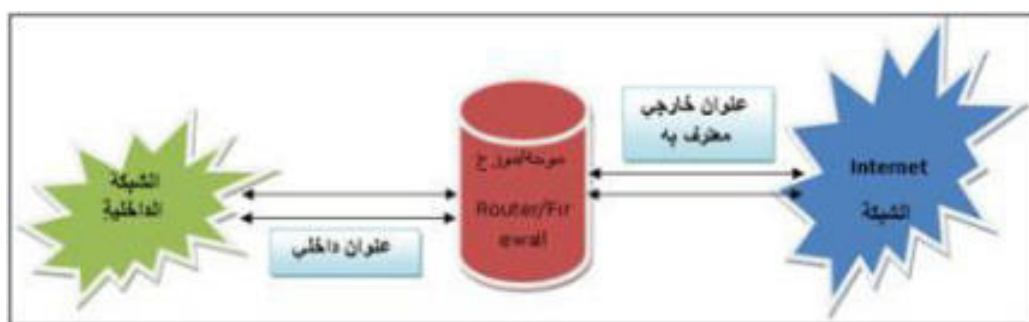


شكل (١١-٧) يوضح وضع جدار الحماية Firewall

هناك العديد من أنواع جدران الحماية التي تلائم كافة أنواع شبكات المعلومات وفقاً لحجم الشبكة والمؤسسة التي تعمل عليها، فهناك جدران الحماية التي تكون للمؤسسات الحكومية والشركات الكبيرة ذات سرعات وقدرات عالية جداً، مثل ما توفره شركة Cisco، كما أن هناك جدران حماية للمنشآت الصغيرة والشركات المحدودة، وهناك أيضاً برامج جدران الحماية التي يتم تحميلها على الحواسيب الشخصية لحماية الجهاز فقط.

## ثانياً: تحويل العناوين الرقمية Network Address Translation

تقنية NAT تعتمد على إعطاء كل حاسوب متصل بالشبكة رقم مميز يختلف عن باقي الأجهزة، وتقوم منظمة Internet Assigned Numbers (Authority IANA) بإعطاء هذه الأرقام ولا يكون معترفاً بها إلا عن طريقها، ونظراً لقلّة هذه الأرقام فإنه يعطى رقم واحد للشبكة ثم تقوم هذه الشبكة بإعطاء أرقام داخلية للحواسيب المترتبة بها بحيث لا يتكرر أي رقم، وعندما يرغب جهاز حاسوب من الشبكة الداخلية في الاتصال بشبكة خارجية يأتي هنا دور تقنية NAT حيث نقوم بتصيب جهاز حاسوب يلعب دور الوسيط بين الشبكة الداخلية والشبكة الخارجية ويحمل الرقم المعترف به المُعطى من قبل IANA للشبكة الأم، ويكون مهمته تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي معترف به من قبل IANA ومن ثم يقوم بإرسال المعلومات من الشبكة لية إلى الشبكة الخا وكذلك في استقبال المعلومات الخارج يقوم بعكس الوظيفة وإرسال المعلومات إلى رقم الجهاز في الشبكة الداخلية، وغالباً ما يكون هذا الجهاز الوسيط الذي يقوم بتطبيق تقنية NAT إما جدار حماية ناري Firewall أو موزع Router.

