الفصل الأول والثاني

عنوان الموضوع:

مقدمة في الشبكات الحاسوبية ومفهوم النموذج الطبقي المرجعي: النماذج OSI و TCP/IP

الكلمات المفتاحية:

بنيان، شبكة، عقدة، مُجمِّع، مُبدِل، الشبكات الخطية، الشبكات الحلقية، الشبكات النجمية، بُنية طبقية، طبقة، واجهة الطبقة، بروتوكول، تقييس، قياس، معيار، الطبقة الفيزيائية، الترميز، الترنيم، الدمج، الفرز، المعطيات، تمثيل المعطيات، بنى المعطيات، طبقة ربط المعطيات، طبقة الشبكة، التوجيه، طبقة النقل، طبقة الجلسة، طبقة العرض، طبقة التطبيقات، قواعد دلالية، قواعد صرفية، تقسيم الشبكة.

ملخص:

يتعرف الطالب في هذا الفصل على تعريف الشبكة ومفهوم النموذج المرجعي بالإضافة إلى طبقات النموذج المرجعي OSI وطبقات النموذج المرجعي TCP/IP

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- تعريف شبكة حاسوبية وبنيانها العام
- عائلات الشبكات الحاسوبية وطرق تشكيلها
- مفهوم البنية الطبقية
- مفهوم النموذج المرجعي
- أسلوب تبادل المعلومات اعتماداً على البنى الطبقية
- النموذج المرجعي OSI
- النموذج المرجعي TCP/IP

تعريف شبكة حاسوبية

- وسيلة ربط مجموعة من الحواسب بهدف استخدام موارد مشتركة
- تتألف من عتاد صلب ومن عتاد برمجي
- يوفر الولوج إلى حواسبها استخدام موارد مشتركة مثل، الطابعات، والبريد إلكتروني، والتطبيقات المكتبية أو التقنية، والمودمات والفاكسات، وغيرها
- تطورت بنية الشبكات من مجرد مجموعة من الطرفيات غير الفعّالة إلى مجموعات من الحواسب الكاملة.
- من أهم الميزات التي تقدمها الشبكات:
  - مشاركة المعطيات
  - مشاركة التطبيقات
  - مشاركة الأجهزة
  - الاتصالات
  - التوافقية
  - الأمن
  - الدخول إلى الانترنت

تُعرَّف الشبكات على أنها وسيلة لربط مجموعة من الحواسب بهدف استخدام مواردها بشكلٍ مشترك. وتتألف الشبكات عادةً من عتادٍ صلب ومن عتادٍ برمجي. عموماً، يؤمن الولوج إلى حواسب الشبكة، إمكانية استخدام مواردها المشتركة مثل الطابعات، والبريد إلكتروني، والتطبيقات المكتبية أوالتقنية، والمودمات، والفاكسات، وغيرها.

لقد تطورت بنية الشبكات من مجرد مجموعة من الطرفيات غير الفعّالة المرتبطة بحاسوب مركزي (1970s) إلى مجموعات من الحواسب الكاملة التي تتعامل فيما بينها بأسلوب موحد قياسي

من أهم مزايا الشبكات:

مشاركة المعطيات: تسمح عملية مشاركة المعطيات لمجموعة من المستخدمين بتبادل المعلومات بشكل مُنظم وسريع. فقد تكون هذه المعطيات عبارة عن تقريرٍ مفصل قام بإعداده موظف في سورية واستفاد منه موظف آخر في دبي.

مشاركة التطبيقات: توفر مشاركة التطبيقات استخدام البرمجيات والتطبيقات التي جرى تنصيبها على المخدم من قبل المستخدمين، الأمر الذي يوفر عملية تنصيب البرامج على كل الحواسب. كما يستطيع المخدم معرفة المستخدمين الذين يقومون باستخدام برنامج معين، ومنع دخول المستخدمين غير المخولين بالدخول.

مشاركة الأجهزة: تتيح عمليات مشاركة الأجهزة للمستخدمين إمكانية الاستفادة من الطرفيات الموجودة على الشبكة، كالطابعات، والماسحات الضوئية، وأجهزة الفاكس، وغيرها. لذا، تستطيع الشركات توفير المال من خلال شراء عدد أقل من التجهيزات. علاوةً على ذلك، تؤمن الشبكات استخدام الأجهزة ذات الكلفة العالية بشكلٍ أفضل، مما يبرر صرف تكاليف باهظة لشرائها.

الاتصالات: تسهل الاتصالات على مستخدمي الشبكة العديد من الأمور، وخاصةً من خلال استخدام البريد الإلكتروني، والرسائل الفورية، مما يجعل الاتصالات بين الموظفين والمستخدمين أسهل وأسرع.

التوافقية: تسهل التوافقية عملية صيانة البرمجيات والتطبيقات. وبما أن تخزين البرمجيات وتحديثها يجري مركزياً، فهذا يعني أن المستخدمين سيمتلكون نفس الأدوات، وسيستخدمون نفس البرامج. وبما أن مدراء النظم والمعلوماتية في الشركة سيعملون على تعديل البرمجيات الموجودة على المخدم فقط، فهذا يعني أن هذه العملية ستتم مرة واحدة فقط، وستكون التطبيقات متوفرة لكل مستخدمي الشبكة.

الأمن: يُعتبر أمن المعلومات على الشبكة أمراً في غاية الأهمية، إذ يحتاج المستخدم إلى حساب خاص للدخول إلى الشبكة، ولايتم قبول أي دخول إلى أي مورد من موارد الشبكة مالم يُدخِل المستخدم اسم الحساب وكلمة المرور الخاصة به. يمكن أيضاً توزيع صلاحيات دخول إلى معلومات أو أجهزة معينة على الشبكة، ومنع المستخدمين غير المخولين، من الدخول إلى المعطيات الحساسة. ويمكن إعداد حسابات دخول المشتركين بحيث يضطرهم النظام لتغيير كلمات السر الخاصة بهم دورياً، كما يمكنه منعهم من الدخول إلى بعض الأجهزة في أوقات محددة.

الدخول إلى الانترنت: بعد توفير البرمجيات والعتاديات الخاصة، يمكن للمستخدمين الدخول إلى الانترنت اعتباراً من الشبكة الداخلية للشركة. وتعتبر هذه الميزة في غاية الأهمية، فهي توفر للمستخدمين وسائل مختلفة للحصول على كمٍّ ضخم من المعلومات والمصادر المختلفة، كالبرمجيات الإضافية، وبرامج تعريف العتاد.

عائلات الشبكات

تُقسم الشبكات إلى عائلتين رئيسيتين ترتبطان بحجم الشبكة وتوزعها الجغرافي واتساعها:

- **الشبكات المحلية LAN**
- **الشبكات الواسعة WAN**

تُقسم الشبكات إلى عائلتين رئيسيتين ترتبطان بحجم الشبكة وتوزعها الجغرافي واتساعها:

الشبكات المحلية LAN: تدعى الحواسب المرتبطة ببعضها في منطقةٍ جغرافيةٍ واحدة بشبكة منطقة محلية، أو شبكة محلية اختصاراً، أو LAN كما هو شائع، وهو اختصار يرمز إلى Local Area Network. تعود ملكية هذه الشبكات عادةً إلى شركةٍ أو مؤسسةٍ واحدة، تكون مكاتبها في نفس الموقع أو البناء أو ضمن حَرَمٍ واحد. تتألف خارطة شبكة محلية خاصة بمؤسسة، من شبكات محلية فرعية صغيرة في كل قسم من أقسام الشركة. يتم ربط كل شبكة من الشبكات الفرعية الصغيرة مع الشبكات الأخرى باستخدام مجمِّعات أو مبدِّلات (وهي تجهيزات شبكية خاصة سندرسها لاحقاً بالتفصيل). كما يمكن أن يُخصص لكل قسم من أقسام الشركة مخدِّم خاص واحتياجات معلوماتية خاصة. يساعد هذا التوزيع في تلافي حصول ازدحام على المخدِّم أو الشبكة، الأمر الذي يُحسِّن أداء الشبكة ككل. تُعرَّف هذه التقنية بتقنية تقسيم الشبكة إلى شبكات فرعية.

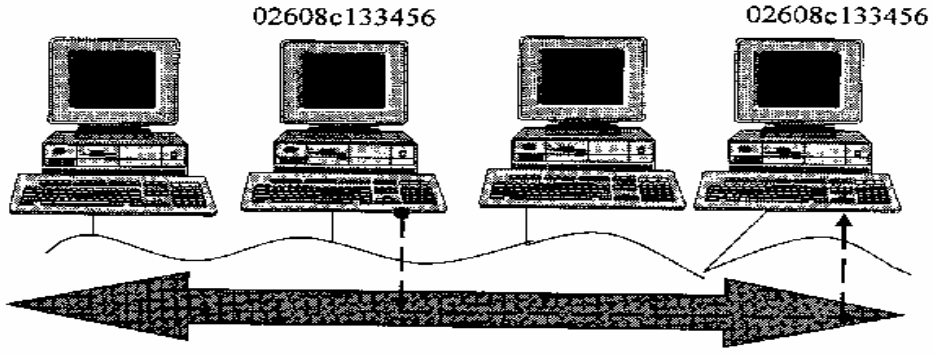
الشبكات الواسعة WAN: هي شبكات تربط بين عدة شبكات موجودة في مناطق متباعدة جغرافياً، ويرمز اختصار WAN إلى Wide Area Networks. تمتد الشبكات الإقليمية ضمن مدينة، أو دولة، أو قارّة، أو حتى عبر الكرة الأرضية. تتم عملية وصل الشبكات الصغيرة ببعضها من خلال بنية اتصالات تمر عبر وسائل الإتصال العامة (مؤسسات الإتصالات وخطوط اتصال دولية)، حيث تزود شركات الاتصالات مثل مؤسسة الإتصالات السورية، المؤسسات بخدمة الربط الإقليمي المطلوب لقاء أجر محدد.

التشكيلات الشبكية

- يجري تنظيم الشبكات وفق بعض الأشكال القياسية التي تساعد على تحديد أسلوب التوزيع المكاني لعقد الشبكة. ونعني بالعقدة، نقطة من الشبكة متصلة بقناتي اتصال على الأقل كحال المُبدلات (التي سنوضح مبدأ عملها لاحقاً).
- يؤثر التشكيل الشبكي على أسلوب عمل وإدارة الشبكة، كما يؤثر على اختيار مكونات الشبكة.
- يمكن للشبكات أن تتشكل حسب بعض الأشكال القياسية الآتية:
  - التشكيل الخطي
  - التشكيل الحلقي
  - التشكيل النجمي

التشكيلات الشبكية الخطية والحلقية

- يمكن تشبيه أسلوب التشكيل الخطي لشبكة، بحالة طريق سريع يصل بين عدة مدن حيث يمكن لوسائط النقل أن تعبر هذا الطريق بين أية مدينتين
- تلعب وسائط البث في مثالنا، دور الطريق السريع وتلعب العقد في مثالنا، دور المدن، وتلعب المعلومات المتبادلة بين العقد في مثالنا، دور وسائط النقل
- بالنتيجة، يمكن تبادل المعلومات على وسيط البث بالاتجاهين بين أية عقدتين من شبكة محلية
- إلا أن انقطاع أي عقدة من العقد، يؤدي إلى توقف الشبكة عن العمل



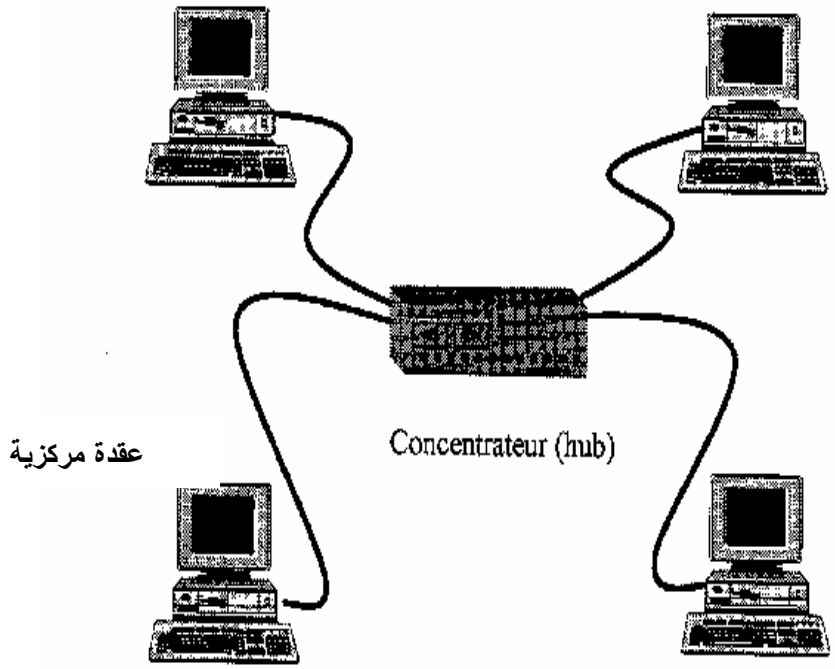
انتبه:

يعتبر التشكيل الحلقي، تشكيلاً خطياً على شكل حلقة.

التشكيلات الشبكية النجمية

يتألف هذا التشكيل من عقدة مركزية تدعى مُجمِّع أو مبِّدل حيث يتم وصل الحواسب إلى هذه العقدة باستخدام كابلات وصل شبكي. تتم كل عملية إرسال أو استقبال عبر هذه العقدة.

تتميز هذه البنية في كونها سهلة التركيب وفيها سماحية أكبر للأخطاء، فالعطل الذي يطرأ على عقدة من الشبكة، لا يؤثر على عمل الشبكة.



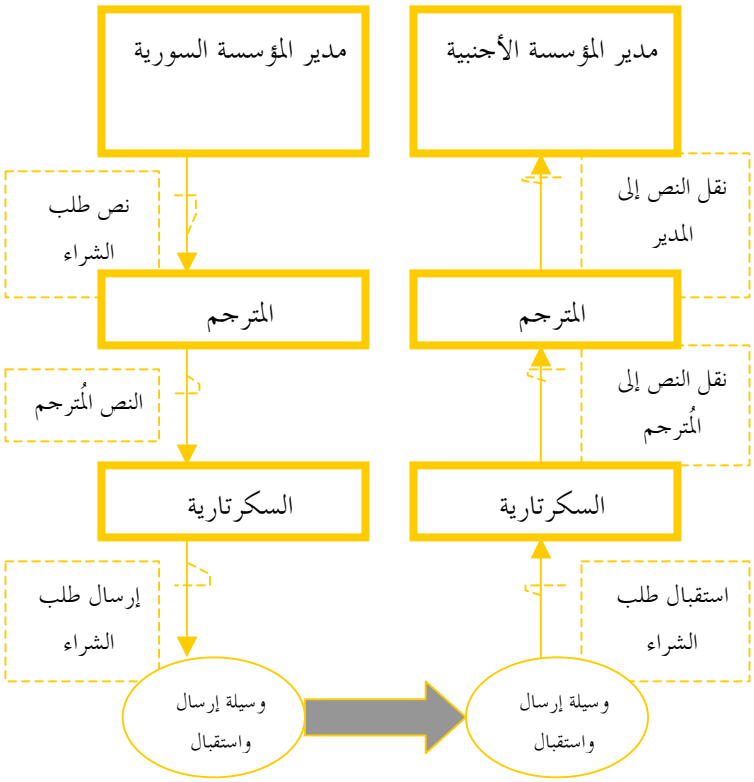
البنية الطبقية

لتخفيض تعقيد عملية تصميم الشبكات وتطويرها، تم الاتفاق على تنظيم بنى الشبكات على شكل سلسلة من الطبقات أو المستويات المستقلة، التي تم بناء كلٍ منها اعتماداً على سابقتها. يعتمد هذا الأسلوب على مبدأ "فرِّق تسُد" مما يُسهِّل السيطرة على البنية الكلية. فدراسة الكُلّ يعود إلى دراسة أجزاء منفصلة مستقلة عن بعضها البعض.

يمكن تشبيه أسلوب العمل بأسلوب العمل البيروقراطي ضمن مؤسسة:

لنفرض حالة مؤسستين، أحدهما سورية والأخرى أجنبية. يعمل كل مدير من المدراء مع مترجم ومع قسم سكرتارية، ويستخدم وسيلة إرسال واستقبال خاصة بشركته للتراسل مع العالم الخارجي.
تحتاج المؤسسة السورية لشراء احتياجاتها التقنية من المؤسسة الأجنبية. لذا يحتاج مدير المؤسسة السوري لإرسال طلب شراء إلى المؤسسة الأجنبية. يمر طلب الشراء بمراحل الصياغة والترجمة والإرسال حتى يصل إلى الشركة الأجنبية حيث يعود ويمر بمراحل الإستقبال والتحضير قبل أن يصل إلى مدير المؤسسة الأجنبية.
للرد على طلب الشراء السابق، يقوم مدير المؤسسة الأجنبية بصياغة عرضه وتحويله إلى الترجمة ومن ثم إلى السكرتارية وهكذا حتى يصل الرد إلى المؤسسة السورية.

يمكن توضيح المراحل السابقة بالبنية الطبقية التالية:



ندون من أسلوب العمل السابق الملاحظات التالية:

- تعمل كل طبقة على نحوٍ مستقل عن الطبقة التي تسبقها
- ندعو أسلوب العمل المشترك الواجب توفره بين إحدى طبقات البنية الأولى (مثل حالة السكرتيرة في المؤسسة السورية) مع نفس الطبقة في البنية الثانية (مثل حالة السكرتيرة في المؤسسة الأجنبية) بـــ "البروتوكول"
- تعتمد كل طبقة من طبقات البنية السابقة (السكرتارية مثلاً) على أسلوب تخاطب معياري يتيح لها التواصل مع الطبقة الأدنى (أداة الإرسال) ومع الطبقة الأعلى (المترجم). ندعو هذا الأسلوب المعياري بواجهة الطبقة
- تعتمد كل طبقة على المعلومات الواردة من الطبقة الأعلى عند قيامها بعملية الإرسال وتقوم بإيصال نتيجة العمل إلى الطبقة

الأدنى

- تعتمد كل طبقة على المعلومات الواردة من الطبقة الأدنى عند قيامها بعملية الاستقبال وتقوم بإيصال نتيجة العمل إلى الطبقة الأعلى

يمكن تمثيل الشكل السابق بحركة

هيئات التقييس الدولية

- **ISO (International Standardization Organization)**
  - هيئة تابعة للأمم المتحدة
  - لها ممثلين وطنيين محليين في عدة دول:
    - ANSI – USA
    - AFNOR – France
    - DIN – Germany
    - BSI – UK
    - HSC – Japan
- **IUT-T (International Union of Telecommunication)**
  - تضم الصناعيين ومزودي الخدمة العاملين في مجال الاتصالات

بنيان الشبكات: عموميات (1)

يتم تنظيم بنيان الشبكات تنظيماً تسلسلياً على شكل طبقات أو مستويات، وفق القواعد التالية:

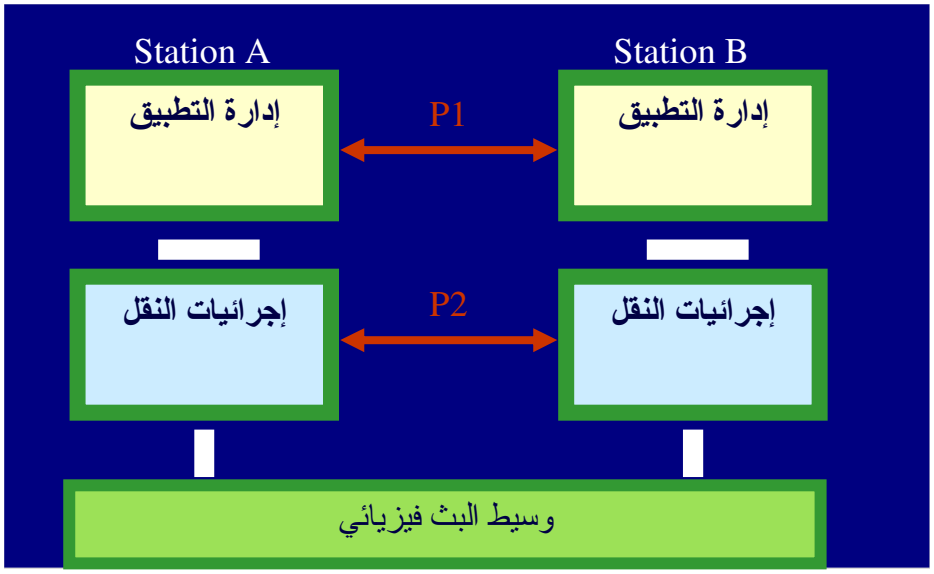
1. تختلف أسماء وأعداد ووظائف هذه الطبقات تبعاً لنمط البنيان الشبكي ونوعه؛
2. تعمل كل طبقة على توفير مجموعة من الخدمات للطبقة الأعلى؛
3. لا علاقة للطبقات الأعلى بأسلوب تنجيز الخدمات في الطبقات الدنيا؛

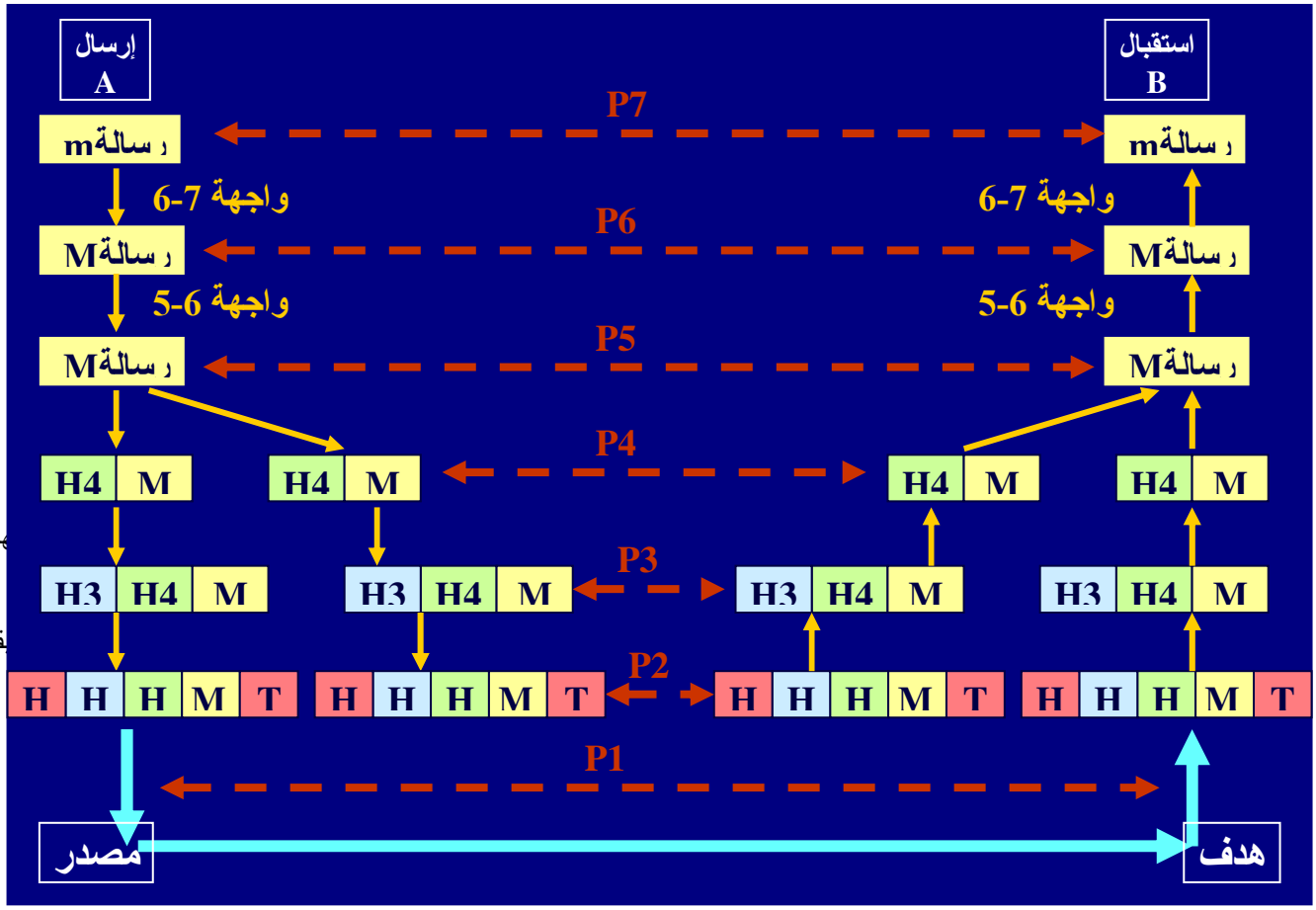
4. نُعرِّف البروتوكول على أنه أسلوب تفاهم بين طبقتين متناظرتين؛

