الفصل الأول
مقدمة في شبكات الحاسب الآلي
Introduction to Networking

الشبكة الحاسوبية: هي مجموعة من الأجهزة المتصلة مع بعضها لتحقيق فوائد مشتركة مثل مشاركة الموارد والبيانات ومركزية الإدارة والسرية .

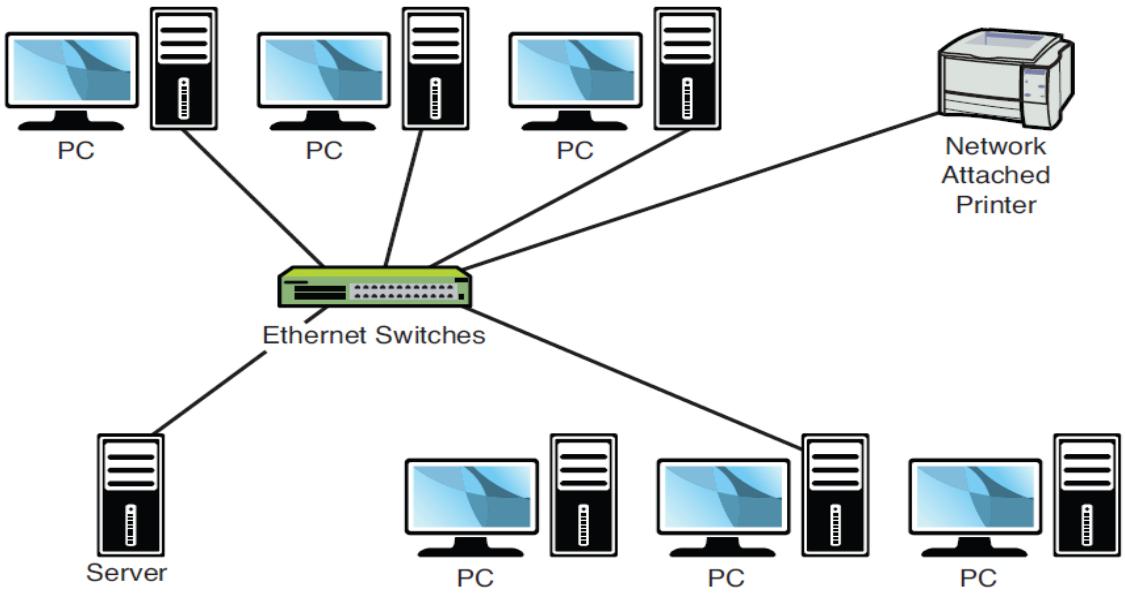
أنواع الشبكات

تُصنف الشبكات الحاسوبية حسب حجمها والتوزيع الجغرافي إلى : شبكات LAN وشبكات WAN.

الشبكة المحلية LAN

هي شبكة حاسوبية توجد في مكان جغرافي واحد وعادة ما تكون في منطقة صغيرة مثل مدرسة – مكتب ... تكون هذه الشبكة عادة ذات سرعة عالية وتكلفة رخيصة مقارنة مع شبكة WAN

الشكل 1.1 يظهر مثال عن شبكة LAN

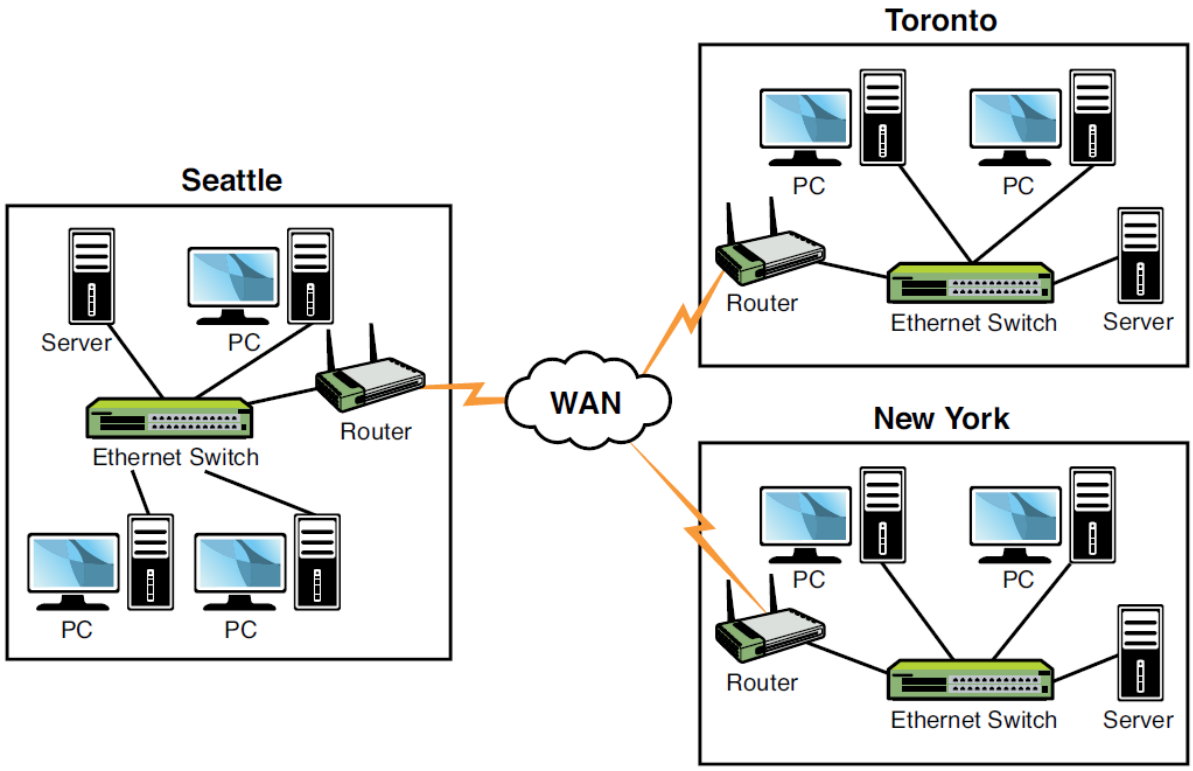


الشكل 1.1

الشبكة الواسعة WAN

هي شبكة حاسوبية تمتد إلى أكثر من مكان جغرافي واحد تكون أبطأ من شبكة LAN وغالباً ما تتطلب تجهيزات أغلى وأكثر (leased line - router) وإعدادات معقدة أكثر. تسمى أحياناً بشبكة MAN إذا كانت ضمن مدينة واحدة. لا يوجد فعلياً حدود واضحة للتمييز بين WAN و MAN وأما من الناحية التقنية فكلاهما متشابه لذلك لم يعد اسم MAN متداولاً بكثرة ولكن يمكن القول أن MAN هي أكبر من LAN وأصغر من WAN.

الشكل 1.2 يظهر مثال عن شبكة WAN



الشكل 1.2

نماذج الشبكة (Networking Models)

يوجد نموذجين أساسيين للشبكة: شبكة الند للند (Peer-to-Peer) وشبكة المخدم/العميل (Client/server) إن اختيار أحد هذين النموذجين يحدده عوامل مختلفة مثل الهدف من الشبكة وعدد المستخدمين الموجودين في الشبكة والميزانية المخصصة لها.

نموذج شبكة الند للند (Peer-to-Peer)

هي شبكة لامركزية أي أنها لا تقدم مركزية في التحكم أو مركزية في التخزين. هي أرخص وأسهل في الإعدادات من شبكات المخدم/العميل. لا تعمل بشكل جيد مع أعداد كبيرة من المستخدمين فكلما ازداد عدد المستخدمين انخفض الأداء في الوصول إلى الملفات والموارد. توجد هذه الشبكات عادة في المكاتب الصغيرة أو لعدد محدود من أجهزة الحاسب. القاعدة العامة في هذه الشبكات هو ألا يزيد عدد المتصلين بهذه الشبكة عن 10 أجهزة.

نموذج المخدم / العميل (Client/server)

ميزة هذا النموذج هي **المركزية** أي أنها تسمح بإدارة مركزية لكل خدمات الشبكة من إدارة المستخدمين، التخزين، الأمان، النسخ الاحتياطي وغيرها من الخدمات. يحتاج هذا النوع من الشبكات إلى خبرات تقنية عالية للإعداد وإدارة الشبكة إضافة إلى تكلفة مادية عالية نوعاً ما سواءً بالتجهيزات أو بالبرمجيات. إن تخصيص مخدم (server) خاص لهذا النموذج من الشبكات يجعل التكلفة عالية ولكن تعوضها الفوائد التي يقدمها من حيث مركزية الإدارة والسرية مما يجعلها خياراً للعديد من الشركات .

الجدول 1.1 يلخص خصائص كل من النموذجيين

الميزة	Peer-to-peer	Client / server
الحجم	العدد الأقصى الموصي به هو 10 أجهزة	يمكن أن تحوي آلاف الأجهزة وإن ما يحدد هذا العدد هو إمكانيات الشبكة من حيث المخدم و التجهيزات والتكلفة المادية
الإدارة	(الإدارة لامركزية) أي أن كل جهاز أو محطة عمل يدير نفسه بنفسه لا حاجة إلى مدير شبكة	(الإدارة مركزية) أي أنه بحاجة غالباً إلى مدير شبكة لإدارة وصيانة الشبكة
السرية	كل جهاز مسؤول عن سرية ملفاته وتجهيزاته	يتم إدارة سرية وأمان الشبكة كلها في موقع واحد
التكلفة المادية	الحد الأدنى من التكلفة لإعداد وتشغيل الشبكة	تكلفة عالية لأنها بحاجة إلى تجهيزات وبرمجيات خاصة وإدارة للشبكة
الإعداد والتشغيل	سهولة في الإعداد والتشغيل	تتطلب عادة إعدادات معقدة نوعاً ما ومهارة تقنية في التشغيل

الجدول 1.1

أسئلة الوحدة

ما هو العدد الأعظمي الذي يُنصح به لعدد الأجهزة في شبكة الند للند؟

عندما يتم إعداد شبكة WAN في مدينة واحدة ،ماذا تُسمى عندئذ ؟

طوبولوجيا الشبكات المحلية (Topology)

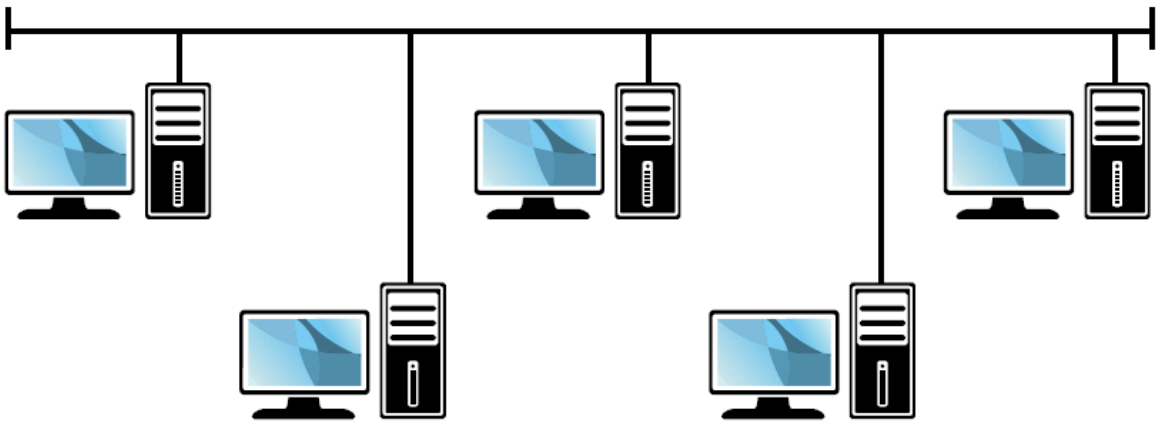
يشير مصطلح الطوبولوجيا إلى التصميم الفيزيائي والمنطقي للشبكة الحاسوبية. حيث أن التصميم الفيزيائي يشير إلى طريقة ربط الحواسيب والكابلات وباقي التجهيزات الشبكية مع بعضها أما التصميم المنطقي يشير إلى الطريقة التي تظهر بها الشبكة إلى الأجهزة التي تستخدمها أي طريقة عبور ونقل البيانات ضمن الشبكة. يوجد العديد من أنواع طوبولوجيا الشبكة هذه الأيام أهمها : الخطي (Bus)، النجمي (Star)، الحلقي (Ring)، المختلط (Mesh)، اللاسلكي (Wireless).

طريقة التوصيل الخطي Bus

هي عبارة عن خط رئيسي يصل بين جميع الأجهزة في الشبكة حيث يتصل كل جهاز مع هذا الخط عبر وصلة. يوضع مقاومة إنهاء (terminator) في نهايات الخط لمنع حدوث انعكاس للإشارة.لا حاجة إلى عقدة مركزية Hub أو مبدل Switch.

أشهر معايير طوبولوجيا الشبكة الخطية هو IEEE802.3

الشكل 1.3 يبين طريقة التوصيل الخطي



الشكل 1.3

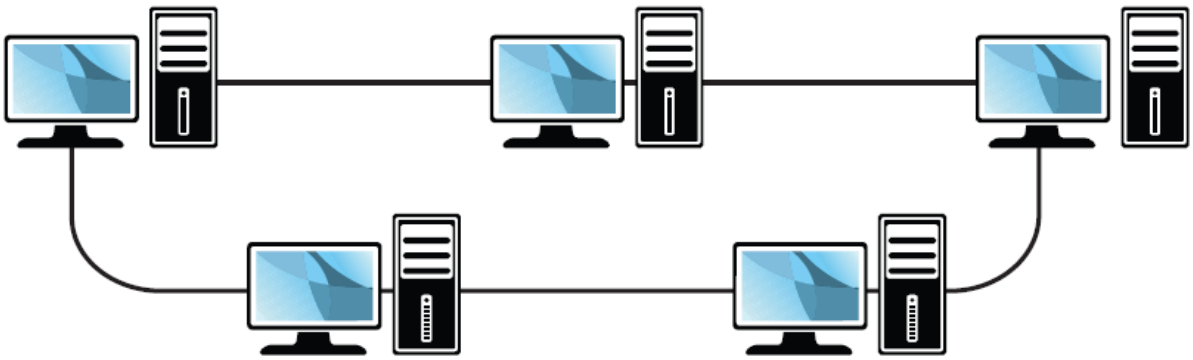
الجدول 1.2 يلخص ميزات ومساوئ هذا النوع من التوصيل

المحاسن	المساوئ
هي الأرخص والأسهل إعداداً مقارنة مع غيرها	يمكن أن يحدث انقطاع للشبكة عند إضافة أو إزالة الحواسيب من الشبكة
تحتاج إلى كابلات أقل	في حال حدوث انقطاع للكيبل الرئيسي يؤدي إلى توقف الشبكة
لا تحتاج إلى تجهيزات شبكية خاصة	يوجد صعوبة في إصلاحها

الجدول 1.2

طريقة التوصيل الحلقي (Ring Topology)

سُميت حلقة لأن البيانات تنتقل بشكل دائري من حاسب إلى آخر في الشبكة. حيث تتصل جميع الحواسيب بكيبل ولا تحتاج إلى عقدة مركزية Hub أو مبدل Switch. الشكل 1.4 يبين طريقة التوصيل الحلقي.



الشكل 1.4

الجدول 1.3 يلخص محاسن ومساوئ طوبولوجيا الحلقة

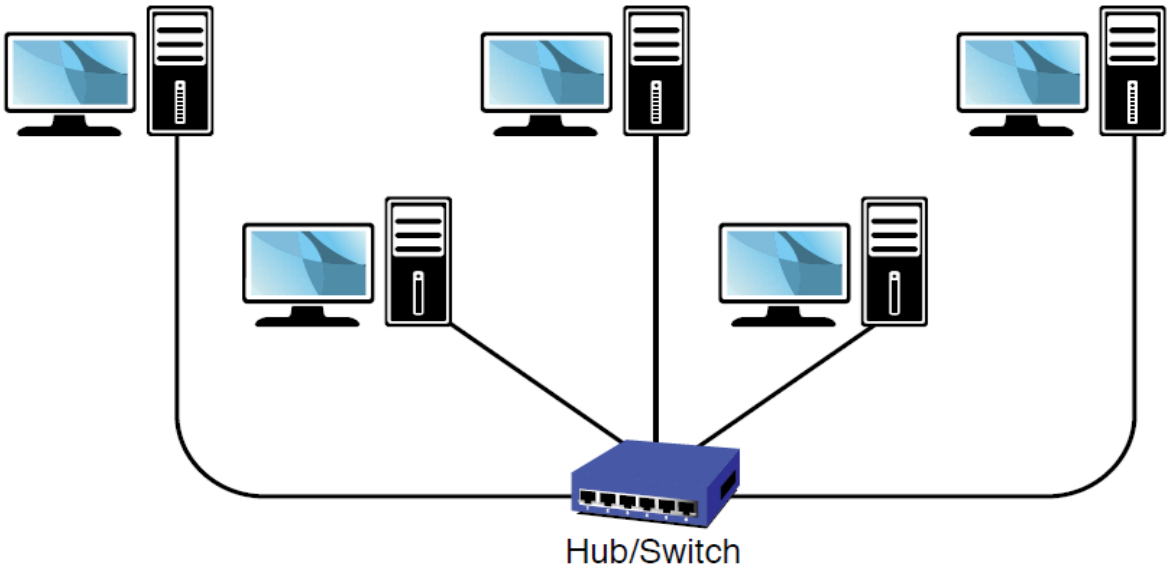
المحاسن	المساوئ
سهلة الإعداد	حدوث عطل في أحد الحواسب يؤدي إلى انقطاع الشبكة
سهلة الإصلاح	توسيع الشبكة بإضافة حواسيب أخرى يمكن أن يؤدي إلى انقطاع الشبكة

الجدول 1.3

طريقة التوصيل النجمي (Star Topology)

في هذا النوع من طرق التوصيل فإن كل الحواسيب وأجهزة الشبكة الأخرى تتصل إلى جهاز مركزي يسمى Hub أو Switch. كل جهاز في الشبكة يحتاج إلى كيبل يتصل بالعقدة المركزية. يمكن توسيع الشبكة بدون حدوث انقطاع لأن ذلك يتم بإضافة كيبل إلى الجهاز المركزي. وحدوث أي انقطاع في أي كيبل يؤدي فقط إلى انقطاع الجهاز المتصل به وليس إلى انقطاع الشبكة ككل .

الشكل 1.5 يبين طوبولوجيا النجمة



الشكل 1.5

تعتبر طوبولوجيا النجمة أكثر تصاميم الشبكة انتشاراً هذه الأيام ولكن بسبب أن كل الأجهزة متصلة بنقطة مركزية واحدة فإن حدوث أي عطل في هذه العقدة يؤدي إلى توقف الشبكة أي يوجد لهذه الشبكات **نقطة فشل واحدة**.

الجدول 1.4 يلخص محاسن ومساوئ طوبولوجيا النجمة

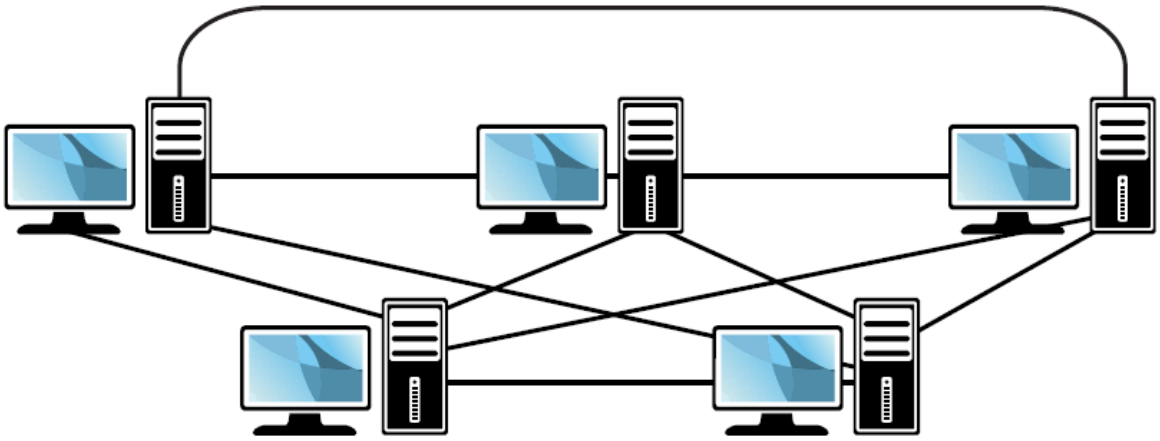
المحاسن	المساوئ
توسيع الشبكة سهل، أي يمكن إضافة أجهزة إلى الشبكة بدون توقف الشبكة	تحتاج إلى عدد أكبر من الكابلات مقارنة مع غيرها من الطوبولوجيا
حدوث مشاكل في أحد الكابلات يؤثر فقط على الجهاز المتصل به وليس على كل الشبكة	إن وجود عقدة مركزية يؤدي إلى وجود نقطة فشل واحدة .
سهلة الإعداد والإصلاح	تحتاج إلى تجهيزات شبكية إضافية

الجدول 1.4

طريقة التوصيل المتشابك (Mesh Topology)

في هذا النوع من التوصيل كل جهاز في الشبكة يتصل بكل الأجهزة الأخرى. الهدف من هذا التصميم هو تأمين مستوى عالي من الـ redundancy وفي حال حدوث انقطاع في أحد الكابلات فإنه يوجد دائماً مسار آخر لمرور الإشارات. تكلفة هذه الشبكات عالية بسبب عدد الكابلات الكبير لذلك لا تعتبر الخيار الأول للشبكات .

الشكل 1.6 يبين طريقة الربط المتشابك.



الشكل 1.6

الجدول 1.5 يلخص المحاسن والمساوئ لهذه الطريقة

المحاسن	المساوئ
يؤمن مسارات بديلة بين الأجهزة في الشبكة	تحتاج إلى المزيد من الكابلات
يمكن توسيع الشبكة بدون توقف الشبكة	تركيبها صعب ومعقد

الجدول 1.5

الطوبولوجيا اللاسلكية (Wireless Topology)

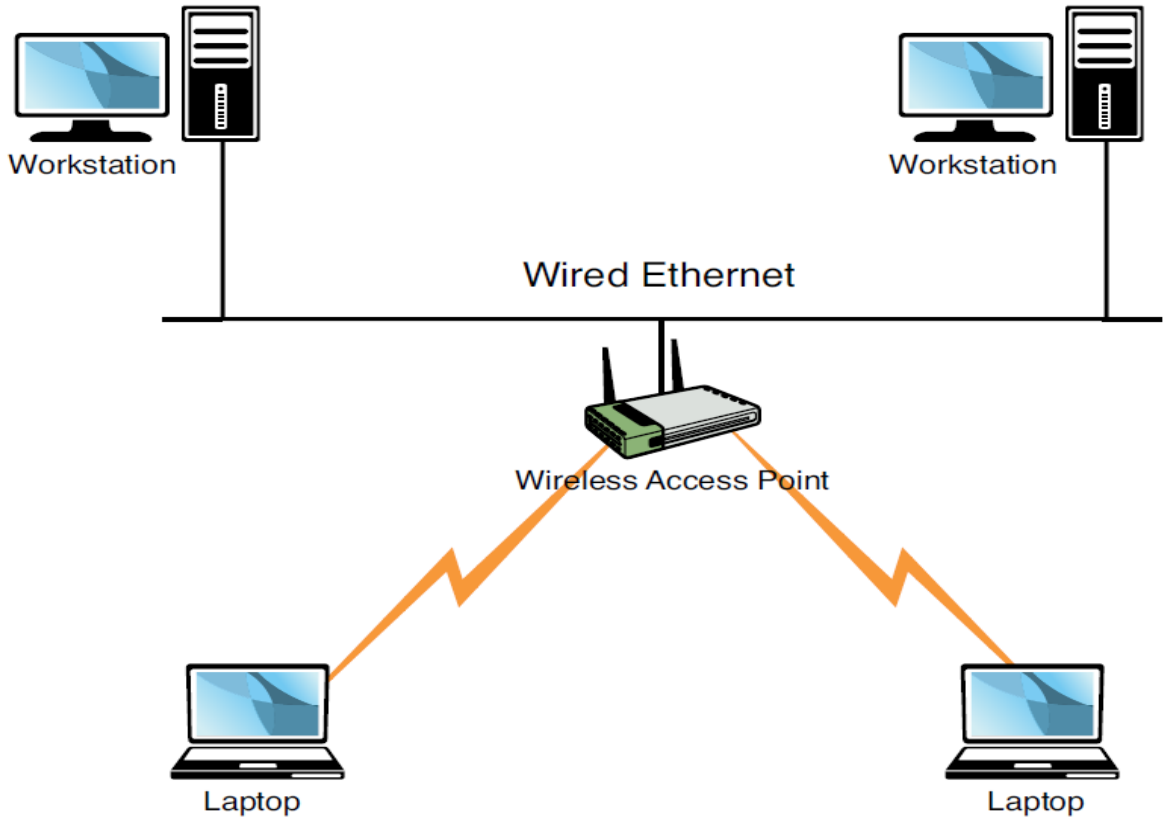
يمكن إنشاء الشبكة اللاسلكية باستخدام إحدى الطريقتين التاليتين :

- طوبولوجيا البنية (Infrastructure)
- طوبولوجيا Ad hoc

طوبولوجيا البنية (Infrastructure)

تستخدم لتوسيع شبكات LAN السلكية لإضافة أجهزة لاسلكية حيث تتصل هذه الأجهزة اللاسلكية بشبكة LAN عن طريق تجهيزه تسمى نقطة الوصول اللاسلكي (Access Point) واختصاراً بـ **AP** حيث تشكل هذه النقطة جسر

بين شبكة LAN السلكية واللاسلكية. نقطة الوصول AP تتصل بالشبكة السلكية أي هي جزء من بنية الشبكة السلكية وهذا هو سبب تسميتها بـ طوبولوجيا البنية. يمكن استخدام نقطة وصول واحدة إذا كانت المساحة الجغرافية المطلوب تغطيتها لاسلكياً صغيرة مثل بيت واحد أو مكتب صغير ويمكن استخدام عدة نقاط وصول لتغطية المساحات الأوسع. الشكل1.7 يبين شبكة البنية.