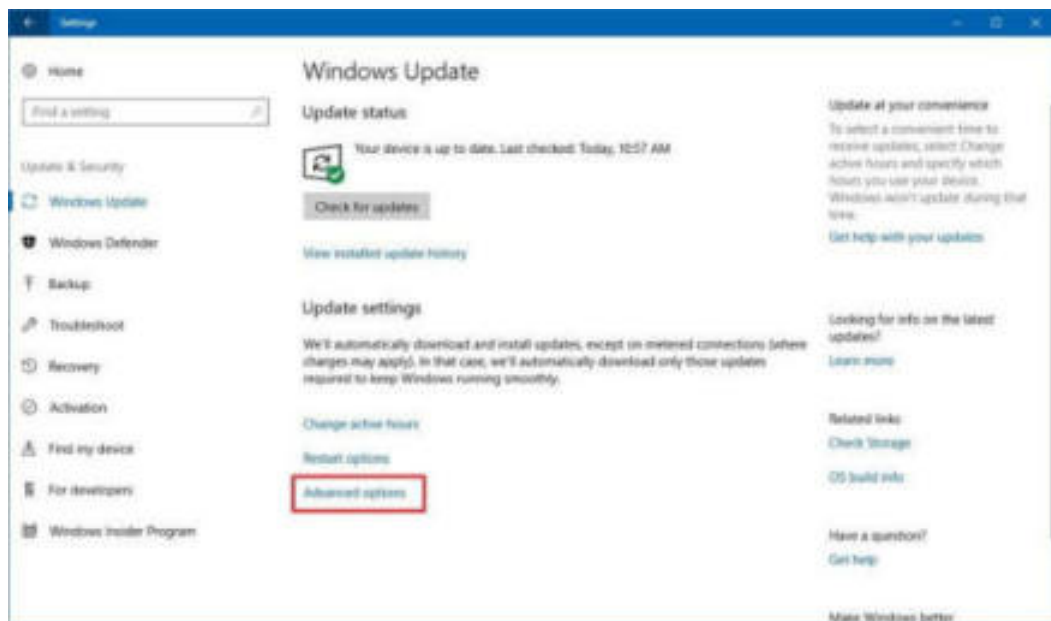


شكل (١٢-٧) يوضح تقنية عمل NAT

وفي هذه الحالة يقوم الجهاز الذي يعمل بتقنية NAT على أنه جدار حماية ناري بين أجهزة الشبكة الداخلية وأجهزة الشبكات الخارجية الأخرى، فلا يستطيع مستخدمو أجهزة الشبكات الخارجية معرفة العناوين الرقمية لأجهزة الحاسوب في الشبكة الداخلية مما يحد من عمليات الاختراق التي تعتمد على معرفة رقم IP للأجهزة.

### ثالثاً: التحديث التلقائي Automatic Update

يعد التحديث الدائم والتلقائي للبرامج وأنظمة التشغيل من أهم نقاط حماية أمن شبكات المعلومات، ذلك أن عملية بناء هذه النظم هي غاية في التعقيد ولا تخلو من بعض الأخطاء التي تحدث في فترات البناء وتعمل الشركات عادة على إيجاد التحسينات المستمرة لسد نقاط الضعف في هذه البراظمة، وهذه التحسينات دائماً فيما يعرف بالتحديثات، تأتي أهمية أن يقوم الشخص بعمليات التحديث الدائم للبرامج والأنظمة التي يتبناها في جهازه الشخصي على المستوى الفردي وعلى مستوى البرامج والأجهزة المستخدمة في شبكات المعلومات، ونظراً لصعوبة مطالبة الشركات لمستخدمي هذه البرامج بتحديث البرامج بأنفسهم فإن معظم الشركات المصنعة لهذه البرامج قامت بإضافة خاصية التحديث الآلي والتلقائي لهذه البرامج، ولكي تعمل هذه الخاصية يقوم البرنامج المثبت في الشبكة بالاتصال تلقائياً وعلى فترات معينة بالشركة المنتجة له والقيام بالبحث عن أية تحديثات جديدة وتنزيلها تلقائياً.



شكل (١٣-٧) يوضح خيارات التحديث التلقائي

## رابع غير Encryption

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.