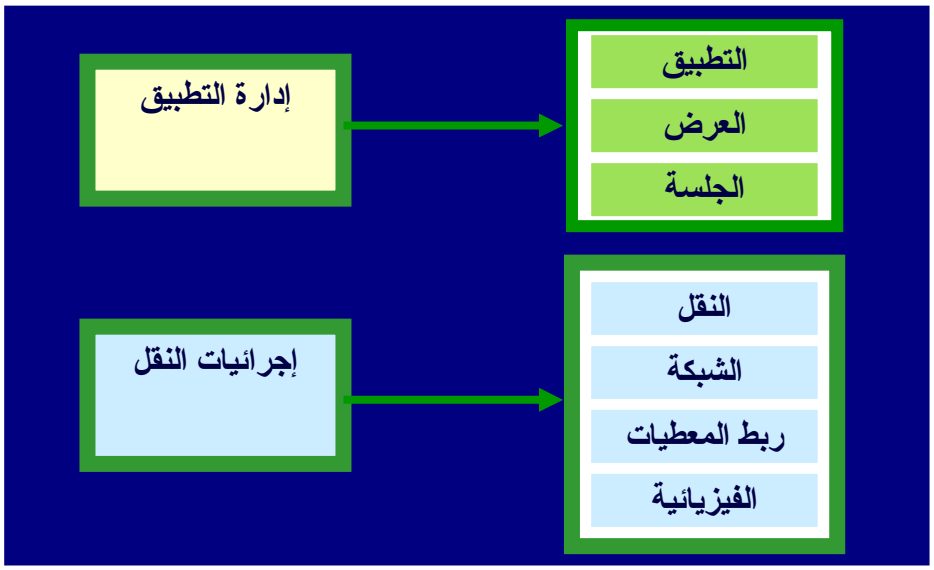
5. تتبع المعطيات طريقاً متسلسلاً من الطبقة الأعلى وحتى الطبقة الأدنى عند الإرسال ومن الطبقة الأدنى حتى الطبقة الأعلى عند الإستقبال وذلك مهما كان عدد الطبقات؛

يمكن أيضاً إضفاء حركة على الأشكال

بنيان الشبكات: صورة عمومية عن تبادل المعلومات







يوصِّف النموذج المرجعي، بشكلٍ قياسي، دور كل طبقة من طبقات بنيان الشبكة، وواجهة تعاملها مع الطبقات المحيطة بها، دون الدخول في تفصيل عملها. أما التوصيف التفصيلي لعمل كل طبقة ولإجرائياتها فيُدعى برتوكول الطبقة وهي مجموعة من القواعد والاجرائيات التي تحدد كيفية تفاهم طبقة مع طبقة نظيرة لها في عقدة شبكية أخرى.

يعتبر النموذج المرجعي OSI والذي يعني نموذج الوصل البيني الخاص بالأنظمة المفتوحة (Open System Interconnection)، نموذجاً أساسياً لإتمام عملية الاتصال بين حواسب ذات بنية شبكية مفتوحة.

يتألف النموذج من سبع طبقاتٍ لكل منها وظائف محددة ومسؤوليات منفصلة عن الطبقات الأخرى. تفصل بين هذه الطبقات واجهات تعامل قياسية.

عند تعديل إجرائية منتمية إلى طبقة ما، يكفي أن توفر هذه الإجرائية المعلومات إلى الطبقة الأدنى بالشكل القياسي المُعتمد، وأن تحصل على معلوماتها من الطبقة الأعلى وفقاً للواجهة القياسية المعتمدة أيضاً.

نستعرض فيما يلي الطبقات السبعة الخاصة بالنموذج حسب ترتيبها التنازلي:

- طبقة التطبيقات **Application**
- طبقة التقديم **Presentation layer**
- طبقة الجلسة **Session layer**
- طبقة النقل **Transport layer**
- طبقة الشبكة **Network layer**
- طبقة ربط المعطيات **Data link layer**
- الطبقة الفيزيائية **Physical layer**

النموذج المرجعي OSI: الطبقة الفيزيائية

- تكون هذه الطبقة مسؤولة عن إدارة الحامل الفيزيائي وتجهيزاته
- يُعرِّف كلاً من القياس ISO-10022 والتوصية UIT رقم X.211 الخدمات التي توفرها هذه الطبقة
- توفر هذه الطبقة الوسائل الميكانيكية والكهربائية والوظيفية اللازمة لتفعيل وإدارة الوصلات الفيزيائية المسؤولة عن إيصال المعطيات الثنائية بين طرفي الإتصال

- تتألف عناصرهذه الطبقة من:
  - الحامل الفيزيائي
  - تجهيزات الترميز (encoders) والترنيم (Modulators)
  - تجهيزات الدمج والفرز (Multiplexers)
- تدخل عملية تصميم وتنفيذ هذه الطبقة في مجال عمل مهندس الإلكترونيات
- تكون هذه الطبقة مسؤولة عن إدارة الحامل الفيزيائي وتجهيزاته
- يُعرِّف كلاً من القياس ISO-10022 (أيزو) والتوصية UIT (يو آي تي) رقم X.211 (إكس 211) الخدمات التي توفرها هذه الطبقة
- توفر هذه الطبقة الوسائل الميكانيكية والكهربائية والوظيفية اللازمة لتفعيل وإدارة الوصلات الفيزيائية المسؤولة عن إيصال المعطيات الثنائية بين طرفي الإتصال
- تتألف عناصرهذه الطبقة من:
  - الحامل الفيزيائي
  - تجهيزات الترميز (encoders) والترنيم (Modulators)
  - تجهيزات الدمج والفرز (Multiplexers)

تدخل عملية تصميم وتنفيذ هذه الطبقة في مجال عمل مهندس الإلكترونيات

النموذج المرجعي OSI: طبقة ربط المعطيات

- تعتمد هذه الطبقة في عملها على الطبقة الفيزيائية
- يُعرِّف كلاً من القياس ISO-8886 والتوصية UIT رقم X.212 الخدمات التي توفرها هذه الطبقة
- تقوم هذه الطبقة بإدارة عملية إيصال المعطيات وتنظيم حركة المرور اعتماداً على التشكيل الشبكي الموجود
- تمتلك آليات اختبار أخطاء الإرسال، لتحديد فيما إذا كانت الطرود المُرسَلة قد وصلت على نحو صحيح

النموذج المرجعي OSI: طبقة الشبكة

- تعمل هذه الطبقة على توفير إمكانيات فتح وإدارة وإغلاق الإتصال الشبكي بين نظم مفتوحة. إذ تؤمن هذه الطبقة الوظائف التالية:
  - إدارة الشبكات الفرعية التي تتألف منها شبكة بينية كاملة
  - تأمين شروط إيصال طرد من المصدر إلى الهدف
  - الإحتفاظ بعنوان العقدة
  - تحديد وجهة الطرود على نحو دقيق
  - إدارة التدفق (كمية الطرود الصادرة والواردة)
- تساعد هذه الطبقة على تأمين عمليات الربط بين شبكات غير متجانسة

النموذج المرجعي OSI: طبقة النقل

- تكون هذه الطبقة مستقلة عن الشبكة
- تتلقى معطياتها من طبقة الجلسة لتقوم
  - بتقطيعها
  - بتأمين تسلسلها
- تساعد هذه الطبقة أيضاً على إدارة عدة اتصالات للعقدة الشبكية وتحديد الرسائل التابعة لكل اتصال عبر عمليات تجميع وفرز

النموذج المرجعي OSI: طبقة الجلسة

- تؤمن هذه الطبقة التزامن بين أطراف الإتصال
- تقوم بوظائف من نمط إدارة إعادة الإرسال وتأمين ذاكرة لعمليات الإرسال
- بالنتيجة، تلعب هذه الطبقة دور قائد الأوكسترا

النموذج المرجعي OSI: طبقة العرض

- تهتم هذه الطبقة بالقواعد الصرفية والدلالية للمعطيات حيث تقوم
  1. بتمثيل المعطيات المُرسَلة بين أطراف الإتصال
  2. بتمثيل بنى المعطيات
  3. بترميز المعطيات وفق قياسات محددة ASCII أو EBCDIC للسماح لتجهيزات مختلفة بإقامة اتصال فيما بينها
  4. بضغط وتشفير المعطيات
- تعتمد هذه الطبقة مثلاً على القواعد الصرفية المجردة لتمثيل المعطيات ASN.1 تبعاً للمقاييس (ISO 8824 و UIT X.208) التي قامت ISO بتقييسها

- تهتم هذه الطبقة بالقواعد الصرفية والدلالية للمعطيات حيث تقوم:
  1. بتمثيل المعطيات المُرسَلة بين أطراف الإتصال
  2. بتمثيل بنى المعطيات
  3. بترميز المعطيات وفق قياسات محددة ASCII أو EBCDIC للسماح لتجهيزات مختلفة بإقامة اتصال فيما بينها
  4. بضغط وتشفير معطيات
- تعتمد هذه الطبقة مثلاً على القواعد الصرفية المجردة لتمثيل المعطيات ASN.1 (إي إس إن واحد) تبعاً للمقاييس (ISO 8824 و UIT X.208) التي قامت ISO بتقييسها

النموذج المرجعي OSI: طبقة التطبيق

- توفر لإجراءات التطبيقات إمكانيات الولوج إلى بيئة الشبكة
- من الأمثلة الشهيرة عن محتوى هذه الطبقة: تطبيق نقل الملفات FTP، تطبيق العمل عن بعد Telnet، تطبيق البريد الإلكتروني Email ... وغيرها

النموذج المرجعي TCP/IP والإنترنت: سرد تاريخي

- تنامت خلال عقد الستينات من القرن الماضي، أهمية مفهوم الربط البيني (Interconnection)
- سمحت الأبحاث التي نفذتها DARPA بتصميم وتنفيذ منظومة شبكية تدعى ARPANET في عام 1969
- وضعت الهيئة الآنفة الذكر مجموعة من المواصفات القياسية لأساليب ومبادئ الاتصال بين هذه المواقع جرت تسميتها TCP/IP
- لم تعد الشبكة في عام 1980 شبكة أبحاث عسكرية فقط، وتحولت الشبكة إلى شبكة الإنترنت التجارية خلال بضعة سنوات، وأصبحت الإنترنت في يومنا هذا مجموعة من الشبكات الخاصة تملكها مجموعة من مزودي الخدمة الذين يتصلون ببعضهم البعض عبر وصلات خاصة بهم ندعوها Peering Points

- بعد ازدياد استخدام الإنترنت، ظهرت خوارزميات/ الإقلاع البطيئ (slow start)، وخوارزميات تجنب الإزدحام (congestion avoidance)، وبروتوكولات إعادة الإرسال السريعة(fast retransmit) والاستعادة السريعة (fast recovery)
- لحسن الحظ، تبدو الإنترنت وكأنها استطاعت تجاوز هذه المحنة، حيث تبدو حالياً وكأنها قادرة على تقديم خدمات تتفوق عدد طلبات المستثمرين في المستقبل المنظور على الأقل.

تنامت خلال عقد الستينات من القرن الماضي، أهمية مفهوم الربط البيني (Interconnection) بين مختلف مراكز الحساب التابعة للقوات الأميركية، وازدادت أهمية التكنولوجيا المرتبطة بهذا المفهوم. لذا قررت الحكومة الأميركية تمويل الأبحاث المتعلقة بهذا المجال عبر هيئة عسكرية للأبحاث مرتبطة بوزارة الدفاع وتدعى DARPA (Defense Advanced Research Project Agency).

سمحت الأبحاث التي نفذتها DARPA بتصميم وتنفيذ منظومة شبكية تدعى ARPANET في عام 1969 أضحت بعد ذلك النواة الأساسية لشبكة NSF-NET التي ربطت على مستوى الأراضي الأميركية، بين مختلف المواقع العسكرية الأميركية المزودة بحواسب عملاقة. ووضعت الهيئة الآنفة الذكر مجموعة من المواصفات القياسية لأساليب ومبادئ الاتصال بين هذه المواقع جرت تسميتها فيما بعد ببروتوكولات الإنترنت أو مجموعة البروتوكولات TCP/IP باستخدام أسمي البروتوكولين الأساسيين في المجموعة وهما البروتوكولين، TCP و IP.

لم تعد الشبكة في عام 1980 شبكة أبحاث عسكرية فقط، فقد كان الوقت قد حان لتنسحب هيئة الأبحاث الوطنية من الأعمال التجارية المرتبطة بهذه الشبكة. وتحولت الشبكة إلى شبكة الإنترنت التجارية خلال بضعة سنوات. أما الشبكة NSF-NET فتوقفت عن العمل في نيسان 1994. وأصبحت الإنترنت في يومنا هذا مجموعة من الشبكات الخاصة تملكها مجموعة من مزودي الخدمة الذين يتصلون ببعضهم البعض عبر وصلات خاصة بهم ندعوها Peering Points.

كانت الإنترنت في منتصف الثمانينات مؤلفة من مواقع ARPANET الأصلية بالإضافة إلى مواقع عدة جامعات تستخدم حواسب VAX (من DEC) مزودة بنظام Berkeley UNIX ضمن شبكات Ethernet محلية تعمل بسرعة 10Mb/s، وتتصل بالمواقع الأخرى عبر خطوط تلفونية مكرسة بسرعة 56Kb/s. في ذلك الوقت، ومع قدوم شهر أيلول من كل عام وعودة الطلاب إلى جامعاتهم، كانت الإنترنت تعاني من حالات إزدحام لذا قام أحد الباحثين وهو Van Jacobson من مختبرات Lawrence Berkeley، بمعاينة سلوك البروتوكولات عند ظهور حمل زائد وتحديد مشاكل هذا السلوك.

ضمن هذا السياق ظهرت خوارزميات/ الإقلاع البطيئ (slow start)، وخوارزميات تجنب الإزدحام (congestion avoidance)، وبروتوكولات إعادة الإرسال السريعة (fast retransmit) والاستعادة السريعة (fast recovery). إلا أن ضغط السوق وقاعدة Moore التي تَدَّعي أن سرعة العتاد الصلب تتضاعف كل 18 شهر قد أديا إلى تسارع تطور الإنترنت. فاعتباراً من نهاية الثمانينات وحتى وقتنا هذا، ازدادت سرعة الشبكات بمقدار 1000 مرة. كما ازدادت سرعة الدارات المكرَّسة بمقدار 12000 مرة وازداد عدد المنصات العاملة 50000 مرة.

في عام 1996، توقع Bob Metcaffe مخترع Ethernet تراجع الإنترنت نتيجة لعدم كفاية سرعة البنية التحتية لتلبيـــة متطلبـــات المستثمرين. لحسن الحظ، تبدو الإنترنت وكأنها استطاعت تجاوز هذه المحنة، حيث تبدو حالياً وكأنها قادرة على تقديم خدمات تتفوق عدد طلبات المستثمرين في المستقبل المنظور على الأقل.

في الواقع، تبدو الحقيقة المتمثلة في أن الإنترنت تعمل بنفس سلسلة البروتوكولات TCP/IP التي جرى تصميمها منـــذ 25 عامـــاً، حقيقةً غريبةً ومضحكةً بآن واحد وخصوصاً لأولئك الذين يعانون ومنذ فترة من تسارع ظهور أجيال جديدة مـــن العتـــاد الـــصلب وأنظمة الاستثمار والتي تجعل من أنظمتهم البرمجية أنظمة غير فعالة. لذا من الضروري أن نرفع قبعاتنا احتراماً لكل مـــن Bob Kahn وVint Cerf وJon Postel وVan Jacobson ولجميع من ساهم في تـــصميم وتنفيـــذ سلـــسلة البروتوكـــولات الـــسابقة وملحقاتها.

كيف تجري عملية إدارة الإنترنت في ايامنا هذه ؟

الهيئات المعنية بإدارة الإنترنت وحكمها:

- **ICANN** (Internet Corporation for Assigned Names and Numbers) www.icann.org
- **ISOC** (Internet Society): www.isoc.org
- **IETF** (Internet Engineering Task Force) www.ietf.org.

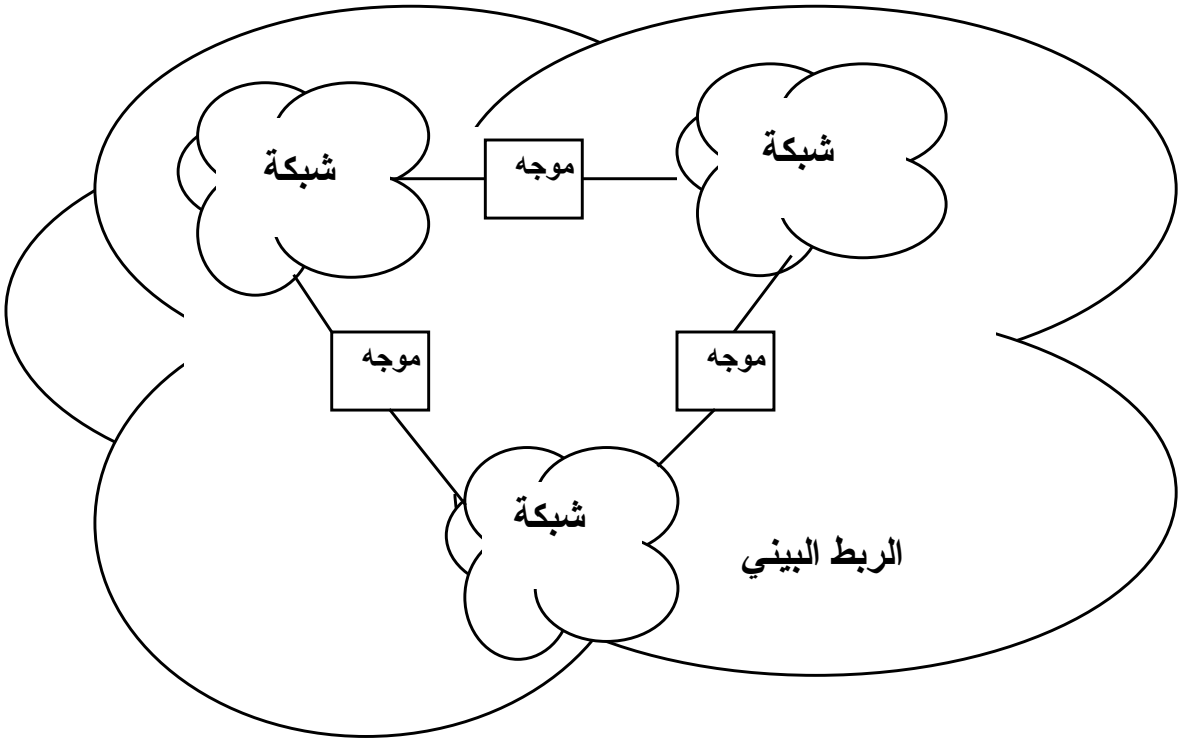
يعتبر تطوير الإنترنت عملاً تعاونياً ومفتوحاً على الجميع. لكن قيادة الإنترنت في وقتنا الـــراهن، ونتيجـــة لـــدخولها فـــي صـــلب التطورالإقتصادي العالمي، يقلق عدداً كبيراً من المسؤلين عن قطاعات اقتصادية معينة، نتيجة اعتبارهم أن إدارة الإنترنت تقع بـــين أيدي مجموعة من محترفي المعلوماتية المُسَـــيَرين من قبل الحكومة الأميركية.

على كل حال، هناك عدد من الهيئات المعنية بإدارة الإنترنت وحكمها:

- ICANN (Internet Corporation for Assigned Names and Numbers) وهي هيئة الإنترنت المسؤولة عن توزيـــع الأسماء والأرقام. ويمكننا القول أنها الهيئة المسؤولة فعلياُ عن الإنترنت (www.icann.org)
- ISOC (Internet Society) وتعتبر هيئة ذات أعضاء يمثلون مستثمري الإنترنت (www.isoc.org)
- IETF (Internet Engineering Task Force) وهي هيئة تطوير الإنترنت وتقييس النواحي التقنية فيها. وتعتبر هيئة مفتوحة على الجميع (www.ietf.org)

خصائص مجموعة البروتوكولات TCP/IP

- استقلالية تامة عن التكنولوجيا التي تحدد نوعية الشبكة الفيزيائية المستخدمة ومكوناتها
- توصيف قياسي لأساليب النقل وللتطبيقات
- قابلية ربط تجهيزات مختلفة ومتباينة
- توفير إمكانية الربط البيني بين عدة شبكات ونظم معلومات باستخدام أجهزة خاصة تدعى الموجهات وهو ما يوضحه الشكل التالي:



القياسات الشبكية

يجري توثيق الأعمال التقنية المرتبطة بالإنترنت وبعائلة البروتوكولات TCP/IP في وثائق تُعرف بإسم RFC (Request for Comments). إذ تنتهي جميع مواصفات البروتوكولات وكافة التعديلات وكافة النشرات الاستعلامية على شكل RFC.