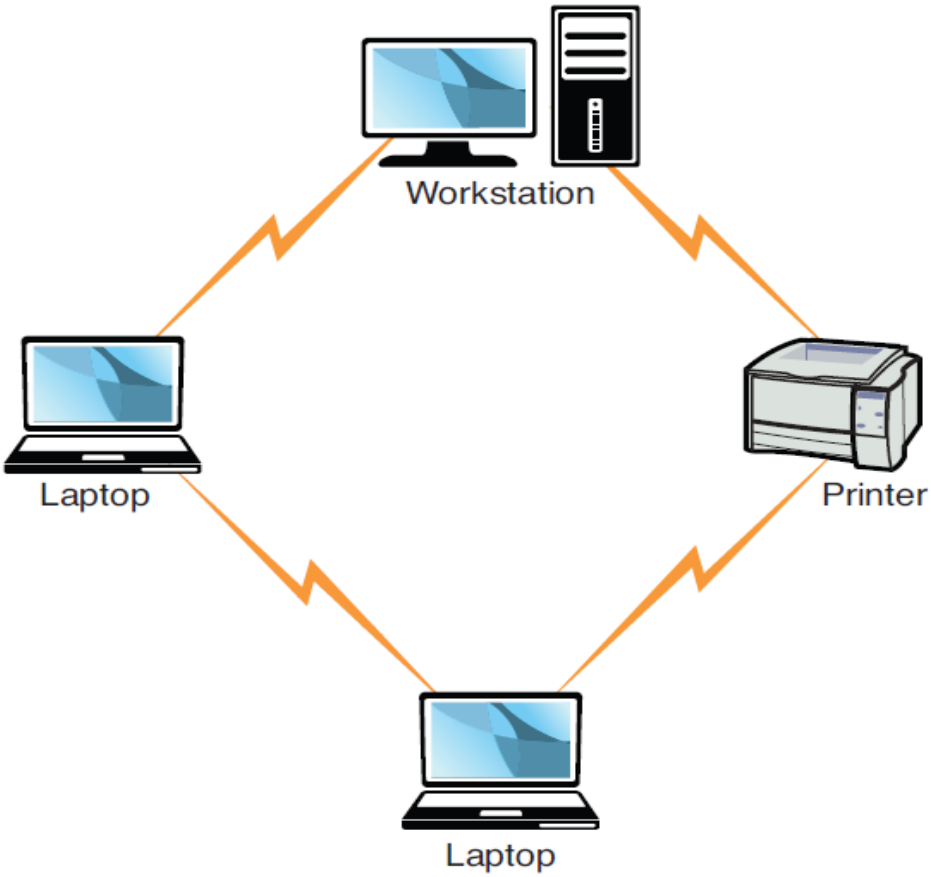


الشكل 1.7

طوبولوجيا Ad hoc

في هذا النوع تتصل الأجهزة مع بعضها مباشرة بدون نقطة وصول. هذا النوع شائع عند الاتصال بعدد محدود من الأجهزة بشكل مؤقت. مثال ربط عدة حواسيب محمولة Laptop في قاعة اجتماعات

الشكل 1.8 يظهر مثال عن Ad hoc



الشكل 1.8

أسئلة الوحدة

1. طلب منك إعداد شبكة حاسوبية بحيث تخفض عدد حالات الفشل المحتملة إلى الحد الأدنى. ماذا تختار من بين الطبولوجيا التالية للشبكة؟
2. أي من الطبولوجيا التالية تسمح بتوسيع الشبكة مع أقل قدر ممكن من الإزعاج لمستخدمي الشبكة؟
3. طلب منك ربط مكتبين مع بعض بطريقة لاسلكية. أي من الطرق التالية سوف تستخدم؟
4. ما هي طريقة ربط الشبكات التي تقدم أعلى مستوى من الأداء ولكن تحتاج أيضاً إلى تكلفة عالية أثناء الإنشاء؟
5. أي من العباؤات التالية تعتبر صحيحة فيما يتعلق بـ طبولوجيا BUS للشبكات الحاسوبية المحلية؟

1. انقطاع الكيبل يؤدي إلى تعطيل الشبكة كلها
2. كل الأجهزة تتصل مع جهاز مركزي
3. تستخدم عمود فقري واحد لوصل كل التجهيزات الشبكية
4. تستخدم طريقة الربط الحلقي بين الأجهزة

الفصل الثاني

نماذج الشبكة والبروتوكولات

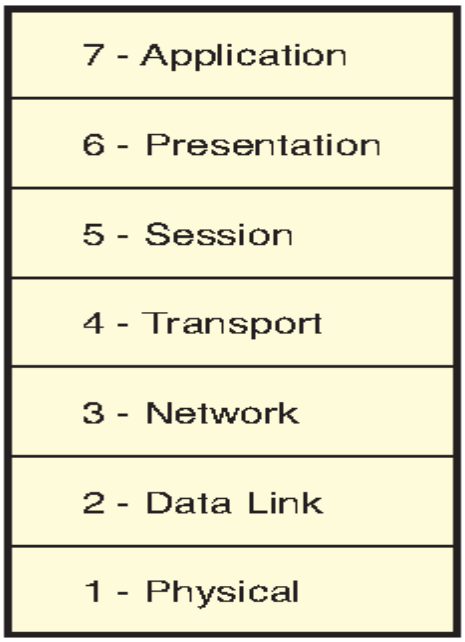
Models & Network Protocols

إن من أكثر الأشياء التي يجب أن تُفهم في عالم الشبكات هو نموذج OSI. هذا النموذج تم إنشاؤه من قبل المنظمة العالمية للمعايير ISO في عام 1978 وتم تعديله عام 1984.

نموذج الطبقات السبع OSI

هو نموذج عالمي لتوحيد النظم المختلفة لضمان قدرة الشبكات المختلفة على الاتصال مع بعضها. وقد تميز بالمرونة ولم يتحيز إلى منتج معين. تم تقسيم الوظائف الواجب اتباعها في تصميم شبكات الحاسب الآلي إلى سبع وظائف أُطلق على كل منها اسم طبقة (Layer) ولهذا عرف النموذج المعياري **OSI** بنظام الطبقات السبع. الوظائف التي يجب أن تنجزها كل طبقة مستقلة عن باقي الطبقات وهذا يسمح بتطوير هذه الوظائف بدون تغيير جذري لهذه البنية. يتكون هذا النموذج من سبع طبقات هي من الأسفل إلى الأعلى:

1. الطبقة الفيزيائية (Physical layer)
2. طبقة ربط المعطيات (Data Link layer)
3. طبقة الشبكة (Network layer)
4. طبقة النقل (Transport layer)
5. طبقة الجلسة (Session layer)
6. طبقة العرض (Presentation layer)
7. طبقة التطبيقات (Application layer)



الطبقة الفيزيائية (Physical layer)

تعرّف هذه الطبقة الخصائص الفيزيائية للشبكة وهي:

- **الأجزاء الصلبة** (Hardware) حيث تعرّف نوع الوسط المستخدم في الشبكة مثل نوع الكابلات - الوصلات ....

- **الطوبولوجيا** (Topology) حيث تعرّف نوع الطوبولوجيا المستخدمة في الشبكة إضافة إلى ذلك فإن هذه الطبقة تعرف الجهود الكهربائية المستخدمة في وسط النقل وتردد الإشارات وهذه الخصائص هي التي تحدد السرعة وعرض الحزمة وأطول مسافة يمكن أن تستخدم لنوع محدد من وسط النقل.

طبقة ربط المعطيات (Data Link layer)

هذه الطبقة مسؤولة عن كشف الأخطاء وتصحيحها والعنونة الفيزيائية (MAC Address)

طبقة الشبكة (Network layer)

تقوم هذه الطبقة بعملية التوجيه (Routing) حيث إنها تؤمن آلية نقل البيانات من شبكة إلى شبكة أخرى. هذه الطبقة لا تحدد كيف تمر البيانات ولكن تؤمن آلية عمل ذلك من خلال بروتوكولات التوجيه ويكون التوجيه إما ساكن (Static) أو توجيه ديناميكي (Dynamic) عن طريق بروتوكولات مثل (RIP- Ospf). تسمى البيانات في هذه الطبقة بـ الرزمة (Packet).

طبقة النقل (Transport layer)

المهمة الأساسية لهذه الطبقة هي تأمين آلية لنقل البيانات بين أجهزة الشبكة ويتم ذلك بثلاث طرق:

- ❖ تفحص الأخطاء: تتأكد من صحة البيانات المرسلة والمستقبلة.
- ❖ عنونة الخدمات: تتأكد هذه الطبقة من أن البيانات تمر إلى الخدمة الصحيحة في الطبقات الأعلى من الشبكة.
- ❖ التجزئة: حيث يتم تقسيم البيانات إلى كتل بقياس مناسب لكل الطبقات.

إن البروتوكولات التي تعمل في هذه الطبقة تقسم إلى عديمة الاتصال (connectionless) مثل بروتوكول UDP أو موجهة الاتصال (connection-oriented)مثل TCP.

هذه الطبقة مسؤولة أيضاً عن التحكم بتدفق البيانات أي كيفية قبول جهاز الاستقبال للبيانات وذلك باستخدام طريقة الـ buffering حيث أن المعلومات يتم تخزينها تلقائياً وتنتظر حتى يصبح جهاز الاستقبال قادر على إدخالها.

طبقة الجلسة (Session layer)

هذه الطبقة مسؤولة عن تقديم آلية للتحكم في الحوار بين التطبيقات وذلك من خلال التزامن وتحديد نظام الحوار (full duplex – half duplex) وإدارة بدء وانتهاء الجلسة .

طبقة التقديم (Presentation layer)

تقوم هذه الطبقة بتحويل البيانات المرسلة أو المستقبلة من قبل التطبيقات إلى صيغة يمكن نقلها عبر الشبكة مثل (ملفات النصوص – ملفات الصور – ملفات الصوت). تقوم هذه الطبقة أيضاً بمهمة التشفير وفك التشفير ومهمة الضغط وفك الضغط.

طبقة التطبيقات (Application layer)

هي الطبقة التي تتعامل مع المستخدم مباشرة أي تحويل البيانات المستقبلة إلى صيغة يفهمها المستخدم وتحويل البيانات المرسلة من قبل المستخدم إلى صيغة تفهمها التطبيقات الأدنى في نموذج OSI أي تتعامل هذه الطبقة مع تطبيقات المستخدم مثل متصفحات الإنترنت، معالجات النصوص، مشغلات الوسائط،.....

الجدول 2.1 يلخص مهام طبقات OSI

الطبقة	الوصف
1	تعرف الخصائص الفيزيائية والكهربائية للشبكة ونوع الطوبولوجيا المستخدمة
2	تؤمن كشف وتصحيح الأخطاء و تؤمن العنونة الفيزيائية للأجهزة
3	تؤمن توجيه البيانات والعنونة المنطقية للأجهزة
4	تؤمن إدارة التحكم بالتدفق وتؤمن التجزئة وتفحص الأخطاء و تؤمن خدمات الاتصال بين المرسل والمستقبل
5	تؤمن تزامن نقل البيانات بين التطبيقات أو بين الأجهزة
6	تحويل البيانات من صيغة يفهمها المستخدم إلى صيغة تفهمها الشبكة والعكس. تؤمن التشفير وفك التشفير- الضغط وفك الضغط
7	تؤمن الوصول إلى الشبكة عن طريق البرمجيات وواجهة المستخدم

الجدول 2.1

نموذج TCP / IP

هذا النموذج من الاتصال يقدم الخدمات نفسها التي يقدمها نموذج OSI ولكن بأربع طبقات بدل من سبع طبقات. تم تطوير هذا النموذج منذ نشأة الإنترنت وهذا النموذج ليس بروتوكولاً واحداً أو اثنين بل هو عبارة عن مجموعة من البروتوكولات ولقد أُخذ هذا الاسم من أشهر اثنين فيه وهما بروتوكول TCP وبروتوكول IP.

يُعد نموذج TCP / IP هو النموذج الرئيسي لشبكة الإنترنت ولشبكات الإيثرنت.

طبقات TCP / IP

طبقة واجهة الشبكة (Network Interface Layer)

وهي الطبقة التي تقابل الطبقة الفيزيائية وطبقة المعطيات في نموذج OSI

طبقة الإنترنت (Internet Layer)

تقابل هذه الطبقة طبقة الشبكة في نموذج OSI ويوجد عدة بروتوكولات تعمل في هذه الطبقة.

طبقة النقل (Transport Layer)

تقابل هذه الطبقة طبقة النقل في نموذج OSI وأشهر البروتوكولات التي تعمل في هذه الطبقة هي TCP – UDP.

طبقة التطبيقات (Application Layer)

تقابل هذه الطبقة الطبقات الثلاثة العليا (7-6-5) في نموذج OSI ويوجد العديد من البروتوكولات التي تعمل في هذه الطبقة مثل HTTP- FTP ....

معالجة البيانات ضمن نموذجي الاتصال

تقدم الطبقة الدنيا خدماتها إلى الطبقة التي تعلوها. يتم تعريف الطبقات بحيث لا تستدعي التغييرات في طبقة ما تغييرات في طبقات أخرى وبذلك نكون قد قسمنا مسألة واحدة إلى مجموعة من مسائل جزئية أبسط. في حالة الإرسال تضيف كل طبقة ترويسة للبيانات قبل أن تمررها إلى الطبقة التي تعلوها (تدعى هذه العملية بالتغليف) وأما في حالة الاستقبال تزيل كل طبقة الترويسة التي أضافتها الطبقة المقابلة عند الإرسال وثم تقوم بمعالجة البروتوكولات الموجودة فيها وتمرر ما تبقى إلى الطبقة الأعلى.

ملاحظة: الطبقة الثانية تضيف رأس وتذييل إلى قطعة البيانات

البروتوكولات (Protocols)

عندما تتصل الحواسيب مع بعضها البعض في الشبكة تحتاج إلى عدة أمور منها القواعد التي تحدد كيف يتم هذا الاتصال. تسمى هذه القواعد بالبروتوكولات وهي اللغة المشتركة بين كل الأنظمة في الشبكة .

يمكن تعريف البروتوكول بشكل عام بأنه مجموعة القواعد والقوانين التي تؤدي إلى تنفيذ العمل المُتفق عليه بشكل سليم وخالي من الأخطاء.

أما البروتوكول المستخدم في شبكات الحاسب الآلي يمكن تعريفة بأنه مجموعة القواعد والقوانين التي تنظم عملية الاتصال بين الحواسيب بحيث يضمن تبادل المعلومات بشكل سليم وخالي من الأخطاء .

لا يمكن للحواسيب أن تتصل ببعضها ما لم تشترك بلغة عامة لتبادل الرسائل وهذه اللغة تؤمنها البروتوكولات. يوجد العديد من البروتوكولات التي تعمل ضمن الشبكة ولكل بروتوكول خصائص ومميزات ومساوئ. قبل البدء في خصائص البروتوكولات يجب التنويه أنه يوجد نوعان من البروتوكولات:

- النوع الأول هي بروتوكولات **اتصال موجه** (connection-oriented)

- النوع الثاني هي بروتوكولات **عديمة الاتصال** (connectionless)

في الاتصال الموجه يتم إرسال رسالة تأكيد من المستقبل على أن البيانات قد تم استلامها وهذا يجعله موثوق ولكن يحتاج إلى حمل زائد وعرض حزمة أكبر. أحد أشهر البروتوكولات في هذا النوع هو بروتوكول TCP.

أما البروتوكولات عديمة الاتصال فإنها تؤمن عملية الإرسال ولا يوجد تأكيد على أن البيانات قد وصلت إلى المستقبل أم لا. إذا حدث خطأ في الإرسال لا توجد أي آلية لإعادة إرسال البيانات أي تعتبر البروتوكولات من هذا النوع غير موثوقة. يحتاج الاتصال من خلال هذا النوع من البروتوكولات إلى عرض حزمة أقل وبالتالي فإن استخدام هذا النوع شائع في نقل الصوت والفيديو حيث أن فقدان عدد من رزم البيانات لا تشكل مشكلة كبيرة. أحد أشهر البروتوكولات من هذا النوع هو بروتوكول UDP

البروتوكولات الأكثر استخداماً

بروتوكول الإنترنت (IP Protocol)

معرف بالنشرة RFC791. يُستخدم هذا البروتوكول لنقل البيانات من عقدة في الشبكة إلى عقدة أخرى وهو عديم الاتصال أي أنه غير موثوق في استقبال البيانات. وهو بحاجة إلى بروتوكول من مستوى أعلى مثل TCP للتأكد من أن البيانات المرسلة عبر IP قد وصلت إلى وجهتها. يعمل هذا البروتوكول في الطبقة الثالثة من طبقات OSI أي في طبقة الشبكة. يقوم هذا البروتوكول بعملية العنونة المنطقية.

بروتوكول التحكم بالنقل (TCP Protocol)

معرف بالنشرة RFC793. وهو بروتوكول اتصال موجه يؤمن الموثوقية للاتصالات عبر IP. يضيف بروتوكول TCP ميزات أخرى مثل التحكم بالتدفق وكشف الخطأ وتصحيحه لهذا السبب فإن التطبيقات التي تحتاج إلى ضمان وصول البيانات إلى المستخدم بشكل سليم تماماً تستخدم بروتوكول TCP. يعمل هذا البروتوكول في طبقة النقل من نموذج OSI .

بروتوكول معطيات المستخدم (UDP Protocol)

معرف بالنشرة RFC768. هو الأخ لبروتوكول TCP حيث أنه بروتوكول نقل كما هو الحال في بروتوكول TCP ولكن الفرق الأكبر بينهما أنه لا يتأكد من وصول البيانات إلى المستخدم أي هو بروتوكول (أرسل وانسى). يعمل هذا البروتوكول في الطبقة الرابعة من نموذج الاتصال OSI وهو بروتوكول عديم الاتصال يحتاج إلى حمل أقل في الشبكة مقارنة مع TCP حيث أن رأس الرزمة في TCPهو 14 حقل أما في UDP فهو 4 حقول فقط لذلك يستخدم في التطبيقات مثل نقل الصوت والفيديو وفي حالات المراقبة في الزمن الحقيقي والقياس عن بعد.

بروتوكول نقل الملفات (FTP)

معرف بالنشرة RFC959. يؤمن نقل الملفات من حاسوب إلى آخر ضمن الشبكة. يعمل في الطبقة السابعة من نموذج OSI أي في طبقة التطبيقات. شائع الاستخدام لتوزيع الملفات عبر الإنترنت وأيضاً للشركات التي تحتاج بشكل دائم لتوزيع ملفات ذات حجوم كبيرة. من الشائع استخدام بروتوكول FTP مع أداة ثالثة (Third Party) مثل (cateFTP – smartFTP) بدلاً من الأداة الموجودة في النظام.

بروتوكول نقل الملفات الآمن SFTP

إن أحد أكبر المشاكل التي يعاني منها بروتوكول FTP هو عدم السرية على الرغم من اتباع طرق بسيطة في التحقق ولكن مازالت عرضة لعمليات القرصنة بشكل سهل والحل هو بروتوكول SFTP والذي يعتمد على تقنية SSH التي تؤمن قناة موثوقة بين المرسل والمستقبل وتؤمن أيضاً إمكانية التشفير.

بروتوكول نقل الملفات البسيط (TFTP Protocol)

يقوم بالعمل نفسه الذي يقوم به بروتوكول FTP ولكن لا يمتلك أي نوع من السرية. يُستخدم غالباً مع التنزيلات البسيطة مثل نقل firmware إلى جهاز مثل الراوتر. يعمل هذا البروتوكول مع بروتوكول UDP.

بروتوكول نقل البريد البسيط (SMTP Protocol)

معرف بالنشرة RFC821 يعرف كيفية نقل رسائل البريد الالكتروني بين المحطات يستخدم TCP لكشف الأخطاء. لا يتطلب أن تكون المحطة المُرسل إليها فعالة ولهذا السبب يمكن للمستخدم أن يقرأ رسائل البريد الالكتروني في أي وقت لاحق من إرسالها يمكن أن يُستخدم لإرسال واستقبال البريد الالكتروني أما بروتوكول pop3 – imap تُستخدم فقط لاستقبال البريد .

بروتوكول نقل النصوص التشعبية (HTTP Protocol)

معرف بالنشرة RFC268. هو بروتوكول يسمح بنقل النصوص والصور والوسائط والمواد الأخرى من مخدم HTTTP.

مثال عملي: إن متصفح الإنترنت يعتبر عميل (http client) وموقع الإنترنت يعتبر مخدم (http server) يستخدم بروتوكول http عنوان URL لتحديد ما هي الصفحة التي يجب تنزيلها من المخدم ويجلبها للمستخدم. فمثلا

لو طلب متصفح الإنترنت العنوان التالي http://www.microsoft.co./support سيقوم البروتوكول بتنزيل صفحة support من الموقع.

بروتوكول نقل النصوص التشعبية (HTTPS Protocol)

أحد مشاكل بروتوكول HTTP هو أن إرسال النصوص يكون بشكل صريح أي بدون تشفير وهذا يعتبر غير مناسب لبعض التطبيقات مثل التجارة الالكترونية. والحل هو استخدام بروتوكول HTTPS والذي يستخدم نظام يُسمى SSL والذي يقوم بتشفير البيانات المرسلة بين المحطات. عندما طلب أي تطبيق يستخدم هذا البروتوكول فإن عنوان URL سيبدأ بـ https:\\ بدلاً من http:\\ .

مثال : https://www.mybankonline.com

أو عند ادخال معلومات حساب المستخدم في موقع يقدم خدمة البريد الالكتروني مثل موقع gmail - yahoo.

بروتوكول pop3 – imap4

إن البروتوكول POP3 معرف بالنشرة RFC1939 أما الإصدار اللاحق هو IMAP4 المعرف بالنشرة RFC1731.

على الرغم من أن بروتوكول SMTP هو من يستقبل الرسائل ولكن المستخدم على الأغلب لا يقرئها فوراً لهذا يتم تخزينها في مكان مركزي وعندها يأتي دور هذه البروتوكولات في تحميل هذه الرسائل إلى المستخدم. معظم الناس تصل إلى رسائل البريد الالكتروني عبر تطبيقات مثل outlook أو net222 أو eudore وهي جميعها تستخدم بروتوكولات pop3 – imap4

أحد مشاكل pop3 هو أن كلمة المرور المستخدمة للوصول إلى علبة البريد يتم إرسالها عبر الشبكة بشكل صريح وهذا يعني أنه بالإمكان سرقة ومعرفة هذه الكلمة وهنا يأتي دور بروتوكول imap4 والذي يقدم ميزة إضافية على pop3 وهي أنها تستخدم نظام تعرّف وهذا يجعل كلمة المرور أصعب.

ملاحظة: البروتوكولات pop3 – iamp4 تُستخدم لتنزيل الرسائل من المخدم إلى المستخدم وليس لإرسالها فإن الإرسال هي مهمة بروتوكول SMTP.

بروتوكول TELNET

معرف بالنشرة RFC854. وهو بروتوكول وصول يؤمن فتح جلسات على مضيف بعيد وتنفيذ تعليمات عليه .

إن هذا البروتوكول شائع الاستخدام في الوصول إلى الراوتر وأجهزة الشبكة الأخرى القابلة للإدارة. أحد مشاكله هو أنه غير آمن ولذلك غالباً ما يتم استخدام البديل الأكثر سرية وهو SSH.

بروتوكول SSH

هو البديل الآمن لـ telnet يؤمن السرية وذلك عن طريق تشفير البيانات المرسلة بين الأنظمة مما يجعل صعوبة في كشفها من قبل المخترقين وتضيف أيضاً أنظمة تحقق أقوى من telnet. يوجد إصدارين من SSH وهي SSH1 و SSH2 وهو الأكثر أماناً ويجب على المرسل والمستقبل أن يستخدما الإصدار نفسه من SSH. إن هذا البروتوكول متوفر من أجل كل منصات التشغيل الموجودة حالياً بما فيها أنظمة **ويندوز – يونكس – لينكس**.

بروتوكول ICMP

معرف بالنشرة RFC792. وهو بروتوكول يعمل في طبقة الشبكة لتأمين كشف الخطأ. في الحقيقة إن ICMP هي أداة يستخدمها بروتوكول IP لتأمين إيصال البيانات بشكل أفضل ويُستخدم في العديد من المهام وأكثرها شهرة هي أداة ping والتي ترسل العديد من الرسائل إلى محطة أخرى فإذا وصلت هذه الرسائل إلى المحطة المطلوبة فإنها سترد عبر إرسال رسائل صدى (Echo) إلى المحطة المرسلة وبذلك يتم التأكد من سلامة الاتصال بين هذين الجهازين. سيتم شرح أداة ping في فصل لاحق.

بروتوكول arp- rarp

إن البروتوكول arp معرف بالنشرة RFC826. وهو يقوم بتحويل عناوين IP المنطقية إلى عناوين MAC الفيزيائية.

عندما يتصل جهاز بجهاز آخر فإنه يقوم بتحديد إذا ما كان الجهاز المطلوب تابع للشبكة نفسها التي ينتمي إليها المرسل فإذا كان تابع لها يتم الدخول إلى الذاكرة المؤقتة ARP cache والتي تحتوي على عناوين IP وما يقابلها من عناوين MAC لجميع الأجهزة في الشبكة وفي حال لم يجدها يقوم بإرسال Broadcast إلى جميع الأجهزة في الشبكة وعندها سيقوم صاحب الـ IP المطلوب بالرد، أما إذا لم يجدها فسوف يحول الطلب إلى البوابة الافتراضية للبحث عنها في شبكات أخرى متصلة بهذه الشبكة وعندها يتم الحصول على عنوان الـ MAC للجهاز المطلوب ويحصل الاتصال بين هذين الجهازين.

عند التعامل مع الذاكرة المؤقتة لـ ARP يمكن إضافة المدخلات يدوياً أو ديناميكياً. في حالة الإدخال الديناميكي لن يتم ذلك بواسطة المستخدم ولكن تتم الإضافة والتحديث بشكل تلقائي وهو الخيار الأكثر استخداماً. أما الإدخال اليدوي يتم بواسطة المستخدم وذلك باستخدام تعليمة arp-s وعندها سيكون الإدخال دائم ما لم يتم حذفها يدوياً باستخدام التعليمة arp-d.

البروتوكول RARP يقوم بالمهمة نفسها التي يقوم بها ARP ولكن بالعكس أي يحول عناوين MAC الفيزيائية إلى عناوينIP المنطقية وهذا البروتوكول معرف بالنشرة RFC903.

بروتوكولات التوجيه (RIP – OSFP)

تقوم هذه البروتوكولات بتوجيه البيانات عبر الشبكة من خلال اختيار أفضل المسارات بين المرسل والمستقبل. سيتم دراسة التوجيه في بحث لاحق.