## بروتوكولات تشفير الشبكات اللاسلكية

صناعة الشبكات اللاسلكية من أسرع الصناعات تطوراً في عالم الشبكات وخصوصاً لدى المستخدمين ذوي نطاق محدود مثل استخدامها في المنازل

والشركات الصغيرة بالرغم من قصورها من الناحية الأمنية. وهذه التقنية في تطور مستمر من حيث السرعة وسعة النقل كذلك من النواحي الأمنية. ومع كل هذا التطور مازال هناك الكثير من الشركات الكبرى لديها الكثير من المخاوف في استخدام هذه التقنية وذلك لسبب قصورها من الناحية الأمنية والخطر الذي سوف تتعرض له الشركات أثناء استخدامها.

### أنواع بروتوكولات التشفير:

#### ١. " WEP " Wired Equivalent Privacy

بروتوكول يستخدم في تشفير البيانات المتنقلة داخل شبكة لاسلكية وذلك لمنع المخترقين من الحصول على البيانات.

وهو من أقدم بروتوكولات تشفير الشبكات اللاسلكية وتستخدم مفتاح سري مشترك Shared Secret K نوعين من المفاتيح إما ٤٠ بت ١٠٤ بت والذي يضاف إليه القيمة الابتدائية " Initial Vector " وهو عبارة عن ٢٤ بت. والشائع استخدامه هو ١٠٤ بت "١٢٨ بت" ويسمى هذا النوع من المفاتيح مفتاح التشفير المشترك " PSK ".

#### عيوب WEP:

بعد انتشار استخدامها قامت بحوث ودراسات هدفها كشف عيوب الـ WEP ومنها:

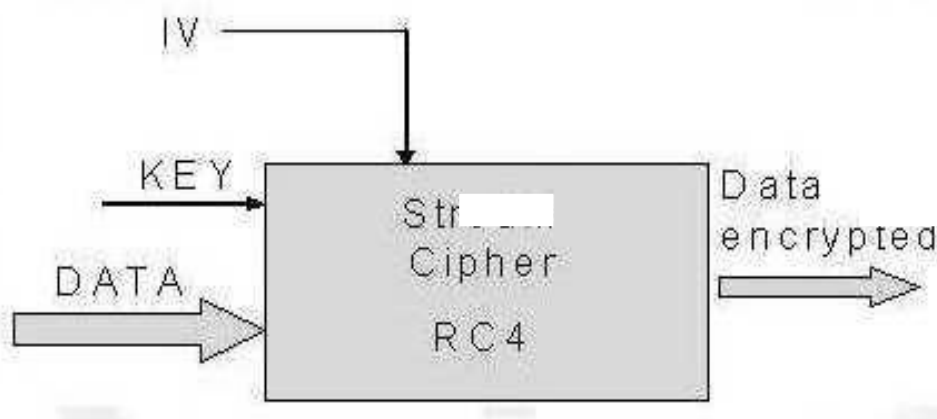
- استخدامها لمفتاح سري مشترك يتم توزيعه يدويا على جميع المستخدمين مما يجعل عملية التغير متعبة وخصوصا في الشركات



الكبرى مما يمد في عمر المفتاح السري المشترك وبالتالي يسهل عملية الاختراق وكشف المفتاح.

• قصر طول المفتاح مما يجعل اكتشاف المفتاح مهمة سهلة للمخترقين.

• رأس حزمة البيانات المرسل غير مشفر مما يتيح معرفة عنوان المرسل والمستقبل وذلك يسهل عملية المخترقين في معرفة المفتاح. مما يجعل استخدامه غير ملائم لفئة الشركات الكبرى وهو مناسب لمستخدمي المنازل والمؤسسات.