تبدأ وثائق RFC عادةً حياتها كوثائق تُدعى مسودات الإنترنت، وبعد العديد من الإجتماعات والمراسلات يتم اعتماد المعيار المتفق عليه على شكل وثائق RFC متسلسلة. كما تسمح آلية التوثيق، بالإضافة إلى توثيق قياسات ومعايير البروتوكولات، بشرح المفاهيم المتعلقة ببعض الأعمال المرتبطة بإدارة الإنترنت.

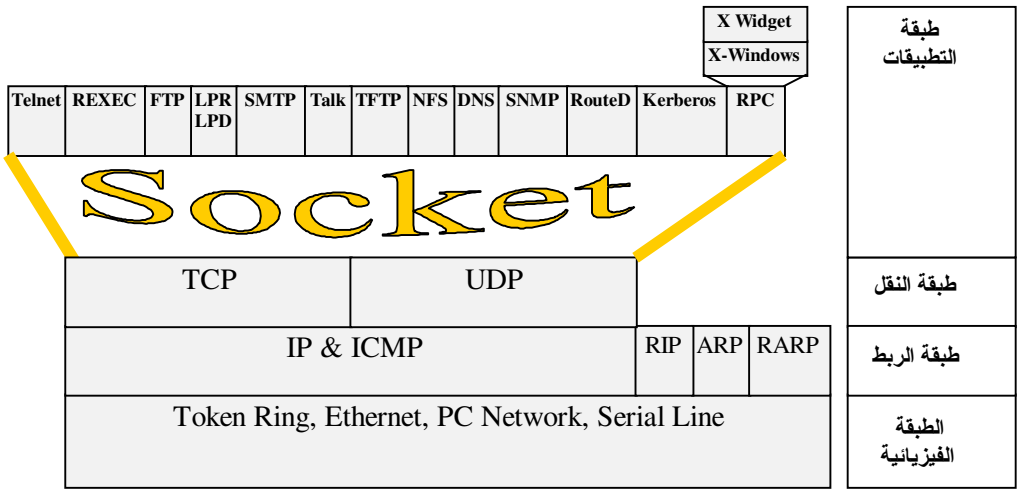
يجري ترقيم الوثائق RFC تسلسلياً. كما تمتلك الوثائق RFC عادةً عناوين ذات دلالة (مثل Algorithms for Synchronizing Network Clocks)، ولكن تجنباً للغموض، يجري عادة ذكرهم اعتماداً على أرقامهم.

لا يتم تغيير محتوى وثيقة RFC بعد اعتمادها ونشرها. ويتم توزيع التعديلات على شكل وثيقة جديدة برقم جديد. وقد اصطُلح علـــى أن تحتوي الوثائق المعدلة على جميع المعلومات التي تسمح للوثيقة الجديدة بالحلول (ولو نظرياً) مكان الوثيقة القديمة.

بالرغم من الاتفاق على أن هذه الوثائق ليست الطريقة الأكثر أناقة لتعلم موضوع ما، إلا أنه من المتفق عليه بالمقابـــل، أنهـــا تقـــدم معلومات دقيقة مفصلة ومجانية.

يمكن الحصول على الوثائق RFC من عدة مصادر من بينها الموقع www.rfc-editor.org والذي يعتبر مركـــزاً لتوزيـــع الوثـــائق السابقة وكل الوثائق المرتبطة بها.

بنية مجموعة البروتوكولات TCP/IP

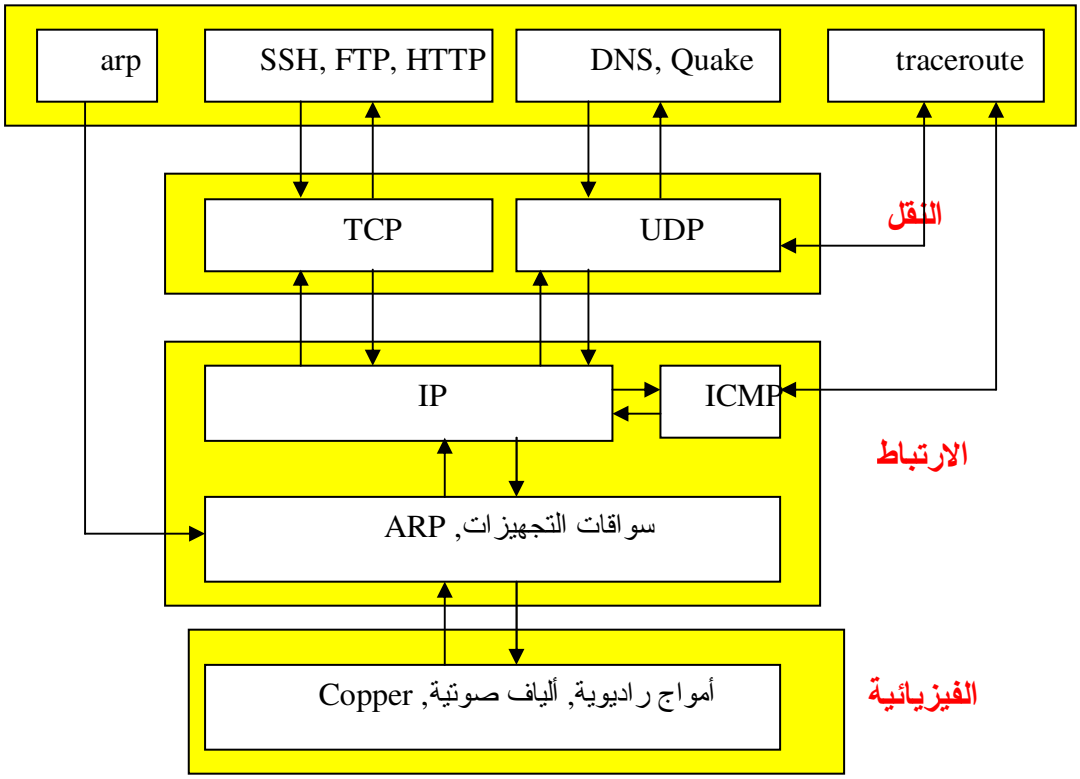


تتضمن هذه البروتوكولات مجموعة من المكونات المعرفة في عدة وثائق RFC:

- البروتوكول IP (Internet Protocol) الذي يقوم بإعداد طرود المعطيات لإرسالها من جهاز إلى آخر (RFC791)
- البروتوكول ICMP (Internet Control Message Protocol) الذي يوفر عدة مستويات دعم للبرتوكول IP تتـــضمن إدارة رسائل الأخطاء، والرسائل المساعدة في عملية التوجيه، بالإضافة إلى المساعدة في عملية سرد أعمال مجموعة البروتوكـــولات (RFC792)
- البروتوكول ARP (Address Resolution Protocol) الذي يقوم بترجمة العناوين IP إلى عناوين فيزيائية (RFC823)
- البروتوكـــــــــــــــــــــــــولان UDP (User Datagram Protocol) و TCP (Transmission Control Protocol) اللذان يديران عملية إيصال المعطيات إلى تطبيقات محددة على الجهاز الوجهـــة. إذ يقدم UDP عملية نقل غير موثوقة ولكن بأفضل سرعة ممكنة، بينما يضمن TCP عملية نقل موثوقة ثنائية الإتجاه مع مراقبـــة وتحكم بعملية التدفق، ومع تصحيح للأخطاء الناتجة عن النقل وتبادل المعطيات بين الجهازين (RFC768 و RFC793)

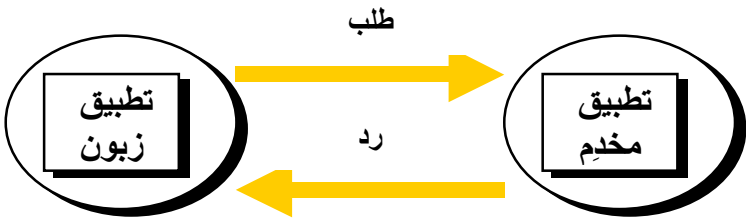
نموذج شبكة TCP/IP

الطبقة	الوظيفة
طبقة التطبيقات	استقبال برامج المستثمرين
طبقة النقل	إدارة عملية نقل المعطيات
طبقة الإرتباط (ربط المعطيات)	إدارة عملية الاتصال الأساسية والعنونة والتوجيه
الطبقة الفيزيائية	إدارة العتاد الصلب الخاص بالشبكة وسواقات الأجهزة والكابلات ووسائط البث الفيزيائية



طبقة التطبيقات

يتألف كل تطبيق من برنامجين منفصلين: الأول الزبون والثاني مخدِّم، يتخاطبان فيما بينهما بلغتهما الخاصة المدعوة "بروتوكول تطبيقي" (Application Protocol).



طبقة النقل: البروتوكولTCP

- يجري اتصال مُسبق مع الهدف (Connected Mode)
- يسمح للتطبيقات المُعتمِدة على خدماته، بإهمال مشكلة وثوقية نقل معطياتها كونه مزود بآليات تحقُق من وصول المعطيات كاملةً وبشكلها الصحيح
- يجري اتصال غير مرتبط ببنية المعلومات المُرسَلة
- يُنشئ ما يدعى بالدارة الوهمية (Virtual Circuit) بين الجهازين اللذين يشكلان طرفا الاتصال
- يشبه الاتصال TCP بأسلوب عمله، الاتصال الهاتفي

طبقة النقل: البروتوكول UDP

- لا يجري اتصال مُسبق مع الهدف (Connectionless Mode)
- لا يمتلك آليات تحقق من وصول المعطيات كاملة وبشكلها الصحيح مما يجعله يتميز بسرعة أداء أعلى من TCP
- يجري اتصال غير مرتبط ببنية المعلومات المُرسَلة
- يشبه الاتصال UDP بأسلوب عمله، الإرسال البريدي

طبقة الارتباط (طبقة ربط المعطيات)

- البروتوكولIP
  Internet Protocol

- البروتوكول ARP
  Address Resolution Protocol

- البروتوكول ICMP
  Internet Control Message Protocol

- Ethernet
- Token Ring
- Fiber Optic
- ATM

إنشاء اتصالTCP

- يحتاج الزبون لإنشاء اتصال مع مخدم بهدف ارسال حزمة معطيات
- يرسل الزبون طرداً حاوياً على طلب ندعوه طلب تزامن يحتوي مؤشر تزامن SYN (synchronization flag)؛
- يتلقى المخدم الرسالة ويرد عليها بطرد رد تزامن ندعوه SYN-ACK (SYN Acknowledgment)
- يُنشئ الزبون الإتصال بإرسال طرد للمخدم يحتوي على ACK للدلالة على ارتباطه بالمخدم وعلى بدء إرسال المعطيات، ويبدأ بعدها بإرسال طرود المعطيات

إنهاء اتصالTCP

- يضع الطرف الذي يقرر إنهاء الاتصال بوضع مؤشر FIN على طرديعبر عن طلب الإنهاء، ويُرسل هذا الطرد
- يرسل الطرف المتلقي لطلب لإنهاء طردين: طرد عليه مؤشر ACK للتأكيد على تلقيه الطرد الأول، وطرد آخر عليه مؤشر FIN
- يرسل الطرف الأول أو طالب الإنهاء طرد عليه مؤشر ACK للتأكيد على رد الطرف الثاني وينتهي عندها الاتصال

الفصل الثالث و الرابع

عنوان الموضوع:

الطبقة الفيزيائية

الكلمات المفتاحية:

تحليل فوريية، الهارمونيك، التدفق، عرض الحزمة، بنيان، بنيان فيزيائي، بنيان منطقي، كابل، أزواج مجدولة، أسلاك مُغَلَفة، أسلاك مُصفحة، محطة عمل، عقدة نهائية، العناصر الفعالة، لوحات التوزيع، خزن حائطية، مآخذ وصل جدارية، التسليك الهيكلي، البنية الهرمية–النجمية، لوحات التوزيع الفرعية، كابلات التوزيع، خزن التجهيزات، دارة محلية، مقسم هاتفي، وصلة مقسم، المعطيات الصاعدة، المعطيات النازلة، ISDN، ADSL، PRI، BRI، حزمة عريضة.

ملخص:

نستعرض في هذا الفصل العناصر الأساسية والمهمة التي تنتمي إلى الطبقة الفيزيائية من طبقات نموذج شبكي مرجعي.

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- الأساس النظري لعملية تراسل المطيات وتحليل فوريية
- العتاد الصلب الأساسي
- أسلوب التوصيل المنهجي
- الأنظمة الهاتفية وخدمات الوصل الشبكي عبر الهاتف
- خدمات الحزم العريضة

الأسس النظرية لتراسل المعطيات

يجري إرسال المعلومات على حوامل فيزيائية عبر تغيير بعض المُعاملات الفيزيائية، مما يجعل بالإمكان تمثيل التغيرات في هذه المعطيات رياضياً وخوارزمياً. فإذا مثلنا التيار الكهربائي أو الكُمون الكهربائي بتابع الزمن f(t)، يمكننا عندها اقتراح نموذج رياضي يمثل التغيرات التي تطرأ على الإشارة، ويمكننا في هذه الحالة تحليل النموذج رياضياً.

من أهم النماذج الرياضية المُستخدمة في تمثيل عمليات إرسال المعلومات، تحليل فوريية الذي وضعه الرياضي الفرنسي جان باتيست فوريية والذي أثبت أنه بالإمكان تحليل تابع رياضي دوري g(t) له الطور T، إلى سلسلة (غير منتهية نظرياً) من التوابع الدورية الجيبية.

الأسس النظرية لتراسل المعطيات: تحليل فوريية

- ليكن g(t) تابع دوري له الطور T يمثل إشارة ما. يمكن كتابة التابع على الشكل:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi n f t) + \sum_{n=1}^{\infty} a_n \cos(2\pi n f t) \quad (1)$$

حيث يمثل:

- $f = \frac{1}{T}$ التردد الأساسي للإشارة
- a_n, b_n مطالي إشارتي التجيب (cos) والجيب (sin) ذوي المرتبة n على الترتيب.

ندعو التمثيل السابق "**سلسلة فوريية**"

- يمكن التعامل مع إشارة ذات مدة محدودة (وهي حالة جميع الإشارات)، وكأنها إشارة تتكرر على نحو دوري (أي أن شكلها بين اللحظة 0 واللحظة T مشابه لشكلها بين اللحظتين T و 2T)

- بجداء طرفي المعادلة (1) بالعبارة $\sin(2\pi k f t)$ وحساب تكامل الطرفين بين 0 و T بالنسبة للزمن t، نحصل على:

$$a_n = \frac{2}{T}\int_0^T g(t)\sin(2\pi n f t)\,dt \quad (2)$$

- بجداء طرفي المعادلة (1) بالعبارة $\cos(2\pi k f t)$ وحساب تكامل الطرفين بين 0 و T بالنسبة للزمن t، نحصل على:

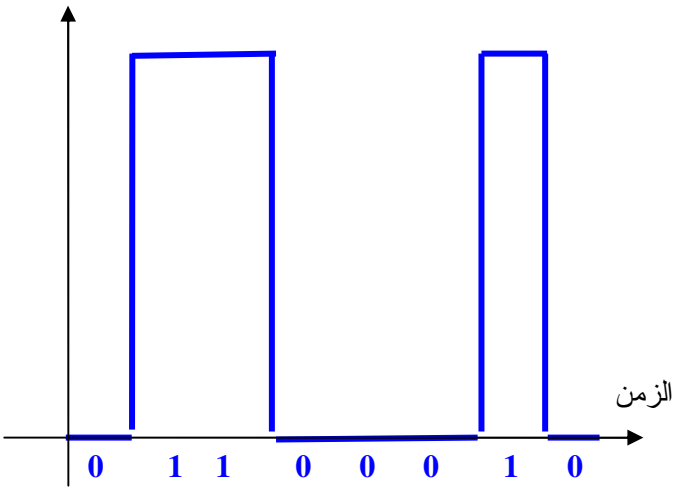
$$b_n = \frac{2}{T}\int_0^T g(t)\cos(2\pi n f t)\,dt \quad (3)$$

- من (1) و (2) و (3) يمكننا أن نستنتج: $c = \frac{2}{T}\int_0^T g(t)\,dt$

لإشارات وعرض الحزمة

لفهم العلاقة بين تحليل فوريية و إرسال المعطيات، نستعرض المثال التالي:

- يجري إرسال الحرف b المُرَّمز بالترميز ASCII على بايت كامل، عبر إرسال السلسلة الثنائية (من اليسار إلى اليمين): 0110 0010. تمثل الإشارة التالية الإشارة الخارجة من الدارة المُرسِلة في الحاسب:



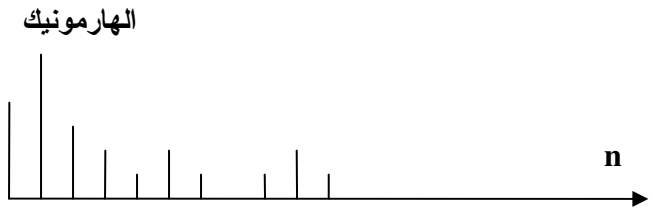
- يعطي تحليل الإشارة السابقة، وفق تحليل فوريية، المعاملات التالية:

$$a_n = \frac{1}{\pi n}\left[\cos\left(\frac{\pi n}{4}\right) - \cos\left(\frac{3\pi n}{4}\right) + \cos\left(\frac{6\pi n}{4}\right) - \cos\left(\frac{7\pi n}{4}\right)\right]$$

$$b_n = \frac{1}{\pi n}\left[\sin\left(\frac{3\pi n}{4}\right) - \sin\left(\frac{\pi n}{4}\right) + \sin\left(\frac{7\pi n}{4}\right) - \sin\left(\frac{6\pi n}{4}\right)\right]$$

$$c = \frac{3}{8}$$

- يعطي التعبير الرياضي $\sqrt{a_n^2 + b_n^2}$ القيم الوسطى للمطالات من المرتبة n، حيث تعتبرهذه القيم مهمة جداً لأن مربعاتها تتناسب مع كمية الطاقة المُرسَلة مع الإشارات عند كل تردد. ندعو مربعات القيم الوسطى للمطالات **بالهارمونيك** ونمثل هذه القيم في الشكل التالي:



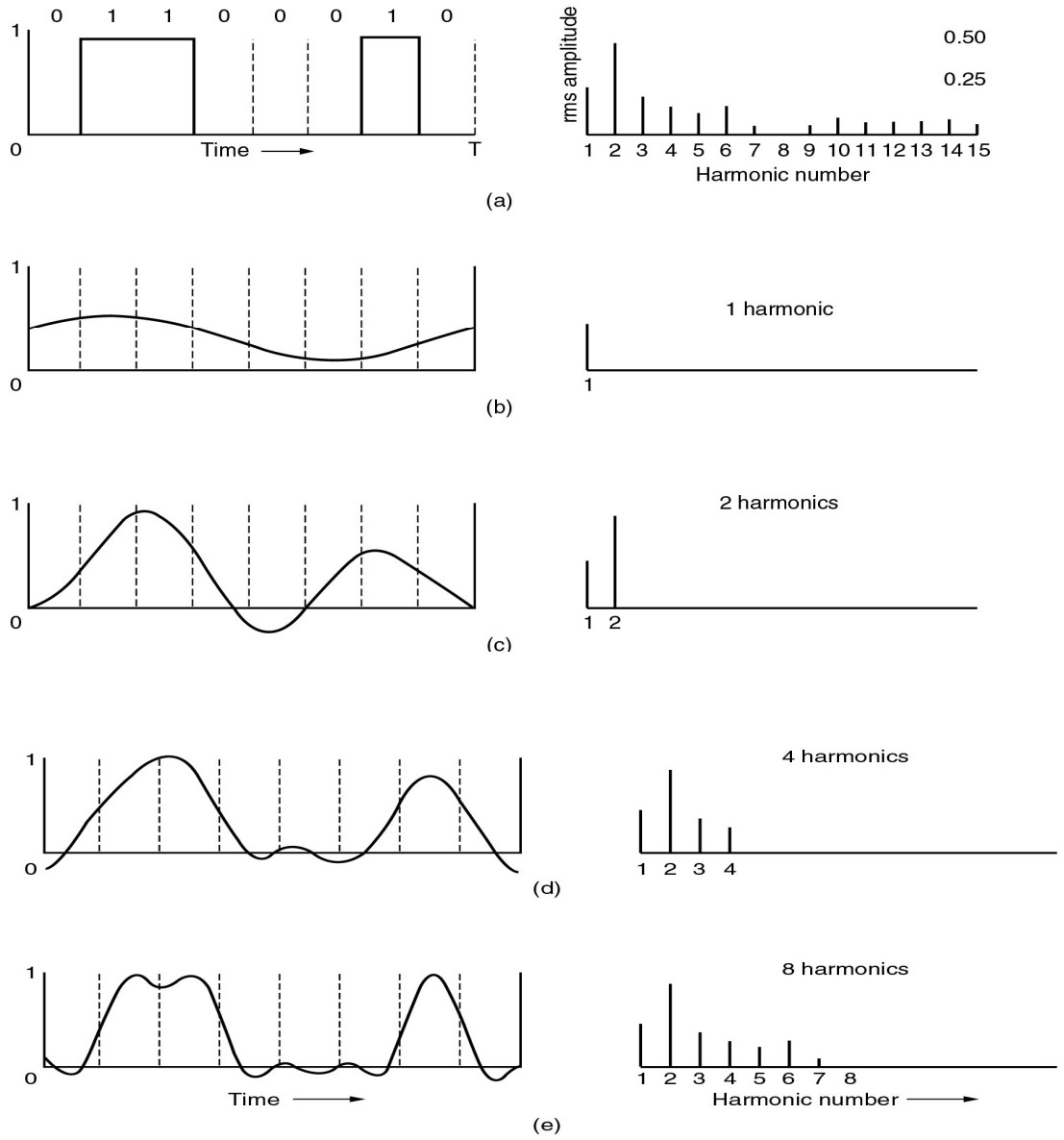
- تعاني الإشارات عند إرسالها من تخامد ناجم عن وسائط الإرسال ومحيط الإرسال مما يؤدي إلى حدوث اختلالات في المعلومات المُرسَلة. يؤثر التخامد على مطال الإشارة وبالتالي يؤثر على الهارمونيك الظاهر في الشكل السابق

- عملياً، يبقى التخامد الذي يطال مطال الإشارة مهملاً طالما أن تردد الإشارة (وهو مقلوب الطور الذي يعبر عن عدد التغيرات في الثانية) أخفض من تردد fc ندعوه تردد القطع (نُذكر هنا بأن التردد هو عدد الأطوار في الثانية ويُقدر بالهرتز). بالنتيجة، نُعرف **عرض الحزمة** بأنه مجال الترددات التي يمكن للإشارة أن تمر ضمنه دون تخامد يُذكر. فعندما يجري إرسال الإشارة على أدوات إرسال ذات عرض حزمة ضيق ينخفض عدد المطالات التي يمكن أن تمر ويصبح الشكل السابق المعبر عن هارمونيك الإشارة المارة، كما يلي:

- يكون تردد الهارمونيك الأول مساوياً لمقلوب الطور T (عدد التغيرات في الثانية) فإذا كان هو الوحيد الذي يظهر، دلّ ذلك على أن تردد القطع مساوي تماماً لتردد الإشارة

- يتغير شكل الإشارة المارة بتغير المطالات المسموح لها بالمرور، كما هو الحال فيما يلي: يرجى رسم الأشكال الظاهرة في المقترحات مع استخدام الترجمة التالية:

Time	الزمن
Harmonics	الهارمونيك
Harmonic Number	عدد الهارمونيك



- ندعو عدد التغيرات التي تطرأ على قيمة الإشارة خلال ثانية واحدة **بالبود**، وتؤثر عدد هذه التغيرات على سرعة إرسال الإشارة (بالإضافة طبعاً إلى تأثير نوعية الحامل الذي يرسل الإشارة). في حال كانت تغيرات القيم التي تطرأ على الإشارة هي تغيرات ثنائية تنحصر في قيمتين هما 0 و 1 الممثلتين لقيمتي كمون كهربائي (كما هو الحال في مثالنا)، فإن عدد التغيرات في الثانية يكون مساوياً لعدد البتات المُرسلة في الثانية (bits/s) والذي ندعوه **التدفق الثنائي**.\

- لنفرض الآن أن لدينا تدفقاً ثنائياً مقداره b بت في الثانية، يكون الزمن اللازم لإرسال ثمانية بتات ممثلة لحرف هو $\frac{8}{b}$ ثانية. يكون تردد الهارمونيك الأول هو بمقدار عدد التغيرات بالثانية أي $\frac{b}{8}$ هرتز. من ناحية أخرى يمتلك الخط الهاتفي التماثلي عرض حزمة تقارب 3000 هرتز، ويكون تردد القطع فيها قريباً من 3400 هرتز، وعليه يكون تردد الهارمونيك الأعلى الذي يمكن أن يُرسَل هو $\frac{3000}{b/8}$ أي $\frac{24000}{b}$

- يعرض الجدول التالي العلاقة بين التدفق الثنائي (لمعطيات مؤلفة من قيمتين 0 و 1) والهارمونيك:

يرجى عرض الجدول التالي ورسمه بعد تعديل العناوين وفق مايلي:

عدد الهارمونيك المُرسَلة	تردد الهارمونيك الأول مقدراً بالهرتز	الطور T مقدراً بالميلي ثانية	التدفق مقدراً بالبت في الثانية

Bps	T (msec)	First harmonic (Hz)	# Harmonics sent
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

-

نُعرف **عرض الحزمة** بأنه مجال الترددات التي يمكن للإشارة أن تمر ضمنه دون تخامد يُذكر.