الجدول 2.2 يلخص مهام مجموعة بروتوكولات TCP / IP

البروتوكول	***الاسم الكامل***	***الوصف***	***الطبقة التي يعمل بها***
IP	بروتوكول الإنترنت	بروتوكول عديم الاتصال يُستخدم لنقل البيانات داخل الشبكة	3
TCP	بروتوكول التحكم بالنقل	بروتوكول اتصال موجه يؤمن التحكم بالتدفق والترتيب وإعادة الإرسال لرزم البيانات التي لم تصل	4
UDP	بروتوكول معطيات المستخدم	بروتوكول عديم الاتصال على عكس TCP يُستخدم للتطبيقات التي لا تتطلب ميزات TCP	4
FTP	بروتوكول نقل الملفات	تحميل ورفع الملفات من وإلى مستخدم بعيد إضافة إلى مهمات الإدارة الأساسية للملف	7
SFTP	بروتوكول نقل الملفات الآمن	تحميل ورفع الملفات باستخدام SSH	7
TFTP	بروتوكول نقل الملفات البسيط	بروتوكول نقل ملفات ولكن لا يملك ميزة الأمان ولا إمكانية اكتشاف الخطأ يستخدم UDP وهو عديم الاتصال	7
SMTP	بروتوكول نقل البريد الالكتروني البسيط	إرسال واستقبال البريد عبر الشبكة	7
HTTP	بروتوكول نقل النصوص التشعبية	استقبال الملفات من مخدم ويب (Web (Server	7
HTTPS	البروتوكول الآمن لنقل النصوص التشعبية	استقبال آمن للملفات من مخدم ويب	7
POP3-IAMP4		استقبال وتنزيل البريد الالكتروني من مخدم تم تخزين الرسائل عليه	7

TELNET		فتح جلسات على جهاز بعيد	7
SSH		فتح جلسات آمنة على جهاز بعيد	7
ICMP		فحص المسار	4
ARP	بروتوكول تحويل العناوين	تحويل عناوين IP إلى ما يقابلها من عناوين فيزيائية (MAC) لتأمين الاتصال بين التجهيزات	
RARP	بروتوكول تحويل العناوين العكسي	تحويل عناوين MAC إلى ما يقابلها من عناوين IP	
NTP	بروتوكول زمن الشبكة	تأمين معلومات مزامنة الوقت بين التجهيزات المتصلة مع بعضها في الشبكة	

الجدول 2.2

خدمة أسماء المجالات DNS

إن DNS تقوم بخدمة هامة في الشبكات المعتمدة على TCP/IP حيث أنها تقوم بتحويل اسم المضيف مثل WWW.MICROSOFT.COM إلى عنوان IP مثل 209.202.161.67. هذه الطريقة تسمح للمستخدمين

يتذكر أسماء بدل من أرقام وهذا طبعاً أسهل بكثير. إن DNS هو بروتوكول مستقل أي يمكن أن يُستخدم في أنظمة مختلفة.

قبل ظهور الإنترنت استخدمت الشبكات ملف نصي يُسمى HOSTS لأداء هذه المهمة. مثال عن محتوى هذا الملف النصي

```
192.168.3.45    server1  s1          #The main
                                     file and
                                     print server
192.168.3.223   mail     mailserver  #The email server
127.0.0.1       localhost
```

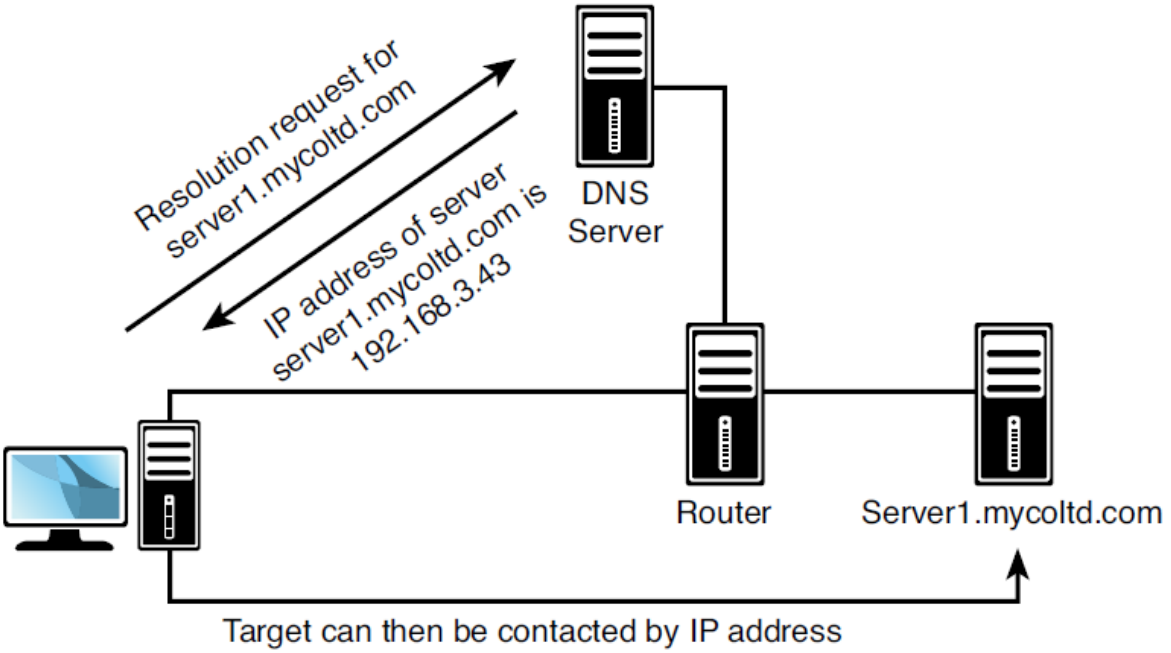
ملاحظة: التعليق في ملف HOSTS يسبقه الرمز(#)

يجب أن يتم إضافة كل المدخلات بشكل يدوي وكل نظام يقوم بعملية التحويل هذه يجب ان يملك نسخة من هذا الملف وعندما ازداد حجم الشبكات أصبحت الحاجة ضرورية لجعل عملية التحويل هذه بشكل أوتوماتيكي عندها ظهرت تقنية الـ DNS .

ملاحظة: مازال ملف الـ HOSTS مستخدم إذا كان عدد المستخدمين في الشبكة قليل ولا يتغيرون كثيراً أو لا يتغيرون أبداً، عندها يمكن استخدام ملف الـ HOSTS .

يقوم DNS بمهمته في تحويل الأسماء إلى عناوين عن طريق إضافة برمجية DNS على مخدم يُسمى (DOMAIN SERVER) الذي يقوم باستقبال ومعالجة والرد على الطلبات الآتية من الأنظمة التي تريد تحويل الأسماء إلى عناوين IP. تُسمى هذه الأنظمة التي تطلب من المخدم بـ عميل DNS (DNS Client)

الشكل2.3 يظهر عملية تحويل DNS



الشكل 2.3

في حال كان فضاء العناوين كبير فإن مخدم واحد لـ DNS لا يستطيع أن يُخدم كل الأسماء وبالتالي يمكن الاستعانة بأكثر من مخدم خاص لهذه المهمة. أحد مشاكل DNS هو أن تحديث محتوياته لا تتم بشكل تلقائي عند حدوث أي تغير وإنما يتم ذلك بشكل يدوي. تم حل هذه المشكلة باستخدام DDNS حيث تمكّن هذه الطريقة من تحديث التغيرات للأنظمة في الزمن الحقيقي (REAL TIME).

فضاء عناوين DNS (The DNS Namespace)

يعتمد DNS في تخزين الأسماء على البنية الهرمية حسب التالي :

المجال الجذري (Root Domain)

إن المجال الجذري هو في أعلى الهرم ويتم تمثيله بـ نقطة (.)

المجالات ذات المستوى الأعلى (TOP-LEVEL DOMAIN)

تكون مؤلفة من حرفين أو ثلاثة وهي مصنفة حسب نوع المؤسسة أو المكان الجغرافي

خدمة WINS (Windows Internet Name Service)

هو نظام يسمح بتحويل أسماء NetBiosname إلى عناوين IP في الشبكات التي تستخدم **أنظمة** ويندوز حصراً. باستخدام هذا النظام يمكن تحقيق الاتصال بين تجهيزات الشبكة المحلية بواسطة أسماء NetBiosName بدل استخدام عناوين IP حيث أن لكل جهاز عنوان IP خاص به مثل 192.168.1.3وكذلك اسم NetBios مثل pc2 وهذا يسهل على المستخدم كثيراً.

تذكرة: إن خدمة DNS تقوم بترجمة أسماء المضيفين إلى عناوين IP مثل تحويل WWW.google.com إلى 10.10.2.9. أما خدمة WINS تقوم بتحويل أسماء NetBios إلى عناوين IP مثل تحويل PC3 إلى 192.168.1.5.

يتم تحويل أسماء NetBIOS إلى عناوين IP باستخدام WINS ومن ثم إلى عناوين MAC باستخدام بروتوكول ARP.

إن عملية تحويل NetBiosname تتم بثلاث طرق :

- باستخدام مخدم WINS وهي أبسط الطرق.
- التحويل اليدوي باستخدام ملف LMHOSTS.
- الطريقة الثالثة وهي الأنسب إذا كان هنالك تغيير دائم في الشبكة وهي الطريقة الأكثر انتشاراً في الحياة العملية وهي باستخدام Broadcast ولكن هذه الطريقة تمتلك عيبين رئيسين:
  - تؤدي إلى حمل إضافي في الشبكة.
  - لا يمكن تجاوز الراوتر وهذا يعني أن عملية التحويل بين أجزاء الشبكة غير ممكن.

خدمة DHCP

حتى يستطيع أي جهاز من الاتصال بالشبكة فهو بحاجة إلى امتلاك عنوان IP وقناع شبكة. أحد الطرق لإعطاء عناوين IP إلى الأنظمة هو استخدام العنونة اليدوية وهذا يتطلب عمل يدوي لإضافة عنوان لكل نظام وسيحتفظ بهذا العنوان حتى يتم تغييره يدوياً. هذه الطريقة تحوي أكثر من مشكلة منها صعوبة إدارة العناوين وقلة الفاعلية والكفاءة وازدياد احتمال حدوث الأخطاء البشرية. الطريقة الأنسب والأسهل هي استخدام DHCP.

إن DHCP معرّف بالنشرة RFC2131. هي خدمة تقوم بإعطاء عناوين IP لمن يطلبه من العملاء أي من الأنظمة التي تكون فيها ميزة DHCP مفعلة (DHCP Client)

مبدأ عمل DHCP

عندما يقوم أي نظام بسؤال مخدم DHCP لإعطائه عنوان IP سيقدم المخدم عنوان من العناوين التي يملكها إلى العميل على شكل آجار أي لمدة محددة من الزمن وبعد تجاوز 50% من مدة الآجار يقوم العميل بمحاولة تجديد المدة. إذا لم يستطع المخدم تجديد المدة ستنتهي مدة الآجار بعد انقضاء 100% من المدة وسيتوقف العميل عن استخدام هذا العنوان. إن مدة الآجار التي يقدمها مخدم DHCP يتم ضبطها من إعدادات المخدم. إن مخدم DHCP إضافة إلى تقديمه عنوان IP وقناع الشبكة فإنه يقدم معلومات أخرى مثل: عنوان البوابة الافتراضية - عنوان مخدم DNS - عنوان مخدم WINS .

يقوم مخدم DHCP بتوزيع العناوين بشكل عشوائي ولكن يمكن إعداده بحيث يعطي عناوين محددة إلى أجهزة محددة وتسمى هذه العملية (Reversation) أي أن عنوان IP المعطى لجهاز محدد لن يتغير وسيبقى محجوزاً له. ويمكن أيضاً ضبط الإعدادات من أجل **الاستثناءات** أي تحديد عناوين IP معينة لا يقوم DHCP بتوزيعها.

ميزات استخدام DHCP

- ❖ عدم الحاجة إلى الإدخالات اليدوية لكل نظام وهذا يوفر الكثير من الوقت والجهد.
- ❖ تقليل الأخطاء البشرية التي تحدث عند ضبط الإعدادات يدوياً مثل استخدام عنوان مكرر .
- ❖ عدم الحاجة إلى إعادة ضبط الأنظمة إذا تم تغير مكانها إلى جزء آخر من الشبكة أو في حال حدوث تغيير بهيكلية عنونة IP ضمن الشبكة.
- ❖ تعتبر برمجية مستقلة أي يمكن استخدامها على أنظمة مختلفة على سبيل المثال يستطيع مخدم يعمل بنظام LINUX أن يقدم عناوين لأنظمة Windows أو Macintosh.

ولكن الجانب السلبي في طريقة DHCP هو اعتمادها على Broadcast وهذا بدوره يؤدي إلى حمل زائد على الشبكة. كما أن تطبيق برمجية DHCP على المخدم يؤدي إلى حمل معالجة إضافي على المخدم.

طريقة العمل في DHCP

إن أفضل طريقة لمعرفة كيف يعمل الـ DHCP هو النظر إلى مستخدم (DHCPClient) يحاول أن يتصل بشبكة فيها مخدم DHCP (DHCPServer).

عندما يحاول نظام تعمل فيه خدمة DHCP الاتصال بشبكة، سوف يرسل رسالة عبرBroadcast للبحث عن مخدم DHCP تُدعى هذه الرسالة بـ DHCPDiscover. سيقوم المخدم بالتقاط هذه الرسلة والتأكد من أنه يستطيع إرسال عنوان لهذا النظام وثم يختار عنوان من العناوين التي يملكها ويرسلها مع المعلومات الإضافية إلى النظام مع

مدة الآجار تُسمى هذه الرسالة بـ DHCPOFFER ويتم ذلك أيضاً عبر الـ Broadcast (لأن النظام إلى الآن لم يتصل بالشبكة).

عندما يستقبل النظام هذا العرض المقدم من المخدم أو العروض المقدمة في حال وجود أكثر من مخدم DHCP في الشبكة يقوم عندها النظام باختيار أحد هذه العروض (وهو على الأغلب صاحب مدة الآجار الأعلى) ويرسل إلى المخدم صاحب العرض المقبول رسالة موافقة تُسمى DHCPReqest يخبره فيها أنه وافق على عرضه عندها يقوم المخدم بإرسال رسالة إلى النظام تُسمى DHCPACK وبعد استقبال هذه الرسالة يقوم النظام المستقبل بتهيئة إعدادات TCP / IP حسب المعلومات المرسلة إليه من المخدم.

الفصل الثالث

العنونة والتوجيه Addressing & Routing

عنونة IP (IP Addressing)

حتى تستطيع الأجهزة الاتصال ببعضها في الشبكات المعتمدة على TCP /IP يجب على كل نظام أن يمتلك عنوان فريد خاص به، أي لا يملكه أحد غيره ضمن الشبكة الواحدة. وإنّ الشبكات تستخدم العنوان IP لأداء هذه المهمة. يوجد اصدارين منه IPV4 و IPV6.

يتألف عنوان IPV4 من 32bit مقسمة على أربع مجموعات كل مجموعة تمثل 8bits تسمى هذه المجموعة بـ Octet كل Octet يشير إلى رقم عشري. كل bit في كل Octet يأخذ القيمة 0 أو 1

- إذا كانت كل البتات تأخذ القيمة 1 عندها سيأخذ الـOctet القيمة 255
- إذا كانت كل البتات تأخذ القيمة 0 عندها سيأخذ الـOctet القيمة 0

إذاً قيمة كل Octet هي من 0 وحتى 255 وذلك حسب عدد الأصفار والواحدات.

الجدول3.1 يبين أمثلة تحويل من قيم عشرية إلى ثنائية

القيمة العشرية	القيمة الثنائية	طريقة الحساب
10	00001010	8 + 2 =10
192	11000000	128 + 64 =192
205	11001101	128 + 64 +8 + 4 +1
223	11011111	128 + 64 + 16 +8 +4 +2+ 1

الجدول 3.1

يتألف عنوان IP من حقلين: حقل يعرّف الشبكة أي عنوان الشبكة (Net ID) وحقل يعرف المستخدم (Host ID) أي بكلمات أخرى يشبه إلى حد ما عنوان الشارع وعنوان البيت ضمن الشارع. كل الأجهزة الموجودة ضمن شبكة واحدة يجب أن يكون لها عنوان شبكة (Net ID) **نفسه**، كل الأجهزة الموجودة ضمن شبكة واحدة يجب أن يكون لها عنوان مستخدم (Host ID) **مختلف** عن الآخر.

إن الذي يحدد أي جزء من عنوان IP يشير إلى عنوان المستخدم وأي جزء يشير إلى عنوان الشبكة هي مجموعة أخرى من الأرقام تُسمى قناع الشبكة وهي أيضاً أربع مجموعات من البتات. في كل مجموعة ثمانية بتات وكل بت يأخذ القيمة 0 أو 1.

مثال عن عنوان IP وقناع الشبكة الخاص به

عنوان IP	192.168.1.10
قناع الشبكة	255.255.255.0

وفي مثالنا هذا فإن أول ثلاث مجموعات من اليسار تشير إلى عنوان الشبكة وآخر مجموعة تشير إلى عنوان المستخدم حيث أن عدد الواحدات في قناع الشبكة يشير إلى عدد بتات عنوان الشبكة.

صفوف عناوين IP

تُصنف عناوين IP إلى خمسة تقسيمات منطقية تُسمى الصفوف هذه الصفوف هي A-B-C-D-E ولكن عملياً ثلاثة فقط هي المتوفرة للمستخدمين وهي A-B-C أما الصف D محجوز لعنونة Multicast والصف E محجوز للتطوير المستقبلي. يتم التمييز بين الصفوف الثلاثة باستخدام قناع شبكة مختلف لكل صف.

- الصف A يستخدم فقط أول مجموعة لعنونة الشبكة والباقي لعنونة العقد في الشبكة.
- الصف B يستخدم فقط أول مجموعتين لعنونة الشبكة والباقي لعنونة العقد في الشبكة.
- الصف C يستخدم فقط أول ثلاث مجموعات لعنونة الشبكة والباقي لعنونة العقد في الشبكة.

وبالتالي سيكون الصف A يحتوي العدد الأقل من عناوين الشبكة ولكن العدد الأكبر من عناوين العقد. بالمقابل سيكون الصف C يحتوي عدد كبير من عناوين المستخدمين أو العقد وعدد قليل من عناوين الشبكات.

الجدول 3.2 يظهر مجالات العنونة ضمن كل صف وعدد الشبكات وعدد العقدة في كل شبكة

الصف	المجال	عدد الشبكات	عدد العقد في كل شبكة	القيمة الثنائية لأول Octet
A	1 to 126	126	16,777,214	0xxxxxxx
B	128 to 191	16,384	65,534	10xxxxxx
C	192 to 223	2,097,152	254	110xxxxx
D	224 to 239	N/A	N/A	1110xxxx
E	240 to 255	N/A	N/A	1111xxxx

الجدول 3.2

ملاحظة: الرقم 127 غير مستخدم في أي مجال والسبب أن العنوان 127.0.0.1 محجوز للحلقة العكسية (Loopback). هذه الحلقة تُستخدم لعمليات الإصلاح.

قناع الشبكة الجزئية (Subnet Mask)

يشبه عنوان IP حيث أنه مؤلف من 32bit مقسم على أربع خانات كل خانة فيها ثمانية بتات ولكن الفرق أن لهذا القناع مهمة واحدة فقط وهي تحديد أي جزء من عنوان IP يشير إلى عنوان الشبكة وأي جزء يشير إلى عنوان العقدة. حيث تقابل الواحدات عنوان الشبكة والأصفار تقابل عنوان العقدة.

كل صف من عناوين IP يستخدم قناع شبكة افتراضي. الجدول 3.3 يظهر القناع الافتراضي لكل صف.

الصف	***قناع الشبكة***
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

الجدول 3.3

التجزئة (Subnetting)

إن التجزئة هي عملية يُقصد بها تقسيم الشبكة إلى شبكات جزئية وبالتالي يمكن التحكم بعدد الشبكات الجزئية دون التقيد بالحدود التي تفرضها الصفوف الثلاث A-B-C، فإن استخدام أحد هذه الصفوف ربما يعطي عناوين للعقد زائد عن الحاجة وبالتالي فإن زيادة عدد الشبكات الجزئية يقلل من عدد العقد ضمن كل شبكة جزئية وبالتالي نحصل على كفاءة في استخدام العناوين وتقليل من هدرها.

مثال عملي: شركة تملك 1000 جهاز حاسوب وبحاجة إلى إعطاء عناوين لها. إن اختيار الصف A غير صحيح لأنه يستطيع عنونة 254 عقدة فقط في كل شبكة جزئية وإن اختيار الصف B سيسبب فائض كبير جداً من العناوين غير المستخدمة، ولكن باستخدام التجزئة يمكن الحصول على شبكة جزئية تحوي العدد المناسب من العناوين المطلوبة دون هدر كبير.

أسباب استخدام التجزئة في الشبكات

- ❖ تسمح باستخدام العناوين بكفاءة دون هدر كبير.
- ❖ تجعل الشبكات أكثر أمناً وقابلية للإدارة وذلك عن طريق تقسيم الشبكة الواحدة إلى شبكات متعددة (بشكل منطقي وليس فيزيائي) وهذا بدوره يقلل من حمل الشبكة وأيضاً إن عملية التقسيم هذه تنشئ أكثر من Broadcast Domain وهذا يقلل من احتمالات التصادم في الشبكة.

ملاحظة: التجزئة لا تزيد من عدد عناوين IP المتاحة ولكن تزيد من عدد الشبكات الجزئية ونتيجة لذلك سينقص عدد عناوين IP المتاحة في كل شبكة جزئية. وهي أيضاً تُنشئ العديد من Broadcast Domain وكما نعلم أن Broadcast لا تمر عبر الراوتر وبالتالي فهي محدودة ضمن الشبكة الجزئية ولا تسبب حمل زائد على باقي الشبكات الجزئية.

الشبكات العامة والشبكات الخاصة

الشبكات العامة هي الشبكات التي يستطيع أي شخص الوصول إليها وأفضل مثال عليها هي شبكة الإنترنت. الشبكات الخاصة هي الشبكات التي يكون الوصول إليها محدود ويتم التحكم به من قبل مالك الشبكة مثال عليها الشبكة الحاسوبية ضمن المدرسة أو شركة تجارية.

إن كلا النوعين من الشبكات تعتمد على مجموعة بروتوكولات TCP/IP تستخدم عناوين IP ولكن الاختلاف يكون في المجال المُستخدم من هذه العناوين حيث تم تقسيم العناوين إلى عناوين تُستخدم في الشبكات الخاصة وعناوين تُستخدم في الشبكات العامة.

منظمة IANA هي المسؤولة عن إعطاء عناوين IP إلى الشبكات العامة، ويتم الحصول على إحدى هذه العناوين للدخول إلى الإنترنت عن طريق مزود خدمة الإنترنت مقابل رسوم يدفعها الزبون .

مجالات العناوين الخاصة (Private IP)

تم تحديد مجالات عنونة خاصة يمكن استخدامها في الشبكات الخاصة، لهذا السبب سُميت بالعناوين الخاصة Private IP. إن موجهات الإنترنت مبرمجة على تجاهل أي بيانات تأتي من هذه العناوين وبالتالي إذا أرادت شبكة خاصة أن تتصل بالإنترنت باستخدام هذه العناوين فإنها لن تتجاوز أول موجه ستجده. إذاً العناوين الخاصة مخصصة للعمل في الشبكات الخاصة وغير صالحة للاستخدام للدخول إلى الإنترنت لأنها لا تستطيع العبور من موجهات الشبكات العامة.

يوجد ثلاث مجالات للعناوين الخاصة معرّفة في النشرة RFC1918 حيث تم اختيار مجال من كل صف عناوين. الجدول 3.4 يبين مجالات العناوين الخاصة ضمن كل صف

الصف	مجال العناوين الخاصة	قناع الشبكة الافتراضي
A	10.0.0.0 **TO** 10.255.255.255	255.0.0.0
B	172.16.0.0 **TO** 172.31.255.255	255.255.0.0
C	192.168.0.0 **TO** 192.168.255.255	255.255.255.0

الجدول 3.4

البوابة الافتراضية Default Gateway

هو الجهاز الذي يسمح للأجهزة الموجودة في شبكة ما من الاتصال بأجهزة أخرى ضمن شبكات أخرى أو ضمن مقاطع أخرى للشبكة الواحدة.

إذا أراد جهاز الاتصال بجهاز آخر فإنه بداية يحدد إذا ما كان هذا الجهاز ضمن الشبكة نفسها فإذا لم يكن كذلك فإنه بحاجة إلى جدول توجيه ساكن ليدله على المسار الصحيح أو بحاجة إلى جهاز يعمل كبوابة للخروج من هذه الشبكة وهذه هي مهمة البوابة الافتراضية.

وإن النظام الذي لا يملك جدول توجيه ساكن او إعدادات لبوابة افتراضية فإنه سيصبح محدود العمل ضمن مقطع الشبكة الخاص به.

ملاحظة: يجب أن تكون البوابة الافتراضية من الشبكة نفسها التي يستخدمها النظام الذي يريد التحدث مع أحد الأنظمة خارج الشبكة.

أنواع العنونة في IPV4

يوجد ثلاث أنواع من عناوين IPV4 وهي: Unicast – Multicast – Broadcast

عناوين Unicast

تُستخدم للاتصال من نقطة إلى نقطة Point-To-Point حيث يتم الإرسال إلى عنوان واحد محدد.

عناوين Broadcast

يتم إرسال البيانات إلى جميع الأجهزة المتصلة بالشبكة.

عناوين Multicast

يمكن من خلالها إرسال البيانات إلى مجموعة محددة من الأجهزة ضمن الشبكة ولن تصل إلى جميع الأجهزة المتصلة بالشبكة.

بروتوكول الإنترنت الجديد IPV6

إن الإصدار IPV4 يتألف من 32bit وهذا يستطيع أن يؤمن أكثر من 4 مليارات عنوان ولم يكن أحد يتوقع أن هذا العدد الضخم لن يكفي. ولكن مع ظهور الإنترنت وازدياد عدد المستخدمين على مستوى العالم وازدياد عدد الأجهزة التي تتصل بالإنترنت واقتراب هذا العدد من النفاد، تم مناقشة إصدار جديد للعنونة قبل الوقوع في خطر نفاد العناوين

المتاحة، وبالفعل تم إنتاج إصدار جديد للعنونة وهو **IPv6** والذي يتألف من 128 بت بدلاً من 32 بت. وهذا يسمح بمجال هائل جداً من العنونة تقدر بـ 340,282,366,920,938,463,463,374,607,431,768,211,456 عنوان !!

كل الأجهزة الحديثة حالياً تدعم IPV6 إضافة إلى IPV4. أي سيعمل الإصداران مع بعضهما إلى أن يختفي IPV4.

طريقة العنونة في IPV6

طريقة العنونة في IPV4 تعتمد على تقسيم البتات إلى 4 خانات تفصلها نقطة (.) وكل خانة يُعير عنها بما يكافئها من الأعداد العشرية. أما طريقة العنونة في IPV6 تختلف عن ذلك حيث يتم تقسيم 128 بت على 8 خانات وفي كل خانة 16 بت يُعبر عن كل خانة بما يكافئها من الأعداد الست عشرية وتفصل الخانات عن بعضها (:).

مثال: 2001:0:4137:9e50:2811:34ff:3f57:febc

في حال وجود عدة خانات متتالية تحوي أصفاراً يمكن اختصارها. المثال التالي يبين هذه العملية

العنوان: 2001:0000:0000:0000:3cde:37d1:3f57:fe93 يمكن اختصاره ليصبح :

. 2001::3cde:37d1:3f57:fe93.

يجب الانتباه إلى أن عملية الاختصار تتم مرة واحدة فقط للعنوان، ولا يمكن اختصار الأصفار إذا وُجد رقم على يسارها أي 4000 لا يمكن اختصارها إلى 4 ولكن يمكن اختصار0004 إلى 4.

ملاحظة: IPV5 هو بروتوكول عنونة تجريبي لم يُستخدم عملياً ولكن ربما يتم استخدامه في الأمور السرية.