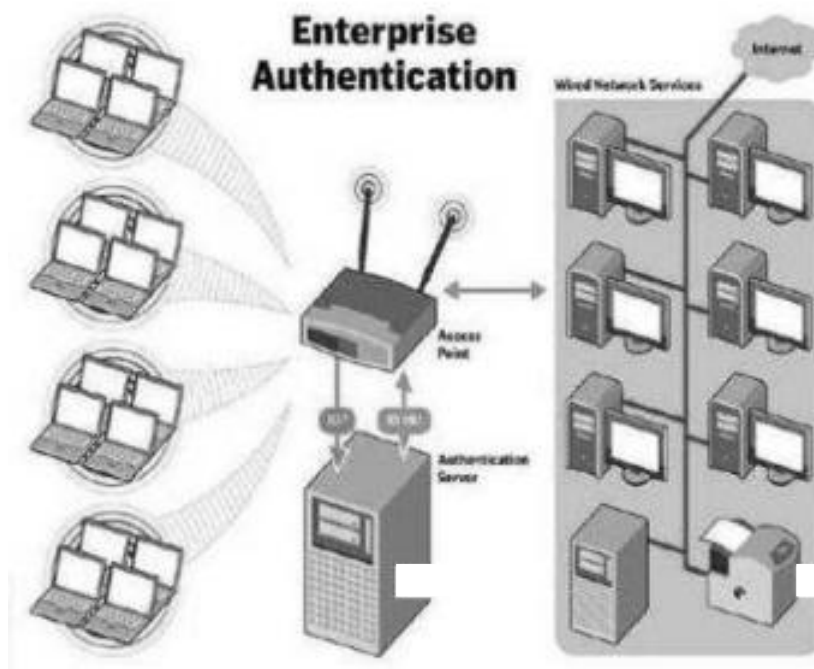
شكل (١٤-٧) يوضح طريقة عمل بروتوكول التشفير WEP

## ٢. Wi-Fi Protected Access “WPA”:

هي عبارة عن برنامج “Firmware” صمم لتصحيح عيوب ال WEP يحمل على الأجهزة المستخدمة “نقاط الوصول “AP” (أي لا يتطلب تغييرها وهو مرحلة انتقاله أو وسيطة بين ال WEP و ٨٠٢.١١١١ ويزيد من مستوى حماية البيانات وكذلك في التحكم في الدخول إلى الشبكة اللاسلكية حيث لا يسمح إلا للأشخاص المصرح لهم مما يجذب الشركات الكبرى إلى استخدامه.

إعداد د/ أميرة إبراهيم عبد الغني

بالنسبة للاستخدام في الشركات يتطلب وجود خادم للشبكة للتحقق من هوية المستخدم " Authentication Server " من نوع ٨٠٢.١ x مع WAP بروتوكول.



شكل (١٥-٧) رسم يوضح طريقة عمل بروتوكول التشفير WPA

أما لمستخدمي المنازل والمؤسسات الصغيرة ليس هناك حاجة إلى توفير خادم الشبكة " Authentication Server " كل ما على المستخدم عمله هو إدخال المفتاح السري " Pre-shared Key " أو الرقم السري على جهازه الذي يريد من خلاله الدخول على الشبكة. لكل مستخدم رقم سري خاص به هو الذي يحدد هويته ومدى الصلاحيات المقدمة لهذا المستخدم وهو بعكس الـ WEP الذي يستخدم مفتاح واحد لجميع المستخدمين. ولإتمام عملية الـ WPA يجب إدخال جميع الأرقام السرية في نقطة الوصول " Access Point " ويتكون

هذا المفتاح من ١٢٨ بت ولكن بقيمة ابتدائية مكونة من ٤٨ بت مما يجعل WPA أقوى تجاه الاختراق من WEP .

كما نلاحظ أن هذا الطول مساوي للمفتاح في WEP مما يعني انه ليس هناك اختلاف؟ الاختلاف هو في تغير المفتاح تلقائيا مما يعني أن مستخدم ال WPA لن يقوم باستخدام المفتاح لفترة طويلة وهنا تكمن متانة هذا النظام.