ندعو عدد التغيرات التي تطرأ على قيمة الإشارة خلال ثانية واحدة **بالبود**، وتؤثر عدد هذه التغيرات على سرعة إرسال الإشارة (بالإضافة طبعاً إلى تأثير نوعية الحامل الذي يرسل الإشارة). في حال كانت تغيرات القيم التي تطرأ على الإشارة هي تغيرات ثنائية تنحصر في قيمتين هما 0 و 1 (كما هو الحال في مثالنا)، فإن عدد التغيرات في الثانية يكون مساوياً لعدد البتات المُرسلة في الثانية والذي ندعوه **التدفق الثنائي**.

تعريف التدفق

يُعبِّر التدفق ضمن مقطع شبكي عن الكمية العظمى للمعطيات التي يمكن إرسالها عبر وصلة هذا المقطع خلال فترة زمنية. يُقدَر التدفق بالبِت في الثانية (Bits by Second).

يختلف مستوى التدفق باختلاف العتاد الصلب المُستخدم. ويتعلق التدفق بالبطاقة الشبكية المتصلة بالعقدة الشبكية (الحاسب، أو المُخدِّم، أو غيرها) والتي تشكل أحد أطراف المقطع الشبكي، وببوابة الموزع التي تشكل الطرف الآخر من المقطع الشبكي، وبنوعية الأسلاك المُستخدمة وأطوالها.

عتاد الشبكات المحلية

العتاد الصلب الأساسي:

- الحامل
  - أسلاك نحاسية: كبلات متناظرة، وكبلات غير متناظرة
  - ألياف ضوئية
- الموزعات
- المُلحقات

أساليب الوصل الشبكي ومبادئه

سنستعرض في هذا الفصل عتاد الشبكات المحلية ذات التدفق العالي من خلال التركيز على حامل الشبكة المؤلف من أسلاك الربط وعلى المُبدلات، ومن خلال إعطاء لمحة عن أساليب الوصل الشبكية ومبادئها.

علاقة التشكيل الشبكي الفيزيائي بأسلوب العمل

لكل شبكة محلية تشكيل فيزيائي حقيقي ندعوه بالطبولوجيا الفيزيائية، بالإضافة إلى منطق عمل ندعوه بالطبولوجيا المنطقية:

- تمثل الطبولوجيا الفيزيائية حقيقة الربط الشبكي وطريقة توزع الأسلاك وارتباطها ببعضها البعض. فالتشكيل النجمي يعني، من الناحية الفيزيائية، وجود موزع مركزي (وهو مركز تجميع للأسلاك) تتفرع منه أسلاك باتجاه عقد الشبكة
- في حين تعكس الطبولوجيا المنطقية أسلوب الاتصال المُتَّبع. فقد تعمل الشبكة ذات التشكيل الفيزيائي النجمي، بأسلوب حلقي، بحيث يتم التراسل بين العقد المتصلة بالموزع وكأنها متصلة بحلقة لا يحق فيها لأي محطة البدء بالإرسال قبل حلول دورها. في هذه الحالة يمثل الموزع، حلقة النقل

علاقة التشكيل الشبكي الفيزيائي بأسلوب العمل

لكل شبكة محلية تشكيل فيزيائي حقيقي ندعوه بالطبولوجيا الفيزيائية، بالإضافة إلى منطق عمل ندعوه بالطبولوجيا المنطقية:

- تمثل الطبولوجيا الفيزيائية حقيقة الربط الشبكي وطريقة توزع الأسلاك وارتباطها ببعضها البعض. فالتشكيل النجمي يعني، من الناحية الفيزيائية، وجود موزع مركزي (وهو مركز تجميع للأسلاك) تتفرع منه أسلاك باتجاه عقد الشبكة
- في حين تعكس الطبولوجيا المنطقية أسلوب الاتصال المُتَّبع. فقد تعمل الشبكة ذات التشكيل الفيزيائي النجمي، بأسلوب حلقي، بحيث يتم التراسل بين العقد المتصلة بالموزع وكأنها متصلة بحلقة لا يحق فيها لأي محطة البدء بالإرسال قبل حلول دورها. في هذه الحالة يمثل الموزع، حلقة النقل

الحامل: الكابلات المتناظرة

لهذه الكابلات نمطين أساسيين يتعلق بعدد النواقل التي يتألف منها الكابل:

1. الزوج المجدول:
   - يتألف من زوج من الأسلاك المجدولة
   - لها مقاومة من مرتبة 100أوم، أو 120أوم، أو 150أوم
   - تكون نسبة شدة الحقل الكهربائي إلى شدة الحقل المغناطيسي ثابتة على طول السلك
2. السلك الرباعي:
   - الذي يتألف من أربعة نواقل:
     - إما على شكل زوجين مجدولين
     - أو على شكل أربعة أسلاك منفصلة

يمكن تصنيع الكابلات المتناظرة على نحوٍ يسمح بتأمين عزلها عن أثار التحريض الكهرطيسي الناجم عن مرور كابلات تغذية كهربائية بالقرب منها. يتم العزل:

- بالتغليف: ويعني تغليف مجموعة الأسلاك بطبقة معدنية إضافية أو بطبقة رقيقة من الألمنيوم
- أو بالتصفيح: ويعني إحاطة كل زوج بطبقة معدنية أو بطبقة رقيقة من الألمنيوم

من أهم فئات الكابلات المتناظرة:

- كابلات زوجية غير مصفحة وغير مغلفة ندعوها كابلات U.T.P مثل كابلات ATT Cat 5 و Alcatel
- كابلات مغلفة ندعوها F.T.P مثل +INRA، و ACOME، و INTERCO
- كابلات مغلفة ومصفحة: S.F.T.P مثل ITT
- كابلات ذات زوج مصفح: S.T.P مثل IBM Type 1

كابلات ذات أسلاك مجدولة غير مصفحة

كابلات ذات أسلاك مجدولة مُصفحة

لهذه الكابلات نمطين أساسيين يتعلق بعدد النواقل التي يتألف منها الكابل:

3. الزوج المجدول:
   - يتألف من زوج من الأسلاك المجدولة
   - لها مقاومة من مرتبة 100أوم، أو 120أوم، أو 150أوم
   - تكون نسبة شدة الحقل الكهربائي إلى شدة الحقل المغناطيسي ثابتة على طول السلك
4. السلك الرباعي:
   - الذي يتألف من أربعة نواقل:
     - إما على شكل زوجين مجدولين
     - أو على شكل أربعة أسلاك منفصلة

يمكن تصنيع الكابلات المتناظرة على نحوٍ يسمح بتأمين عزلها عن أثار التحريض الكهرطيسي الناجم عن مرور كابلات تغذية كهربائية بالقرب منها. يتم العزل:

- بالتغليف: ويعني تغليف مجموعة الأسلاك بطبقة معدنية إضافية أو بطبقة رقيقة من الألمنيوم
- أو بالتصفيح: ويعني إحاطة كل زوج بطبقة معدنية أو بطبقة رقيقة من الألمنيوم

من أهم فئات الكابلات المتناظرة:

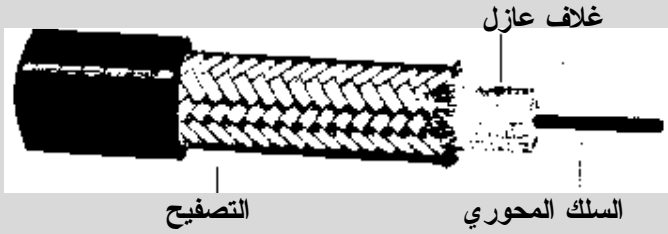
- كابلات زوجية غير مصفحة وغير مغلفة ندعوها كابلات U.T.P **(نقرؤها يو تي بي)** مثل كابلات ATT Cat 5 **(نقرؤها إي تي كات فايف)**، و Alcatel
- كابلات مغلفة ندعوها F.T.P **(نقرؤها إف تي بي)** مثل +INRA، و ACOME، و INTERCO
- كابلات مغلفة ومصفحة: S.F.T.P **(نقرؤها إس إف تي بي)** مثل ITT
- كابلات ذات زوج مصفح: S.T.P **(نقرؤها إس تي بي)** مثل IBM Type 1

الحامل: الكابلات غير المتناظرة

لهذه الكابلات نمطين أساسيين يتعلق بطريقة تركيب النواقل التي يتألف منها الكابل:

- كابل محوري:
  - مؤلف من ناقل محوري محاط بغلاف مطاطي عازل
  - بالإضافة إلى ناقل خارجي يحيط بالناقل المحوري ويتوضع بين غلاف الناقل المحوري والغلاف الخارجي
- كابل ثنائي المحور:
  - مؤلف من ناقلين محوريين محاط كل منهما بغلاف مطاطي عازل
  - بالإضافة إلى ناقل خارجي يحيط بالناقلين المحوريين ويتوضع بين غلاف الناقلين والغلاف الخارجي
  - يمتاز هذا النوع بتأمين نوعية نقل أفضل

عادةً، تكون نسبة قطر الناقل الخارجي إلى قطر الناقل المحوري تساوي 3.5 تقريباً



كابلات محورية

الألياف الضوئية

تتألف الكابلات المُصنَّعة من الألياف الضوئية، من اسطوانة رفيعة جداً تُشكل السلك المحوري، وتكون مُحاطة بطبقة من الزجاج، أسطوانية الشكل، ندعوها بالغلاف الضوئي، والتي تكون مُحاطة بدورها بغلاف عازل.

تنتقل الإشارات المُعَبرة عن المعلومات المتبادلة على شكل نبضات ضوئية.

غلاف عازل الغلاف الضوئي الزجاجي السلك المحور

بعض المعايير المرتبطة بالكابلات المستخدمة

	الكابلات النحاسية المجدولة	الكابلات المحورية	الكابلات الضوئية
الكلفة	منخفضة للكابلات غير المُصفحة ومرتفعة للكابلات المُصفحة	متوسطة	عالية
الطول الأعظمي للكابل الواصل بين عقدتين قبل حدوث تخامد في الإشارة	100 متر	150 متر	بين 500 متر و 3000 متر حسب نمط الكبل الضوئي
مستوى عزل الكابل عن الحقول الكهرطيسية الناجمة عن التمديدات الكهربائية	منخفض في حال اختيار كبل غير مُصفِّح أو غير مُغَلَّف، عالي في حال اختيار كابل مصفح	متوسط	عالي جداً
الوثوقية	جيدة	جيدة	ممتازة
التدفق الممكن عبر هذه الكابلات	1000/100 ميغابت في الثانية	10 ميغابت في الثانية	10000/1000/100 ميغابت في الثانية

الموزعات: مبدلات أو مُجمعات

هي عبارة عن أجهزة ذات بوابات يتصل بكل بوابة منها كابل يعمل على ربط حاسب من حواسب الشبكة. يُعتبر الشكل الأساسي للموزعات والذي كان يُدعى المكررات، أحد عتاديات الطبقة الفيزيائية في حين لاتُعتبر المبدلات التي لايقتصر عملها على التقوية والتكرار، من ضمن عتاديات اطبقة الفيزيائية ولكننا سنستعرضها هنا بسرعة ونعود إليها لاحقاً بالتفصيل.

عندما يرسل حاسب متصل بالموزع معطيات إلى حاسب آخر متصل بدوره بالموزع فإن المعطيات تمر عبر الموزع عند انتقالها بين الحاسبين.

تُعتبر المبدلات الموزعات الأساسية المُستخدمة في الشبكات المحلية لما توفره من سرعةً عالية وأمان أفضل. وتحقق المُبدلات عادةً المواصفات العامة التالية:

- مزودة بعدة بوابات (8، 12، 16، 24، 48، 64) بحيث تتصل كل بوابة منها بمحطة عمل أو بمبدلة أخرى
- مزودة بمؤشرات ضوئية ظاهرة LED تُظهر صحّة عمل كل بوّابة من بواباتها
- قابلة للتركيب داخل خزن خاصة لحمايتها
- تكون المُبدلات الحديثة قابلة للإدارة عن بُعد باستخدام بروتوكولات شبكية خاصة تسمح بمراقبة عمل المُبدلة اعتباراً من محطة عمل وتغيير إعداداتها إذا لزم الأمر

الملحقات

البطاقات الشبكية:

يجري تركيبها ضمن الحاسب وتشكل واجهة الاتصال الفيزيائية بينه وبين الكابل، ويجري عبرها إرسال المعطيات من الحاسب إلى الكابل باتجاه حاسب آخر. تساعد البطاقة الشبكية على تحضير المعلومات المُراد إرسالها عبر الشبكة والتحكم بعملية الإرسال كما تقوم باستقبال المعلومات الواردة من الشبكة لإيصالها إلى الحاسب.

بما أن البطاقة الشبكية ترتبط بالكابل، فإن اختلاف نوع الكابل المُستَخدم يؤدي لاختلاف نوع البطاقة الشبكية. فاستخدام كابل محوري يُحَتم وجود مدخل خاص بهذا الكابل على البطاقة الشبكية، في حين يُحتم اختيار كابلات نحاسية ثنائية، اختيار بطاقة شبكية لها مداخل خاصة بهذه الكابلات وتعمل بنفس سرعة التدفق الأعظمي للكابل أو بسرعة تدفق أكبر.

خزن التجهيزات

وهي عبارة عن مكان مقفول توضع فيه العناصر الفعالة للشبكة (المبدلات، المجمعات، وغيرها) وذلك بغية حمايتها من العبث غير المسموح به، أو من العوامل المحيطة كالحرارة، والرطوبة، والغبار. كما تساهم خزن التجهيزات بإعطاء مظهر متناسق لتجهيزات الشبكة. تُزوَد خزن التجهيزات عادةً بمراوح داخلية للمحافظة على درجة حرارة ورطوبة مناسبتين، إضافةً إلى وجود مؤشرات تبين الوضع الراهن للعمل دون الحاجة إلى فتحها فيزيائياً.

لوحات التوزيع:

لتنظيم دخول كابلات التوصيل إلى الخزن التي تحوي المُبدلات وقبل وصولها إلى بوابات المُبدلة، توضع لوحة توزيع مزودة بعدد من المخارج من النمط RJ45 ، حسب عدد بوابات المُبدلة، وتكون متوافقة مع كابلات التوصيل .

مبادئ الوصل الشبكي

يشكل عام، يتم اتباع منهجية التسليك الهيكلي في تصميم ووصل الشبكات بحيث يتوافق التصميم مع المعيار ISO 11801 الذي يعتمد على استراتيجية البنية الهرمية – النجمية حيث يتم تمديد أسلاك الشبكة ضمن الأبنية على مستويين:

- مستوى أفقي
- مستوى شاقولي

قبل التطرق لتفاصيل الوصل الأفقي والشاقولي، نستعرض فيما يلي المبادئ العامة التي يجب على عملية التصميم والوصل أن تحققها للشبكة:

- أن توفر الأداء الأمثل ونوعية الخدمة الأفضل
- أن تكون كلف التثبيت والاستثمار كلف مناسبة لما هو مطلوب
- أن تكون متوافقة مع المعايير الدولية
- أن تكون سهلة الاستثمار
- أن تكون طبولوجيا التوزيع الفيزيائية، نجمية ليكون قابلاً للتوسع بسهولة
- أن تكون الطبولوجيا المنطقية مستقلة عن الطبولوجيا الفيزيائية
- أن تعتمد على التقنيات الأكثر انتشاراً والتي أثبتت فعاليتها (نهايات ورؤوس RJ45 على مستوى محطات العمل على سبيل المثال)
- أن تحترم القواعد المتعلقة بقدرات التقنيات المستخدمة (الأطوال العظمى للكابلات مثلاً)
- أن تعتمد مبدأ توزيع نجمي اعتباراً من موزع مركزي متصل عمودياً بموزعات فرعية، بحيث يكون كل موزع فرعي مسؤولاً عن الوصل الأفقي

الوصل الأفقي

يُعبر الوصل الأفقي عن عملية تركيب ووصل مكونات الشبكة الخاصة بطابق واحد (نسميها أيضاً الشبكة الطابقية)، وتشمل مآخذ الوصل، ولوحات التوزيع الفرعية، والعناصر الفعالة أي الموزعات سواء كانت مجمعات أو مبدلات، والأسلاك الواصلة بين مآخذ الوصل والعناصر الفعالة.

يمكن وضع هذه التجهيزات ضمن خزانة أو عدة خزن خاصة في كل طابق، ومع مراعاة الأطوال الحدية للأسلاك الواصلة بين مآخذ الوصل والعناصر الفعالة.

فيما يلي عرض للمكونات الشبكية التي يتم تركيبها أثناء عملية الوصل الأفقي:

- العناصر الفعالة أو الموزعات
- العناصر غير الفعالة
  - المآخذ الجدارية
  - كابلات الوصل

أما منهجية الوصل فتكون على النحو التالي:

- وصلة أولى بين حاسب المستخدم والمأخذ الجداري
- تليها وصلة بين المأخذ الجداري ولوحة التوزيع
- ثم وصلة بين لوحة التوزيع والمبدلة

يُعبر الوصل الأفقي عن عملية تركيب ووصل مكونات الشبكة الخاصة بطابق واحد أو بمستوى أفقي واحد (نسميها أيضاً الشبكة الطابقية)، وتشمل مآخذ الوصل الجدارية، ولوحات التوزيع الفرعية، والموزعات سواء كانت مُجمعات أو مُبدلات، بالإضافة إلى الكابلات الواصلة بين مآخذ الوصل الجدارية والموزعات.

يمكن وضع هذه التجهيزات ضمن خزن خاصة، ومع مراعاة الأطوال الحدية للكابلات الواصلة بين مآخذ الوصل الجدارية والموزعات.

فيما يلي عرض للمكونات الشبكية التي يتم تركيبها أثناء عملية الوصل الأفقي:

- **العناصر الفعالة أو الموزعات:** تكوِّن هذه العناصر قلب الشبكة وتكون مسؤولة عن تبادل المعلومات بين بواباتها المتصلة بالحواسب عن طريق المآخذ الجدارية. تكون هذه الموزعات عبارة عن مبدلات أو مُجمعات. تُستخدم حالياً المبدلات التي تؤمن اتصال أكثر أماناً وأكثر سرعةً من المُجمعات.
- **العناصر غير الفعالة:** ويُقصد بها المآخذ الجدارية والكابلات التي تسمح بوصل التجهيزات بالمبدلات. ونحتاج هنا إلى العناصر التالية:
  - **المآخذ الجدارية:** وهي العناصر التي تتوضع في نهاية الأسلاك القادمة من المُبدلات وتتصل بها التجهيزات. تُعتبر المآخذ من النوع RJ45 ، الأكثر شيوعاً في هذا النوع من الشبكات، نظراً لتوافقها مع الأسلاك النحاسية المجدولة وسهولة تركيبها.
  - **كابلات الوصل:** وهي الكابلات التي تصل بين المآخذ الجدارية والمُبدلات من جهة، وبين المآخذ الجدارية والتجهيزات الحاسوبية من جهة أخرى. ففي الشبكات المحلية تُستخدَم أنواع عديدة من الكابلات أشهرها وأكثرها استخداماً هي الكابلات ذات الأسلاك النحاسية المجدولة المُصفحة أو العادية. تسمح هذه الكابلات بتمرير المعطيات بسرعة كافية لتحقيق المتطلبات.