أنواع العنونة في IPV6

إن عنوان الحلقة العكسية في IPV4هو 127.0.0.1 أما في IPV6 فهو 0:0:0:0:0:0:0:0 أو 0:0:0:0:0:0:0:1

الجدول 3.5 يظهر المقارنة بين IPV4 وIPV6

مهمة العنوان	IPV4	IPV6

عنوان الحلقة العكسية	127.0.0.1	0:0:0:0:0:0:0:1 (::1)
عناوين الشبكات العامة	مجالات العناوين العامة	Global unicast
عناوين الشبكات الخاصة	10.0.0.0 172.16.0.0 192.168.0.0	كل العناوين التي تبدأ بـ (FEC0::)
عناوين الإعداد التلقائي	169.254.0.0	كل العناوين التي تبدأ بـ FE80::

الجدول 3.5

إعطاء عناوين IP

كل نظام في الشبكة الحاسوبية المعتمدة على TCP/IP يحتاج أن يملك عنوان IP خاص به ولا يتكرر على الشبكة نفسها ويوجد طريقتين لإعطاء العناوين للمستخدمين:

الطريقة اليدوية (Static Addressing)

يتم إعداد العنوان بشكل يدوي وهذا يسبب مشكلتين رئيستين:

- ❖ إن إعداد عنوان لنظام واحد يعتبر أمر سهل ولكن إعداد مئات أو آلاف الأنظمة يعتبر أمر شاق جداً وستقع أخطاء بشرية في الإعداد على الأغلب. وإذا تم إدخال عنوان IP خاطئ فلن يستطيع النظام الاتصال بباقي الأنظمة في الشبكة.
- ❖ إذا تم تغير هيكلية الشبكة الحاسوبية لأي سبب كان فإنه يتوجب إعادة عنونة جميع الأجهزة في الشبكة وإن مثل هذا الإعداد لشركة كبيرة صعب جداً وهدر كبير للوقت. لهذا الأسباب فإن معظم الشبكات تستخدم العنونة الآلية.

العنونة الآلية (Dynamic Addressing)

يتم في هذه الطريقة إعطاء عناوين IP إلى جميع الأنظمة في الشبكة بشكل أوتوماتيكي وبدون تدخل يدوي ويتم ذلك باستخدام بروتوكول DHCP الذي هو جزء من مجموعة بروتوكولات TCP /IP حيث يتم تنصيب برمجية DHCP على جهاز مركزي يزود باقي الأنظمة بالعناوين اللازمة بمدة أجار معينة تُجدد تلقائياً.

عند وصل أي جهاز جديد مع الشبكة فإنه يطلب إعطاءه عنوان مناسب فيرد عليه مخدم DHCP ويعطيه عنوان من العناوين التي يملكها مع قناع الشبكة، عندها يستطيع هذا الجهاز الدخول إلى الشبكة والاتصال بباقي الأجهزة. يمكن لـ DHCP أن يعطي معلومات أكثر من عنوان IP وقناع الشبكة فيمكنه إعطاء عنوان البوابة الافتراضية ومعلومات DNS.

إن استخدام DHCP في العنونة يقلل من الأخطاء البشرية أثناء الإعداد اليدوي وخصوصاً تكرار إعطاء عنوان مُستخدم من قبل نظام آخر على الشبكة نفسها ويلغي الحاجة إلى إعادة تهيئة الأنظمة في حال تم تغير مكانها في الشبكة أو إذا تم تطبيق تغيير في هيكلية الشبكة وسياسات العنونة.

ملاحظة: بعض الأجهزة تحتاج إلى العنونة اليدوية (الثابتة) ولو كانت ضمن شبكة تستخدم خدمة DHCP فمثلاً يجب على مخدم DHCP ومخدم DNS ومخدم الويب وغيره من الأنظمة ذات المهام الحساسة أن تمتلك عناوين ثابتة لا تتغير وإلا فلن تستطيع باقي الأجهزة من الوصول إلى الخدمات التي تقدمها هذه الأنظمة في حال تغير عنوانها.

يحتاج أي نظام حتى يستطيع الاتصال بشبكة إلى عنوان IP وقناع شبكة، فهذه معلومات ضرورية أما عناوين البوابة الافتراضية ومخدم DNS فهي اختيارية ولكن بدونها ستكون الإمكانيات محدودة.

ما يلي يلخص قائمة بالمعلومات المستخدمة للاتصال بالشبكة:

- **عنوان IP**: كل نظام يجب أن يمتلك عنوان IP فريد أي خاص به ولا يتكرر على الشبكة نفسها.
- **قناع الشبكة**: من خلاله يستطيع النظام تحديد أي جزء من عنوان IP يدل على عنوان الشبكة وأي جزء يدل على عنوان العقدة.
- **البوابة الافتراضية**: يستطيع النظام من خلالها الاتصال بشبكة بعيدة بدون الحاجة إلى وجود جدول توجيه.
- **مخدم DNS**: يمكّن المستخدم من استخدام الأسماء بدل من عناوين IP وهذا يُسهل عليه كثيراً، من الشائع استخدام عنوانين لـ DNS في إعدادات TCP/IP فإذا كان أحد المخدمين لا يعمل سيقوم الآخر بأداء المهمة.

تذكير: عنوان IP وقناع الشبكة ضروري للاتصال بالشبكة وأما البوابة الافتراضية و DNS اختيارية ولكن بدونها ستكون الخيارات محدودة.

بروتوكول BOOTP

صُمم هذا البروتوكول لمحطات العمل التي لا تملك قرص صلب وتحتاج إلى معلومات للاتصال بالشبكة مثل عنوان IP وقناع الشبكة وغيرها من المعلومات ولا يوجد طريقة لتخزين المعلومات بدون قرص صلب.

عندما يتم إعداد النظام ليستخدم BOOTP وعند تشغيلها فإنه سيرسل طلب إلى مخدم BOOTP الموجود في الشبكة، عند وصل الطلب إلى المخدم سيقارن بين عنوان MAC للنظام مع قاعدة البيانات الموجودة عنده، إذا وجدها سيرسل للنظام المُرسل المعلومات اللازمة.

يجب الانتباه إلى أن BOOTP يعتمد على Broadcast. فمن الضروري تهيئة الراوتر لتمرير طلبات BOOTP.

العنونة التلقائية APIPA

هذه الطريقة من العنونة من إنتاج شركة ميكروسوفت أُنتجت في نظام ويندوز98 وبقيت موجودة في الإصدارات اللاحقة.

بواسطة هذه الطريقة يستطيع النظام إعطاء عنوان IP لنفسه في حال فشل في أخذ عنوان من مخدم DHCP ولكن من خلال هذا العنوان لا يستطيع النظام إلاّ الاتصال بباقي أجزاء الشبكة المتصل بها فقط، لأنه لا يستطيع إعطاء عنوان لبوابة افتراضية وبالتالي سيكون الاتصال محدود جداً ضمن الشبكة المحلية.

إذاً الفكرة من APIPA هو تأمين اتصال بين الأنظمة في الشبكة الجزئية نفسها إذا حدث فشل في مخدم DHCP، ولكن من الناحية العملية غير مستخدمة كثيراً.

إن العناوين التي تستطيع الأنظمة أخذها تلقائياً من ضمن المجال: 169.254.0.0 - 255.255.0.0

ملاحظة: إذا كان النظام لا يدعم ميزة APIPA ولا يستطيع استقبال عنوان من مخدم DHCP فإنه سيأخذ العنوان: 0.0.0.0

دراسة حالة عملية:

شبكة حاسوبية مؤلفة من 30 حاسب عليها نظام ويندوز وتعتمد على مخدم DHCP لإعطاء العناوين لحواسيب الشبكة، وتم إقلاع 10حواسيب وأخذوا عناوين IP من مخدم DHCP، وبعدها حدث عطل في المخدم، عندئذ كل الحواسيب التي ستقلع لاحقاً لن تأخذ عناوين من المخدم، وبالتالي ستعطي نفسها عناوين APIPA من المجال 169.254.0.0. عندها لن تستطيع هذه الحواسيب من الاتصال بالحواسيب العشرة التي أخذت عناوينها من مخدم DHCP، لهذا السبب فإن استخدام طريقة APIPA في الحياة العملية محدودة.

العناوين الفيزيائية MAC

سُمي العنوان MAC بالعنوان الفيزيائي لأنه مطبوع بشكل فيزيائي على كرت الشبكة (NIC). يتألف عنوان MAC من 48 بت أو 6 بايت. يستخدم الترقيم الست عشري (أي الأرقام من 0-9 والأحرف من A-F).

مثال عن عنوان MAC: 00:D0:59:09:07:51

يجب على عناوين MAC أن تكون **فريدة** على مستوى العالم لذلك تم وضع آلية لمنع تكرار هذه العناوين، حيث تم تعريف أي كرت شبكة في العالم بالطريقة التالية: أول ثلاث بايتات من العنوان يُعرف الشركة المصنعة وآخر ثلاث بايتات هي أرقام تُعطى من قبل المصنع. بهذه الطريقة يمكن جعل بطاقات الشبكة فريدة على مستوى العالم. يمكن معرفة عنوان MAC الخاص بأي جهاز بعدة طرق منها استخدام التعليمة التالية في أنظمة ويندوز IPconfig /all>> أو باستخدام التعليمة getmac>>

تقنية NAT

المبدأ الأساسي لهذه التقنية هو جعل العديد من الحواسيب تختفي خلف عنوان IP وحيد، السبب الرئيسي لهذه التقنية هو ببساطة عدم كفاية عناوين IPV4. فبواسطة هذه التقنية يمكن لشبكة محلية الاتصال بالإنترنت من خلال عنوان Public IP واحد. أي يمكن استخدام عناوين خاصة ضمن الشبكة المحلية للاتصال مع بعضها ضمن الشبكة، ولكن عند الاتصال بشبكات خارجية (الإنترنت مثلاً) تستخدم عنوان Public IP واحد. وسيظهر من وجهة نظر مستخدم بعيد أن الطلبات تأتيه من عنوان واحد فقط وليس من عناوين الحواسيب التي اتصلت به. يحتفظ NAT بالمسار الذي خرجت منه رزم البيانات (أي عنوان الجهاز المرسل) للتأكد أنه عند رجوع البيانات ستصل إلى وجهتها الصحيحة.

تؤمن طريقة NAT أيضاً مستوى من الأمان للشبكة المحلية التي تستخدمها لأن كل عناوين الأجهزة ضمن الشبكة مختبئة خلف عنوان واحد وهذا يقلل خطر الهجمات على الشبكة.

تقنية PAT

هي تقنية تسمح لعدة مستخدمين ضمن شبكة محلية بالاتصال بالإنترنت باستخدام عنوان Public IP واحد بدل من استخدام عنوان عام لكل مستخدم ويتم ذلك عبر إعطاء جميع المستخدمين الراغبين بالاتصال بالإنترنت عنوان IP نفسه ولكن بمنفذ مختلف يميز كل مستخدم عن الآخر.

مثال عملي: مستخدم في شبكة محلية يملك العنوان: 192.168.2.2 يريد الاتصال بمخدم ويب وليكن عنوانه 213.23.231.85. فإن الطلب سيذهب إلى راوترPAT الذي يقوم بإعطائه عنوان Public IP الذي يملكه وليكن : 20.34.67.9 مع رقم منفذ خاص بهذا المستخدم صاحب العنوان الخاص، ويضيف رقم المنفذ هذا إلى جدول خاص اسمه جدولPAT، عندما يرد مخدم الويب على هذا الطلب، فإن راوترPAT سيستقبل الرد ثم يتفحص الجدول ليحدد المستقبل المقصود ويحول البيانات إليه.

ملاحظة: لا تخلط بين Proxy _ PAT _ NAT مع العلم أن البروكسي يملك تقنية NAT.

المنافذ (Ports)

إن كل تطبيق أو بروتوكول مرتبط برقم منفذ خاص به، ويتم استخدام هذا الرقم من قبل الأنظمة لتحديد أي بروتوكول أو خدمة سيتم التعامل معها.

مثال توضيحي: إن البروتوكول **HTTP** مرتبط بالمنفذ رقم **80** فعندما يتم إرسال طلب من متصفح انترنت (Chrome مثلاً) إلى مخدم ويب (WWW.Amazon.cpm مثلاً) فإن هذا الطلب يتم إرساله إلى المنفذ 80 في النظام المستقبل. عند وصول الطلب إلى المستقبل يتفحص رقم المنفذ وعندما يرى أنه 80 فإنه يوجه الطلب إلى تطبيق مخدم الويب للرد عليه.

تحتوي مجموعة TCP/IP على 65535 منفذ متاح للاستخدام، المنافذ من 0 وحتى 1023محجوزة (منافذ معروفة جيداً)

الجدول 3.6 يبين أهم المنافذ المستخدمة

البروتوكول	المنفذ المخصص له
منافذ TCP	
FTP	20
FTP	21
SSH	22
TELNET	23
SMTP	25
DNS	53
HTTP	80
POP3	110
IMAP4	143
HTTPS	443
منافذ UDP	
TFTP	69
DNS	53
DHCP SERVER	67
DHCP CLIENT	68

الجدول 3.6

ملاحظة: ورد في الجدول أن لـ FTP منفذان 20 و21 حيث أن المنفذ 20 هو منفذ للبيانات أما المنفذ21 فهو لأوامر التحكم. في الحياة العملية يُستخدم المنفذ 21 وأما المنفذ 20 نادر الاستخدام في الشبكات الحديثة.

إدارة التوجيه في شبكات TCP /IP

في هذه الأيام أصبحت للشركات فروع متباعدة جغرافياً وبالتالي أصبحت أجزاء الشبكة الواحدة متباعدة فيزيائياً وتتصل فيما بينها عن طريق الموجه أو الراوتر (ROUTER). حيث يمكن تعريف الراوتر أنه تجهيزة شبكية توجه البيانات بين الشبكات.

عندما يستقبل الراوتر البيانات يتوجب عليه تحديد المسار الأنسب لإرسال البيانات عبره إلى المستقبل، ولتحقيق ذلك فإن موجهات الشبكات تستخدم قطعتين من المعلومات: عنوان البوابة الافتراضية و جداول التوجيه.

البوابة الافتراضية Default Gateway

البوابة الافتراضية هي عنوان IP للراوتر والذي هو بمثابة الطريق إلى شبكات بعيدة حيث أن إرسال البيانات من شبكة لأخرى تتم عن طريقه -الحواسيب الموجودة على الجانب الآخر من الراوتر يُقال لها الشبكات البعيدة- بدون البوابة الافتراضية تصبح اتصالات الإنترنت غير ممكنة لأن حاسب المستخدم لا يملك طريقة لإرسال البيانات لأي شبكة خارجية.

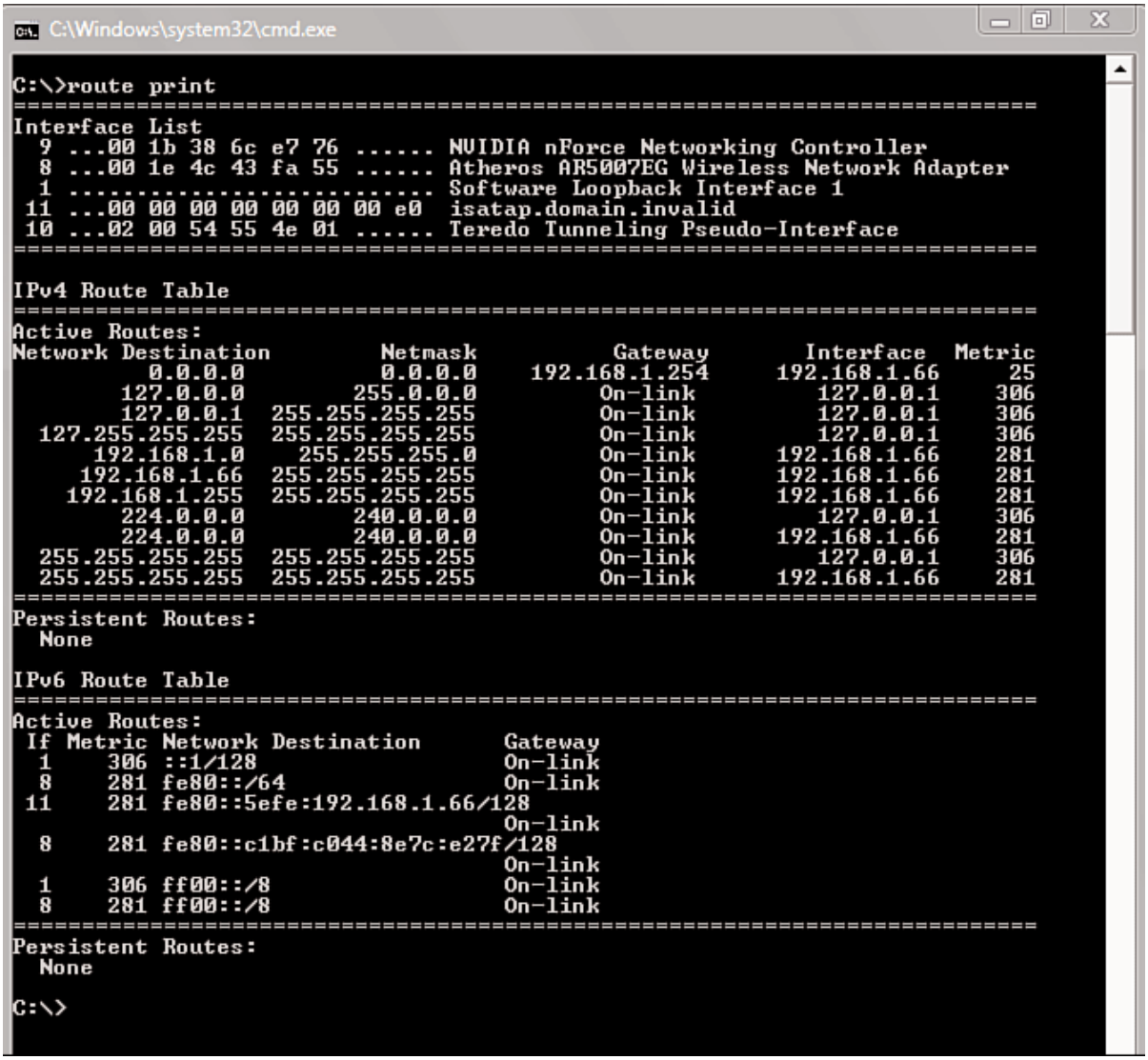
من الشائع أن يتم تهيئة عنوان البوابة الافتراضية بشكل أوتوماتيكي من خلال إعدادات الـ DHCP .

جداول التوجيه

قبل إرسال أي رزم بيانات يجب مراجعة جدول التوجيه وهو الذي يحدد أفضل مسار أو طريق ممكن للبيانات لتصل إلى هدفها.

كل حاسب في شبكات TCP /IP يملك جدول توجيه يتم تخزينه محلياً، ويمكن إظهاره باستخدام التعليمة >> route print

الشكل3.1 يظهر جدول التوجيه في حاسب يعمل عليه نظام تشغيل Windows7



الشكل3.1

المعلومات التي تظهر في هذا الشكل هي:

- Destination: عنوان الحاسب المضيف
- Network mas : قيمة قناع الشبكة
- Gateway: أي العنوان الذي أُرسلت البيانات منه، يمكن أن يكون مخدم أو راوتر أو أي نظام يعمل كبوابة.
- Interface: عنوان كرت الشبكة التي استُخدمت لإرسال رزم البيانات إلى المستقبل.
- Metric: القيمة الأدنى منه يعني أن التوجيه أسرع، في حال وجود أكثر من مسار يتم اختيار المسار صاحب القيمة الأدنى من هذا المحدد .

يمكن إنشاء جداول التوجيه بطريقتين: التوجيه الساكن والتوجيه الديناميكي

التوجيه الساكن Static Routing

في هذه الطريقة يتم إدخال معلومات التوجيه بشكل يدوي إلى جداول التوجيه ولكن ذلك يؤدي إلى ضياع الوقت وحدوث أخطاء إضافة إلى أن حدوث أي تغيير في مخطط الشبكة يتطلب إعادة ضبط للموجهات بشكل يدوي. لهذه الأسباب فإن التوجيه الساكن يمكن تطبيقه فقط للبيئات الصغيرة أي التي تحتوي على راوتر أو راوترين والحل الأفضل هو استخدام التوجيه الديناميكي.

يمكن إضافة توجيه ساكن إلى الجدول باستخدام التعليمة route add >>

مثال: route add 192.168.2.1 mask (255.255.255.0) 192.168.2.4

الهدف القناع البوابة

إن إضافة العناوين بهذه الطريقة سوف تُمحى عند إعادة إقلاع الجهاز، ولجعلها ثابتة لا تُمحى يمكن استخدام التعليمة >>route add –p

التوجيه الديناميكي Dynamic Routing

يتم استخدام بروتوكولات توجيه خاصة وتستطيع الموجهات (Routers) تمرير معلوماتها إلى موجهات أخرى وبالتالي يستطيع الراوتر من بناء جداول توجيه بدون تدخل المستخدم.

أشهر بروتوكولات التوجيه: بروتوكول **EIGRP** وبروتوكول **OSPF**.

الفصل الرابع
مكونات الشبكة
Components & Device

بطاقة الشبكة NIC

هو جهاز يمكّن الحاسب من الاتصال بالشبكة، ويقوم بمهمة إرسال واستقبال البيانات من وإلى الحاسب. حيث يستقبل البيانات القادمة من الشبكة ويحولها إلى الصيغة التي يفهمها الحاسب، ويقوم بإرسال البيانات الصادرة من الحاسب إلى الشبكة وتحويلها إلى إشارات تفهمها الشبكة. كما يقوم أيضاً بتنظيم حركة مرور البيانات من وإلى الحاسب. يمكن أن تكون بطاقة الشبكة سلكية تتصل بكيبل أو لاسلكية تستخدم الأمواج الراديوية (RF).

يوجد لكرت الشبكة عادة عدة أضواء تدل على حالة عمله وهي:

ضوء الوصلة (Link)

يضيء إذا حدث اتصال بين كرت الشبكة والشبكة. وفي حال لم يضيء يكون هذا مؤشر على وجود شيء غير صحيح في كابلات الشبكة أو في الموصلات.

ضوء النشاط (Activity)

يشير إلى نشاط الشبكة. يجب أن يكون تحت الشروط الطبيعية في حالة رجفان (ومضان)، أما إذا كان ثابت فهذا يعني انشغال الشبكة أو وجود مشكلة في مكان ما بالشبكة.

ضوء السرعة (Speed)

يشير إلى أن كرت الشبكة متصل بسرعة محددة (10-100-1000)MB

ملاحظة : أحياناً يوجد في بعض كروت الشبكة ضوئين فقط.

وحدة التوصيل المركزي Hub

هو جهاز بسيط يقوم بتوجيه البيانات الواصلة إليه إلى كل التجهيزات المتصلة معه، وليس إلى جهاز محدد، أي أنه يؤمن ممر للإشارات الالكترونية لتمر عبره وبالتالي يمكن أن يسبب حمل إضافي عبر الشبكة.

يوجد منه نوعان: غير فعال (**Passive**) لا يقوم بأي مهمة غير تمرير الإشارات. وفعال (**Active**) يقوم بالإضافة إلى تمرير الإشارات إلى جميع الأجهزة المتصلة معه فإنه يقوم بإعادة توليد الإشارات قبل إرسالها، ويمكن أن يخزن البيانات تلقائياً (Buffering).

لا يقوم الـ Hub بأي عمليات على البيانات التي تمر عبره فهو يعمل في الطبقة الأولى من طبقات OSI. ويأتي بعدة أشكال وحجوم (5-8) منفذ وحتى 32 منفذ. أصبح استخدامه قليل جداً وحل مكانه الـ Switch.

المبدل Switch

هو عقدة مركزية للشبكة، أي تتصل الأجهزة بها عبر كابلات مجدولة (Twisted Pairs) –كيبل لكل جهاز– كما هو الحال في الـ Hub، ولكن الفرق الرئيسي بينهما هو كيفية تعامله مع البيانات المستقبلة. في حين يقوم الـ Hub بتوجيه البيانات المستقبلة إلى جميع النقاط المتصلة به. يقوم الـ Switch بتوجيهها فقط إلى منفذ واحد وهو الذي يتصل معه الجهاز المستقبل. إنه يقوم بذلك من خلال تعلم عناوين MAC للأجهزة المتصلة معه. عندما يرسل جهاز رسالة لجهاز آخر فإنه سيوجه هذه الرسالة إلى الجهاز المطلوب فقط ويتجاهل الأجهزة الأخرى. يمكن لـ Switch أن يحسن من أداء الشبكة، حيث إنه يقلل من عدد التصادمات التي تحدث في الشبكة.

ويستطيع العمل بنمطي الاتصال: النمط **Full-Duplex** (بهذه الطريقة يمكن للجهاز أن يرسل و يستقبل البيانات في اللحظة نفسها أي الاتصال بالاتجاهين) وبالنمط **Half-Duplex** (بهذه الطريقة يمكن للجهاز أن يرسل أو يستقبل البيانات في اللحظة نفسها أي الاتصال باتجاه واحد).

يعمل الـ Switch في الطبقة الثانية من طبقات OSI ويوجد إصدارات تعمل في الطبقة الثالثة من طبقات OSI.

الموجه Router

يقوم الراوتر بربط شبكتين أو أكثر مع بعض حيث يقوم بتوجيه الرسائل بين الشبكات لتذهب كل رسالة إلى مكانها الصحيح. يعمل في الطبقة الثالثة من طبقات OSI.

عندما يستقبل الراوتر رزم البيانات يقرأ المعلومات في رأس قطعة البيانات (Header) ليحدد عنوان الجهاز المستقبل (الجهاز الهدف). وبعد تحديد العنوان المطلوب ينظر في جداول التوجيه عنده ليحدد كيفية ايصال هذه البيانات إلى المستقبل.

يوجد حالياً العديد من أنواع (Routers) رخيصة الثمن ومخصصة للاستخدام المنزلي بحيث لا يتجاوز عدد المستخدمين 10.

طبعاً يجب أن يحتوي الراوتر على أكثر من كرت شبكة بحيث يتصل كل كرت مع شبكة محددة.

نقطة الوصول اللاسلكية Wireless Access Point

يرمز لها اختصاراً AP و هو جهاز إرسال واستقبال، يُستخدم لإنشاء شبكة محلية لاسلكية WLAN وذلك عن طريق الربط بين الشبكة المحلية السلكية LAN مع أجهزة لاسلكية، أي يعمل عمل الجسر. كما يمكن أن يعمل على توسيع الشبكة اللاسلكية بإضافة أكثر من APs، أي يعمل في هذه الحالة كراوتر.

يُستخدم الراوتر في نمط الشبكة اللاسلكية (**Infrastructure**)التي تحتاج إلى عقدة مركزية لاسلكية.

المسافة الفعلية التي يستطيع هذا الجهاز تغطيتها لاسلكياً تعتمد على المعيار اللاسلكي المستخدم (a –g -n)، والبيئة التي يعمل فيها.

أصبح AP هذه الأيام أكثر من مجرد نقطة وصول فقد أصبح يؤمن إمكانية الجدار الناري وخدمة الـ DHCP أي أصبح يعمل عمل: (Switch – Router – DHCP Server – Firewall).

يأتي AP في حجوم وأشكال مختلفة ومتنوعة جداً، العديد منها رخيص الثمن ومصمم للاستخدام في منزل أو مكتب صغير، بحيث يملك طاقة منخفضة للهوائي ومنافذ محدودة للتوسع.