لا يوجد نظام متكامل مما يعني أن هناك بعض العيوب التي ترافق ال WPA وهي:

- ما تزال تعتمد على المفتاح الذي يمكن التقاطه في حين الإرسال ومن ثم  
الاختراق المعجمي " Attack dict " للحصول على ال
- قد يعاني من توقف الخدمة DOS وذلك إذا أدخلت كلمة المرور أكثر من مرة بطريقة غير صحيحة سيتم حجب المستخدم عن الدخول إلى الشبكة اللاسلكية.

### ٣.٢ " WPA٢ " Wi-Fi Protected Access

وهو بروتوكول معزز ل (WPA) ويتميز بأنه يستخدم خوارزمية AES للتشفير، كما انه يستخدم في الشبكات الثنائية ad-hoc ، وهو متوفر بطريقة (PSK) أو باستخدام آلية توثيق ٨٠٢.١ /EAP والتي يمكن خلالها استخدام الشهادات الإلكترونية.

## الخلاصة

إذا قمت باتباع الإجراءات السابقة، سوف تكون قد وضعت عدة طبقات حماية لجعل عملية اختراق الشبكة عملية صعبة خصوصا من الهواة أو من يبحثون عن شبكة مفتوحة أو سهلة للاتصال بشبكة الانترنت. تستطيع ان تطلب مساعدة الخبراء إذا كنت تريد التأكد من أمان شبكتك اللاسلكية.

### لا تقم بتسمية الشبكة اللاسلكية بـ :

- اسم يدل علي شخصيتك أو مكانك أو يوفر اي معلومات تربط الشبكة بشخصك أو منزلك.
- اسم يدل علي نوع جهاز الراوتر أو الشركة الموفرة للانترنت.
- إذا امكن، يفضل عدم بث اسم الشبكة اللاسلكية.
- لا تقم الشبكة بدون تشفير حتى الة مشاركتها مع الغير.
- استخدم بروتوكول WPA2 .
- استخدم كلمة سر تتكون من احرف، ارقام، وعلامات.
- استخدم كلمة سر اطول من ٨ احرف علي الاقل.
- استخدم كلمة سر مبهمه ليس لها معني سواء لشخصك أو في اللغة. لا تقم باستعمال ارقام الهاتف أو تواريخ الميلاد في كلمة السر.
- يجب تغيير الحساب الافتراضي لصفحة اعدادات الراوتر الي اسم مستخدم مختلف وكلمة سر مختلفة قوية.
- يفضل تفعيل خاصية عدم السماح لأجهزة جديدة بالاتصال بالشبكة ان وجد.
- يفضل تفعيل خاصية "MAC filtering" للسماح للأجهزة المعروفة فقط بالاتصال بالشبكة و تعطيل خاصية الـ "WPS" لسهولة اختراقها .



# المراجع

## References

## أولاً: المراجع العربية

أسامة الحسيني (١٩٩٧). الشبكة الكمبيوترية العالمية إنترنت  
INTERNET/ اتضع قدمك على الطريق السريع للمعلومات. القاهرة: مكتبة  
ابن سينا للنشر و التوزيع و التصدير.

أمل عبد الفتاح سويدان، منال عبد الفتاح مبارز (٢٠٠٧). التقنية في  
التعليم: مقدمات أساسية للطالب المعلم. المملكة الأردنية الهاشمية ،عمان:  
دار الفكر.

جودت أحمد سعادة، عادل فايز السرطاوي (٢٠٠٧) . استخدام الحاسوب  
في ميادين التربية عمان-الأردن : دار الشروق لل  
والتوزيع.

حشمت قاسم (٢٠٠٥). الاتصال العلمي في البيئة الالكترونية. القاهرة :  
دار غريب للطباعة والنشر والتوزيع.

حمدي أحمد عبد العزيز (٢٠٠٨). التعليم الالكتروني: الفلسفة - المبادئ -  
الأدوات - التطبيقات . معهد الدراسات والبحوث التربوية، القاهرة: دار  
الفكر.