أما منهجية الوصل المُتَّبعة في الوصل الأفقي فتكون كما يلي:

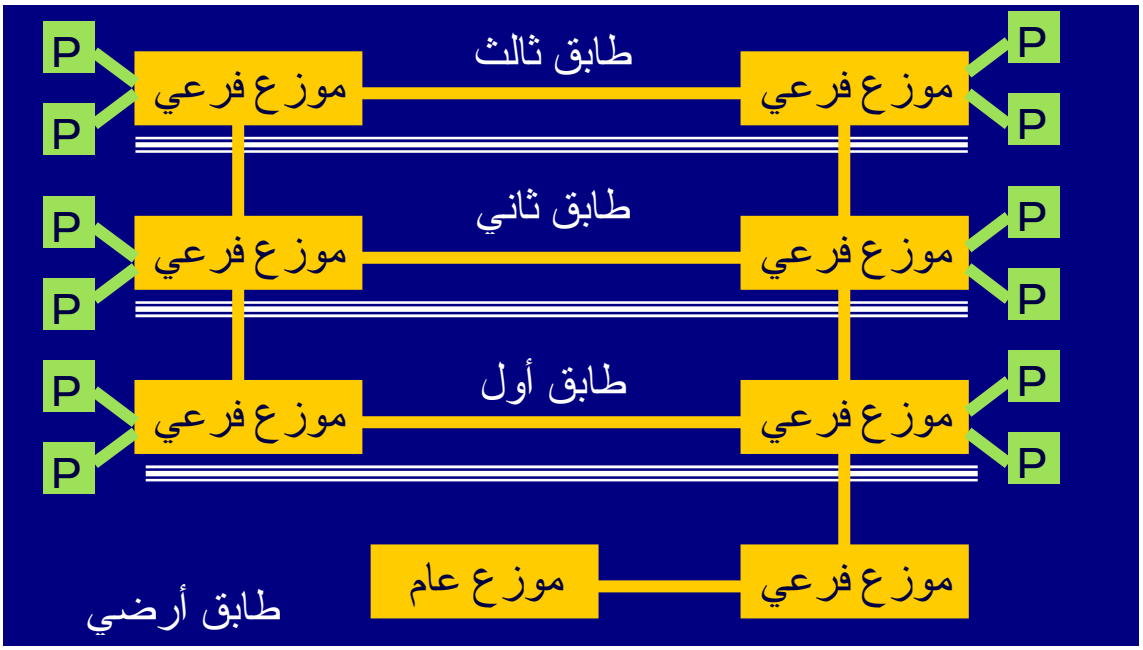
لضمان مرونة الوصل وإمكان تبديل وصل المآخذ الجدارية بسهولة، توضع لوحة توزيع بجانب كل مُبدلة، وبحيث لا تزيد المسافة العظمى بين المُبدلة وأي مأخذ من مآخذ الوصل الجدارية عن الطول الأقصى المقبول للكابل. وبذلك يتم الوصل بين المستخدم والمُبدلة على ثلاث مراحل:

- وصلة أولى بين حاسب المستخدم والمأخذ الجداري، حيث تتصل محطة العمل بالمأخذ عن طريق كابل قياسي بطول 3 متر أو 5 متر.
- تليها وصلة بين المأخذ الجداري ولوحة التوزيع، حيث تتصل المآخذ الجدارية مع الطرف الأول للوحة التوزيع عن طريق كابلات مارة ضمن سكك معدنية أو مجاري بلاستيكية جدارية حتى علب المآخذ الجدارية.
- وأخيراً وصلة بين لوحة التوزيع والمُبدلة، حيث يتصل مخرج المُبدلة مع الطرف الثاني للوحة التوزيع مباشرةً، وهي عملية بسيطة نظراً لكونهما متوضعان في نفس المكان. نستخدم لذلك كابلات قياسية تسمى كابلات التوزيع وبطول يقل عن 1م.

الوصل الشاقولي

يهدف المستوى الشاقولي إلى تأمين الوصل بين الشبكات الطابقية المختلفة:

- يُعبر الوصل العمودي عن عملية الربط التي تقوم بوصل الموزعات فيما بينها. تتألف الكابلات من:
  - الكابلات الشاقولي: وهي كابلات وصل ذات استطاعة عالية تصل بين موزع مركزي وموزع فرعي
  - كابلات الفروع: وهي كابلات وصل ذات استطاعة عالية تصل بين الموزعات الفرعية
- يتصل كل موزع بمجموعة من الموزعات الأخرى لإنشاء طبولوجيا متشابكة
  - تسمح بوصل أي نقطتين اعتماداً على أقصر طريق ممكن
  - وتمتلك سماحية ضد الأعطال
- يجري توصيل كافة الخزن الطابقية الموزعة ضمن مبنى إلى خزانة مركزية موجودة في مكان يتم تحديده مسبقاً وعلى نحو يحقق وصل أمثلي لكافة الشبكات الطابقية. يجب تأمين كافة شروط العزل والتهوية والتمديدات الكهربائية لضمان عمل تجهيزات الشبكة بالشكل المناسب في الأماكن المختارة

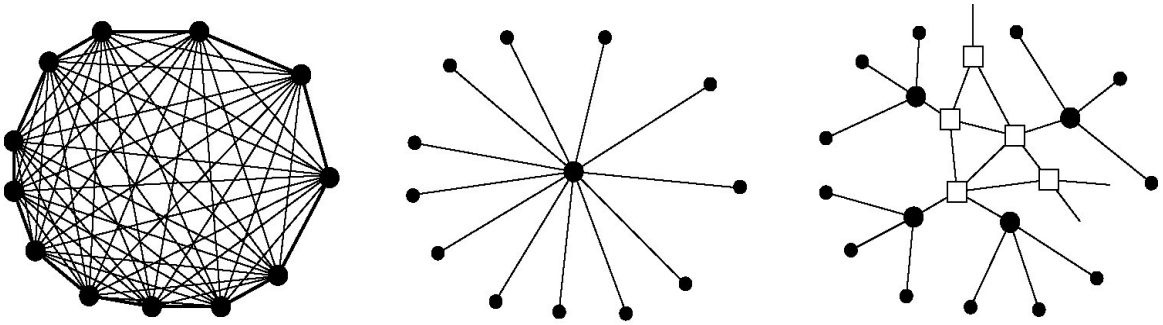


نشاط

بفرض أنك تحتاج لتجهيز شبكة حاسوبية. بالتعاون مع المشرف:

إبحث عن مواصفات فنية تفصيلية لعناصر غير فعالة (مآخذ جدارية، كابلات توصيل، لوحات توزيع) اعتباراً من المواقع التالية:
www.3M.com
www.dlink.com

- للأنظمة الهاتفية أشكال متعددة:



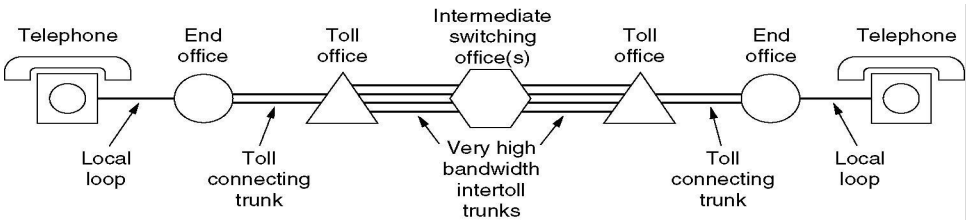
(a) (b) (c)

a. شبكية كاملة الارتباط
b. نجمية ذات مبدلة مركزية
c. هرمية لها عدة مستويات

- تتألف دارة هاتفية مصممة لاتصالات متوسطة المدى من العناصر الأساسية التالية:
  - **الدارة المحلية** المؤلفة من مجموعة الكابلات النحاسية المجدولة التي تصل المنزل أو المكتب أو أي موقع بالدارة المحلية
  - **وصلات المقاسم** المكونة من مجموعة الكابلات الليفية التي تصل المقاسم المحلية بمقاسم التبديل
  - **مقاسم التبديل** المسؤولة عن تحويل الاتصالات من وصلة إلى أخرى

- يمكن تمثيل الدارة الهاتفية الآنفة الذكر على الشكل التالي:

يرجى رسم الشكل التالي مع ترجمة المقاطع الإنكليزية وفق الجدول المرافق:



- للأنظمة الهاتفية أشكال متعددة:

d. شبكية كاملة الارتباط
e. نجمية ذات مبدلة مركزية
f. هرمية ذات مستويين

- تتألف دارة هاتفية مصممة لاتصالات متوسطة المدى من العناصر الأساسية التالية:
  - **الدارة المحلية** المؤلفة من مجموعة الكابلات النحاسية المجدولة التي تصل المنزل أو المكتب أو أي موقع بالدارة المحلية

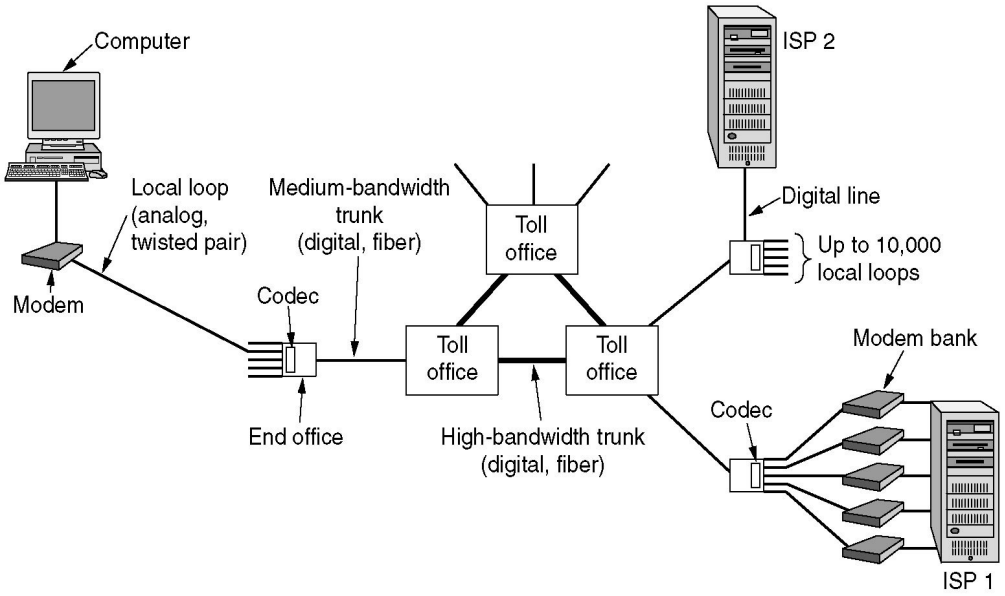
- **وصلات المقاسم** المكونة من مجموعة الكابلات الليفية التي تصل المقاسم المحلية بمقاسم التبديل
- **مقاسم التبديل** المسؤولة عن تحويل الاتصالات من وصلة إلى أخرى

Telephone	تليفون
Local Loop	دارة محلية
End Office	مقسم محلي
Toll Office	مقسم
Intermediate Switching Office	مقسم تبديل
Toll Connecting Trunk	وصلة مقاسم
Very High bandwidth Intertoll Trunck	وصلة تبديل ذات سعة عالية

الدارة المحلية: مودمات، ISDN، ADSL

يمكن التعبير عن اتصال شخص ما بمزود خدمة الإنترنت اعتباراً من مودم محلي متصل بالمنظومة الهاتفية من خلال الشكل التالي:

يرجى رسم الشكل التالي مع ترجمة العبارات وفق الجدول المرافق



Computer	حاسوب
Local Loop (analog twisted pair)	دارة محلية (زوج مزدوج تماثلي)
Modem	مودم
Codec	جهاز ترميز/فك ترميز
End Office	مقسم محلي
Toll Office	مقسم

وصلة متوسطة السعة (رقمية، ليفية)	Medium-bandwidth trunk (digital, fiber)
وصلة عالية السعة (رقمية، ليفية)	Medium-bandwidth trunk (digital, fiber)
مزود خدمة	ISP
خط رقمي	Digital Line
أكثر من 10000 دارة محلية	Up to 10000 Local Loop
مجموعة مودمات	Modem Bank

المودمات الهاتفية العادية

تتلخص مهمة المودم في تحويل المعطيات من إشارات الحاسب الرقمية إلى إشاراتٍ تماثليةٍ صوتيةٍ يجري إرسالها عبر خطوط الهاتف، ومن ثم تحويل المعطيات القادمة إلى الحاسب من تماثليةٍ صوتية إلى رقمية. لذا أتى مصطلح: Modem من مصطلحي تعديل الإشارة **MOdulate** وفك تعديل الإشارة **DEModulate**.

يغذي الحاسب المودم بالمعطيات الرقمية الثنائية اعتباراً من المعالج، ويحول المودم هذه المعطيات إلى إشارات تماثلية يجري إرسالها عبر خطوط الهاتف. يستلم المودم الموجود في الطرف الآخر هذه الإشارات، ويعيد تحويلها إلى معطيات رقمية ويرسلها إلى معالج الجهاز.

تشير كلمة **تماثلي** إلى المعطيات التي يجري تمثيلها وبثها بشكلٍ مستمر، في حين ترمز كلمة **رقمي** إلى معطيات يجري بثها على مراحل، لذا تأخذ الإشارات التماثلية في مخطط بياني شكل موجاتٍ جيبية، في حين تأخذ الإشارات الرقمية شكل الموجات المربعة. تتميز المعطيات الرقمية بعدم تأثرها بالتشويش أو الضجيج الموجود على خطوط الهاتف.

يعتبر الصوت إشارةً تماثليةً، فهو متواصل ولاينقطع. ولكي يتم إرسال المعطيات عبر خط الهاتف، يحول المودم المعطيات الرقمية إلى إشارات صوتية أو تماثلية. ويحول المودم الذي يستقبل المعطيات بدوره هذه الإشارات الصوتية إلى أصلها الرقمي.

سرعات المودمات الهاتفية العادية

- تصل سرعة المودم اليوم إلى 56 كيلوبت/الثانية. وقد كانت سرعة المودمات الأقدم لاتتجاوز 33 كيلوبت/الثانية (33.600 بت/الثانية)
- يجري تحويل الإشارات الرقمية إلى أخرى تماثلية وبالعكس، في مقياس **V.34**، وتكون الحدود القصوى لنقل المعطيات هي 35 كيلوبت/الثانية نظرياً
- يختلف مقياس **V.90** الذي يُعرَف بإسم "**تقنية التعديل الرمزي للنبضة**"عن نظام **V.34**، بأنه يفترض أن شبكة مؤسسة

الهاتف العامة هي شبكة رقمية، لذا تصل سرعة المودمات التي تستخدمه إلى 56 كيلوبت/الثانية

- تُعتبر عملية نقل المعطيات عمليةً لامتناظرة، لذا تُرسَل المعطيات من المودم، والتي نسميها **المعطيات الصاعدة** تماثلياً، بنفس طريقة نظام **V.34** للإرسال، وتُستَقبَل **المعطيات النازلة** بسرعات أكبر باستخدام تقنيات نظام **V.90**

يجري تقييم المودمات على أساس سرعة نقل المعطيات بالثانية. تصل سرعة المودم اليوم إلى 56 كيلوبت/الثانية. وقد كانت سرعة المودمات الأقدم لاتتجاوز 33 كيلوبت/الثانية (33.600 بت/الثانية). طبعاً، هناك موديمات رقمية أسرع مثل موديمات نظام خط **ISDN** المزدوج الاستعمال التي سندرسها لاحقاً، والتي توفر سرعات عالية تصل إلى (128 كيلوبت/الثانية).

لتلافي المشاكل الناجمة عن اختلاف سرعات المودمات المُرسِلة والمُستقبِلة، يجري التحكم بالتدفق إما عن طريق البرمجيات أو عن طريق العتاديات. فعندما يجري التحكم بالتدفق عن طريق البرمجيات، يقوم المودم المُستقبِل بإعلام المُرسِل بالتوقف مؤقتاً، ويتم ذلك بإرسال إشارة رمز خاص **(Control-S)**. وعندما يصبح المودم جاهزاً للاستقبال مرة أخرى يقوم بإرسال إشارة رمز آخر **(Control-Q)**. أما التحكم بالتدفق عن طريق العتاديات فيعتمد على الأسلاك الموجودة في كبل الموديم، أو عتاديات الموديم إذا كان داخلياً. ويعتبر هذا الأسلوب أسرع وأكثر وثوقية من التحكم بالتدفق عن طريق البرمجيات.

يفترض نظام المودمات التقليدي أن طرفي الاتصال يستخدم في حواره خط اتصال يمر عبر منظومة هاتفية تعود لمؤسسة الهاتف التي قد تحتفظ بمقاسم تماثلية، عندها يجري تحويل الإشارات الرقمية إلى أخرى تماثلية، ومن ثم إلى رقمية مرة أخرى، الأمر الذي يُخفِّض من سرعات النقل إلى 33.6 كيلوبت/الثانية (أي 33600 بت في الثانية)، وخاصةً إذا كانت تقنية المودم تستخدم مقياس **V.34**، ولأن الحدود القصوى لنقل المعطيات على شبكات مؤسسات الهاتف العامة التماثلية لاتتجاوز 35 كيلوبت/الثانية نظرياً.

يختلف نظام **V.90** عن نظام **V.34**، حيث يفترض هذا النظام بأن شبكة مؤسسة الهاتف العامة هي شبكة رقمية، لذا تستطيع المودمات التي تستخدم هذه التقنية تسريع استقبال المعطيات من الانترنيت إلى الحاسب بسرعات تصل إلى 56 كيلوبت/الثانية. وبهذا يختلف هذه النظام عن غيره من المقاييس المستخدمة في المودمات الأخرى، فهو يقوم بترميز المعطيات القادمة عوضاً عن تعديلها (وهو مايجري في الموديمات التماثلية). وتُعرَف تقنية نظام **V.90** أيضا باسم "**تقنية التعديل الرمزي للنبضة**".

عموماً، تُعتبر عملية نقل المعطيات عمليةً لامتناظرة، إذ لايتطلب إرسال المعطيات التي تتألف في أغلب الأحيان من أوامر بسيطة من لوحة المفاتيح، أو تعليمات صادرة من حركات مؤشر الفأرة، حزمات إرسال عريضة، وبالتالي لايحتاج لسرعات إرسال أكثر من 33.6 كيلوبت/الثانية. لذا تُرسَل المعطيات من المودم، والتي نسميها **المعطيات الصاعدة** تماثلياً، بنفس طريقة إرسال المودمات التي تستخدم نظام **V.34** للإرسال، ويبقى الفرق الوحيد هو في استقبال **المعطيات النازلة** التي تتم بسرعات أكبر باستخدام تقنيات نظام **V.90**.

المودم السلكي

يوفر مودم الاتصال الهاتفي إمكانية الدخول إلى الانترنيت عبر شبكة مؤسسة الهاتف بسرعة 56 كيلوبت/الثانية (56.000 بت/الثانية). أما المودمات السلكية فتوفر سرعات أعلى بكثير، ويتم ذلك باستخدام خدمات شبكات تلفزيون الكابل وبسرعات تصل إلى ميغابت/الثانية (مليون بت/الثانية).

عندما يجري تركيب مودم سلكي داخل الحاسب، يجري تركيب "**فاصل إشارة**" في علبة التوصيل الرئيسية خارج الموقع (المنزل أو المكتب)، وتكون مهمته فصل الكبل المحوري إلى خطين: الأول يصل إلى المودم السلكي، والآخر يصل إلى جهاز التلفزيون.

يجري توصيل المودم السلكي عادةً بالحاسب عن طريق بطاقة شبكة **Ethernet** من طراز **10BaseT**، ويُستخدَم كبل شبكة من فئة **Categoty-5** لوصل المودم السلكي ببطاقة الشبكة الموجودة في الحاسب، ويجري إرسال المعطيات من الحاسب إلى الموديم السلكي بسرعة 10 ميغابت/الثانية.

ستدعم تقنيات الموديم السلكي في المستقبل تقنية "**المسرى التسلسلي العالمي**"، وتقنيات أخرى لوصل المنازل بالشبكات السريعة عن طريق الخطوط الهاتفية العادية.

نظام ISDN

يوفر نظام ISDN إمكانية نقل المعطيات بمعدل 144 كيلوبت/الثانية في الأحوال الطبيعية باستعمال خط هاتفي واحد (يدعى اصطلاحاً Telco) مؤلف من أربعة أسلاك.

لتوفير إمكانية نقل الأصوات، يتم تقسيم القناة الأصلية بسعة 144 كيلوبت/الثانية إلى قناتين فرعيتين: تحوي الأولى خطي اتصال تصل سعة كل منهما إلى 64 كيلوبت/الثانية، وتدعى هذه القناة بالقناة B (Bearer). وتحوي القناة الأخرى خطاً واحداً وسعتها 16 كيلوبت/الثانية، وتدعى بالقناة D (Data).

تنقل كل قناة B مكالمة هاتفية، ويكون لكل قناة رقم خط هاتفي خاص يدعى DN أو رقم الدليل Directory Number. بالإمكان طلب دمج قناتي B لتشكيل قناة واحدة بسعة 128 كيلوبت/الثانية من خلال إجراء يدعى "بالربط" أو Bonding.

يجري وصل خط ISDN الهاتفي بأربعة أسلاك إلى علبة الهاتف خارج المبنى والتي تسمى Network Terminator (NT1 اختصاراً)، حيث يتم تجزئة القناة ذات سعة 144 كيلوبت/الثانية إلى قناتين فرعيتين B وقناة واحدة D. تنقل القناة B الإشارات الصوتية والمعطيات، بينما تنقل القناة D إشارات النظام بين أجهزة ISDN والمقسم الموجود في مؤسسة الهاتف.

تسمى الخدمة التي تستخدم قناتي B وقناة D باسم BRI أو "رسوم التعرفة الأساسية للوصل" وهو مصطلح خاص بمؤسسة الهاتف، وتدعى هذه الخدمة أحياناً أخرى باسم 2B+D. كما يمكن شراء عدة خطوط ISDN بالجملة: 23 قناة B وقناة D 64 كيلوبت/الثانية، وحيدة، وتسمى هذه الخدمة باسم PRI أو "رسوم التعرفة المتميزة للوصل" ومعظم مزايا ومساوئ هذه الخدمة موروثة من خدمة BRI.

يمكن استخدام طرفية خاصة لنقل المعطيات (لكن دون صوت)، باستخدام البرمجيات الخاصة بالمودم أو الفاكس، ولكن بسعات تصل إلى 64 كيلوبت/الثانية وذلك عبر وصل الحاسب إلى تلك الطرفية باستخدام كابل تسلسلي من طراز RS-232. تضمن الطرفية السابقة توافقية سرعة الاتصال بين الحاسب وقناة خط ISDN ذات سرعة 64 كيلوبت/الثانية، لذا فإن إمكانية إجراء اتصال عبر خط ISDN ممكن حتى ولو كان جهاز الحاسب غير قادر على تجاوز سرعة أكبر من 38.4 كيلوبت/الثانية.

يعتبر موجه ISDN شكلاً متطوراً من أشكال الطرفيات الآنفة الذكر، فهو يصل خط ISDN من طرف، والشبكة المحلية أو المنزلية من الطرف الآخر. كما يمكن له نقل معطيات الشبكة إلى شبكة أخرى أو عبر الانترنيت سواء كانت هذه المعطيات تستخدم بروتوكول TCP/IP أو بروتوكول IPX أو بروتوكول AppleTalk. عموماً يدعم الموجه مختلف الحواسب التي لاتستعمل برمجيات خاصة بنظام ISDN، وذلك لأن الموجه يحتوي الإمكانيات والبرمجيات اللازمة لنقل كافة المعطيات على خط ISDN من شبكة لأخرى، حتى لو كانت هذه الشبكات بعيدة جغرافياً.

يمكن لمؤسسة الهاتف أن تضمن إيصال المعطيات من نقطة لأخرى دون أي ضياع لأن ISDN هو نظام خدمة رقمي ولايتأثر بالتشويش إطلاقاً. ولأن القناة المُستخدمة هي عبارة عن "انبوب رقمي" نقي، لا يجري أية مفاوضات على السرعة، لذا لا يحتاج نظام ISDN لأكثر من ثانيتين لإعداد وإجراء الاتصال، في حين يحتاج الهاتفي العادي في بعض الأحيان إلى دقيقة كاملة للقيام بنفس العملية.