يعمل AP في الطبقة الثانية من طبقات OSI.

المودیم Modem

هو جهاز يقوم بمهمة **التعديل/فك التعديل** حيث يحول الإشارات الرقمية المتولدة من الحاسب إلى إشارات تماثلية يمكن إرسالها عبر خط الهاتف وبالعكس. من خلاله تستطيع الشبكة المحلية LAN الاتصال بمزود خدمة الإنترنت (ISP) عن طريق خط الهاتف التماثلي. يمكن للموديم أن يكون مدمج مع اللوحة الرئيسية للحاسب أو جهاز خارجي يتصل بالحاسب.

الجدار الناري Firewall

هو جهاز شبكي يمكن أن يكون (هاردوير أو سوفت وير) مهمته التحكم بالوصول إلى الشبكة، وهو مصمم لحماية البيانات وموارد الشبكة من الهجمات الخارجية. يوضع عادةً عند نقاط الدخول والخروج من الشبكة.

على سبيل المثال يمكن وضعه بين الشبكة الداخلية والإنترنت. عندها يستطيع الجدار الناري التحكم بكل الاتصالات الداخلة والخارجة إلى الشبكة.

ويُستخدم أيضاً للتحكم بالوصول بين مقاطع محددة ضمن الشبكة الواحدة، مثل بين قسم المحاسبة وقسم المبيعات. يمكن تحقيق الجدار الناري من خلال البرمجيات أو من خلال أجهزة محددة. توجد هذه البرمجية في معظم أنظمة التشغيل هذه الأيام.

يمكن أن يكون الجدار الناري متوفر في أجهزة أخرى، على سبيل المثال يملك الراوتر و نقطة الوصول اللاسلكي ميزة الجدار الناري بشكل مدمج فيها.

مخدم DHCP (DHCP Server)

يقوم بإعطاء عناوين IP إضافة إلى معلومات أخرى (قناع الشبكة -عنوان البوابة الافتراضية -عنوان مخدم DNS) بشكل أوتوماتيكي لجميع الأنظمة المتصلة بالشبكة. يُستخدم هذا المخدم بشكل واسع في شبكات Client / Server.

مخدم DNS (DNS Server)

يؤمن تحويل الأسماء إلى عناوين IP. بدون هذا المخدم لا تستطيع الحواسيب في الشبكات المحلية من الوصول إلى الإنترنت.

مخدم البروكسي (Proxy Server)

هو مخدم يوجد بين حاسب المستخدم والإنترنت يقوم بمهمة (وكيل للمستخدم) أي أنه يقوم باستقبال الطلبات المُرسلة من المستخدم إلى الإنترنت وإرسال هذه الطلبات عوضاً عن المستخدم. ويستقبل أيضاً الرد من الإنترنت ثم يرسلها إلى المستخدم.

المهمة الأخرى له هي التخزين المؤقت (**Caching**) حيث يقوم بتخزين نسخة مخبأة من صفحات الإنترنت التي طُلبت من قبل المستخدمين، وفي حال طلبها مرة أخرى سيعطيها من هذه الذاكرة وليس من الإنترنت. وهذا يؤدي إلى زيادة السرعة، ولكن تكون المعلومات غير محدثة أي ليست في الزمن الحقيقي. وهذا غير مناسب في بعض الحالات التي تتطلب أن تكون المعلومات في اللحظة نفسها مثل صفحات الأسواق المالية (البورصة) ولكن في أغلب الحالات تعتبر الـ Caching ميزة مفيدة.

مثال عن استخدام ميزة التخزين المؤقت: لنفترض شبكة حاسوبية في مدرسة و30 طالب يريدون الوصول إلى صفحة ويب معينة. بدون بروكسي سيخرج من الشبكة 30 طلب إلى الإنترنت ولكن بوجود مخدم البروكسي سيُطلب من الإنترنت طلب واحد وأما 29 طلب الباقية من ذاكرة الكاش.

الميزة الأخرى للبروكسي هي إمكانية التحكم بطلبات العملاء فيمكن حجب أو تقييد الوصول إلى بعض المواقع والسماح لأخرى.

الجدول 4.1 يلخص أجهزة الشبكة الأكثر استخداماً

اسم الجهاز	الوصف	نقاط رئيسية
HUB	عقدة مركزية لوصل الأجهزة في الشبكات ذات الكابلات المجدولة	لا تقوم بأي مهمة باستثناء إعادة توجيه البيانات إلى جميع النقاط. يمكن أن تقوم بإعادة توليد الإشارة
Switch	عقدة مركزية لوصل الأجهزة في الشبكات ذات الكابلات المجدولة	يقوم بتوجيه البيانات إلى وجهتها المحددة باستخدام عناوين MAC الموجودة في كل رزمة بيانات
Router	يُستخدم لوصل الشبكات مع بعضها	يستخدم عناوين IP لتوجيه البيانات إلى وجهتها.
Modem	يؤمن إمكانية ربط الشبكات المحلية بخط الهاتف	يحول الإشارات الرقمية المرسلة من الحاسب إلى إشارات تماثلية والعكس في حالة الاستقبال
Nic	يؤمن اتصال الحاسب بالشبكة السلكية أو اللاسلكية	يمكن أن يكون مدمج أو جهاز خارجي
Firewall	يؤمن التحكم بعبور البيانات بين الشبكات	يمكن أن يكون جهاز أو برنامج وهو جزء أساسي من استراتيجية أمان الشبكة
DHCP Server	إعطاء معلومات الـ IP إلى باقي أجهزة الشبكة بشكل تلقائي	يمكن أن يعطي معلومات أخرى مثل قناع الشبكة - عنوان مخدم DHCP - عنوان مخدم DNS
DNS Server	يؤمن تحويل الأسماء إلى عناوين	يستجيب لطلبات المستخدمين عبر تحويل الأسماء التي يطلبونها إلى عناوين IP

Proxy Server	إدارة طلبات الإنترنت من العملاء	زيادة أداء الشبكة عبر ميزة Caching وترشيح (فلترة) طلبات العملاء الخارجية
AP	تأمين الوصول اللاسلكي إلى الشبكة المحلية LAN	تعمل كجسر بين الشبكة السلكية واللاسلكية تعمل كراوتر بين الشبكات اللاسلكية

الجدول 4.1

مكونات الشبكة الافتراضية Virtual Network Components

التطبيقات الافتراضية (Virtualization) أصبحت هذه الأيام منتشرة بشكل واسع بسبب توفير التكلفة والأداء الجيد الذي تقدمها. يمكن تحقيق هذه التطبيقات الافتراضية من خلال حلول مفتوحة المصدر مثل (virtual Box) وشركات أخرى مثل (VMware)، والتي تسمح بأخذ جهاز فيزيائي واحد وجعله يظهر للمستخدمين على أنه عدد من الأجهزة المستقلة.

سطح المكتب الافتراضي Virtual Desktop

يمكن لجهاز الحاسب أن يحتوي - بشكل طبيعي -على أكثر من نظام تشغيل يتم تنصيبها عليه. أما عن طريق استخدام البرمجيات الافتراضية فإن جهاز الحاسب الواحد يمكنه تشغيل أكثر من نظام تشغيل واحد في الوقت نفسه. على سبيل المثال يمكن تشغيل نظام التشغيل ويندوز7 وويندوز 8 ولينكس في الوقت نفسه على جهاز الحاسب نفسه. ومن وجهة نظر الشبكات الحاسوبية فإن كل نظام تشغيل يحتاج لإعدادات مستقلة عن الآخر.

المخدمات الافتراضية Virtual Server

يمكن بهذه الطريقة جعل جهاز فيزيائي واحد أن يقوم بعدة مهام وهذا يؤدي إلى توفير في التكلفة المادية بسبب تخفيض تكلفة الأجهزة الفيزيائية (Hardware). على سبيل المثال يمكن استخدام مخدم واحد ليعمل عمل مخدم DHCP ومخدم DNS ومخدم FTP ومخدم HTTP .

المبدلات الافتراضية Virtual Switches

تعمل نفس عمل المبدلات الفيزيائية ولكن تسمح بأن يتواجد أكثر من مبدل في جهاز واحد. وهذا يوفر من تكلفة الأجهزة بشكل كبير. هذا النوع من المبدلات أصبح يُستخدم بشكل واسع مع الشبكات الافتراضية VLAN. مثال عن حلول مفتوحة المصدر هو Open Vswitch ، يمكن الحصول عليه من www.openvswitch.org

مقسم هاتف افتراضي Virtual PBX

هو نظام هاتف يقوم بمهام مقسم الهاتف الفيزيائي مثل توجيه المكالمات - البريد الصوتي - خدمة الفاكس وغيرها من الخدمات.

الفصل الخامس
التنصيب والإعداد
Installation & Configuration

إن الشبكات الحاسوبية متنوعة من حيث الحجم، تبدأ من شبكة صغيرة من عدة أجهزة متصلة مع بعضها تُسمى شبكات (SOHO) إلى شبكات كبيرة WAN، حتى الوصول إلى شبكة الإنترنت العالمية التي هي شبكة الشبكات.

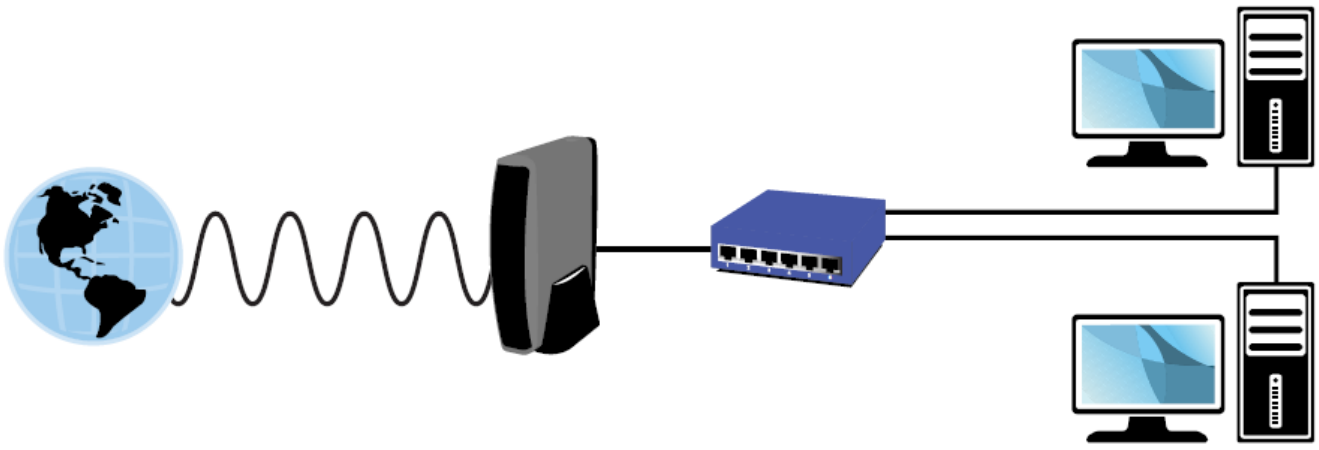
إنشاء شبكة SOHO

تتكون شبكة SOHO عادة من (1-10) مستخدمين ولكن لا يوجد قانون يحدد هذا العدد و المقصود هو عدد قليل من المستخدمين والبيئة الفيزيائية الصغيرة. تتصل هذه الشبكة بالإنترنت من خلال موديم DSL أو كيبل موديم حيث أن الموديم يربط الشبكة بمزود خدمة الإنترنت ISP.

يُستخدم عادة لمثل هكذا شبكات راوتر DSL منزلي والذي يقوم بمعظم المهام المطلوبة لإنجاز شبكة صغيرة مثل Switch و Router ونقطة وصول لاسلكي ومخدم DHCP.

يوجد في مقدمة هذا الراوتر العديد من الأضواء التي تشير إلى حالته وهي على الأغلب: التغذية الكهربائية - نشاط الشبكة - الاتصال مع الإنترنت.

الشكل 5.1 يبين الشبكة **SOHO**



الشكل 5.1

تقنيات الشبكة الواسعة WAN Technologies

إن معظم الشبكات الحاسوبية هي شبكات LAN، ولكن يوجد العديد من الشبكات تتوسع إلى مسافات بعيدة لتصبح شبكات واسعة WAN، وهذا يتطلب تجهيزات وبرمجيات وتقنيات لتحقيق مثل هكذا شبكات.

طرق التبديل Switching Methods

إن البيانات التي تنتقل من جهاز في شبكة لجهاز آخر تحتاج إلى طريق أو عدة طرق لتنتقل عبرها والعودة مجدداً. وهذه هي مهمة التبديل (Switching) حيث تؤمن طرق اتصال بين نقطتين وتتحكم بكيفية مرور البيانات بينهما. أكثر طرق التبديل شهرة هي:

التبديل بالرزم (Packet Switching) والتبديل بالدارات (Circuit switching)

التبديل بالرزم (Packet Switching)

في هذه الطريقة يتم تقسيم رسائل البيانات إلى قطع أصغر تُسمى الرزم (Packet) وكل رزمة تُوقّع بعنوان المصدر(النظام المرسل)، وبعنوان الوجهة (النظام المستقبل)، ورقم يشير إلى ترتيب كل رزمة. هذه المعلومات ضرورية بالنسبة لرزم البيانات لأنها لا تستخدم دائماً المسار نفسه لتصل إلى الجهة المطلوبة يُشار إلى ذلك بالتوجيه المستقل (*independent routing*)، وهذه تعتبر أهم ميزات التبديل بالرزم إذ يمكّن من استخدام أفضل لعرض الحزمة، عبر نقل الرزم بمسارات مختلفة لتجنب مناطق الازدحام العالي في الشبكة.

التوجيه المستقل أيضاً يمكّن رزم البيانات من أخذ مسار بديل إذا كان المسار الأول غير قابل للاستخدام (لأسباب مختلفة).

تعتبر طريقة التبديل بالرزم مشهورة في الشبكات وهي المستخدمة في معظم شبكات WAN.

في نظام التبديل بالرزم عندما يتم إرسال الرزم عبر الشبكة، فإن الجهاز المرسل هو المسؤول عن اختيار أفضل مسار للعبور – هذا المسار يمكن أن يتغير على الطريق – وسيستقبل الجهاز المستقبل الرزم بشكل عشوائي وغير مرتب. عندها سينتظر الجهاز المستقبل حتى تكتمل كل البيانات ثم يعيد ترتيبها حسب الترتيب الموجود في كل رزمة.

يوجد نوعان من التبديل بالرزم: **الدارات الوهمية وبرقيات البيانات.**

الدارات الوهمية Virtual circuits

يتم إنشاء خط اتصال وهمي بين المرسل والمستقبل وهذا الخط يمكن أن يبقى فعال طالما أن الجهازين يستخدمانه لإرسال الرزم، وبعد انتهاء عملية الإرسال يتم إغلاق هذا المسار.

برقيات البيانات Datagrams

لا يتم في هذه الطريقة إنشاء مسار وهمي ولكن ترُسل رزم البيانات بشكل مستقل وهذا يعني أنه يمكن أن تأخذ مسارات مختلفة عبر الشبكة لتصل إلى وجهتها. لتحقيق ذلك يجب أن تحتوي كل رزمة على عنوان المرسل والمستقبل. هذه الطريقة تتأكد من أن الرزم تأخذ أسهل مسار ممكن لتصل إلى وجهتها وتتجنب مناطق الازدحام العالي وهي الطريقة المستخدمة بشكل رئيسي في الإنترنت.

التبديل بالدارات (Circuit switching)

تحتاج هذه الطريقة إلى اتصال فيزيائي محدد بين أجهزة المرسل والمستقبل – على عكس طريقة التبديل بالرزم – وهي الطريقة المستخدمة لنقل الإشارات التماثلية مثل شبكة الخطوط الهاتفية والتي تملك خط محدد بين المرسل والمستقبل وعند حدوث انقطاع في هذا الخط فإن الدارة ستنقطع وتُفقد البيانات. الفائدة الرئيسية لهذه الطريقة هي أنه بعد إنشاء الاتصال سيتحقق اتصال موثوق بين المرسل والمستقبل ولكن السلبية في هذه الطريقة هي أن هذا الخط سيبقى محجوز حتى بعد انتهاء عملية الإرسال ولن يكون متاح لغيره من الاتصالات.

الجدول 5.1 يُظهر مقارنة بين أنواع التبديل

طريقة التبديل	المحاسن	السيئات	مفاتيح رئيسية
التبديل بالرزم (PacketSwitching)	- استخدام أفضل عرض الحزمة في الشبكة - تستطيع الرزم التوجيه ضمن الشبكة لتجنب الازدحام	- يمكن أن تضيع الرزم عندما تأخذ مسار بديل في الطريق - تُقسم الرسائل إلى رزم تحتوي على معلومات المرسل والمستقبل	يوجد نوعان لهذه التقنية: - Virtual circuits تستخدم مسار وهمي بين المرسل والمستقبل . - Datagrams تُرسل قطع البيانات بشكل مستقل لتأخذ مسارات مختلفة لتصل إلى الهدف.
التبديل بالدارات (Circuit switching)	توفر قناة اتصال محددة يتم حجزها ولو لم يحدث اتصال	- تأمين قناة اتصال دائمة - بحاجة إلى خط نقل فيزيائي مخصص	تقدم إمكانية تخزين الرسائل مؤقتاً للتقليل من ازدحام الشبكة .

الجدول 5.1

التقنيات المستخدمة في طريقة التبديل بالرزم :

- البروتوكول X.25
- تبديل الإطارات Frame Relay

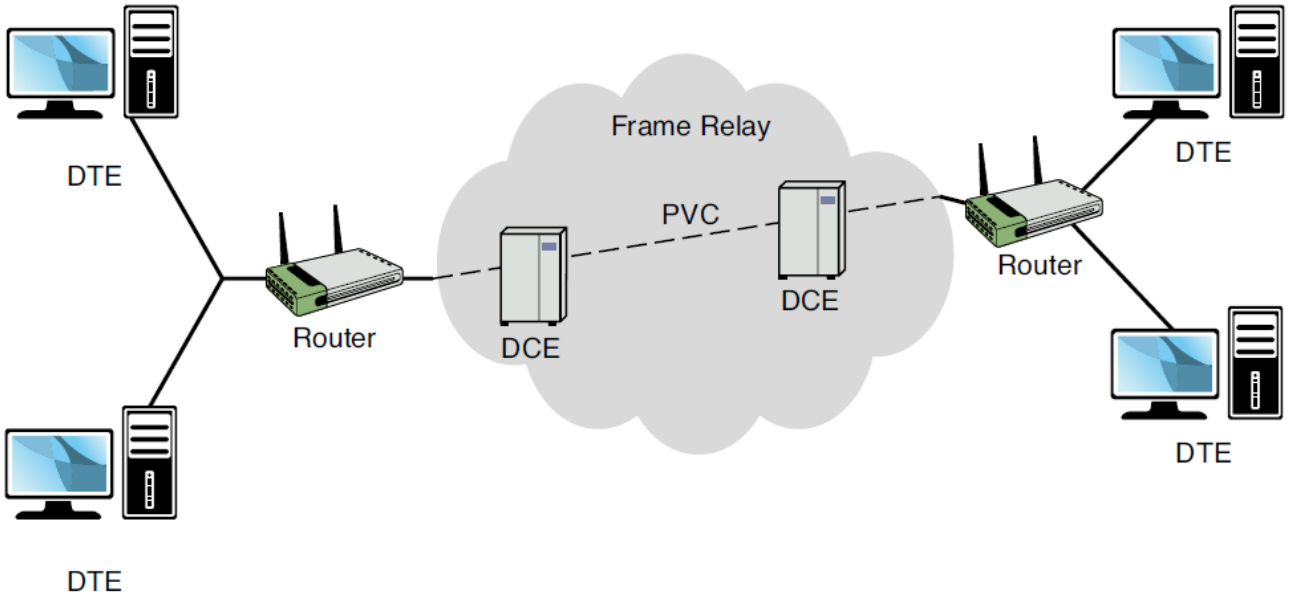
- ❖ نمط النقل غير المتزامن ATM
- ❖ خدمة SMDS

البروتوكول X.25

يعتبر أقدم التكنولوجيا المستخدمة في التبديل بالرزم ولكن حالياً لم يعد مستخدم. كان الهدف من هذه التكنولوجيا هو نقل البيانات الرقمية عبر الإشارات التماثلية في الأسلاك النحاسية. سرعة نقل البيانات فيها 56 Kbps.

تبديل الإطارات Frame Relay

جاءت كتطوير للبروتوكول X.25 ويؤمن وثوقيه أفضل ومعدلات أخطاء أقل لأنه يستخدم الدارات الوهمية (Virtual circuit) ويستخدم حجوم أصغر لرزم البيانات من المستخدمة في X.25. تبلغ سرعة نقل البيانات ما بين 56 Kbps و45 Mbps باستخدام الخطوط T1 وT3 .



تقنية ATM

جاءت هذه التقنية كتحديث لتقنية Frame Relay حيث أنها استبدلت الرزم مختلفة الطول برزم ثابتة الطول. يمكن لهذه الشبكات نقل البيانات والصوت والفيديو بسرعات عالية. ولكنها لم تنتشر كثيراً بسبب ظهور تقنية الإيثرنت بسرعة GB التي قدمت سرعات أعلى.

طول رزمة البيانات 53 byte (48 بايت للبيانات و5 بايت لمعلومات رأس ATM). يتم استخدم الدارات الوهمية (Virtual circuit) لإنشاء اتصال بين جهازين في الشبكة.

تقنية SMDS

هي تقنية لتراسل البيانات بسرعات عالية توفرها شركات الهاتف. تسمح للشركات بربط شبكات محلية (LANs) في مناطق جغرافية واسعة وتعتبر بديل لخطوط T1 وT3. يمكن لتقنية SMDS نقل البيانات إلى عدد كبير من الشبكات المحلية المختلفة في آن واحد لأنها تقوم بتوصيل عدة نقاط ببعضها (any-to-any) أما الخطوط T1 تصل بين نقطة إلى نقطة (point-to-point).

تستخدم هذه التقنية رزم بيانات بطول ثابت.

الشبكة الرقمية للخدمات المتكاملة ISDN

أصبحت هذه التقنية خيار بديل للاتصال الهاتفي البطيء للربط بين أجزاء الشبكة WAN ولكن مع تكلفة أعلى. تؤمن ISDN نقل البيانات والصوت باستخدام التجهيزات الفيزيائية نفسها للشبكة الهاتفية.

الخطوط الرقمية T

هي خطوط **رقمية محجوزة** ذات سرعات عالية والتي يمكن أن تُحجز من شركة الهاتف. تُنشئ هذه الخطوط قناة اتصال دائمة ومتاحة بين نقطتين وتدعم هذه الخطوط نقل الصوت والبيانات. ولأنها خطوط محجوزة فإنها تُعتبر خيار مكلف بالنسبة لشبكات WAN. في أمريكا الشمالية يُستخدم المصطلح DS عوضاً عن المصطلح T. وفي أوروبا تُسمى بـ خطوط E وفي اليابان خطوط J.

يوجد أربع أنواع متاحة من خطوط T :

- T1 : تقدم سرعة نقل 1.544 Mbps
- T2 : تقدم سرعة نقل 6.312 Mbps ويتم ذلك باستخدام 96 قناة B
- T3 : تقدم سرعة نقل 44.736 Mbps ويتم ذلك باستخدام 672 قناة B
- T4 : تقدم سرعة نقل 274.176 Mbps ويتم ذلك باستخدام 4032 قناة B

ملاحظة: بسبب التكلفة العالية لخطوط T يمكن حجز جزء من خدمة خط النقل T. تُعرف هذه التقنية بـ (Fractional T) حيث يمكن حجز عدة قنوات Kbps(64) حسب الحاجة.

تكنولوجيا SONET

تكنولوجيا ربط الأجهزة في شبكات WAN باستخدام الألياف الضوئية. تستطيع نقل البيانات والصوت والفيديو بسرعات عالية تبدأ من 51.84 Mbps .

قامت الشبكة الضوئية SONET بتعريف حوامل لتحديد معدل نقل البيانات.

الجدول 5.2 يبين مستويات حوامل الألياف الضوئية (OCx)

مستوى الحامل OCx	معدل النقل
OC-1	51.84Mbps
OC-3	155.52Mbps
OC-12	622.08Mbps
OC-24	1.244Gbps
OC-48	2.488Gbps
OC-96	4.976Gbps
OC-192	9.953Gbps
OC-678	39.813Gbps

الجدول 5.2

في أوروبا يتم استخدام المصطلح SDH عوضاً عن SONET.

الجدول 5.3 يقارن بين تقنيات الاتصال في WAN

التقنية	سرعة نقل البيانات	وسط النقل الذي يدعمه	طريقة التبديل المستخدمة	الميزات الرئيسية
ISDN	BRI: 64kbps to 128KBPS PRI: 64kbps to 1.5Mbps	الكابلات النحاسة والألياف الضوئية		
T-carrier (T1, T3)	T1: 1.544Mbps T3: 44.736Mbps	الكابلات النحاسة والألياف الضوئية		
ATM	1.544Mbps to 622Mbps	الكابلات النحاسة والألياف الضوئية		
X.25	56kbps/64kbps	الكابلات النحاسة والألياف الضوئية		
Frame Relay	56kbps to 1.544Mbps	الكابلات النحاسة والألياف الضوئية		
SONET/OCx	51.8Mbps to 2.4Gbps	الألياف الضوئية		

الجدول 5.3

تقنيات الاتصال بالإنترنت

أصبحت الإنترنت هذه الأيام جزء أساسي من عالم الأعمال الحديث. يوجد عدة طرق متاحة للاتصال بالإنترنت وذلك يعتمد على التكلفة المادية والتكنولوجيا المتاحة في بلد المشترك.

ملاحظة: إن المصطلح النطاق العريض (Broadband) يشير إلى الاتصال بالإنترنت السريع. يُعتبر كل من DSL وكيبل المودم من تكنولوجيا Broadband .

الاتصال بالإنترنت عبر DSL

هي طريقة للوصول إلى الإنترنت باستخدام خطوط شبكة الهاتف القياسية لتأمين سرعات عالية. بما أن تقنية DSL ليست غالية كثيراً فهي موجودة بكثرة في البيوت وفي المكاتب الصغيرة. في هذه التقنية يتم استخدام تردد لنقل إشارة الكلام وتردد لنقل إشارة المعلومات وهذا يعني أنه بالإمكان التحدث باستخدام خط الهاتف وتحميل البيانات في الوقت نفسه.

أنواع DSL

ADSL: اختصاراً لـ خط اشتراك رقمي غير متماثل وهو أكثر أنواع DSL انتشاراً. يستخدم هذا النوع قنوات مختلفة على خط الهاتف، أحد هذه القنوات تُستخدم لخدمة الهاتف (POTS) لنقل الإشارات التماثلية والقناة الثانية تُستخدم لتنزيل البيانات والثالثة لرفع البيانات.

في ADSL يكون التنزيل (Download) أسرع من الرفع (Upload) وهذا هو سبب تسمية ADSL.

SDSL: توفر سرعات متساوية من أجل التنزيل والرفع للبيانات وهذا مناسب للتطبيقات التجارية مثل حجز مواقع الويب والإنترنت والتجارة الالكترونية.