رجب عبد الحميد حسنين (٢٠١٢). أمن شبكات المعلومات الالكترونية: المخاطر والحلول، مجلة Cybrarians Journal (دورية الكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات)، العدد الثلاثون.

retrieved from

[http://journal.cybrarians.info/index.php?option=com\\_content&view=article&id=٦٢٩:networks&catid=٢٥٧:studies&Itemid=](http://journal.cybrarians.info/index.php?option=com_content&view=article&id=٦٢٩:networks&catid=٢٥٧:studies&Itemid=).

عبد العزيز طلبة عبد الحميد (٢٠١٠): التعليم الالكتروني ومستحدثات تكنولوجيا التعليم. المنصورة : المكتبة العصرية للنشر والتوزيع.

محمد إبراهيم الدسوقي (٢٠١١). قراءات في المعلوماتية والتربية. القاهرة: الطوبجي للنشر.

محمد عبد الحميد (محرر). (٢٠٠٩). منظومة التعليم عبر الشبكات (ط٢). القاهرة: عالم الكتب ، ٤١٥ص.

محمد عبد الكريم الملاح (٢٠١٠). الأسس التربوية لتقنيات التعليم الالكتروني. عمان: دار الثقافة للنشر والتوزيع.



محمد محمد الهادي، حامد عمار (٢٠٠٥). *التعليم الإلكتروني عبر شبكة الإنترنت*، القاهرة : الدار المصرية اللبنانية.

مصطفى السيد (١٩٩٩). *دليلك الشامل إلى شبكة إنترنت (ط٢)*. القاهرة: دار الكتب العلمية للنشر والتوزيع .

### ثانياً: المواقع

<https://www.google.com.eg/search?sourceid=navclient&aq=&oq=%d٩%.٨٥%d٩%.٨٢%d٨%.a٧%d٩%.٨٤%d٨%.a٩+%d٨%.a٨%d٨%.b٩>

<https://www.wikihow.com/Configure-Local-Network-Area>

<https://commotionwireless.net/docs/cck/networking/type-s-of-wireless-networks/>

<https://www.conceptdraw.com/How-To-Guide/wireless-network-topology>

<https://www.windowscentral.com/how-delay-windows-10-april-2018-update-while-still-getting-updates>

[http://cityofange.blogspot.com/2013/09/blog-post\\_18.html](http://cityofange.blogspot.com/2013/09/blog-post_18.html)

<https://www.dnsstuff.com/what-is-network-topology>

[https://itarabs.com/-backbone- /](https://itarabs.com/-backbone-/)

[https://itarabs.com/ -ad-hoc-network/](https://itarabs.com/-ad-hoc-network/)

<http://expert-eng.blogspot.com/2014/02/>

<https://www.dz-res.com/?p=132405>

<https://ar.volgaproject.net/kompyutery/57465-cto-takoe-topologiya-cto-ponimaetsya-pod-topologiyey-lokalnoy-seti.html>

<https://nehakhansite.wordpress.com/tag/topology-types-bus-star-ring-tree-mesh-hybrid/>

<https://wireless360.wordpress.com/2012/03/02/wireless-mesh-network/>

<https://www.computernetworkingnotes.com/ccna-study-guide/data-encapsulation-and-de-encapsulation-explained.html>

<https://www.computernetworkingnotes.com/ccna-study-guide/similarities-and-differences-between-osi-and-tcp-ip-model.html>

<https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.computernetworkingnote.com%2Fccna-study-guide%2Fdata-encapsulation-and-de-encapsulation-explained.>

[https://answers.microsoft.com/en-us/windows/forum/windows\\_10-networking/how-do-i-set-up-an-ad-hoc-wifi-network-in-windows/0caa92d8-e02f-4e7f-aa0c-0abf10ed2039](https://answers.microsoft.com/en-us/windows/forum/windows_10-networking/how-do-i-set-up-an-ad-hoc-wifi-network-in-windows/0caa92d8-e02f-4e7f-aa0c-0abf10ed2039)