خدمة ADSL

تصل هذه الخدمة موديمين من نوع **ADSL** بسلك مزدوج عن طريق الخط الهاتفي العادي. وينشأ عن هذه الدارة ثلاث قنوات معطيات:

- قناة سريعة مخصصة لنقل المعطيات النازلة **Downstream** بسرعات تتراوح بين 1.5 و8 ميغابت/الثانية
- قناة متوسطة السرعة مزدوجة الاستعمال تتراوح سعتها بين 16 و640 كيلوبت/الثانية
- قناة خط هاتفي عادي تدعى **POTS**

تعتمد سرعة قناة استقبال المعطيات **Downstream** على عدة عوامل:

- طول سلك الخط الهاتفي النحاسي
- ثخن هذا السلك
- عدد العلب الهاتفية الموصولة
- التشويش

تزداد حساسية الخط بازدياد طول السلك الهاتفي والترددات، وتنخفض هذه الحساسية بازدياد ثخانة السلك المستخدم. وبغض النظر عن عدد العلب الهاتفية التي تصل المشترك بمقسم الهاتف، يكون أداء خط **ADSL** كالتالي:

معدل السرعة	قطر السلك	المسافة
1.5–2 ميغابت/الثانية	0.5 مم	5.5 كم
1.5–2 ميغابت/الثانية	0.4 مم	4.6 كم
6.1 ميغابت/الثانية	0.5 مم	3.7 كم
6.1 ميغابت/الثانية	0.4 مم	2.7 كم

أما بالنسبة للمواقع التي تبعد أكثر من المسافات المذكورة أعلاه، فيمكن وصلها مع المقسم عن طريق الحلقات المحلية التي تستخدم أنظمة النقل بالألياف الضوئية.

تصل هذه الخدمة موديمين من نوع **ADSL** بسلك مزدوج عن طريق الخط الهاتفي العادي. وينشأ عن هذه الدارة ثلاث قنوات معطيات:

- قناة سريعة مخصصة لنقل المعطيات النازلة **Downstream** بسرعات تتراوح بين 1.5 و8 ميغابت/الثانية
- قناة متوسطة السرعة مزدوجة الاستعمال تتراوح سعتها بين 16 و640 كيلوبت/الثانية
- قناة خط هاتفي عادي **POTS**

يجري عزل قناة **POTS** عن خط موديم **ADSL** الرقمي، وذلك لضمان عدم انقطاع خط **POTS**، حتى ولو انقطع اتصال خط **ADSL**.

بالإمكان شراء موديمات **ADSL** بمواصفات وسرعات مختلفة، وتوفر أدنى هذه الإمكانيات سرعة استقبال بحدود 1.5 وحتى 2 ميغابت/الثانية، وقناة مزدوجة الاستعمال بسعة 16 كيلوبت/الثانية. أما المواصفات الأخرى فتوفر معدلات استقبال بسرعة تصل إلى 6.1 ميغابت/الثانية، وقناة مزدوجة الاستعمال بسعة 640 كيلوبت/الثانية. وهناك موديمات توفر سرعات بحدود 9 ميغابت/الثانية وقناة مزدوجة الاستعمال بسعة 640 كيلوبت/الثانية.

تعتمد سرعة قناة استقبال المعطيات **Downstream** على عدة عوامل:

- طول سلك الخط الهاتفي النحاسي
- ثخن هذا السلك
- عدد العلب الهاتفية الموصولة
- التشويش

وتزداد حساسية الخط بازدياد طول السلك الهاتفي والترددات، وتنخفض هذه الحساسية بازدياد ثخانة السلك المستخدم.

تزداد حساسية الخط بازدياد طول السلك الهاتفي والترددات، وتنخفض هذه الحساسية بازدياد ثخانة السلك المستخدم.

نشاط

بفرض أنك تحتاج لتسجيل اشتراك بالإنترنت. اعتماداً على لائحة مزودي الخدمة الموجودين في سوريا، ضع بالإشتراك مع زملاءك ومع المشرف لائحة أسعار بعروض اشتراكات الإنترنت المنزلية التي يقدمها مزودو الخدمة السوريون.

ابحث عن مكافئاتها من أسعار التزويد بخدمة الإنترنت في بلدان مجاورة مثل لبنان، والأردن، وفي بلدان أوروبية مثل بريطانيا وفرنسا، بعد تحديدك لعدد من مزودي خدمة الإنترنت في البلدان الآنفة الذكر.

خدمات الحزم العريضة

تفتح تقنية الحزم العريضة أبواباً جديدة لخدمات الانترنيت في المنازل، والمكاتب، والشركات حول العالم، وتنقل المعطيات بسرعة الضوء.

يمكن تشبيه الحزمة العريضة بأنبوب ثخين يصل إلى موقع ما، حيث تقوم شركة الهاتف، أو شركة الخدمات التلفزيونية، أو شركة مستقلة بتمديد هذا الأنبوب.

تعد التقنيات الرقمية والألياف الضوئية العنصر الأساسي في مفهوم وعمل الحزمة العريضة. وتوفر هذه التقنيات سرعة نقل أكبر للمعلومات من سرعات الاتصال الهاتفي، أو السلكي، أو اللاسلكي. فبالإمكان تزويد خدمة الحزمة العريضة إلى المنزل، أو مكان العمل عبر هوائيات مثبتة على الأرض، أو عن طريق الأقمار الصناعية. ندعوها عندها بخدمات الحزم العريضة اللاسلكية.

خدمات الحزم العريضة اللاسلكية

يُعتبر الاتصال اللاسلكي أحد خيارات الاتصال، وخاصة إذا لم يكن هناك شركة خدمة مودم سلكي' أو إذ كان الموقع بعيداً جداً عن مقسم مؤسسة هاتف بحيث يتعذر الاشتراك بخدمة اتصالات سريعة مثل Digital Subscriber Line أو DSL (كحال مواقع العمل التابعة لشركات التنقيب عن النفط مثلاً).

ويمكن تلخيص فوائد خدمة الحزمة العريضة اللاسلكية بما يلي:

- ليس هناك داع لإجراء اتصال هاتفي بمزود خدمة الانترنيت
- تكون سرعة التحميل أسرع من اتصال المودمات الهاتفية بخمسين مرة
- تتيح استخدام الإنترنت دون إشغال الخط الهاتفي
- توفر إمكانية تأسيس خطوط اتصال بين المدن والقرى والمواقع النائية

تقنيات الحزم العريضة اللاسلكية

توجد تقنيتين رئيسيتين حالياً للحزم العريضة: خدمة اللاسلكي الثابت، وخدمة الأقمار الصناعية.

الخدمة اللاسلكية الثابتة

يأتي اسم هذه الخدمة من حقيقة أن بث ترددات الإشارة يجري عبر هوائيات وأبراج اتصال ثابتة إلى هوائيات مثبتة على أبنية المنازل والمكاتب. وتستخدم هذه الأنظمة الترددات اللاسلكية الميكروية Microwave لايصال خدمات الاتصال بالانترنيت بسرعات تصل إلى 1.5 ميغابت/الثانية، بالمقارنة مع سرعة موديم الاتصال الهاتفي التي قد تصل إلى 56 كيلوبت/الثانية في أحسن الحالات.

- **نظم التوزيع متعدد النقاط متعدد الأقنية – MMDS:** هي خدمة بث تلفزيوني يستخدم "أنظمة توزيع متعددة القنوات وعدة

نقاط بث"، تُستخدم لبث القنوات التلفزيونية إلى أكثر من مليون مشترك منزلي في الولايات المتحدة، لاسلكياً.

- **نظم التوزيع المحلي متعدد النقاط – LMDS: هي** خدمة بث تلفزيوني محلي يستخدم "أنظمة توزيع محلية متعددة نقاط البث"، وهي شبيه بخدمة MMDS، عدا أنها تقوم بتخديم الشركات في المدن الرئيسية في الولايات المتحدة.

خدمة الأقمار الصناعية

تنبع الحاجة لاستخدام الأقمار الصناعية إلى ضرورة ربط مواقع متباعدة لا يمكن وصلها باستخدام التقنيات السابقة: كحالة حواسب الطائرات، وأنظمة التوجه باستخدام الأقمار الصناعية. على كل حال، يمكن ربط المواقع المختلفة دون الحاجة لتعديل التقنيات الداخلية المستخدمة. من أهم أنماط الأقمار المُستخدمة:

- **الأقمار ذات المدارات البعيدة GEO (Geosynchronous Earth Orbit)**
  - ارتفاع المدار: 22238 ميل
  - التأخير الزمني: من 0.25 إلى 0.5 ثانية
  - التطبيقات: صوت وصورة، بث تلفزيوني
  - التدفق: يصل إلى 155Mbps

- **الأقمار ذات المدارات المتوسطة MEO (Middle Earth Orbit)**
  - ارتفاع المدار: 8000 ميل
  - التأخير الزمني: 0.1 ثانية
  - التطبيقات: صوت (هاتف نقال)، معطيات بتدفق بسيط
  - التدفق: يصل إلى 38.4Mbps

- **الأقمار ذات المدارات المنخفضة LEO (Low Earth Orbit)**
  - ارتفاع المدار: من 400 ميل إلى 1000 ميل
  - التأخير الزمني: 0.05 ثانية
  - التطبيقات: صوت (هاتف نقال)، معطيات بتدفق بسيط وعالي
  - التدفق: يصل إلى 155Mbps

عنوان الموضوع:

العتاد الشبكي

الكلمات المفتاحية:

الشبكات الحاسوبية، بطاقات واجهة الشبكة، نموذج OSI، الطبقة الفيزيائية، طبقة ربط المعطيات، اللوحة الأم، مسار الحاسب، سعة المسار، مآخذ توسعة، PCMCIA، USB، CompactFlash، Fire Wire، البوابات المباشرة على اللوحة الأم، بطاقات واجهة الشبكة على اللوحة، بطاقات واجهة الشبكة اللاسلكية، معايير المسار الداخلي، معايير المسار الطرفي، كرت تعريف الجهاز، IRQ– طلب المقاطعة، المقاطعة، رقم طلب المقاطعة، مجال الذاكرة، بوابة الدخل/خرج الأساسية، المعالج، الذاكرة، المكررات، الموزعات، مجال التصادم، الجسور، قاعدة معطيات التنقية، المبدلات، الموجهات، طبقة الشبكة، البوابات.

ملخص:

يتعرف الطلاب في هذه الوحدة على مختلف العتاديات المستخدمة في تعريف الشبكات، حيث تلقي الوحدة الضوء على البطاقات الشبكة المختلفة، كما تستعرض مختلف تقنيات الربط المستخدمة في الشبكات اليوم.

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- **بطاقات واجهة الشبكة**
- **أنواع بطاقات واجهة الشبكة**
  - مقدمة
  - معايير المسار الداخلي
  - معايير المسار الطرفي
    - مقدمة
    - PCMCIA
    - USB
    - CompactFlash
    - Fire Wire
  - بطاقات واجهة الشبكة على اللوحة
  - بطاقات واجهة الشبكة اللاسلكية
- **تنصيب بطاقة واجهة الشبكة**
  - مقدمة
  - تركيب العتاد
  - التعريف البرمجي
  - IRQ – طلب المقاطعة

- مجال الذاكرة
- بوابة الدخل/خرج الأساسية
- اختيار بطاقة واجهة الشبكة المناسبة

- **المكررات**
- **الموزعات**
  - أنواع الموزعات
- **الجسور**
- **المبدلات**
- **الموجهات**
- **البوابات**

بطاقات واجهة الشبكة
Network Interface Cards NICs

- **بطاقات واجهة الشبكة NICs:** وسائط ربط تسمح لأية أداة باستقبال وإرسال المعطيات عبر الشبكة الحاسوبية.

- تنتمي بطاقات واجهة الشبكة إلى كل من الطبقة الفيزيائية وطبقة ربط المعطيات في نموذج OSI

- تعرف بطاقات واجهة الشبكة NICs (وتدعى اختصاراً ببطاقات الشبكة) بأنها وسائط أو أدوات ربط تسمح لمحطة العمل، المخدم، الطابعة، أو لأية أداة أخرى، باستقبال وإرسال المعطيات عبر الشبكة الحاسوبية. تحتوي الغالبية العظمى من بطاقات واجهة الشبكة على جهاز إرسال واستقبال مهمته إرسال واستقبال إشارات المعطيات التي يتم تبادلها عبر الشبكة.

- تنتمي بطاقات واجهة الشبكة إلى كل من الطبقة الفيزيائية (Physical) وطبقة ربط المعطيات (Data Link) في نموذج OSI، وذلك لأنها من جهة تولد إشارات المعطيات وتبثها إلى الأسلاك مباشرة ومن جهة أخرى تقوم بتجميع وفك تجميع أطر المعطيات. بالإضافة إلى ذلك تفسر هذه البطاقات معلومات العنونة بحيث تضمن وصول المعطيات إلى الجهة المناسبة، كما تقوم هذه البطاقات بتنفيذ الإجرائيات التي تحدد العقدة صاحبة الحق في إرسال المعطيات عبر الشبكة في لحظة محددة.

أنواع بطاقات واجهة الشبكة
1- مقدمة

- **أنواع بطاقات واجهة الشبكة NICs:** تختلف أنواع بطاقات الشبكة حسب:
  - طريقة الولوج
  - سرعة إرسال المعطيات
  - واجهات الربط

- أنواع اللوحات الأم أو الأجهزة المتوافقة
- المصنع

- هناك تشكيلة واسعة من أنواع بطاقات واجهة الشبكة، تختلف هذه الأنواع عن بعضها البعض اعتماداً على كل من:
  - طريقة الولوج (مثلاً شبكة خطية أو حلقية)
  - سرعة إرسال المعطيات (مثلاً 100 ميغابت في الثانية)
  - واجهات الربط (مثلاً RJ-45 أو SC)
  - أنواع اللوحات الأم أو الأجهزة المتوافقة (مثلاً PCI)
  - المصنع (تشمل لائحة أشهر مصنعي بطاقات واجهة الشبكة كلاً من: 3Com، Adapter، D-Link، IBM، Intel، SMC،Linksys، Netgear، SMC، وWestern Digital)

نستعرض في الشرائح التالية أهم أنواع بطاقات الشبكة وميزات كل نوع من هذه الأنواع.

أنواع بطاقات واجهة الشبكة
2 - معايير المسار الداخلي (Internal Bus Standards)

- **مسار الحاسب:** دار، تستخدمها اللوحة الأم لإرسال المعطيات إلى مختلف مكونات الحاسب.

- **سعة المسار:** تتحدد سعة المسار وفق عاملين أساسيين هما:

1. عرض مسار المعطيات الخاص بها (بالبت): عدد البتات التي يمكن نقلها على التوازي في لحظة محددة
2. سرعة الساعة (بالميغاهرتز)

- **توسيع مسار الحاسب:** يمكن **توسيع مسار الحاسب** بحيث يشمل أجهزة إضافية غير تلك الموجودة على اللوحة الأم. تحتوي اللوحة الأم على مآخذ توسعة **(Expansion Slots)**، وهي عبارة عن فتحات ذات وصلات إلكترونية مختلفة، تسمح بوصل مختلف أنواع الأجهزة إلى مسار الحاسب الموسع. تأتي هذه الأجهزة على شكل بطاقة أو لوحة توسعية (Expansion Cards – Boards).

- **مسار الحاسب:** يعرف **مسار الحاسب** بأنه دارة، أو ممر إشارة، تستخدمها اللوحة الأم لإرسال المعطيات إلى مختلف مكونات الحاسب، بما في ذلك المعالج، الذاكرة، القرص الصلب وبطاقات واجهة الشبكة (يدعى مسار الحاسب بالمسار الرئيسي أو مسار النظام أيضاً).

- **سعة المسار:** تتميز المسارات عن بعضها البعض حسب سعتها، حيث تتحدد سعة المسار بشكل أساسي وفق عاملين أساسيين هما عرض مسار المعطيات الخاص بها (ويقاس بالبت) وسرعة الساعة (وتقاس بالميغاهرتز). يعادل **حجم مسار المعطيات** عدد البتات التي يمكن نقلها على التوازي في لحظة محددة، لم يكن حجم هذا المسار ليتجاوز 8 بت في الحاسبات الشخصية الأولى، إلا أن المصنعين استطاعوا لاحقاً توسيع المسار بحيث تستطيع نقل 16 بت، ثم 32 بت. اليوم تستخدم معظم الحواسيب الشخصية مسارات بعرض 64 بت، أو حتى 128 بت. وكلما ازداد عدد البتات التي يمكن للمسار التعامل معها، كلما ازدادت سرعة الأجهزة المربوطة إلى هذا المسار.
- **توسيع مسار الحاسب:** يمكن **توسيع مسار الحاسب** بحيث يشمل أجهزة إضافية غير تلك الموجودة على اللوحة الأم.

تحتوي اللوحة الأم على مآخذ توسعة **(Expansion Slots)**، وهي عبارة عن فتحات ذات وصلات إلكترونية مختلفة، تسمح بوصل مختلف أنواع الأجهزة مثل بطاقات الصوت، الفيديو، أو بطاقات واجهة الشبكة إلى مسار الحاسب الموسع. تأتي هذه الأجهزة على شكل بطاقة أو لوحة توسعية (Expansion Cards - Boards)، يؤدي إدخال هذه البطاقة في المأخذ التوسعي إلى تأسيس وصلة إلكترونية بين البطاقة واللوحة الأم، وبهذا ترتبط الأداة بهذه الطريقة بدارة الحاسب الرئيسية، وتصبح جزءاً من مساره.

أنواع بطاقات واجهة الشبكة
3 - معايير المسار الطرفي (Peripheral Bus Standards)
1- مقدمة

- **الربط الخارجي:** يمكن ربط بعض الطرفيات إلى مسار الحاسب بشكل خارجي بوساطة تشكيلة واسعة من المآخذ الخارجية لربط هذه الأجهزة مثل:
  - PCMCIA
  - USB
  - CompactFlash
  - Fire Wire
- تمتاز بطاقات واجهة الشبكة الطرفية بسهولة تركيبها مقارنة مع بطاقات واجهة الشبكة التي يتم ربطها مباشرة باللوحة الأم.
- يمكن ربط بعض الطرفيات، مثل بطاقات واجهة الشبكة أو أجهزة المودم، إلى مسار الحاسب بشكل خارجي عوضاً عن وصلها داخلياً، يمكن استخدام تشكيلة واسعة من المآخذ الخارجية لربط هذه الأجهزة تشمل PCMCIA (الاتحاد العالمي لبطاقات ذواكر الحواسب الشخصية Personal Computer Memory Card International Association)، أو USB (المسار التسلسلي العمومي Universal Serial Bus)، أو CompactFlash، أو Fire Wire.
- تمتاز بطاقات واجهة الشبكة الطرفية بسهولة تركيبها، حيث لا يتطلب وصل مثل هذه البطاقات إلى الحاسب أكثر من إدخالها في المأخذ المناسب، أما في حالة بطاقات واجهة الشبكة التي يتم ربطها باللوحة الأم، فلا بد لتركيبها من اتباع سلسلة من الخطوات، بدءاً من إغلاق الجهاز وفتح غطاءه، ثم إدخال البطاقة أو اللوحة في المأخذ المناسب وتثبيتها إليه، ومن ثم إعادة تركيب الغطاء وتشغيل الحاسب مجدداً.

أنواع بطاقات واجهة الشبكة
- معايير المسار الطرفي (3Peripheral Bus Standards)
PCMCIA -2

- **PCMCIA** – الاتحاد العالمي لبطاقات ذواكر الحواسب الشخصية (Personal Computer Memory Card International Association): هي بطاقات يمكن استخدامها لربط أي نوع من أنواع الأجهزة الطرفية تقريباً إلى الحاسب.
- قامت مجموعة من مصنعي أجهزة ونظم الحاسب الشخصي، عام 1989، بتأسيس الاتحاد العالمي لبطاقات ذواكر الحواسب الشخصية (Personal Computer Memory Card International Association) أو PCMCIA، وذلك بهدف

الاتفاق على طريقة قياسية لربط الذواكر الخارجية بأجهزة الحواسب المحمولة، إلا أن PCMCIA عملت لاحقاً، وفي ضوء الطيف الواسع للاستخدامات المحتملة لمثل هذه التقنية، على تعديل طريقتها القياسية وبدأت بتصنيع بطاقات يمكن استخدامها لربط أي نوع من أنواع الأجهزة الطرفية تقريباً إلى الحاسب، واليوم تستخدم بطاقات PCMCIA لربط أجهزة المودم الخارجية، بطاقات الشبكة، الأقراص الصلبة وحتى سواقات الأقراص المضغوطة إلى معظم أجهزة الحواسب المحمولة.

أنواع بطاقات واجهة الشبكة
3 - معايير المسار الطرفي (Peripheral Bus Standards)
USB -3

- **USB**- المسار التسلسلي العمومي (Universal Serial Bus): واجهة قياسية تستخدم لربط عدة أنواع من الطرفيات، وهي متوفرة على اللوحات الأم في معظم أجهزة الحواسب المحمولة أو الشخصية.

- يعرف USB أو المسار التسلسلي العمومي (Universal Serial Bus) بأنه واجهة قياسية تستخدم لربط عدة أنواع من الطرفيات، بما في ذلك أجهزة المودم، تجهيزات الصوت، وبطاقات الشبكة. طورت واجهة USB القياسية لأول مرة عام 1995 على يد مجموعة من مصنعي أجهزة الحاسب والذين كانونا يطمحون إلى تصنيع وسائط ربط متدنية الكلفة وسهلة الاستخدام، بحيث يمكن استخدامها لوصل أي نوع من الأجهزة أو الطرفيات إلى جهاز الحاسب. وقد أصبحت هذه التقنية متوفرة منذ العام 1998 على اللوحات الأم في معظم أجهزة الحواسب المحمولة أو الشخصية.

أنواع بطاقات واجهة الشبكة
3 - معايير المسار الطرفي (Peripheral Bus Standards)
Fire Wire- 4

- **Fire Wire:** يمكن استخدام هذه التقنية في كل مما يلي:
  - ربط معظم أنواع الطرفيات إلى معظم أجهزة الحواسب المحمولة أو الشخصية
  - وصل حاسبين أو أكثر معاً بشبكة صغيرة باستخدام طوبولوجيا المسار (Bus Topology)
- بدأت شركة apple بتطوير تقنية Fire Wire القياسية في ثمانينات القرن الماضي، وتم تثبيت هذه التقنية كمعيار IEEE قياسي عام 1995 باسم IEEE 1394. ورغم أن هذه التقنية مضمنة في لوحات Macintosh الأم منذ زمن طويل، إلا أن تطبيقها على لوحات الحواسيب الشخصية الأم لم يبدأ إلا منذ سنوات قليلة.
  - يمكن استخدام Fire Wire لربط معظم أنواع الطرفيات، مثل الكاميرات الرقمية، أجهزة الفيديو، الأقراص الصلبة أو سواقات الأقراص المضغوطة إلى معظم أجهزة الحواسب المحمولة أو الشخصية.
  - كما يمكن استخدامها أيضاً لوصل حاسبين أو أكثر معاً بشبكة صغيرة باستخدام طوبولوجيا المسار (Bus Topology) – أي بوصل كل حاسب بحاسب آخر وفق طريقة daisy chain. يمكن استخدام Fire Wire في مثل هذه الشبكات لربط عدد من الأجهزة يصل إلى 63 جهاز في كل قطاع، بمسافة تصل إلى 4.5 متر بين العقد، كما أن طول الشبكة ككل يمكن أن يصل إلى أكثر من 72 متراً.