هذا النوع غير شائع في البيئات الصغيرة مثل البيوت والمكاتب الصغيرة ولا يستطيع مشاركة خط الهاتف للمكالمات.

ISDN_DSL (IDSL): يُستخدم هذا النوع عندما لا يتوفر ADSL أوSDSL. ولا تدعم مشاركة خط الهاتف.

RADSL: هو نوع من ADSL يمكن من خلاله تعديل سرعة النقل اعتماداً على جودة الإشارة.

HDSL: متماثلة أي تقدم سرعات متماثلة لتنزيل ورفع البيانات. لا تسمح بمشاركة خط الهاتف مع إشارات المكالمات التماثلية.

VDSL: هي من النوع المتماثل تدعم تطبيقات تحتاج إلى عرض حزمة كبير مثل HDTV-VOIP. يمكن مشاركة خط الهاتف من خلال هذا النوع.

إن السبب وراء وجود عدة أنواع من تقنية DSL هو بكل بساطة أن كل نوع موجه لاستخدام مختلف. فإن عالم الأعمال يحتاج إلى سرعات عالية أما الاستخدام المنزلي ليس كذلك.

الجدول 5.4 يلخص أنواع تقنية DSL

نوع DSL	سرعة التنزيل (Downloading)	سرعة الرفع (Uploading)
ADSL	3Mbps	1Mbps
SDSL	1.5Mbps	1.5Mbps
IDSL	144 Kbps	144 Kbps
RADSL	7Mbps	1Mbps
HDSL	768Kbps	768Kbps
VDSL	13Mbps	1.6Mbps

الجدول 5.4

ملاحظة: هذه السرعات تتفاوت بشكل كبير حسب التكنولوجيا المستخدمة وجودة الاتصال.

السيئة الرئيسية لتقنية DSL هي حساسيتها للمسافة. فمع ازدياد المسافة بين المستخدم ومقسم الهاتف تنخفض سرعة نقل البيانات تدريجياً.

ملاحظة: إن تقنية DSL تعتمد على مبدأ استخدام تردد لنقل الإشارات التماثلية للمكالمات الهاتفية وتردد مختلف لنقل البيانات الرقمية، ولكن في بعض الأحيان يحدث تداخل بين هذه الإشارات، وهذا هو سبب استخدام مرشح (DSL Filter) حيث يقوم هذا المرشح بتقليل هذا التداخل قدر الإمكان مما يؤدي إلى اتصال أسرع وجودة اتصال أفضل.

منهجية إصلاح DSL

إن إصلاح اتصال DSL يشبه إصلاح أي اتصال بالإنترنت وإن اتباع الأمور التالية يساعد في حل المشكلة :

الاتصال الفيزيائي

أول أمر يجب تفحصه هو كابلات الشبكة لأنه مع مرور الزمن تصبح الكابلات ضعيفة ويمكن أن تنقطع بعض الأسلاك النحاسية فيه مسببة مشاكل في الاتصال.

التأكد من سلامة الاتصال مع موديم DSL حيث أنه يحتوي على الأغلب ثلاث منافذ للاتصال واحد من أجل خط الهاتف (RG11) وآخر من أجل الشبكة (RG45) والثالث من أجل التغذية الكهربائية. يجب التأكد من أن كل كيبل في مكانه الصحيح.

كرت الشبكة (NIC)

إن الذي يشير إلى سلامة كرت الشبكة هو الضوء الذي يصدره، ففي حالة عدم وجود أي إضاءة يجب استبدال الكرت لأنها الطريق الأسهل.

التعريفات (Drivers)

التأكد من التنصيب الصحيح لتعريف كرت الشبكة وأنه تعريف مناسب للكرت. في بعض الحالات يتم حل المشكلة باستخدام التعريف الأحدث لكرت الشبكة.

إعدادات TCP /IP

التأكد من إعطاء عنوان IP صالح وإذا كان بحاجة إلى أخذ العنوان بشكل تلقائي يجب تغيير الإعدادات ليأخذ عنوان من مخدم DHCP.

يمكن استخدام التعليمات التالية:

- تعليمة لاستعراض الإعدادات الحالية : >> IPconfig
- تعليمة للتخلص من عنوان IP الحالي : >>IPconfig /release
- تعليمة للحصول على عنوان IP جديد : >>IPconfig /relnew

ملاحظة: سيتم مناقشة التعليمات الضرورية للشبكة في الفصل الثامن.

مؤشرات الإضاءة في موديم DSL

كل موديم يملك مؤشرات ضوئية يمكن من خلالها تحديد المشكلة. يختلف عدد هذه المؤشرات وترتيبها حسب الشركة المصنعة، ولكن على الأغلب يوجد مؤشر للتغذية (POWER) يضيء هذا المؤشر في حال وجود تغذية، ومؤشر للوصلة (LINK) يضيء هذا المؤشر بشكل ثابت في حالة وجود اتصال فيزيائي صحيح، ويضيئ بشكل رجفان في حالة الاتصال وتبادل البيانات. إضافة إلى وجود مؤشر لحالة الاتصال بالإنترنت يشير إلى وجود اتصال بالإنترنت أم لا.

الاتصال بالإنترنت عبر الكيبل

هي طريقة للاتصال بالإنترنت متاحة في المناطق التي تملك خطوط تلفزيون رقمية. وهي تعتبر حل جيد للبيوت و للمكاتب الصغيرة لأنها موثوقة وليست باهظة الثمن. يتم الاتصال باستخدام جهاز يُسمى موديم الكيبل (Cable

Modem). يملك هذا الجهاز منفذ للكابلات المحورية (Coaxial) للاتصال بمزود الخدمة ومنفذ للكابلات النحاسية المجدولة (Twisted pair) للاتصال بالشبكة الحاسوبية أو إلى الحاسب مباشرة.

معظم الكابلات تقدم سرعة وصول للإنترنت 30Mbps ولكن السرعة الحقيقية تكون أقل من ذلك بكثير لأن هذه السرعة يتم تقاسمها مع الجوار لتصل إلى 1.5 Mbps. هذه التشاركية في السرعة هي السيئة الأكبر لهذه الخدمة لأنه في ساعات الذروة تصبح السرعة ضعيفة.

الاعتبارات الأمنية للاتصال عريض المجال

إن استخدام اتصال عريض المجال (DSL) يؤمن خدمة اتصال دائم بالإنترنت، وهذا يؤدي إلى خطر أمني كبير لأن نظام التشغيل للمستخدم أصبح عُرضة للهجمات الالكترونية على مدار 24 ساعة. ويمكن لأحدهم أن يدخل إلى النظام عن بعد مُستغل وجود الثغرات الأمنية في نظام التشغيل، وغالباً ما تكون هذه الثغرات من Email أو من المنافذ المفتوحة.

يجب أخذ الاحتياطات الأمنية المناسبة وهي وجود جدار ناري (Firewall) وتحديث نظام التشغيل دائماً. لأن الشركات المنتجة لأنظمة التشغيل تنتج دائماً رقع (Patch) للثغرات الأمنية المُكتشفة.

الاتصال بالإنترنت باستخدام الشبكة الهاتفية (POTS)

على الرغم من أنها بطيئة لكنها مازالت شائعة الاستخدام عند الكثير من المستخدمين لأنها تعتمد فقط على خط الهاتف وهو موجود في كل البيوت والمكاتب، حيث يُستخدم خط الهاتف للمكالمات الهاتفية ولنقل البيانات أيضاً.

POTS: هي اختصار لـ :(Plain Old Telephone System)

الاتصال بالإنترنت عبر الهاتف يتطلب أمرين اثنين: موديم وحساب من مزود خدمة الإنترنت **ISP**.

1. ***الموديم***: هو جهاز يحول الإشارات الرقمية المتولدة من الحاسب إلى إشارات تماثلية، ليتم نقلها عبر خط الهاتف – *يمكن أن يكون المودم داخلي أو خارجي* – يستخدم المنفذ COM للاتصال بالحاسب.
2. ***حساب من ISP***: يمكن الحصول عليه بسهولة، ويعتمد على الأغلب على الزمن الذي يقضيه المستخدم على الإنترنت وليس على كمية التنزيل. في الحالة العادية تكون سرعة هذا الاتصال 56Kbps.

ملاحظة: هذا النوع من الاتصال يعتمد على مبدأ من يدخل اولاً يتم تخديمه أولاً (First-come First served) هذا يعني أنه في بعض الاحيان يمكن أن تكون الخطوط مشغولة ولا يمكن الدخول إلى الإنترنت.

منهجية حل مشاكل الاتصال باستخدام POTS

المستخدم لا يستطيع الاتصال

1. تفحص الاتصالات الفيزيائية: إن معظم المشاكل هي بسبب أن الموديم غير موصول، أو موصول بشكل غير صحيح. أو أنه غير موصول بمآخذ التغذية الكهربائية في حالة الموديم الخارجي.
2. التأكد من أن خط الهاتف فيه نغمة الاتصال (الجاهزية): ويمكن ذلك من خلال محاولة الاتصال من خط الهاتف - *المُستخدم للاتصال بـ ISP*- أيضاً فإن الموديم يملك مكبر ويمكن ضبطه لاستخدام المكبر لسماع صوت عند محاولة الاتصال.

المستخدم يتمكن من الاتصال ولكنه لا يستطيع الدخول إلى الإنترنت

1. التأكد من أن المستخدم يتصل بالرقم الصحيح.
2. التأكد من عدم وجود مشكلة بالمزود عن طريق الاتصال بالمزود والسؤال عن المشكلة.

المستخدم يستطيع الاتصال والوصول إلى الإنترنت ولكن يفصل الاتصال بعد لحظات

1. التأكد من اسم المستخدم وكلمة المرور من حيث صلاحيتها ووجود رصيد فيها.
2. التأكد من الضبط الصحيح لإعدادات الموديم.
3. التأكد من الضبط الصحيح لإعدادات الاتصال: مثل عنوان IP -*حالياً كل ISPs تعطي عناوين من خلال DHCP*-
4. تعديل سرعة الاتصال: صُممت المودمات لتتفاوض حول سرعة الاتصال مع الأجهزة التي تتصل معها. في بعض الأحيان تعديل سرعة الاتصال إلى بطيئة يمكن أن يعطي اتصال ومن ثم يتم زيادة سرعة الموديم تدريجياً.

الاتصال بالإنترنت باستخدام الأقمار الصنعية

إن معظم المستخدمين يستعملون تقنيات DSL أو Cable للوصول إلى الإنترنت، ولكن هذه التقنيات غير متوفرة في كل مكان، الكثير من المناطق الريفية لا تملك مثل هكذا طرق اتصال. عندها يوجد طريقة واحدة أساسية وهي عن طريق الأقمار الصنعية. توفر الأقمار الصنعية حلول للوصول إلى الإنترنت بشكل دائم وبسرعة نظرية 512 Kbps للرفع وحتى 2048 Kbps للتنزيل.

تملك هذه الطريقة العديد من السلبيات مثل التكلفة المادية والتأخير الزمني الناتج عن تأخر وصول الإشارة من القمر الصنعي إلى المستخدم. ولكن على الرغم من ذلك تقدم هذه الطريقة بعض الميزات الجيدة وأهمها هي القدرة على التجوال، إذ يمكن الحصول على الإنترنت بدون الحاجة إلى وجود خط هاتف أو كيبل تلفزيوني.

يوجد نظامان من الاتصال بالإنترنت عبر الأقمار الصنعية: نظام الطريق الواحد One-way ونظام الطريقين Tow-way.

نظام One-way

في هذا النظام يكون إرسال الطلبات من المستخدم إلى القمر الصنعي عبر خط الهاتف والتنزيل يكون عبر الأمواج الميكروية من القمر الصنعي إلى جهاز الاستقبال للمستخدم.

نظام Tow-way

يكون إرسال الطلبات واستقبال البيانات عن طريق القمر الصناعي.

السرعة الحقيقية تعتمد على عدة عوامل – *كما هو الحال في كل تقنيات الاتصال اللاسلكي* – وأهمها تأثير الغلاف الجوي على الإشارات الميكروية (ضباب – مطر- ثلوج .....)

الاتصال بالإنترنت باستخدام اللاسلكي

أصبحت هذه الطريقة تنتشر بشكل سريع وتمتاز بميزة التجوال إذ يكفي أن يملك جهاز المستخدم كرت شبكة لاسلكي وسيدخل إلى شبكة الإنترنت إذا كان ضمن نطاق تغطية اللاسلكي ويملك صلاحية الدخول إلى الشبكة. العديد من المطاعم والمقاهي والفنادق تؤمن لزبائنها هذه الطريقة لسهولتها.

ملاحظة: سيتم مناقشة الشبكات اللاسلكية في الفصل السابع

الاتصال بالإنترنت باستخدام الخلوي

أصبحت هذه الطريقة منتشرة كثيراً نتيجة انتشار أجهزة الاتصال المحمولة (هاتف ذكي -IPad- Tablet) والتي يمكنها الاتصال بالإنترنت من خلال شبكة الخلوي، والتي أدخلت نقل البيانات اعتباراً من الجيل الثاني 2.5G والذي يسمى (**GPRS**) والخدمات التي يقدمها الجيل الثالث 3G وحالياً الجيل الرابع 4G والجيل الخامس 5G.

الفصل السادس
التمديد والكابلات

اعتبارات عامة لوسائط النقل

أنماط الاتصال في الشبكات

- الاتصال وحيد الاتجاه (Simplex): وفيه تنتقل البيانات باتجاه واحد فقط عبر الشبكة ويستخدم كامل عرض المجال للكيبل المستخدم في عملية نقل الإشارة، وهذا النمط قليل الاستخدام في شبكات LAN.
- الاتصال نصف مزدوج (Half duplex): وفيه يتم إرسال واستقبال البيانات على الكيبل نفسه، ولكن ليس في الوقت نفسه. يوجد العديد من الشبكات تعمل وفق هذا النمط.
- الاتصال المزدوج (Full duplex): وفيه يتم إرسال واستقبال البيانات على الكيبل نفسه وفي الوقت نفسه. هذا هو النمط السائد في الشبكات الحاسوبية ولكن يجب أن يكون كل من كرت الشبكة والعقدة المركزية (Switch) تدعم هذه الميزة.

التداخل في وسائط النقل

يمكن أن يحدث نوعين من التداخل للبيانات المنقولة عبر الوسط الناقل وهما:

- التداخل الكهرطيسي (EMI): وهذا يحدث عندما يتم تمديد الكابلات بالقرب من جهاز كهربائي مثل المكيف أو إنارة الفلورسنت. فإذا كانت الكابلات ممددة بشكل قريب من هذا الجهاز فإن إشارة البيانات داخل الكيبل يمكن أن تتأثر أو تُفقد. إن وسائط النقل تتنوع بممانعتها من تأثير EMI فمثلاً تعتبر كابلات UTP شديدة التأثر بها أما الكابلات الضوئية (Fiber optic) لا تتأثر بها إطلاقاً لأنها تنقل الإشارات ضوئياً.
- اختلاط الإشارات (Crosstalk): يحدث هذا النوع من التداخل عند تداخل إشارات البيانات في وسطين منفصلين (مثل تأثر إشارات المكالمات الهاتفية مع بعضها)، وأيضاً فإن وسائط النقل تتنوع بممانعتها لهذا النوع من التداخل وتكون الكابلات الضوئية هي صاحبة الممانعة الأعلى.

التخميد في وسائط النقل (Attenuation)

هو مصطلح يشير إلى ضعف إشارات البيانات عندما تسافر عبر وسائط النقل. تختلف وسائط النقل بممانعتها للتخميد حيث تكون الكابلات المحورية Coaxial غالباً أكثر ممانعة من الكابلات النحاسية UTP، وتكون STP

أكثر ممانعة من UTP، والألياف الضوئية هي الأقل تأثراً. لكل نوع من وسائط النقل طول أعظمي يجب ألا يتم تجاوزه حتى يتم تجنب ظاهرة التخميد.

المكرر (Repeater) هو جهاز شبكي يُستخدم لتضخيم الإشارة التي تمر عبره وبذلك يمكن نقلها لمسافات أكبر.

معدل نقل البيانات (Data Rate)

يُقاس معدل النقل بعدد البتات التي يمكن نقلها عبر الوسط بالثانية الواحدة قديماً كانت تُقاس بـ bps أما هذه الأيام بـ Mbps أوGbps .

تختلف وسائط النقل في الشبكات الحاسوبية بمعدل النقل الذي يمكن أن تقدمها أو تدعمها. معظم التطبيقات في الشبكة تحتاج إلى سرعات أعلى من 10 Mbps أو 100Mbps أو 1Gbps وفي بعض الحالات تحتاج إلى 10 Gbps.

ملاحظة: أحياناً يُطلق على معدل البيانات بشكل خاطئ أنها عرض الحزمة، مع العلم أن مصطلح عرض الحزمة يشير إلى عرض المجال من الترددات، أو عدد القنوات التي يمكن للوسط أن يدعمها. مع الانتباه إلى أن عرض الحزمة يؤثر على معدل نقل البيانات ولكن ليس هو نفسه.

أنواع وسائط النقل في الشبكة

يوجد نوعين أساسيين من وسائط النقل في الشبكات: الوسط السلكي (مثل الكابلات النحاسية المجدولة والكابلات المحورية والألياف الضوئية) و الوسط اللاسلكي (مثل الأمواج الراديوية والأمواج تحت الحمراء).

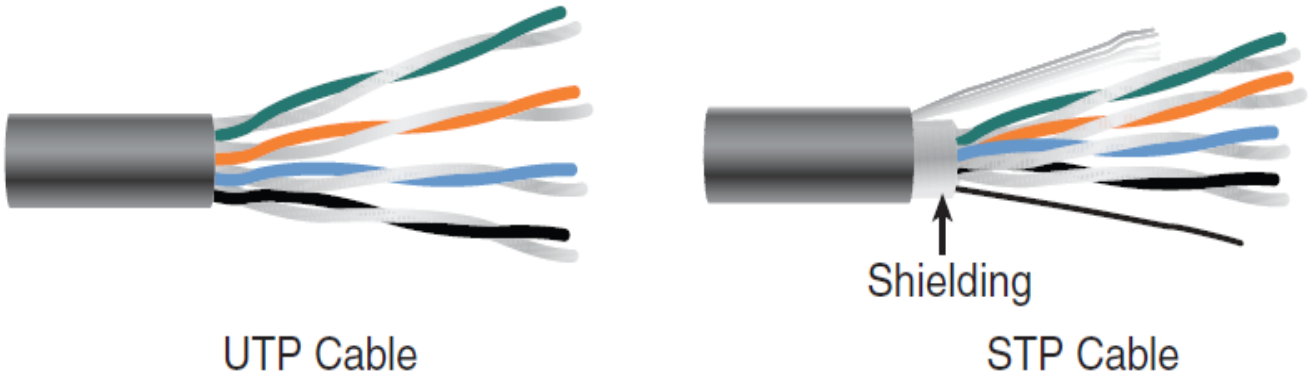
الوسط السلكي لنقل البيانات

الكابلات المجدولة (Twisted Pair)

هي كابلات نحاسية تنقل الإشارات كهربائياً. هي موجودة منذ زمن طويل وتم تصنيعها بشكل أساسي لنقل الصوت وتم استخدامها بشكل واسع في الاتصالات الهاتفية، وحالياً تستخدم أيضاً في الشبكات الحاسوبية بشكل رئيسي. يعود السبب وراء استخدامها الواسع إلى عدة أمور منها أنها أخف وزناً وأكثر مرونة وأسهل في التركيب من الكابلات المحورية والألياف الضوئية، وتعتبر أرخص من غيرها من وسائط النقل ويمكنها تحقيق سرعات عالية وهذه العوامل جعلتها الحل الأمثل لمعظم بيئات الشبكات. ويوجد حالياً نوعان منها: **UTP** و **STP**.

كابلات UTP غير المحجبة هي الأكثر استخداماً في معظم الشبكات، وأما STP تُستخدم في البيئات التي تحتاج إلى ممانعة عالية ضد EMI والتخميد، ولكن زيادة الممانعة تأتي على حساب التكلفة، وتحتاج STP إلى موصلات خاصة. تؤمن كابلات STP التحجيب (shielding) باستخدام مادة عازلة تكون حول الأسلاك داخل الكيبل، هذه الحماية تزيد من المسافة التي يمكن للإشارة أن تعبرها.

الشكل 6.1 يبين الكابلات المجدولة بنوعيها.



الشكل 6.1

يوجد عدة تصنيفات للكابلات المجدولة، هذه التصنيفات من **EIA/TIA** وهي منظمة تهتم بتطوير معايير المكونات الكهربائية والالكترونية والاتصالات والإنترنت، وتعد هذه المعايير ضرورية للتأكد من أن تكون الأجهزة والمكونات موحدة على مستوى العالم.

- Cat 3: يمكن من خلاله نقل البيانات بمعدل 10 Mbps مع عرض حزمة 16Mhz. غير مستخدم حالياً.
- Cat 4: يمكن من خلاله نقل البيانات بمعدل 16 Mbps مع عرض حزمة 20Mhz. غير مستخدم حالياً.
- Cat 5: يمكن من خلاله نقل البيانات بمعدل 100 Mbps مع عرض حزمة 100Mhz لمسافة تصل حتى 100 متر كحد أقصى.
- Cat 5e: يمكن من خلاله نقل البيانات بمعدل 1000 Mbps مع عرض حزمة 100Mhz كحد أدنى لمسافة تصل حتى 100 متر كحد أقصى.
- Cat 6: يمكن من خلاله نقل البيانات بمعدل 10 Gbpsمع عرض حزمة 250Mhz لمسافة تصل حتى 100 متر كحد أقصى.
- Cat 6a: يمكن من خلاله نقل البيانات بمعدل 100 Mbps مع عرض حزمة 500Mhz لمسافة تصل حتى 100 متر كحد أقصى.

الجدول6.1 يلخص أنواع الكابلات المجدولة والسرعات التي يدعمها.

الصف	السرعة (معدل النقل بالثانية الواحدة)
Cat 3	16 Mbps
Cat 4	20 Mbps
Cat 5	100 Mbps
Cat 5e	1000 Mbps
Cat 6	10 Gbps
Cat 6a	10 Gbps

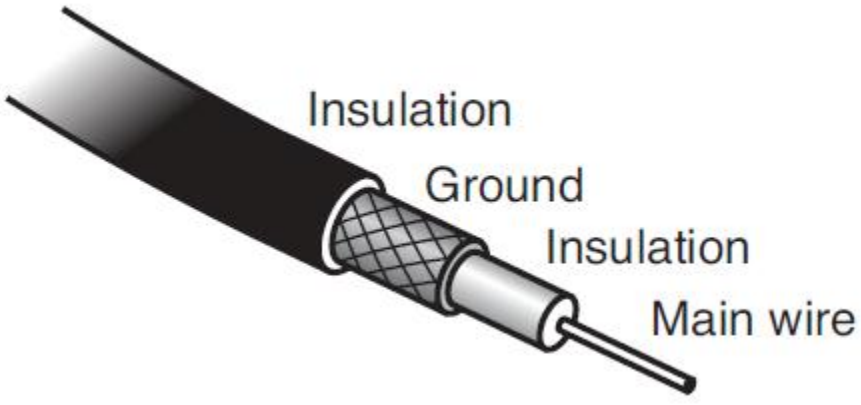
الجدول6.1

ملاحظة: هذه السرعات هي القيم النظرية أما القيم العملية تكون أقل من ذلك.

الكابلات المحورية (Coaxial Cable)

هي كابلات معروفة منذ زمن بعيد تُستخدم في نقل إشارات TV وإشارات الشبكات الحاسوبية. يتألف الكيبل المحوري من سلك نحاسي في المركز وهو الذي يحمل الإشارة ومعزول بمادة بلاستيكية، وفوقها مادة مُحجبة وتشكل الأرضي أيضاً. تم تصميم الكابلات المحورية بهذا الشكل لتضيف مقاومة أعلى للتخميد والتداخل الكهرطيسي (Crosstalk- EMI).

الشكل6.2 يبين الكابل المحوري



الشكل 6.2

يوجد نوعان من هذه الكابلات: **Thick** و**Thin** وهي الأكثر انتشاراً.

الجدول 6.2 يظهر عدة أنواع من النوع Thin

نوع الكيبل	الوصف
RG-59 /U	لا يُستخدم لمسافات طويلة بسبب الضياع الكبير فيه
RG-58 /U	يُستخدم في الاتصالات الراديوية والإنترنت 10Base2
RG-58 A/U	يُستخدم في الاتصالات الراديوية والإنترنت 10Base2
RG-58 C/U	يُستخدم للتطبيقات العسكرية
RG-6	يُستخدم لنقل إشارات TV وكابلات المودم

الجدول 6.2

كابلات الألياف الضوئية *Fiber Optic*

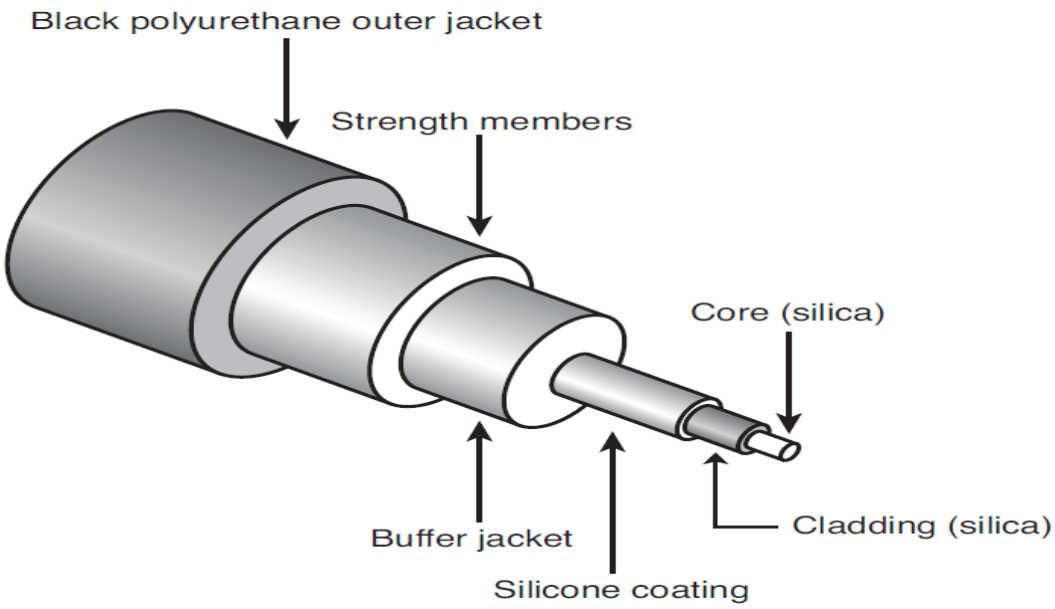
يتم نقل الإشارات فيه بشكل ضوئي عوضاً عن النبضات الكهربائية التي تستعملها الكابلات النحاسية ونتيجة لذلك فإن مشاكل النقل مثل التداخلات والتشويش والتخميد تصبح غير مهمة. يُستخدم هذا النوع من الكابلات لنقل البيانات والصوت والفيديو. هو أكثر أماناً وسرية من كل وسائط النقل لأنه حتى يمكن التنصت عليه يجب قطعه أولاً حيث أنه لا يصدر أي إشعاعات خارج الكيبل. ولكن رغم كل هذه الميزات فلا يُعتبر شائع الاستخدام في الشبكات الحاسوبية بسبب التكلفة المادية العالية جداً وصعوبة تركيبها وصيانتها، إضافة إلى عدم التوافق مع معظم المكونات الشبكة الحاسوبية.

يتألف الليف الضوئي من قلب زجاجي من السيلكا يُسمى النواة، وغلاف سيلكوني له خواص ضوئية تختلف عن خواص النواة (يقوم بعكس الإشارات الضوئية إلى الداخل)، ويتم تغليف الكيبل من طبقة بلاستيكية ومواد أخرى لتوفير الحماية من العوامل الخارجية.

يوجد نوعان من الألياف الضوئية:

- الليف المتعدد الأنماط (Multimode): تنتقل من خلاله عدة حزم من الضوء وهذا يُضعف الإشارات وينقص الطول الأعظمي والسرعة التي تنتقل بها الإشارة.
- الليف وحيد النمط (Single-mode): تنتقل من خلاله حزمة ضوء وحيدة وهذا يسمح بمسافة أطول وسرعة نقل أعلى.

الشكل 6.3 يبين كيبل ضوئي

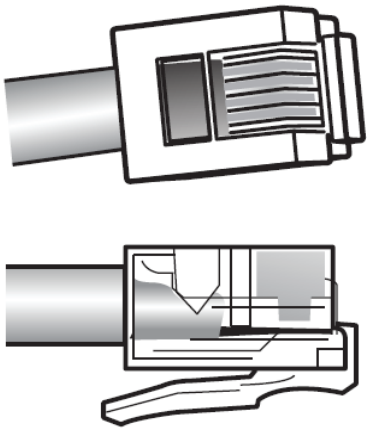


الشكل 6.3

أنواع موصلات الكابلات:

- موصلات BNC: تُستخدم مع الكابلات المحورية، لم تعد مشهورة كما كانت سابقاً ولكنها مازالت مستخدمة في بعض الشبكات.
- موصلات RJ-11: هي موصلات صغيرة بلاستيكية، تُستخدم في كابلات الهاتف يمكن أن تملك حتى 6 Pins ولكن لا تستخدم كلها في العادة، الهاتف يستخدم اثنان فقط .

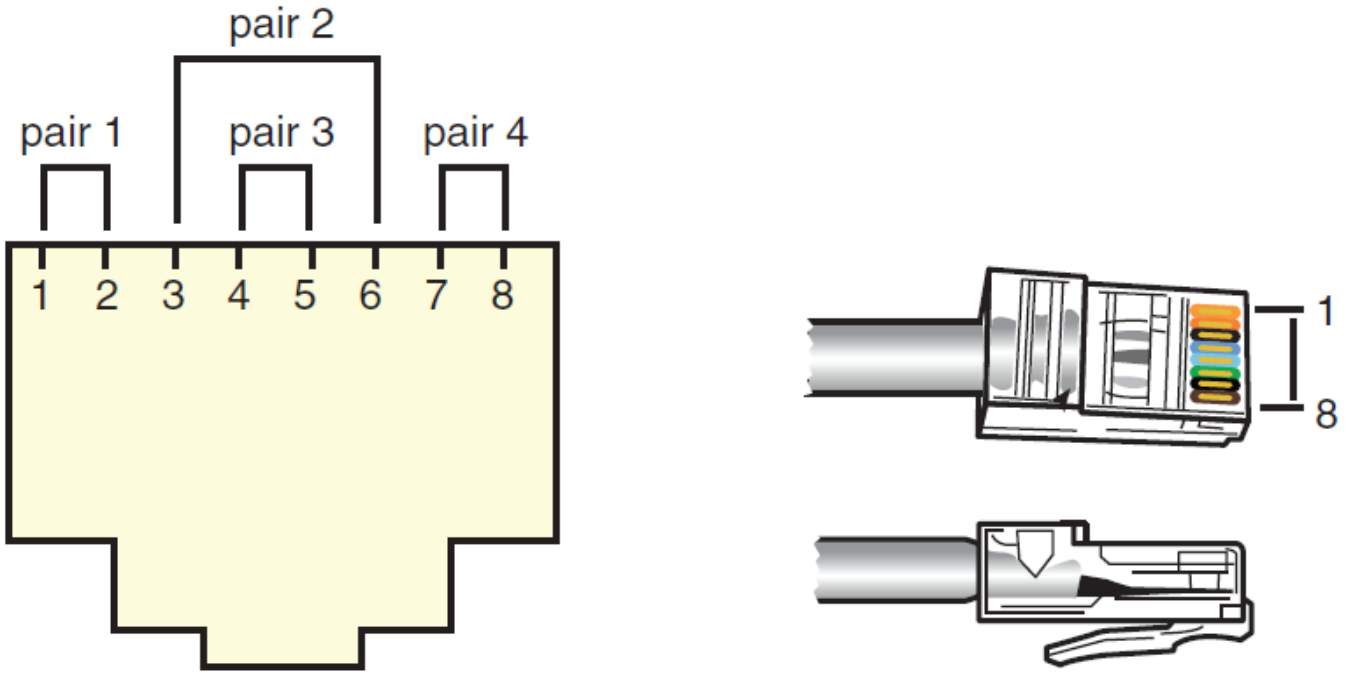
الشكل 6.4 يبين هذا النوع من الموصلات



الشكل 6.4

- موصلات RJ-45: هي الموصلات الأكثر انتشاراً. تُستخدم للكابلات المجدولة، تدعم حتى 8 أسلاك.
- موصلات الليف الضوئي: يوجد عدة أنواع منها ولكل منها استخداماته الخاصة وهي: ST – SC- LC- MT.RJ

الشكل6.5 يبين موصلات RJ45



الشكل 6.5

الفصل السابع
الشبكات اللاسلكية
Wireless Networks

هي الشبكات التي يتم فيها انتقال البيانات من خلال انتشار الموجات بدون استخدام الأسلاك. أصبحت الشبكات اللاسلكية هذه الأيام منتشرة بكثرة لما تقدمه من مرونة في الاتصالات، وأصبحت أحياناً تحل مكان الشبكات السلكية. يمكن اللجوء إلى استخدام الشبكات اللاسلكية في الأماكن التي يصعب مد الكابلات فيها، كالأماكن التاريخية والأماكن المزدحمة حيث تكون هي الخيار الأنسب.

تستخدم الشبكات اللاسلكية الإشارات ذات الترددات الراديوية RF للإرسال والاستقبال. إن الجهاز الذي يقوم بعملية الإرسال والاستقبال يُعرف باسم نقطة الوصول اللاسلكي (AP)، الذي يتصل بدوره مع الشبكة السلكية بكيبل وهو الذي يلعب دور جسر بين الأجهزة اللاسلكية وشبكة LAN السلكية. يمكن استخدام واحد أو أكثر من APs حسب حجم المنطقة المراد تأمين الوصول اللاسلكي إليها.

كل AP محدود بمدى الإرسال (Transmission Range) وهو المسافة التي يمكن للمستخدم استقبال إشارة مفيدة منAP.

المسافة العملية تعتمد على معيار اللاسلكي المُستخدم والشروط المحيطة بين المستخدم وAP.

التعامل مع AP

عند التعامل مع AP يجب إدراك بعض المصطلحات والاختصارات وأهمها:

- **SSID**: يشير إلى اسم الشبكة اللاسلكية، ويمكن إعداد AP بحيث يُنشر هذا الاسم ويسمح بذلك لكل العملاء في المنطقة من رؤية اسم الشبكة. ويمكن ضبطه بحيث لا يتم نشر هذا الاسم. وهذا يعني أن مسؤول الشبكة بحاجة إلى إعطاء اسم SSID للعملاء بدلاً من البحث عنه تلقائياً في أجهزتهم.
- **BSA**: يشير إلى منطقة تغطية AP، أي المنطقة التي يستطيع المستخدم استقبال إشارة لاسلكية مفيدة. وتختلف بحسب عدة عوامل منها قوة الهوائي – *التداخل في المنطقة – نوع الهوائي المستخدم _ وهل هو موجه أم غير موجه*.

حل مشاكل تغطية AP

- ❖ زيادة طاقة الإرسال: بعض AP تملك إعدادات لتغيير طاقة الإرسال. بشكل افتراضي معظم هذه الأجهزة تكون مضبوطة على طاقة الإرسال الأعلى، ولكن يمكن التحكم بطاقة الإرسال حيث أن إنقاص الطاقة يؤدي إلى إنقاص مساحة التغطية، وزيادتها تؤدي إلى مساحة تغطية أوسع.
- ❖ تغير مكان AP: إن تغير مكان AP إلى مكان مناسب بشكل أكثر، يؤدي إلى تحسن ملحوظ بمدى التغطية.
- ❖ تعديل أو تغير الهوائي: إن استبدال الهوائي بهوائي أفضل يؤدي إلى تحسن في مدى التغطية، ولكن لسوء الحظ ليس كل AP يملك إمكانية استبدال الهوائي الخاص به.
- ❖ استخدام المكرر (Repeater): إن استخدام مكرر للإشارة يؤدي إلى زيادة المسافة التي يمكن للإشارة أن تقطعها، ولكن يجب الانتباه إلى أن نستخدم القناة نفسها المُستخدمة في AP.

هوائيات الإشارة اللاسلكية

هي جزء أساسي من كل منظومات الاتصالات اللاسلكية، وتأتي بعدة أشكال وحجوم وكل واحد من هذه التصاميم مخصص لهدف محدد. إن اختيار الهوائي المناسب يقرر نجاح الشبكة اللاسلكية ويوفر من التكلفة المادية لها.

خصائص الهوائيات

ربح الهوائي (Antenna Gain)

يمكن أن يكون الهوائي غير موجه (Isotropic) أي أنه يشع الأمواج في كل الاتجاهات، وكأنه يشكل كرة حول الهوائي. هذا النوع من الهوائيات يكون ربحه 0db. أما إذا كان الهوائي يشع الأمواج في اتجاه معين فيسمى عندئذ الهوائي المَوجه، ويكون له قيمة معينة من الربح.

منطقة التغطية للهوائي (Antenna Area)

إن نوع الهوائي يحدد منطقة التغطية. فالهوائيات غير الموجه تُستخدم لجعل التغطية في كل الاتجاهات، تكون الإشارة ضعيفة لأنها تنتشر في كل الاتجاهات وهذا مناسب لتطبيقات البيوت والمكاتب الصغيرة.

أما الهوائيات الموجه تكون مصممة لتركيز الإشارة في مجال محدد، وهذا التركيز يؤدي إلى زيادة المسافة المقطوعة. يُستخدم هذا النوع للربط بين نقطتين (بين بنائين على سبيل المثال).

الاستقطاب في عالم الأمواج اللاسلكية يشير إلى الاتجاه الذي تأخذه الأمواج – *يمكن أن يكون عمودي أو أفقي أو دائري* – ويجب على هوائي الإرسال والاستقبال أن يكون بنفس الاستقطاب.

الجدول 7.1 يبين مقارنة بسيطة بين الهوائيات الموجهة وغير الموجهة

الخاصية	الهوائي غير الموجه	الهوائي الموجه	الميزات والسيئات
منطقة التغطية اللاسلكية	منطقة تغطية عامة	منطقة تغطية مركزة	الهوائي غير الموجه يسمح بتغطية 360 درجة، وهذا يؤدي إلى منطقة تغطية واسعة
مدى الإرسال	محدود	مدى طويل	الهوائي الموجه له منطقة تغطية في كل الاتجاهات، وهذا يؤدي إلى ضعف بالإشارة وبالتالي منطقة محدودة. أما الموجه يركز إرسال الأشعة ويسمح بمدى أوسع
شكل منطقة التغطية	له شكل محدد	يمكن أن يتغير	الهوائي غير الموجه يشكل حوله منطقة تغطية كروية، أما الموجه يمكن تعديله ليأخذ شكل محدد (عريض أو أكثر تركيزاً)

الجدول 7.1

جودة الإشارة اللاسلكية (Wireless Signal Quality)

إن الإشارات اللاسلكية تسافر عبر الجو، وبالتالي فإنها ستتعرض لعوامل مختلفة وسيؤدي ذلك إلى إضعاف قوتها أو انخفاض جودتها. من العوامل التي تؤثر على جودة الإشارة اللاسلكية العواصف والمطر والجدران والرطوبة وغير ذلك من العوائق في طريق الإشارة اللاسلكية.

أيضاً أحد العوامل التي تسبب في إنقاص جودة الإشارة هو التداخل، لذلك يجب أن تبقى الأجهزة اللاسلكية بعيدة عن التجهيزات التي تصدر إشارات RF مثل المايكروويف والأجهزة الكهربائية وخصوصاً التي تستعمل التردد نفسه مثل الهواتف اللاسلكية.

إطار المرشد اللاسلكي (Beacon): هو مجموعة من المعلومات يتم إرسالها بشكل دوري من جهاز الإرسال اللاسلكي (AP) إلى منطقة التغطية اللاسلكية ويحوي هذا الإطار المعلومات التالية: معلومات عن القناة المستخدمة – معدل نقل البيانات – اسم الشبكة SSID – معلومات التزامن. في الأحوال العادية يتم إرسال هذا الإطار كل 10 ms. تسمح بعض أجهزة AP بتغيير هذه القيمة وهذا مناسب لشبكات البيوت لأنها غير مهمة في هذه الحالة.

تكتشف الأجهزة اللاسلكية هذه المعلومات تلقائياً لتتصل بالشبكة.

معايير الشبكات اللاسلكية (Wireless Standards)

إن معايير الشبكة اللاسلكية يمكن أن تختلف في أمور مثل السرعة – مدى النقل – التردد المستخدم ولكن البنية الفعلية متشابهة وتستخدم البروتوكولات نفسها.

- ❖ IEEE 802.11: سرعة نقل البيانات بطيئة جداً (1 -2 Mbps) وتستخدم التردد 2.4 Ghz. لم يعد مستخدماً هذه الأيام لأنه غير مناسب للشبكات الحديثة.
- ❖ IEEE 802.11a: سرعة نقل البيانات تصل إلى 54Mbps وعرض حزمة 5Ghz. هذا المعيار متوافق مع IEEE 802.11b وIEEE 802.11g .
- ❖ IEEE 802.11b: سرعة نقل البيانات تصل إلى 11Mbps وعرض حزمة 2.4 Ghz تم تصميم هذا المعيار للتكامل العكسي مع المعيار 802.11 أي ليتوافق معه.
- ❖ IEEE 802.11g: سرعة نقل البيانات تصل إلى 54Mbps وعرض حزمة 2.4Ghz يصل مدى الإرسال إلى 150 قدم.
- ❖ IEEE 802.11n: هو المعيار الأحدث وهو الأكثر انتشاراً هذه الأيام، الهدف من هذا المعيار هو زيادة معدل نقل البيانات في كلا مجالين التردد 2.4 GHZ و 5GHZ. سرعة نقل البيانات فيه 100 Mbps ولكن في حال توافر الشروط الجيدة تصل إلى 600 Mbps.

ملاحظة: السرعات العملية أقل من السرعات النظرية بكثير.

دراسة المعيار IEEE 802.11n

تم في هذا المعيار دمج بعض الميزات الجديدة للحصول على مستوى جديد من الاتصالات اللاسلكية، أول هذه الميزات المدمجة هي تقنية هوائيات **MIMO** والميزة الأخرى هي دمج القنوات.

تقنية MIMO: هي التطور الأكبر في هذا المعيار وهي المفتاح لسرعات أعلى. هي اختصار لـ (Multiple Input Multiple Output). أي الاتصال المتعدد عند الإرسال وعند الاستقبال. تقوم هذه التقنية بدمج عدة إشارات لنقلها عبر خط نقل واحد، أي تستطيع نقل عدة إشارات بيانات من هوائيات مختلفة عبر الخط نفسه وبالوقت نفسه، وهذا يحقق معدلات نقل أعلى من نظام الهوائي الواحد. وكلما ازداد عدد الهوائيات ازداد معدل النقل.

تقنية دمج قنوات الاتصال: تؤدي هذه التقنية إلى مضاعفة معدل نقل البيانات. يمكن من خلال المعيار IEEE 801.11n دمج قناتين 20 MHZ في قناة واحدة لتصبح 40 MHZ. في حين أن المعايير IEEE 802.11b/g تستخدم قناة واحدة بعرض 20MHZ.

ملاحظة: إن دمج القنوات يؤدي إلى عدم إمكانية التوافق مع المعايير السابقة.

الجدول 7.2 يلخص المعاير المستخدمة في الشبكات اللاسلكية.

المعيار	التردد المستخدم	السرعة	مدى الإرسال	طريقة النقل
IEEE 802.11	2.4 GHZ	1-2 Mbps	20 feet	DSSS/FHSS
IEEE 802.11a	5GHZ	Up to 54 Mbps	Up to 75 feet	OFDM
IEEE 802.11b	2.4 GHZ	Up to 11 Mbps	Up to 150 feet	DSSS
IEEE 802.11g	2.4 GHZ	Up to 54 Mbps	Up to 150 feet	DSSS
IEEE 802.11n	2.4 / 5 GHZ	Up to 600 Mbps	Up to175 feet	OFDM

الجدول 7.2

أمان الشبكات اللاسلكية (Wireless Security)

WEP: هي أولى المحاولات لجعل الشبكات اللاسلكية آمنة ومحمية، تؤمن هذه الطريقة مستوى من الأمان بشكل مماثل للشبكات السلكية، تم إنتاج هذه الطريقة عام 1997. باستخدام WEP فإن كل رزمة من البيانات التي تُرسل عبر الشبكة سيتم تشفيرها، تم استخدام خوارزمية التشفير RC4 بـ 40 بت في البداية ثم 128 بت.

هذه الطريقة سهلة الإعداد ولكن في المقابل سهلة الكسر.

WPA: تم تطوير هذه الطريقة لتغطية نقاط الضعف في طريقة WEP، وتكون متوافقة مع الأجهزة القديمة التي تستخدم طريقة WEP.

WPA2: تقدم هذه الطريقة أماناً أكثر للشبكة اللاسلكية.

العوامل التي تُؤثر على الإشارات اللاسلكية

بما أن الإشارات اللاسلكية تمر عبر الهواء فإنه تتعرض لأنواع مختلفة من التداخل أكثر من الشبكات السلكية.

العوائق الفيزيائية (Physical objects)

الأشجار والأبنية والجدران وكل الأشياء ذات البنية الفيزيائية، وتأثير هذه العوائق يختلف حسب نوع وكثافة المواد فيها، حيث يُعتبر الحديد والإسمنت من المواد التي يصعب على الإشارات اللاسلكية عبورها.

التداخل مع الإشارات الأخرى

إن الإشارات اللاسلكية المستخدمة في الشبكات تستخدم التردد 2.4GHZ والعديد من الأجهزة اللاسلكية تستخدم التردد نفسه مثل المايكرويف والهاتف اللاسلكي، وهذا يسبب ضجيج وضعف في الإشارة.

التشويش الكهرطيسي

ينتج هذا التشويش من الأجهزة الكهربائية مثل الكومبيوتر والبراد والمراوح ولمبات الإضاءة وغيرها من الأجهزة التي تحتوي على محركات. وتأثير هذا التشويش يعتمد على قرب هذه الأجهزة من جهاز البث اللاسلكي، مع العلم أن الأجهزة الحديثة أنقصت التشويش الذي يصدر عنها.

العوامل البيئية

إن الأحوال الجوية يمكن أن تؤثر بشكل كبير على جودة الإشارة اللاسلكية، فيمكن للمطر أو الضباب أن يضعف من هذه الإشارات.

الجدول 7.3 يبين بعض الأمثلة عن العوائق التي تُوجد في المنزل

العائق	درجة الإعاقة	استخدام العائق
الخشب	قليل	محيط بالجدران الداخلية
الجبس	قليل	داخل الجدران
الأثاث	قليل	الغرف والأسرَة
الزجاج الصافي	قليل	النوافذ
الزجاج الملون	وسط	النوافذ
الأشخاص	وسط	مناطق الازدحام
البلاط السيراميكي	وسط	الجدران

الجدران الإسمنتية	وسط / عالي	الجدران الداخلية
المرايا	عالي	المرايا - الزجاج العاكس
المعادن	عالي	مفروشات المكاتب المعدنية - الحواجز المعدنية الداخلية
الماء	عالي	الأمطار – حوض السمك – النافورة

الجدول 7.3

الإعدادات التي يمكن التحكم بها في AP

- ❖ اسم الشبكة اللاسلكية (SSID): وهو الاسم الذي يميز شبكة عن أخرى ويستطيع المستخدمين من خلاله الدخول إلى الشبكة المطلوبة.
- ❖ قناة الاتصال (Chanel): وهي المجال المخصص من الترددات لنقل البيانات ويجب على كل الأنظمة المتصلة مع بعضها في الشبكة أن تعمل على القناة نفسها.
- ❖ نشر اسم الشبكة (SSID Broadcast): في حال تم تفعيلها (وهي الحالة الافتراضية في معظم الأجهزة) سيتم نشر اسم الشبكة مما يسمح للجميع من اكتشاف الشبكة والوصول السهل إليها ولكن ذلك يسبب ضعف في سرية الشبكة.
- ❖ المصادقة (Authentication): هي طريقة للتحقق من أن من يدخل إلى الشبكة اللاسلكية مسموح له بالدخول، ويوجد عدة أنواع من هذا التحقق وهي WEP-OPEN WEP-Shared وWPA_psk سيتم مناقشة هذه الأنواع فيما بعد.
- ❖ المعيار اللاسلكي (Wireless Mode): حيث يوجد عدة معايير وهي IEEE 802.11 a/b/g/n والأسرع والأكثر استخداماً هو IEEE 802.11n. يجب على المستخدم أن يعمل بالمعيار نفسه الذي يعمل به AP أو أقل منه.
- ❖ فترة DTIM (DTIM period): هي معدل إرسال رسالة إلى الأجهزة المرتبطة بالشبكة لإبقائها جاهزة لاستقبال رسائل البث الإذاعي (Broadcast) فإذا كانت قيمة هذه الفترة 1 – وهي القيمة الافتراضية – هذا يعني أنه سيتم إرسال رسالة تنبيه لأجهزة الشبكة عند كل beacon.
- ❖ معدل الإرسال (transfer rate): يتم ضبطها بشكل افتراضي على القيمة التلقائية (Auto) وهذا يسمح بسرعة اتصال أعظمية، ولكن يمكن إنقاص هذه القيمة لزيادة المسافة التي تقطعها الإشارة ودعم قوة الإشارة في حالة الظروف السيئة.

الفصل الثامن
إدارة الشبكات
Network Management

إن الأمور الأساسية في إدارة الشبكة هي توثيق الشبكة واستخدام أدوات مراقبة أداء الشبكة وصيانتها

أدوات الشبكة

العمل مع الأوامر السطرية Command –Line

ping	تُستخدم لفحص الاتصال بين جهازين في الشبكة باستخدام ICMP
IPconfig	تُستخدم لرؤية وتجديد إعدادات TCP/IP على أنظمة ويندوز
arp	تُستخدم لإظهار والعمل مع ذاكرة الكاش التي تحوي معلومات تحويل عناوين IP إلى MAC
arp ping	تُستخدم لفحص الاتصال بين جهازين في الشبكة باستخدام ARP عوضاً عن ICMP
tracert	تُستخدم لملاحقة المسار الذي أخذته رزمة البيانات أثناء عبورها عبر الشبكة
netstat	تُستخدم لرؤية اتصالات TCP /IP الحالية في النظام .
nbstat	تُستخدم لعرض الاحصائيات والمعلومات حول أسماء Netbios
Nslookup	تُستخدم لإجراء عملية DNS يدوية
route	تُستخدم لعرض وإعداد المسارات في جدول التوجيه

ملاحظة: معظم الأدوات تملك لواحق فرعية يمكن عرضها بكتابة /? بعد الأداة . مثال Netstat /? <<.

أداة ping

إن هذه الأداة شائعة الاستخدام وتعتبر من الأعمال اليومية لأي مسؤول شبكة. المهمة الرئيسية لتعليمة ping هو **فحص الاتصال** بين جهازين في الشبكة لمعرفة إذا ما كانا يستطيعان رؤية بعضهما والمدة الزمنية التي يحتاجها هذا الاتصال. ويتم ذلك من خلال إرسال أربعة طلبات وانتظار صداها من الجهاز الهدف.

الصيغة العامة لتعليمة ping هي: ping *عنوان الجهاز الهدف*

مثال: >> ping 192.168.1.2

ملاحظة: يمكن استخدام اسم الجهاز الوجهة بدل عنوان IP ولكن بشرط وجود طريقة لتحويل الأسماء إلى عناوين IP أي وجود DNS أو Netbios لشبكات ويندوز.

الجدول 8.2 يعرض بعض اللواحق لتعليمة ping.

التعليمة	الوصف
Ping –t	فحص الاتصال بشكل مستمر حتى يتم إيقافه
Ping –a	ترجمة العنوان إلى اسم الجهاز
Ping –n count	فحص الاتصال بعدد محدد من الطلبات (count)
Ping –4	اجبار النظام على استخدام عنوان IPv4
Ping –6	اجبار النظام على استخدام عنوان IPv6

الجدول 8.2

تعتمد التعليمة ping على البروتوكول ICMP لإرسال 4 رسائل إلى الجهاز الهدف، فإذا سمع الجهاز هذه الطلبات سيقوم تلقائياً بالرد عليها بإرسال 4 استجابات، ولكن في بعض الحالات توجد مشكلة ما فلا يتم الرد على هذه الطلبات المُرسلة ويعطي رسائل خطأ.

رسائل الخطأ عند استخدام تعليمة ping:

- رسالة The Destination Host Unreachable: هذه الرسالة تعني أن المسار بين إلى الجهاز الهدف لم يتم إيجاده ولحل هذه المشكلة يجب فحص إعدادات البوابة الافتراضية أو إعدادات TCP /IP للجهاز.

- رسالة Request timed out: هذه الرسالة تعني أن الجهاز المرسل لا يستقبل رد على رسائله من الجهاز الهدف ضمن الفترة الزمنية المخصصة للرد ويمكن أن تكون المشكلة أحد الاحتمالات التالية:

- ❖ جهاز الوجهة غير متصل بالشبكة.
- ❖ جهاز الوجهة مُطفأ.
- ❖ إعدادات جهاز الوجهة غير صحيحة.
- ❖ بعض الأجهزة الوسيطة لا تعمل بشكل صحيح.
- ❖ يوجد ازدحام شديد بالشبكة بحيث يسبب تأخير زمني يتجاوز الزمن المحدد (هذا احتمال نادر).

❖ عنوان IP للوجهة غير صالح.