أنواع بطاقات واجهة الشبكة
3 - معايير المسار الطرفي (Peripheral Bus Standards)

CompactFlash -5

- **CompactFlash:** هي أداة تخزين معطيات محمولة أو أداة دخل خرج محمولة غاية في الصغر، يمكن استخدامها لربط العديد من الطرفيات:
  - تستخدم هذه التقنية في الكاميرات الرقمية حيث تخزن الصور التي يتم التقاطها على بطاقة تخزين من نمط CompactFlash
  - يمكن استخدام تقنية CompactFlash في ربط الشبكات الحاسوبية
- صممت مجموعة مؤلفة من اثني عشرة شركة إلكترونيات، والتي شكلت اتحاد CompactFlash (واختصاراً CFA)، تقنية CompactFlash لتكون أداة تخزين معطيات محمولة أو أداة دخل خرج محمولة غاية في الصغر، يمكن استخدامها لربط العديد من الطرفيات
  - غالباً ما تستخدم هذه التقنية في الكاميرات الرقمية حيث تخزن الصور التي يتم التقاطها على بطاقة تخزين من نمط CompactFlash
  - يمكن استخدام تقنية CompactFlash في ربط الشبكات الحاسوبية كذلك، إلا أن سرعتها المنخفضة نسبياً تحد من استخدامها في هذا المجال، وغالباً ما يتركز استخدامها لربط الأجهزة الأصغر من أن يتم ربطها بوساطة PCMCIA

أنواع بطاقات واجهة الشبكة
4 - بطاقات واجهة الشبكة على اللوحة (On-board NICs)

- **البوابات المباشرة على اللوحة الأم:** يمكن ربط بعض الأجهزة إلى اللوحة الأم مباشرة وذلك بوساطة البوابات المباشرة على اللوحة الأم (on-board ports)، مثل بوابتي الفأرة ولوحة المفاتيح المتكاملتين مع كافة اللوحات الأم.
- تستخدم العديد من الحواسب الحديثة بطاقات واجهة شبكة مباشرة على اللوحة، وهي عبارة عن بطاقات واجهة شبكة متكاملة مع اللوحة الأم
- تتميز بطاقات الشبكة على اللوحة بأنها توفر المساحة كما أنه تحرر مآخذ التوسعة بحيث يمكن استخدامها لربط أجهزة طرفية أخرى
- لا يتم ربط كافة الأجهزة الطرفية بلوحات الحواسيب الأم عن طريق مآخذ توسعة أو مسارات طرفية، حيث يمكن ربط بعض الأجهزة إلى اللوحة الأم مباشرة وذلك بوساطة البوابات المباشرة على اللوحة الأم (on-board ports)، وأبرز مثالين على مثل هذه البوابات هما بوابتي الفأرة ولوحة المفاتيح المتكاملتين مع كافة اللوحات الأم
- تستخدم العديد من الحواسب الحديثة بطاقات واجهة شبكة مباشرة على اللوحة، وهي عبارة عن بطاقات واجهة شبكة متكاملة مع اللوحة الأم
- تتميز بطاقات الشبكة على اللوحة بأنها توفر المساحة كما أنه تحرر مآخذ التوسعة بحيث يمكن استخدامها لربط أجهزة طرفية أخرى

أنواع بطاقات واجهة الشبكة
5 - بطاقات واجهة الشبكة اللاسلكية (Wireless NICs)

- تستخدم بطاقات واجهة الشبكة اللاسلكية هوائي (داخلي أو خارجي) لتبادل المعطيات مع جهاز إرسال المحطة الأساسية أو مع بطاقات شبكة لاسلكية أخرى. يمكن ربط بطاقات واجهة الشبكة اللاسلكية مع أي نوع من المسارات التي عرفناها في هذه الوحدة

تنصيب بطاقة واجهة الشبكة
1- مقدمة

- **مراحل تنصيب بطاقة واجهة الشبكة:**
  - تركيب العتاد الخاص بهذه البطاقة
  - تنزيل البرمجيات المتوافقة مع هذا العتاد
  - قد لا يكتمل تنصيب بطاقة واجهة الشبكة في بعض الأحيان إلا بخطوة ثالثة هي تعريف مجموعة التعليمات والمعطيات التي يتم تخزينها على رقاقة ذاكرة ROM، ويمكن تغيير معلومات هذه الذاكرة بوساطة برنامج تعريف غالباً ما يأتي مرفقاً مع البطاقة نفسها.

- لتنصيب بطاقة واجهة الشبكة لا بد من تركيب العتاد الخاص بهذه البطاقة أولاً، ومن ثم تنزيل البرمجيات المتوافقة مع هذا العتاد. وقد لا يكتمل تنصيب بطاقة واجهة الشبكة في بعض الأحيان إلا بخطوة ثالثة هي تعريف مجموعة التعليمات والمعطيات التي يتم تخزينها على رقاقة ذاكرة ROM (ذاكرة للقراءة فقط) (وغالباً ما تكون على بطاقة الشبكة نفسها)، يمكن تغيير معلومات هذه الذاكرة بوساطة برنامج تعريف غالباً ما يأتي مرفقاً مع البطاقة نفسها، وذلك لأن المعطيات المخزنة على هذه الذاكرة إنما يمكن محوها أو تغييرها بتطبيق شحنات كهربائية محددة على البطاقة (وذلك بوساطة البرنامج المرفق)، يدعى هذا النمط من ذواكر الROM بذواكر EEPROM أي ذواكر القراءة فقط القابلة للمحو والبرمجة إلكترونياً (Electrically Erasable Programmable Read-Only Memory).

تنصيب بطاقة واجهة الشبكة
2 - تركيب العتاد

- **تركيب بطاقات الشبكة:** تختلف طريقة تركيب بطاقات واجهة الشبكة بحسب نوعها:
  - **بطاقات الشبكة التوسعية:**
    1. إغلاق الجهاز، فصله عن الكهرباء وفتح غطاءه
    2. تحديد المأخذ التوسعي الذي سيتم وصل بطاقة الشبكة إليه
    3. إدخال البطاقة أو اللوحة في المأخذ الذي تم اختياره وتثبيتها في مكانها بإحكام
    4. إعادة تركيب الغطاء وتشغيل الحاسب مجدداً.

  - **بطاقات واجهة الشبكة الطرفية:** لا يتطلب وصلها إلى الحاسب أكثر من إدخالها في المأخذ المناسب مباشرة، والتأكد من إحكام إدخالها.

- **تركيب عدة بطاقات شبكة:** يعتمد تحقيق هذا الأمر على التعريف البرمجي الصحيح لكل بطاقة.

- تختلف طريقة تركيب بطاقات واجهة الشبكة بحسب نوعها:
  - **بطاقات الشبكة التوسعية:** لتركيب بطاقات واجهة الشبكة التي يتم ربطها باللوحة الأم لا بد من اتباع سلسلة من الخطوات:
    1. إغلاق الجهاز، فصله عن الكهرباء وفتح غطاءه
    2. تحديد المأخذ التوسعي الذي سيتم وصل بطاقة الشبكة إليه
    3. إدخال البطاقة أو اللوحة في المأخذ الذي تم اختياره وتثبيتها في مكانها بإحكام
    4. إعادة تركيب الغطاء وتشغيل الحاسب مجدداً

  - **بطاقات واجهة الشبكة الطرفية:** لا يتطلب وصلها إلى الحاسب أكثر من إدخالها في المأخذ المناسب مباشرة، والتأكد من إحكام إدخالها، وهذه هي حالة بطاقات الشبكة من نوع PCMCIA، USB، CompactFlash، و Fire Wire

- قد يكون هناك ضرورة في بعض الأحيان لتركيب عدة بطاقات شبكة على بعض المخدمات، وفي الحقيقة فإن تحقيق هذا الأمر إنما يعتمد على التعريف البرمجي الصحيح لكل بطاقة، وذلك لأن التنصيب الفيزيائي لا يعدو أن يكون أكثر من مجرد تكرار الخطوات السابقة نفسها مع اختيار مأخذ مختلف في كل مرة

تنصيب بطاقة واجهة الشبكة
3- التعريف البرمجي

- **كرت تعريف الجهاز (Device Driver):** البرنامج الذي يساعد الأداة التي تم تركيبها على التواصل مع نظام تشغيل الحاسب.

- تأتي معظم نظم التشغيل الحديثة مع حزمة من برمجيات التعريف المتضمنة في النظام نفسه، بحيث يقوم النظام بالتعرف على الأجهزة التي يتم تركيبها بشكل تلقائي.

- يتم تحميل برمجيات تعريف كافة الطرفيات المتصلة بالجهاز إلى ذاكرة الـRAM في كل مرة يقلع فيها الحاسب، بحيث يستطيع الحاسب التواصل والتعامل مع هذه الطرفيات.

- يعرف كرت تعريف الجهاز (Device Driver) بأنه البرنامج الذي يساعد الأداة التي تم تركيبها على التواصل مع نظام تشغيل الحاسب. حيث ينبغي علينا، كلما قمنا بتركيب أداة جديدة إلى الجهاز، أن ننزل برنامج التعريف الخاص بها والمتوافق مع نظام التشغيل الذي نستخدمه.

- تأتي معظم نظم التشغيل الحديثة مع حزمة من برمجيات التعريف المتضمنة في النظام نفسه، بحيث يقوم النظام بالتعرف على الأجهزة التي يتم تركيبها بشكل تلقائي.

- يتم تحميل برمجيات تعريف كافة الطرفيات المتصلة بالجهاز إلى ذاكرة الـــRAM في كل مرة يقلع فيها الحاسب، بحيث يستطيع الحاسب التواصل والتعامل مع هذه الطرفيات.

تنصيب بطاقة واجهة الشبكة
4- IRQ طلب المقاطعة (Interrupt Request)

- عندما تحتاج أحد الطرفيات المتصلة بمسار الحاسب إلى جذب انتباه المعالج إليها، فإنها تصدر مـــا يعـــرف باســـم طلـــب المقاطعة أو IRQ، يعرف **طلب المقاطعة** هذا بأنه رسالة يتم إرسالها إلى الحاسب ليتوقف عما يقوم به ويباشر أمراً آخراً

- تعرف **المقاطعة (Interrupt)** بأنها سلك الدارة الذي تبث عبره الطرفية تياراً بتوتر محدد يمثل هذا التيار إشارة المقاطعة التي ترغب الطرفية بتنفيذها

- ينبغي أن تتمتع كل مقاطعة برقم IRQ مميز، حيث يعرف رقم طلب المقاطعة (IRQ Number) بأنه الرقم الذي يعـــرف كل مكون من مكونات الحاسب ويميزه بالنسبة لمسار الحاسب الرئيسي، أي أن رقم طلب المقاطعة يمثل الوسيلة التي يمكن لمسار الحاسب بوساطتها أن يحدد الأداة أو الطرفية التي قامت بطلب المقاطعة، وبالتالي الأداة أو الطرفيـــة التـــي ينبغـــي إعلامها بالمقاطعة. ترقم المقاطعات من 0 إلى 15، وغالباً ما لا يتعلق رقم المقاطعة بنوع نظام التشغيل المستخدم، كما أن بطاقات تعريف الشبكة عادة ما تستخدم أرقام المقطعات 9، 10، أو 11

- يدير كل من الـــ BIOS ونظام التشغيل إسنادات طلبات المقاطعة، وغالباً ما تتحقق هذه الإدارة دون مشاكل، إلا أنـــه قـــد يحدث في بعض الأحيان أن تحاول طرفيتان استخدام نفس طلب المقاطعة في نفس الوقت، مما يؤدي إلـــى تـــضارب فـــي الموارد ومشاكل في الأداء. تعتبر كل من الإمارات التالية بمثابة دليل على حدوث تضارب متوقع بين طـــرفيتين تريـــدان استخدام نفس طلب المقاطعة:
  - أن يعلق الجهاز لدى الإقلاع أو عند تحميل نظام التشغيل
  - أن يعمل الجهاز بشكل أبطأ كثيراً مما هو معتاد
  - توقف بعض الطرفيات عن العمل (مثل USB أو البوابات التفرعية)
  - حدوث مشاكل مع بطاقات الصوت أو الفيديو، مثل أن تتوقف بطاقة الصوت عن العمل، أو ألا تعمل بطاقـــة الفيـــديو بشكل صحيح
  - أن يفشل الجهاز بالاتصال بالشبكة
  - أن يعاني الجهاز من أخطاء انقطاعات معطيات مؤقتة أثناء إرسال أو استقبال المعطيات عبر الشبكة

تنصيب بطاقة واجهة الشبكة
5- مجال الذاكرة (Memory Range)

- **مجال الذاكرة (Memory Range):** مساحة الذاكرة التي يستخدمها كل من المعالج (CPU) وبطاقة الشبكة (NIC) لتبادل أو تخزين المعطيات.

- تستخدم بطاقات الشبكة مجال ذاكرة في مساحة الذاكرة العالية (High Memory Area)، والتي توفق في الترميز الستة عشري المجال A000-FFFF.

- **مجال الذاكرة (Memory Range):** يشير مجال الذاكرة، باستخدام الترميز الستة عشري، إلى مساحة الذاكرة التي يستخدمها كل من المعالج (CPU) وبطاقة الشبكة (NIC) لتبادل أو تخزين المعطيات. وكما هو الحال مع طلبات المقاطعة، فإن بعض مجالات الذاكرة تحفظ بدورها لتستخدم مع أجهزة محددة، ولاسيما اللوحة الأم. لا يمكن استخدام مجالات الذاكرة المحفوظة هذه مع أي أداة سوى الأداة المحفوظة لأجلها.

- تستخدم بطاقات الشبكة مجال ذاكرة في مساحة الذاكرة العالية (High Memory Area)، والتي توفق في الترميز الستة عشري المجال A000-FFFF. كما أن بعض مصنعي بطاقات الشبكة يفضلون مجالات بعينها، مثل يفضل استخدام المجال C8000-C9FFF في حال كانت بطاقة الشبكة من نوع 3Com PC.

تنصيب بطاقة واجهة الشبكة
6- بوابة الدخل/خرج الأساسية (Base I/O Port)

- تحدد إعدادات بوابة الدخل/خرج الأساسية، باستخدام الترميز الستة عشري، مساحة الذاكرة التي سيتم استخدامها كقناة لنقل المعطيات بين وبطاقة الشبكة وبين المعالج، ومثل طلبات المقاطعة، لا يمكن لطرفيتين استخدام نفس بوابة الدخل/خرج الأساسية.

- تستخدم معظم بطاقات الشبكة مجالي ذاكرة لتحديد قناة نقل المعطيات، حيث تعرف إعدادات بوابة الدخل/خرج الأساسية بداية كل مجال.

تنصيب بطاقة واجهة الشبكة
7 - اختيار بطاقة واجهة الشبكة المناسبة

- **عوامل اختيار بطاقة الشبكة:** ينبغي أن تتوافق بطاقة واجهة الشبكة مع كل من نوع مسار الشبكة، طريقة الولوج، أنواع الوصلات، وسرعة النقل. بالإضافة إلى ذلك لا بد من التأكد من قابلية البطاقة للعمل مع كل من نظام التشغيل والعتاد المستخدمين في الجهاز.

- يوضح الجدول التالي (الجدول2) الميزات التي قد تتمتع بها بطاقات الشبكة والتأثير المحدد لكل ميزة على أداء النظام ككل.
- هناك عدة عوامل أساسية لابد من أخذها بعين الاعتبار عند اختيار بطاقة الشبكة المناسبة لهذا المخدم أو محطة العمل تلك، وبالطبع فإن العامل الأكثر أهمية هو مدى موافقة هذه البطاقة للنظام الموجود، حيث ينبغي أن تتوافق بطاقة واجهة الشبكة مع كل من نوع مسار الشبكة، طريقة الولوج، أنواع الوصلات، وسرعة النقل. بالإضافة إلى ذلك لا بد من التأكد من قابلية

البطاقة للعمل مع كل من نظام التشغيل والعتاد المستخدمين في الجهاز.

الميزة	الوظيفة	الفائدة
اختيار سرعة تلقائي	تسمح لبطاقات الشبكة بتحسس سرعة وأسلوب الشبكة والتكيف معها تلقائياً	تساعد على تحسين كل من التعريف والأداء
معالج أو أكثر على اللوحة مباشرة On-board CPU	تسمح للبطاقة بأن تنفذ عدداً من عمليات معالجة المعطيات بشكل مستقل عن معالج الحاسب	تحسين الأداء
وصول مباشر إلى الذاكرة DMA	تمكن البطاقة من نقل المعطيات إلى ذاكرة الحاسب مباشرة	تحسين الأداء
تشخيصية LED (الأضواء على بطاقة الشبكة)	تشير إلى نقل المعطيات، الاتصال، وأحياناً السرعة	تساعد على حل المشاكل
قنوات ثنائية (dual channels)	تساعد على تكوين بطاقتي شبكة في نفس المأخذ	تحسين الأداء، مناسبة للمخدمات
موازنة الحمل (load balancing)	تسمح لمعالج بطاقة الشبكة بتحديد اللحظة المناسبة لتبديل حركة النقل بين البطاقات الداخلية	تحسين أداء الشبكات ذات حركة النقل الكثيفة، مناسبة للمخدمات
إرسال واستقبال من نمط Look Ahead	تسمح لمعالج بطاقة الشبكة ببدء معالجة المعطيات دون الحاجة لانتظار وصول كامل الحزمة	تحسين الأداء
مقدرات الإدارة (SNMP)	تسمح لبطاقة الشبكة بأن تنفذ مراقبة ذاتية، وأن تحل مشاكلها بنفسها، غالباً ما يتم ذلك بوساطة تطبيقات برمجية خاصة.	تساعد على حل المشاكل، تمكن من كشف المشاكل قبل أن تصبح كارثية
مقدرات إدارة الطاقة	تسمح لبطاقة الشبكة بأن تشارك في مقاييس توفير طاقة الحاسب	تطويل عمر بطاريات الأجهزة المحمولة
تخزين RAM المؤقت RAM Buffering	توفر ذاكرة إضافية لبطاقة الشبكة، مما يوفر بدوره مساحة إضافية لتخزين المعطيات	تحسين الأداء
ذاكرة ROM قابلة للتطوير	تسمح بتطوير للرقاقة الموصولة مباشرة إلى اللوحة الأم	تحسين الأداء وسهولة الاستخدام

المكررات (Repeaters)

- المكررات هي أبسط أنواع أجهزة الوصل والربط التي تولد إشارة رقمية، تعمل المكررات في الطبقة الفيزيائية من نموذج

OSI، وهي لذلك لا تتمتع بأي وسيلة لتفسير المعطيات التي تقوم بنقلها، حيث لا تتمتع المكررات مثلاً بالقدرة على تصحيح أو تحسين الإشارات السيئة أو الخاطئة، حيث تقتصر مهمة المكررات على إعادة توليد أو تكرير الإشارة فقط، وبالتالي فلا يمكن اعتبارها، من هذا المنطلق، أجهزة ذكية، حيث لا يمكنها قراءة المعلومات المتموضعة في الطبقات الأعلى من أطر المعطيات، كما لا يمكنها قيادة المعطيات إلى مستقرها النهائي، فالمكررات لا تقوم بما يتجاوز توليد الإشارة على امتداد كامل القطاع. وتترك مهمة التعرف على المعطيات وقبولها للمستقبل الذي يتلقى هذه الإشارة.

- لا تقتصر محدودية المكررات على وظيفتها، فمجال عمل هذه المكررات محدود بدوره، حيث يحتوي كل مكرر على بوابة دخل واحدة وعلى بوابة خرج واحدة فقط، وبالتالي فإن المكرر لا يقدر إلا على استقبال وتكرار مجرى معطيات (Data Stream) واحد فقط. بالإضافة إلى هذا، فإن تقنية المكررات لا تصلح في الحقيقة إلا للشبكات المعتمدة على طوبولوجيا المسار (Bus Topology).

- تمتاز المكررات بأنها تعتبر طريقة غير مكلفة لتوسيع الشبكة، إلا أن المكررات وبسبب محدوديتها، بالإضافة إلى انخفاض تكلفة التقنيات الأخرى مع الزمن، أصبحت نادرة الاستخدام في الشبكات الحديثة. حيث يستعاض عنها بتقنية الموزعات.

الموزعات (Hubs)

- يعرف الموزع (Hub) بأنه مكرر ذي بوابات خرج متعددة، حيث يحتوي الموزع على عدة بوابات معطيات يمكن وصل الكابلات من عقد الشبكة إليها. تعمل الموزعات مثلها مثل المكررات ضمن الطبقة الفيزيائية من نموذج OSI. ويقبل الموزع الإشارات القادمة من العقد المرسلة ويكرر هذه الإشارات ويعيد بثها إلى كافة العقد المتصلة معه. تحتوي معظم الموزعات على بوابة واحدة، تدعى بوابة uplink ، تسمح هذه البوابة بربط الموزع مع موزع آخر أو أي أداة ربط أخرى. يمكن استخدام الموزعات في شبكات Ethernet كنقاط ربط مركزية تصل الأفرع في نماذج الشبكات النجمية أو الهجينة ذات الأساس النجمي. تدعى الموزعات في الشبكات الحلقية نقاط الوصول متعددة المحطات (Multistation Access Points) أو اختصاراً MAUs.

- يمكن استخدام الموزعات لربط محطات العمل، المخدمات، أو الحواسب الشخصية، كما يمكن استخدمها لربط مختلف أنواع الأجهزة الأخرى بالشبكة مثل مخدمات الطباعة، مخدمات الملفات، أو المبدلات. تتشارك جميع الأجهزة التي ترتبط بالموزع بنفس الكمية من عرض الحزمة (Bandwidth)، وبمجال التصادم (Collision Domain) نفسه.

- يعرف **مجال التصادم** (Collision Domain) بأنه قطاع محدد فيزيائياً أو منطقياً ضمن شبكة Ethernet، ينبغي على كافة الأجهزة الواقعة ضمنه أن تتحقق من التصادمات وأن تعمل على تسويتها.

- يمكن أن يختلف تموضع الموزعات في الشبكة من تصميم لآخر كما هو موضح فيما يلي:

1. تشتمل البنية الأبسط على موزع وحيد يتصل بأدوات ربط أخرى، مثل المبدلات أو المكررات.
2. تتضمن البنى الأكثر تعقيداً موزعات أخرى، يختص كل منها بمجموعة صغيرة من عقد الشبكة، تمتاز هذه الشبكات بأنها لا تحتوي على نقطة فشل وحيدة.