- رسالة Unknown Host: هذه الرسالة تعني أن اسم الجهاز الوجهة لا يمكن ترجمته ويكون السبب عادة في نظام تحويل الأسماء إلى عناوين (DNS - WINS)

رسالة Expired TTL :

استعمال أداة ping في اصلاح الشبكة

يمكن استخدام هذه الأداة للمساعدة في عزل المشكلة وعرفة أين تقع المشكلة، واتباع الخطوات التالية يساعد في معرفة المشكلة:

1. التأكد من إعدادات TCP/IP على الجهاز باستخدام التعليمة >>ping 127.0.01 حيث أن 127.0.0.1 هو عنوان الحلقة الخلفية المحلية (Loopback) وفي حال استخدام IPv6 يكون عنوانها 0:: .
2. التأكد من التثبيت الصحيح لكرت الشبكة (NIC) وذلك عن طريق استخدام تعليمة ping للعنوان المثبت على كرت الشبكة للجهاز.
3. التأكد من أن الجهاز يستطيع رؤية باقي الأجهزة ضمن الشبكة وذلك عن طريق استخدام تعليمة ping لأي جهاز في الشبكة.
4. التأكد من الجهاز قادر على الاتصال بجهاز بعيد وذلك عن طريق استخدام تعليمة ping لأي جهاز خارج الشبكة (الإنترنت مثلاً)، وبذلك يتم التأكد من سلامة إعدادات البوابة الافتراضية.

ملاحظة: يمكن تجريب الخطوة الرابعة بدايةً فإذا كانت صحيحة هذا يعني أن كل الخطوات السابقة صحيحة.

تعليمة IPconfig

تُستخدم هذه التعليم لعرض إعدادات TCP / IP لأنظمة **ويندوز**. عند استخدامه تظهر المعلومات الأساسية مثل عنوان IP وقناع الشبكة والبوابة الافتراضية وعند استخدام IPconfig /all ستظهر تفصيلات أكثر.

الجدول 8.3 يظهر بعض الحلول للمشاكل الشائعة باستخدام المعلومات التي تعرضها التعليمة IPconfig /all

الحالة	الحقل الذي يجب تفحصه
المستخدم لا يستطيع الاتصال بأي نظام آخر	التأكد من صحة عنوان IP وقناع الشبكة. إذا كانت الشبكة تستخدم DHCP يجب التأكد من تفعيل ميزة DHCP
المستخدم يستطيع الاتصال بأي نظام داخل الشبكة نفسها ولكن لا يستطيع الاتصال بنظام بعيد	التأكد من أن البوابة الافتراضية تم إعدادها بشكل صحيح.
المستخدم لا يستطيع تصفح الإنترنت	التأكد من أن مخدم DNS تم إعداده بشكل صحيح

الجدول 8.3

الجدول 8.4 يعرض بعض اللواحق لتعليمة IPconfig.

/?	تعرض شاشة المساعدة
/all	تعرض معلومات إضافية
/release	تحرير عنوان IPv4 لكرت الشبكة
/ release 6	تحرير عنوان IPv6 لكرت الشبكة
/renew	تجديد عنوان IPv4
renew6	تجديد عنوان IPv6
/flushdns	مسح ذاكرة الكاش لـ DNS
/displaydns	عرض معلومات عن ذاكرة cash لـ DNS
/registerdns	إعادة استئجار DHCP وإعادة التسجيل في DNS

الجدول 8.4

ملاحظة: تعليمة IPconfig /release و تعليمة IPconfig /renew تُستخدم فقط عندما تكون الشبكة تستخدم مخدم DHCP.

ملاحظة: في أنظمة Linux تُستخدم التعليمة ifconfig عوضاً عن IPconfig .

تعليمة arp

إن بروتوكول ARP مهم جداً في الشبكة لأنه يقوم بتحويل عناوين IP المنطقية إلى عناوين MAC الفيزيائية. حيث أن الاتصالات بين الأجهزة في الشبكة تحتاج إلى عناوين MAC.

عندما يريد حاسب إرسال بيانات إلى حاسب آخر في الشبكة فإنه بحاجة إلى الحصول على عنوان MAC للحاسب الوجهة، ولاكتشاف هذا العنوان يقوم بروتوكول ARP بإرسال رسائل اكتشاف لتحصل على عناوين MAC

للأجهزة المتصلة بالشبكة، عندما يتم إيجاد الحاسب المطلوب يُرسل عنوانه الفيزيائي إلى الحاسب المُرسل، ويتم إضافة هذه المعلومات في ذاكرة تخزين مؤقت هي ذاكرة الكاش (ARP cash)، يوجد بداخل هذه الذاكرة قائمة بعناوين IP وما يقابلها من العناوين الفيزيائية MAC.

يتم فحص هذه الذاكرة أولاً قبل إرسال رسائل الاكتشاف لتحديد إذا كانت المعلومات المطلوبة موجودة فيها، وإلا يتم إرسال رسائل الاكتشاف.

المدخلات في هذه الذاكرة يمكن إضافتها يدوياً، وبهذه الطريقة ستبقى دائمة حتى يتم حذفها. أو يمكن إضافتها بشكل ديناميكي، وذلك عندما يقوم نظام بالاتصال بنظام آخر في الشبكة.

الجدول 8.5 يعرض بعض اللواحق لتعليمة arp

اللاحقة	الوصف
/?	يعرض خيارات تعليمة arp
-a أو -g	يعرض قائمة بالعناوين المنطقية وما يقابلها من عناوين فيزيائية المخزنة في ذاكرة (arp cash) ونوعها إذا كانت ستاتيكية أو ديناميكية
-s	إضافة مُدخل إلى الذاكرة بشكل ستاتيكي
-d	حذف مدخل من الذاكرة
-N if_addr	عرض محتويات ذاكرة arp لكرت شبكة محدد .حيث if_addr هو عنوان كرت الشبكة المقصود.

الجدول 8.5

تعليمة ping arp

إن أسهل طريقة لفحص الاتصال بين جهازين في الشبكة هو استخدام التعليمة ping، والتي تستخدم البروتوكول ICMP لإجراء الاتصال، ولكن في بعض الحالات ولأسباب تتعلق بأمان الشبكات يتم استخدام الجدار الناري أو أجهزة أخرى تقوم بحجب طلبات ICMP وتمنعها من المرور، وهذا يخفف من المخاطر الأمنية المتعلقة باختراق الشبكة وتمنع حدوث أحد أنواع الهجمات الذي يُسمى (ping attack)، حيث يقوم المهاجمون بإرسال مستمر لطلبات ping إلى مخدم محدد مما يؤدي إلى إنهاك مصادر النظام بالرد على هذه الطلبات، ويجعله غير قادر على الاستجابة للطلبات من أنظمة أخرى.

إذاً في الحالات التي يتم حجب طلبات ICMP لا يمكن استخدام التعليمةping. ولكن يوجد طريقة أخرى هي arpping حيث أن هذه الأداة لا تستخدم بروتوكول ICMP ولكن تستخدم بروتوكولARP عوضاً عنه. إن بروتوكول ARP غير قابل للتوجيه (Routable) أي لا يستطيع العمل في شبكات متفرقة، ويعمل فقط في الشبكات المحلية. إن أداة arp ping غير مدمجة في أنظمة ويندوز، ولكن يمكن تحميل عدد من البرامج التي تسمح باستخدامها مثل برنامج Hardping v1.11.

تعليمة tracert

هي أداة لتعقب الأثر حيث إنها تتبع أثر المسار بين جهازين وتكتب معلومات حول كل خطوة من رحلة البيانات بين الجهازين، ويتم ذلك باستخدام رسائل ICMP، كل الأنظمة تؤمن هذه الأداة ولكن اسم التعليمة والنتيجة التي تعرضها تختلف من نظام لآخر.

الصيغة العامة لهذه التعليمة في أنظمة التشغيل المختلفة

نظام التشغيل	الصيغة
Windows	tracert IPadress
Linux	traceroute IP address
MACintosh	traceroute IP address

تقدم هذه التعليمة معلومات مفيدة مثل عنوان كل راوتر مرت البيانات من خلاله، وفي بعض الحالات اسم الراوتر (ذلك يعتمد على إعدادات الراوتر نفسه)، ومعلومات عن الفترة الزمنية مقدرة بالميلي ثانية (ms) للرحلة الدائرية لرزمة البيانات من المصدر إلى الراوتر ثم العودة إلى المصدر. هذه المعلومات يمكن أن تساعد في معرفة مكان الضعف في الشبكة.

مثال عن تعليمة tracert :

```
C:\>tracert 24.7.70.37
Tracing route to c1-p4.sttlwa1.home.net [24.7.70.37]
over a maximum of 30 hops:
1 30 ms 20 ms 20 ms 24.67.184.1
2 20 ms 20 ms 30 ms rd1ht-ge3-0.ok.shawcable.net
[24.67.224.7]
3 50 ms 30 ms 30 ms rc1wh-atm0-2-1.vc.shawcable.net
[204.209.214.193]
4 50 ms 30 ms 30 ms rc2wh-pos15-0.vc.shawcable.net
[204.209.214.90]
5 30 ms 40 ms 30 ms rc2wt-pos2-0.wa.shawcable.net
```

العمود الأول يشير إلى عدد القفزات، الأعمدة الثلاثة اللاحقة تشير إلى الزمن الذي استغرقته رزمة البيانات لتصل إلى الوجهة. العمود الأخير هو اسم المضيف وعنوانIP الذي قام بالرد.

تعليمة netstate

تعرض هذه التعليمة احصائيات بروتوكولات اتصالات TCP / IP الحالية في النظام.

الجدول 8.6 يعرض بعض اللواحق لتعليمة netstat

التعليمة	الوصف
/?	تعرض شاشة المساعدة
-a	تعرض حالة منافذ الاتصالات
-e	تعرض احصائيات البيانات المتبادلة مع الإنترنت
-n	تعرض قائمة بالعناوين وأرقام المنافذ بصيغة عددية
-p protocol	تعرض الاتصالات من أجل بروتوكول محدد
-r	تعرض جدول التوجيه
-s	تعرض معلومات احصائية عن كل بروتوكول

الجدول 8.6

التعليمة netstat بدون أي لاحقة تُظهر أربع أنواع من المعلومات كما في المثال

```
C:\>netstat
Active Connections
Proto Local Address Foreign Address State
TCP laptop:2848 MEDIASERVICES1:1755 ESTABLISHED
TCP laptop:1833 www.dollarhost.com:80 ESTABLISHED
TCP laptop:2858 194.70.58.241:80 ESTABLISHED
TCP laptop:2860 194.70.58.241:80 ESTABLISHED
TCP laptop:2354 www.dollarhost.com:80 ESTABLISHED
TCP laptop:2361 www.dollarhost.com:80 ESTABLISHED
TCP laptop:1114 www.dollarhost.com:80 ESTABLISHED
TCP laptop:1959 www.dollarhost.com:80 ESTABLISHED
```

```
TCP laptop:1960 www.dollarhost.com:80 ESTABLISHED
TCP laptop:1963 www.dollarhost.com:80 ESTABLISHED
TCP laptop:2870 localhost:8431 TIME_WAIT
TCP laptop:8431 localhost:2862 TIME_WAIT
TCP laptop:8431 localhost:2863 TIME_WAIT
TCP laptop:8431 localhost:2867 TIME_WAIT
TCP        laptop:8431        localhost:2872        TIME_WAIT
```

Proto: قائمة بالبروتوكولات المستخدمة سواءً كانت TCP أو UDP.

Local adress: عنوان الحاسب المحلي ورقم المنفذ المستخدم.

Foreign address: عنوان الهدف ورقم المنفذ المستخدم.

State: حالة الاتصال فيما غذا كان قائم أم غير ذلك.

التعليمة netstat -e

تظهر نشاط كرت الشبكة (NIC) وتعرض عدد رزم البيانات التي تم إرسالها واستقبالها

مثال:

```
C:\WINDOWS\Desktop>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      17412385          40237510
Unicast packets               79129             85055
Non-unicast packets             693               254
Discards                          0                 0
Errors                            0                 0
Unknown protocols               306
```

- Bytes: عدد البايتات التي أرسلها واستقبلها كرت الشبكة منذ تشغيل الحاسب.
- Unicast packets: عدد رزم البيانات المرسلة والمستقبلة مباشرة من خلال هذا الكرت.
- Non-unicast packets : عدد رزم البيانات المرسلة والمستقبلة عن طريق Broadcast و Multicast
- Discards: عدد رزم البيانات التي لم يقبلها كرت الشبكة، يمكن أن يرفضها لأنها مدمرة.
- Errors: الأخطاء التي تحدث أثناء عملية الإرسال والاستقبال، هذا العدد يجب أن يكون قليل وإلا يعني وجود مشكلة في الشبكة.
- Unknown protocols: عدد رزم البيانات التي لا يستطيع النظام التعرف عليها.

تعليمة Netstat –r

تُستخدم غالباً لعرض جدول التوجيه

مثال

```
C:\WINDOWS\Desktop>netstat -r
Route table

===========================================================================
=====
===========================================================================
=====
Active Routes:
Network Destination        Netmask          Gateway       Interface
Metric
          0.0.0.0          0.0.0.0      24.67.179.1    24.67.179.22
1
      24.67.179.0    255.255.255.0    24.67.179.22    24.67.179.22
1
     24.67.179.22  255.255.255.255        127.0.0.1       127.0.0.1
1
   24.255.255.255  255.255.255.255    24.67.179.22    24.67.179.22
1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1
1
        224.0.0.0        224.0.0.0    24.67.179.22    24.67.179.22
1
  255.255.255.255  255.255.255.255    24.67.179.22               2
1
Default Gateway:       24.67.179.1
===========================================================================
=====
Persistent Routes:
  None
```

ملاحظة: المعلومات التي يعرضها netstat –r هي نفسها التي تعرضها rout print.

التعليمة nbtstat

تُستخدم لعرض معلومات وإحصاءات عن NetBios . وهذه التعليمة خاصة بأنظمة ويندوز لأن أسماء NetBios متاحة فقط لأنظمة ويندوز.

الجدول 8.7 يعرض بعض اللواحق لتعليمة nbtstst

التعليمة	الوصف
nbtstat -a	تعرض جدول بأسماء NetBios وعناوينMAC المقابلة
nbtstat -A (IP adress)	تعرض أسماء الأجهزة البعيدة التي تأخذ عنوان IP
nbtstat –c (cache)	تعرض محتوات ذاكرة الكاش الخاصة بأسماءNetBios
nbtstat –n (names)	تعرض أسماء NetBios المحلية
nbtstat –R (Reload)	مسح وإعادة تحميل جدول أسماء NetBios

الجدول 8.7

تعليمة nslookup

هي أداة تُستخدم لحل المشاكل المتعلقة بـ DNS، حيث تعطي معلومات حول إعدادات DNS للنظام (اسم المخدم وعنوانه) وهي خاصة بأنظمة ويندوز، أما في أنظمة Linux – Unix –Macintosh تُستخدم التعليمة: dig .

تعليمة route

يمكن من خلالها إظهار وتعديل جدول التوجيه في أنظمة ويندوز وLinux

الجدول 8.8 يعرض بعض اللواحق لتعليمة route

اللاحقة	الوصف
Add	إضافة مسار بشكل يدوي إلى جدول التوجيه
Delete	حذف مسار بشكل يدوي من جدول التوجيه
Change	تعديل مسار بشكل يدوي من جدول التوجيه
-p	بدون هذه اللاحقة ستكون إضافة مسار إلى جدول التوجيه مؤقتة وسيتم حذفها عند اول عملية إقلاع للجهاز، أما باستخدامها فسيكون إدخال المسار بشكل دائم.
Print	عرض جدول التوجيه للنظام
-f	مسح جميع مدخلات البوابات من جدول التوجيه

الجدول 8.8

مصطلحات

Adhoc	تخطيط للشبكة اللاسلكية حيث تتصل الأجهزة مع بعضها مباشرة بدون استخدام نقطة وصول لاسلكيAP
Address	مجموعة من الأرقام تُستخدم لتعريف جهاز على الشبكة مثل عنوان IP 192.168.1.10
Administrator	هو الشخص المسؤول عن التحكم بموارد وبيانات الشبكة الحاسوبية وحسابات المستخدمين وأمان الشبكة
Access point	هو جهاز إرسال واستقبال يُستخدم لإنشاء اتصال بين أجهزة لاسلكية والشبكة المحلية LAN . عادة يتم اختصار الاسم إلى AP
ADSL	خط الاشتراك الرقمي غير المتماثل ، تقنية اتصال بالإنترنت باستخدام خط الهاتف التماثلي ، تكون فيه سرعة تحميل البيانات أعلى من سرعة الرفع
APIPA	طريقة عنونة مستخدمة فقط في أنظمة ويندوز بحيث يستطيع النظام إعطاء نفسه عنوان IP في حال غياب مخدم DHCP ليستطيع النظام التواصل مع غيره من الانظمة في نفس المقطع من الشبكة وتكون هذه العناوين ضمن المجال 169.254.X.X
Attenuation	التخميد أي الفقد الذي تعاني منه البيانات عند إرسالها لمسافات عبر وسط النقل في الشبكة
ATM	تقنية تبادل بالرزم تؤمن سرعة نقل للبيانات من 1.544 Mbps حتى 622Mbps
Authentication	هي عملية التحقق من المستخدمين في الشبكة وإن أكثر طريق للتحقق مشهورة هي باستخدام اسم مستخدم وكلمة مرور
Baud rate	
Band width	عرض الحزمة أو عرض مجال الترددات وعدد القنوات التي يمكن لوسط النقل أن يدعمها . له علاقة بمعدل النقل ولكن يوجد عوامل أخرى تحدد السرعة القصوى التي يدعمها الوسط
Baseband	مصطلح يشير إلى نقل إشارة واحدة فقط في وسط النقل في الوقت نفسه .
Bluetooth	طريقة اتصال منخفضة التكلفة والطاقة وذات مدى قصير مصممة للاتصالات بين الأجهزة، تستخدم التردد 2.4 Ghz وبسرعة نقل تصل حتى 24 Mbps.
Broad band	
Broadcast	نظام تسليم بيانات يتم فيه إرسال نسخة من البيانات إلى كل الأجهزة المتصلة بالشبكة.

Buffer	منطقة من الذاكرة في الجهاز تُستخدم للتخزين المؤقت للبيانات قبل توجيهها إلى جهاز آخر أو إلى مكان آخر.
Channel	قناة اتصال أي طريق نقل للبيانات
Client	عقدة في الشبكة تستخدم خدمات معينة من عقدة أخرى في الشبكة.مثل جهاز الحاسوب مع مخدم DHCP
Client / server	بنية شبكة بحيث أن العملاء في الشبكة يطلبون ويعاجون البيانات على جهاز مركزي يُسمى المخدم
CNAME	هو لقب أو اسم مستعار لمضيف في قاعدة بيانات DNS ويُستخدم لإعطاء حاسب واحد أكثر من اسم.
Circuit Switching	هي طريقة لإرسال البيانات بين نقطتين عن طريق تخصيص مسار بينهما ويتم نقل البيانات عبر الممر نفسه
Coaxial cable	الكابلات المحورية وهو كيبل لنقل البيانات مؤلف من قلب نحاسي ينقل الداتا مغلف بغلاف بلاستيكي ومحيط به الأسلاك التي تشكل الأرضي.
Cracker	شخص يحاول كسر حواية النظام أو الوصول إلى برمجيات غير مرخص له بالدخول إليها.
Default gateway	البوابة الافتراضية وهو الجهاز الذي من خلاله تستطيع أجهزة الشبكة تبادل البيانات مع شبكات خارجية (مثل الإنترنت) وهو في العادة يكون الراوتر نفسه.
DHCP	بروتوكول يؤمن توزيع عناوين IP بشكل تلقائي إلى محطات العمل في الشبكة ويمكن من خلاله إرسال معلومات أكثر من مجرد عنوان
DNS	نظام يُستخدم لترجمة أسماء النطاقات إلى عناوين IP مثل تحويل www.google.com إلى 10.10.23.12
EMI	تداخل إشارات كهرطيسية خارجية مع إشارة البيانات والتي تسبب ضعف في سلامة الإشارة وتزيد من معدل الأخطاء
Encryption	التشفير تعديل البيانات بحيث لا يستطيع أحج قراءتها بدون امتلاك طريقة فك التشفير
Ethernet	أكثر طريقة مشهورة من تكنولوجيا الشبكات المحلية LAN يمكن من خلالها استخدام كابلات مجدولة او نحاسية أو ضوئية
Firewall	برنامج أو نظام أو جهاز يقوم بتدقيق البيانات المتبادلة بين الشبكات المختلفة
Frequency	التردد وهو عدد الدورات التي تقوم بها الإشارة خلال واحدة الزمن ، يُقاس بواحدة الهرتز

	HZ
FTP	بروتوكول نقل الملفات بين نظامين وهو جزء من مجموعة بروتوكولات TCP / IP ويعمل في الطبقة السابعة من طبقات OSI
Full Duplex	نظام اتصال يتم نقل البيانات من خلاله بالاتجاهين في الوقت نفسه قارن مع half duplex
Frame	مجموعة من الواحدات تُرسل كوحدة واحدة من خلال الشبكة في مستوى الطبقة الثانية من طبقات OSI
Hacker	شخص يحاول الهجوم على نظام الحاسب وبرمجياته
Half duplex	نظام انصال يسمح بنقل البيانات باتجاه واحد في الوقت نفسه
Host	يشير عادة إلى أي جهاز في الشبكة يملك عنوان IP
Host ID	هو رقم تعريف يُستخدم لتعريف عميل أو أحد الأجهزة في الشبكة
Host Name	هو اسم الجهاز في الشبكة
http	بروتوكول يُستخدم من قبل متصفحات الإنترنت لنقل الصفحات والروابط والصور من جهاز بعيد إلى مستخدم الحاسب
https	بروتوكول يقوم بعمل بروتوكولhttp ولكن من خلال مسار مشفر يضمن سرية البيانات التي تمر عبره
Hub	جهاز شبكي يعمل كنقطة اتصال مركزية في الشبكة التي تستخدم الكابلات المجدولة
Hyper terminal	برنامج اتصالات يعمل في بيئة ويندوز يمكّن المستخدمين من إنشاء اتصال بعيد لجاز بعيد
IEEE	منظمة عالمية من بين مهامها تطوير معايير للاتصالات والشبكات
IANA	منظمة مسؤولة عن عناوين IP وأسماء النطاقات
Infrared	طريقة نقل البيانات بشكل لاسلكي باستخدام الأشعة تحت الحمراء
Interference	تشويش أي شيء يُضعف من جودة الإشارة
Interface	جهاز (كرت - مقبس) يتم من خلاله وصل قطعة بالحاسب لنقل البيانات من مكان إلى آخر مثل كرت الشبكة يربط بين الحاسب ووسط النقل
IP address	عنوان فريد لتعريف الجهاز وتعريف الشبكة المتصل بها
ISO	منظمة مسؤولة عن إنتاج معايير عالمية لعدة أمور بما فيها الحواسيب والشبكات

ISP	شركة تؤمن للمستخدم إمكانية الوصول إلى الإنترنت مقابل رسوم يدفعها.
LAN	مجموعة من الحواسيب المتصلة مع بعضها في مكان جغرافي واحد بحيث يتم مشاركة البيانات والخدمات
Metric	
Multicast	طريقة لإرسال البيانات من مرسل واحد إلى مجموعة محددة من العقد في الشبكة
Network ID	جزء من عنوان IP وهو الذي يحدد قسم الشبكة
OSI	نموذج اتصال مكون من سبع طبقات تم إنشاءه من ISO
Port	
POTS	نظام الهاتف التماثلي انظر pstn
Private network	هي شبكة الوصول إليها محدود ومُتحكم به
POE	تقنية يمكن من خلالها نقل القدرة الكهربائية عبر الكابلات المجدولة المستخدمة لنقل البيانات في الشبكات
Protocol	مجموعة من المعايير او القواعد التي تتحكم بنقل البيانات والتخاطب بين التجهيزات الشبكية
Proxy server	مخدم يعمل بين محطة العمل والإنترنت يسمح بمستوى من الأمان ويسرع طلبات الإنترنت
PSTN	مصطلح يشير إلى شبكات الهاتف على مستوى العالم وتستخدم النقل الرقمي للبيانات ماعدا الاتصال بين المستخدم والمقسم المحلي حيث تكون تماثلية
Public network	هي شبكة عامة يمكن لأي شخص أن يتصل بها بأقل قدر ممكن من التقييد وأشهر مثال على الشبكة العامة هي شبكة الإنترنت
Route	مسار أو طريق مخصص لنقل البيانات بين عقدتين في الشبكة
Router	جهاز يعمل على توجيه البيانات لتصل إلى وجهتها
Server	جهاز في الشبكة يعمل على تنفيذ الطلبات القادمة من المستخدمين مثال مخدم ملفات – مخدم DHCP
Session	جلسة
SOHO	شبكة حاسوبية صغيرة تُخدم عادةً من 10-1 مستخدمين
SSH	تؤمن فتح جلسة مع جهاز بعيد مع طرق للتحقق وتشفير البيانات التي تسافر عبر الشبكة ،

	تستخدم المنفذ22
SSID	اسم الشبكة اللاسلكية تُستخدم للتمييز بين الشبكات اللاسلكية المتواجدة في مكان واحد
Subnet mask	قناع الشبكة يُستخدم لتحديد أي جزء من عنوان IP للمستخدم وأي جزء لعنوان الشبكة
Telnet	بروتوكول من مجموعة بروتوكولات TCP /IP يُستخدم للاتصالات البعيدة حيث يسمح للمستخدم من الدخول إلى أنظمة بعيدة واستخدام الموارد كما لو أنه متصل معه بشبكة محلية
T_Carrier	خط رقمي عالي السرعة يُؤجر من قبل شركات الهاتف تدعم نقل كل من البيانات والصوت وتستخدم عادة لإنشاء شبكات WAN
Topology	الطوبولوجيا المخطط الفيزيائي للشبكة ومخطط تدفق البيانات عبر الشبكة
Unicast	يتم من خلاله إرسال البيانات من مستخدم في الشبكة إلى مستقبل واحد .
UPS	نظام يؤمن حماية من ارتفاع الجهد وانقطاع التغذية الكهربائية مما يعطي الوقت الكافي لإغلاق الأنظمة والأجهزة قبل فقدان التغذية الكهربائية
URL	هو اسم يُعطي لتعريف الموقع الالكتروني والصفحات في الويب مثال : www.amazon.com/product
VLAN	الشبكة المحلية الافتراضية هي مجموعة من الأجهزة موجودة في مقطع واحد أو أكثر من الشبكة LAN يتم ضبط إعداداتها لتشكل شبكة واحدة وكأنها متصلة مع بعضها على Switch واحد وهي في الحقيقة ليست كذلك
VOIP	نقل الصوت عبر بروتوكول الإنترنت
VPN	شبكة تستخدم الإنترنت للربط بين أكثر من شبكة خاصة أو لتحقيق اتصال بين مستخدم بعيد وشبكة محلية
WIFI	
WINS	خدمة تحويل من أسماء NETBIOS إلى عناوين IP تعمل في بيئات ويندوز فقط.
WLAN	هي شبكة محلية تستخدم طرق النقل اللاسلكي مثل الأمواج الراديوية او الاشعة تحت الحمراء عوضاً عن استخدام الكابلات التقليدية
Workstation	محطة العمل هو جهاز في الشبكة لا يقدم أي خدمات لوحده ولكن يستخدم الخدمات التي يقدمها المخدم له