الموزعات (Hubs)

أنواع الموزعات

أنواع الموزعات: تمتاز الموزعات بتنوعها الواسع وذلك لاختلاف أنواع الوسائط وسرعة نقل المعطيات التي يمكن لكل نوع دعمها والتعامل معها، وفيما يلي بعض هذه الأنواع:

1. **الموزعات البليدة (Passive Hubs):** هي أبسط أنواع الموزعات، ولا يتعدى ما تقوم به مجرد تكرار الإشارات.
2. **الموزعات الذكية (Intelligent Hubs):** تتميز هذه الموزعات بالقدرة على القيام ببعض العمليات الإضافية مثل تنقية المعطيات، السماح بالإدارة عن بعد، أو تشخيص وضع الشبكة. تدعى الموزعات الذكية أيضاً الموزعات المدارة (Managed Hubs)، وذلك لأنه يمكن إداراتها من أي مكان من الشبكة.
3. **الموزعات الوحيدة (Standalone Hubs):** تقوم هذه الموزعات بتخديم مجموعة من الحواسب المعزولة والمستقلة عن باقي الشبكة، أو التي تشكل بحد ذاته شبكة صغيرة. تستخدم هذه الموزعات في الشبكات المكتبية أو شبكات المؤسسات الصغيرة، ويمكن أن تكون موزعات بليدة أو ذكية، كما تمتاز بسهولة تركيبها ووصلها.تدعى الموزعات الوحيدة بموزعات مجموعة العمل (Workgroup Hubs). إلا أن الموزعات الوحيدة تعرض الشبكة لخطر نقطة الفشل الوحيدة (Single Point of Failure)، حيث يؤدي فشل أحد هذه المكررات إلى توقف كامل الشبكة عن العمل.
4. **الموزعات القابلة للمراكمة (Stackable Hubs):** يشابه هذا النمط من الموزعات، الموزعات الوحيدة إلا أن الموزعات القابلة للمراكمة مصممة خصيصاً لتيتم ربطها مع مكررات أخرى، حيث تنظر الشبكة إلى مجموعة الموزعات القابلة للمراكمة المتصلة مع بعضها البعض على أنها موزع منطقي واحد كبير. يسمح استخدام مثل هذا النمط من الموزعات بتحرير الشبكة من عبء الاعتماد على مكرر وحيد، مما يمكنها من الاستمرار بالعمل حتى لو توقفت بعض موزعاتها عن العمل.

الجسور (Bridges)

- **الجسور (Bridges):** تعرف الجسور بأنها أجهزة الوصل التي تربط قطاعي شبكة مع بعضهما البعض وذلك بتحليل أطر المعطيات الواردة وتحديد الجهة التي ينبغي إرسال هذه الأطر إليها وذلك اعتماداً على عنوان الـMAC المضمنة في كل إطار. تعمل الجسور في طبقة ربط المعطيات (Data Link) من نموذج OSI. تشابه الجسور المكررات في كونها تحتوي على بوابة دخل وحيدة وبوابة خرج وحيدة، إلا أنها تمتاز عن المكررات في قدرتها على تفسير معلومات العناوين الفيزيائية.

- **ميزات استخدام الجسور:**

1. أحد الميزات الأساسية التي تتمتع بها الجسور وتميزها عن المكررات والموزعات هي استقلالية الجسور عن البروتوكولات المستخدمة. حيث يمكن للجسور أن تصل بين قطاعين شبكيين يستخدم كل منهما بروتوكولات مختلفة سواءً في الطبقة الفيزيائية أو في طبقة ربط المعطيات. تمنح هذه الاستقلالية عن البروتوكولات المستخدمة الجسور القدرة على نقل المعطيات بشكل أسرع مما هو الحال عليه مع المكررات التقليدية، إلا أن الجسور من جهة أخرى، تستغرق في بث المعطيات عبر الشبكة وقتاً أطول من المكررات أو الموزعات وذلك لأن الجسور تعالج كل طرد معطيات يصل إليها، في حين لا تقوم المكررات أو الموزعات بمثل هذه العملية.
2. يمكن استخدام الجسور لتوسيع شبكات Ethernet وذلك دون أن تترافق عملية التوسيع هذه مع توسيع مجال التصادم.

أي بعبارة أخرى فإن إضافة جسر جديد إلى الشبكة تزيد الطول الكلي للقطاع بما يتجاوز حدوده العظمى الأصلية.

3. تساهم الجسور في تحسين أداء الشبكة وذلك لأنه يمكن برمجتها لتنقية واستبعاد أنواع محددة من أطر المعلومات (مثل أطر البث غير الضرورية).

- بغرض الترجمة بين نوعين مختلفين من قطاعات الشبكة، تقرأ الجسور عنوان MAC المحدد للجهة التي يتم إرسال الأطر إليها وتقرر إما إرسالها قدماً إلى الجهة المحددة أو تنقيتها:
  - إذا ما قرر الجسر أن العقدة المرسل إليها تقع في قطاع شبكي آخر، يقوم بإعادة إرسال طرد المعطيات قدماً إلى ذلك القطاع.
  - أما إذا كان العنوان المرسل إليه يقع ضمن نفس القطاع الشبكي الذي ينتمي إليه العنوان المرسل منه، يقوم الجسر بتنقية (أي رمي أو طرح) إطار المعطيات.

- بينما تبث عقد الشبكة أطر المعطيات عبر الجسر، يقوم الجسر بتشكيل قاعدة معطيات التنقية (Filtering Database) لعناوين MAC المعروفة ومواقعها الفعلية ضمن الشبكة، يستخدم الجسر قاعدة معطيات التنقية هذه في تقرير إذا ما كان ينبغي إرسال الأطر قدماً إلى الجهة المحددة أو تنقيتها.

المبدلات (Switches)

- المبدلات هي عبارة عن أجهزة ربط تقسم الشبكة إلى عدة أجزاء منطقية أصغر حجماً، تعرف هذه الأجزاء باسم القطاعات. تعمل المبدلات التقليدية في طبقة ربط المعطيات (Data Link) من نموذج OSI، إلا أن المبدلات الأحدث تعمل في الطبقة الثالثة أو حتى الطبقة الرابعة من النموذج نفسه. تقوم المبدلات، مثلها مثل الجسور، بتفسير عناوين MAC، وفي الحقيقة يمكن النظر إلى المبدلات على أنها جسور متعددة البوابات. تحتوي معظم المبدلات على معالج داخلي، ذاكرة خاصة بها، نظام تشغيل، وعدة بوابات مما يسمح بربط عدة عقد بالمبدلة في آن معاً.

- يمكن للمبدلات أن تستفيد من عرض الحزمة المحدود بشكل أفضل من الجسور وذلك بسبب احتواءها على عدة بوابات، حيث يمكن اعتبار كل بوابة جسراً بحد ذاتها، حيث تخصص لكل جهاز متصل بأحد هذه البوابات قناة مستقلة خاصة به، أي بعبارة أخرى تحول المبدلة القناة المشتركة إلى عدة قنوات مستقلة.

- أصبحت المبدلات البديل الذي يستخدم عوضاً عن المكررات، كما أنه تسهل إزالة احتقانات حركة المعطيات عبر الشبكات المحلية (LANs)، كما أن بعض مدراء الشبكات يستخدمون المبدلات كبديل للمكررات وذلك لأنها توفر مستويات أمان وأداء أفضل من المكررات.

1. تحقق المبدلات مستويات أمان أفضل من المكررات لأنها تعزل حركة نقل المعطيات الخاصة بجهاز ما عن حركة نقل المعطيات الخاصة ببقية الأجهزة.
2. تحقق المبدلات مستويات أداء أفضل من المكررات لأنها توفر قنوات مستقلة لكافة الأجهزة، كما أن عتاد المبدلات مصمم بما يتوافق مع تمرير المعطيات بشك سريع.

استبدلت المبدلات المكررات في بعض الشبكات المكتبية أو الشبكات صغيرة المدى وذلك بسبب الانخفاض الكبير الذي شهدته تكلفة هذه المبدلات، كما أنها أصبحت أسهل استخداماً وتركيباً وتعريفاً من المكررات، بالإضافة إلى ذلك فإن المبدلات توفر ميزة فصل حركة نقل المعطيات حسب بوابة النقل.

- تعاني المبدلات بدورها من نقطة ضعف أساسية فعلى الرغم من أن المبدلات تحتوي على صيوان (Buffer) لحفظ معلومات الدخل ومعالجة التدفقات المفاجئة في حركة نقل المعطيات، إلا أنها قد لا تستطيع تصريف المعطيات في حال تدفقت بشكل كثيف ومستمر، وإذا ما حدث هذا فإنه لا يمكن للمبدلات تلافي خطر فقدان المعطيات.

الموجهات (Routers)

- يعرف الموجه بأنه جهاز ربط متعدد البوابات يوجه المعطيات بين عقد الشبكة. يمكن أن تتكامل الموجهات مع شبكات LAN أو WAN والتي قد يتعامل كل منها مع سرعات نقل مختلفة أو يستخدم تشكيلة واسعة من بروتوكولات نقل المعطيات.

- عندما يستقبل الموجه طرد المعطيات، يقوم بقراءة معلومات العنوان المنطقي، ويحدد استناداً إلى هذه المعلومات الشبكة التي ينبغي إرسال طرد المعطيات إليها، ومن ثم يحدد أقصر مسار للوصول إلى تلك الشبكة، وأخيراً، يقوم الموجه بإرسال طرد المعطيات إلى العقدة التالية على ذلك المسار.

- تعمل الموجهات في طبقة الشبكات (Network Layer) وهي الطبقة الثالثة من نموذج OSI، ويمكن أن تأتي الموجهات بشكل أجهزة مستقلة مخصصة كموجهات، أو بشكل أجهزة حاسب مبرمجة للعمل كموجهات.

- على العكس من المبدلات، فإن الموجهات تعتمد على نوع البروتوكول المستخدم في الشبكات التي ترتبط بها، وبالتالي ينبغي تصميم هذه الموجهات أو تعريفها بحيث تتوافق مع بروتوكول من بروتوكولات طبقة الشبكات محدد بعينه وذلك قبل أن يصبح بالإمكان استخدامها لتوجيه المعطيات التي يتم نقلها باستخدام هذا البروتوكول. وبشكل عام فإن الموجهات غالباً ما تكون أبطأ من المبدلات أو الجسور وذلك لأنها تستغرق وقتاً إضافياً في تفسير معلومات الطبقة الثالثة أو ما يعلوها من طبقات.

البوابات (Gateways)

- يمكن تصنيف البوابات تحت تصنيف محدد من تصنيفات عتاديات الشبكات، ويمكن تعريفها كمجموعة مركبة من عتاديات وبرمجيات شبكية تصل نوعين مختلفين من الشبكات مع بعضهما البعض، حيث غالباً ما تستخدم البوابات لوصل الشبكات

التي تستخدم بروتوكولات، أو بناً مختلفة، وعلى عكس باقي أجهزة الربط التي تناولناها في هذه الوحدة، تقوم البوابات بإعادة تحزيم المعطيات بحيث يمكن لنظام آخر قراءتها، وحتى تتمكن البوابات من القيام بهذه المهمة، ينبغي عليها العمل على عدة طبقات مختلفة من طبقات النموذج OSI. حيث ينبغي عليها أن تتواصل مع التطبيق، تأسيس وإدارة الجلسات، ترجمة المعطيات المرمزة، وتفسير معطيات العنونة المنطقية والفيزيائية.

- يمكن أن تقام البوابات على المخدمات، الحواسب الصغرية، أجهزة الربط أو محطات العمل، وغالباً ما تكون البوابات أبطأ بكثير من الموجهات أو الجسور وذلك بسبب عمليات الترجمة المعقدة التي ينبغي للبوابات القيام بها، وبسبب بطئها هذا فإن البوابات غالباً ما تسبب اختناقات في حركة نقل المعطيات عبر الشبكة.

الفصل السادس و السابع

عنوان الموضوع:

شبكات TCP/IP

الكلمات المفتاحية:

أنظر معجم المصطلحات المرافق.

ملخص:

نستعرض في هذا الفصل بروتوكولات وإجرائيات مجموعة بروتوكولات الإنترنت TCP/IP، ونتناول طريقة عمل شبكة عامله بمجموعة البروتوكولات تلك.

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- مفهوما التغليف والترجمة
- بروتوكولات المجموعة TCP/IP
- عنونة الحزم: العناوين MAC، والعناوين IP
- مفهوم التوجيه
- مفهوم حلّ العناوين

مقدمة

- تشير وثائق RFC إلى أن بنية الإنترنت تتألف من أربع طبقاتٍ فقط سنُفصِّــلها لاحقاً في الفقرات التالية

- تعطي الوثيقة RFC 871 بعنوان "**نظرة إلى نموذج ARPANET المرجعي**"، توصيفاً لفلسفة نموذج TCP/IP والمهام الوظيفية لكل طبقة منه

- مجموعة البروتوكولات TCP/IP هي الأكثر استخداماً على أنظمة التشغيل Linux/Unix وMac-OS وWindows

- يمثل البروتوكول IP (Internet Protocol)، البروتوكول المسؤول عن عملية توصيل المعطيات بين مختلف الأجهزة

- يمثل كلٌ من البروتوكول TCP والبروتوكول UDP، بروتوكولا نقل ينتميان إلى طبقةٍ أعلى من طبقــة البروتوكــول IP ويتحكمان بعملية النقل بين تطبيقات محددة

تشير وثائق RFC إلى أن بنية الإنترنت التي ندعوها "**نموذج اتصال الإنترنت**"، تتألف من أربع طبقاتٍ فقط سنُفصِّــلها لاحقــاً في الفقرات التالية. ويستخدم بعض المؤلفين مصطلحات أخرى "**كنموذج TCP/IP**" أو "**نموذج إدارة الدفاع (DOD)**" عند توصيف النموذج الذي نحن بصدده

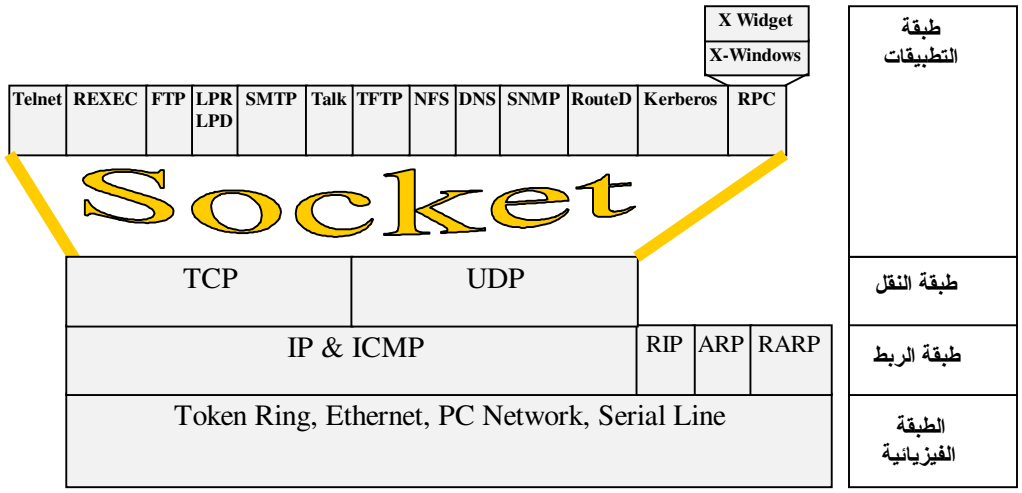
تعطي الوثيقة RFC 871 بعنوان "**نظرة إلى نموذج ARPANET المرجعي**"، توصيفاً لفلسفة نموذج TCP/IP والمهام الوظيفية لكل طبقة منه. يرجع تاريخ الوثيقة الآنفة الذكر إلى أيلول 1982 وهو تاريخ تشكيل شبكة ARPANET مهد شبكة الإنترنت والشبكة التي جرى عليها تطوير وتجربة الكثير من تقانات الإنترنت. إلا أن عملية التحديث قد طالت العديد من التقانات منذ هذا التاريخ بما فيها شبكة ARPANET نفسها، بحيث أصبح تعبير "نموذج ARPANET المرجعي" قديماً وغير مناسبٍ للواقع. لذا، يمكننا تسمية هذا النموذج بنموذج الاتصال TCP/IP أو بنموذج اتصال الإنترنت كون هذا التعبير:

- يسمح بتحديد ارتباط النموذج بتقانات "الإنترنت" بشكل واضح
- ويشدد على طبيعة "الاتصال" في هذا النموذج

تعتبر مجموعة البروتوكولات TCP/IP المبنية وفق معايير النموذج المرجعي TCP/IP، البروتوكولات الأكثر استخداماً على أنظمة التشغيل Linux/Unix وMac-OS وWindows ومع معظم أنظمة التشغيل الأخرى، مما يجعلها تُشكل لغة الإنترنت.

يمكن للأجهزة التي تستخدم مجموعة البروتوكولات TCP/IP أن تتبادل المعطيات بالرغم من اختلافها. إذ يمثــل البروتوكــول IP (Internet Protocol) في هذه المجموعة، البروتوكول المسؤول عن عملية توصيل المعطيات بين مختلف الأجهزة في حين يمثــل كــلٌ مــن البروتوكــول TCP (Transmission Control Protocol) والبروتوكــول UDP (User Datagram Protocol)، بروتوكولا نقل ينتميان إلى طبقةٍ أعلى من طبقة البروتوكول IP ويتحكمان بعملية النقل بين تطبيقات محددة.

عائلة TCP/IP السعيدة



يشترك كلاُ من TCP/IP والإنترنت بنفس التاريخ الذي يعود إلى عدة عقودٍ ماضية. إذ يعود النجاح التقني للإنترنت بشكل أساسي للتصميم المرن والأنيق لمجموعة البروتوكولات TCP/IP، ولكون هذه البروتوكولات قياسية مجانية مفتوحة لا تملكها جهة محددة. وقد ساهم انتشار الإنترنت في إعطاء TCP/IP أهمية استثنائية ميزته عن غيره من البروتوكولات.

وتعتبر مجموعة البروتوكولات TCP/IP سلسلةً مصممةً لتعمل مع بعضها البعض. تتضمن هذه البروتوكولات مجموعة من المكونات المُعرَّفة في عدة وثائق RFC:

- البروتوكول UDP (User Datagram Protocol) والبروتوكول TCP (Transmission Control Protocol) اللذان يقومان بعملية نقل المعطيات إلى تطبيقات محددة على الجهاز الوجهة، حيث يقدم UDP عملية نقل غير موثوقة ولكن بأفضل سرعة ممكنة بينما يضمن TCP عملية نقل موثوقة ثنائية الإتجاه مع مراقبة وتحكم بعملية التدفق ومع تصحيح للأخطاء الناتجة عن النقل وتبادل المعطيات بين الجهازين (RFC768 و RFC793 على الترتيب)
- البروتوكول IP (Internet Protocol) الذي يقوم بتوصيل طرود المعطيات من جهاز إلى آخر (RFC791)
- البروتوكول ICMP (Internet Control Message Protocol) الذي يوفر عدة مستويات دعم للبرتوكول IP تتضمن رسائل الأخطاء والرسائل المساعدة في عملية التوجيه بالإضافة إلى المساعدة في عملية سرد أعمال مجموعة البروتوكولات (RFC792)
- البروتوكول ARP (Address Resolution Protocol) الذي يقوم بترجمة العناوين IP إلى عناوين فيزيائية (RFC823)

بعد تنفيذ ونشر TCP/IP، نفذت هيئة ISO (اعتماداً على النموذج المرجعي OSI) مجموعة بروتوكولات خاصة بها مصممة على أساس سبع طبقات ودعتها بإسم نموذجها المرجعي OSI، ولكن هذا التصميم لم يحظ بشعبية نظراً لضخامته وتعقيده وعدم فعاليته، حتى أن البعض كان يسخر من عدد الطبقات قائلاً أن هذا التصميم مازال يحتاج لإضافة طبقة أرستقراطيين، وطبقة برجوازيين، وطبقة بروليتاريا، على طبقاته السبع.

طبقة النقل: البروتوكول TCP والبروتوكول UDP

تعتبر طبقة النقل، الطبقة المسؤولة عن تأمين وصول المعطيات بشكل صحيح بين عقد الاتصال. وتشترك جميع بروتوكولات هذه الطبقة في اكتشاف الأخطاء وفي إعادة ترتيب المعطيات التي تصل بترتيب يختلف عن ترتيب إرسالها. يعمل في هذه الطبقة البروتوكولان TCP وUDP اللذان نستعرض خصائصهما فيما يلي:

TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
يعتمد البروتوكول TCP على مبدأ الاتصال التأكيدي الذي يُسهل عملية التخاطب بين تطبيقين.	يعتمد البروتوكول UDP مبدأ الاتصال غير التأكيدي ويدعى بمبدأ حزمي التوجه.
يعمل على نحو مشابه للإتصال التلفوني: يتم نقل الكلمات إلى الشخص المقابل وبالعكس، وتجري المحافظة على الإتصال حتى في حال توقف الطرفان عن الكلام.	يشبه عمل UDP، عملية إرسال رسالة عبر مكتب البريد.
يوفر TCP نقلاً موثوقاً للمعطيات ومراقبةً للتدفق بالإضافة إلى مراقبته للإختناقات.	لا يقدم اتصالاً ثنائي الاتجاه كما لا يقوم بأي عملية مراقبة للإزدحام ولا يضمن وصول الطرود بترتيب الإرسال.
يجبر البروتوكول TCP مختلف المستثمرين على الاشتراك في عرض الحزمة ويعمل بأسلوب يجعل الأداء العام للشبكة جيداً.	يمتاز البروتوكول UDP بنقله الطرود بالسرعة الممكنة.
تاريخياً، تم اعتماده للتعويض عن عدم وثوقية البنية الشبكية التحتية.	تطور البنية التحتية الشبكية وازدياد ووثوقيتها جعلته يكتسب أهمية متزايدة.
نظراً لازدياد شعبية الإنترنت والازدياد المضطرد لمستثمريها، تزداد الحاجة لحركة مرور من النمط TCP لتجنب الاختناقات وتوفير مشاركة فعالة لعرض الحزمة.	قياس مستوى استخدام البروتوكولات خلال السنوات القليلة الماضية يظهر ارتفاعاً بمقدار 5% من إجمالي عدد البايتيات لحركة المرور من النمط UDP في عامي 1997-1998 و7% في عامي 1998-1999.
انتشار الوب وانتشار تطبيقات أخرى كالبريد الإلكتروني التي تعتمد في النقل على TCP عوضاً عن UDP، أبقى على ارتفاع منسوب استخدام TCP.	مازالت تطبيقات شبكية كالألعاب وتطبيقات نقل الموسيقى والصور والفيديو المعتمدة على UDP غير منتشرة بكثرة حتى الآن على مستوى الإنترنت.

قرائة النصوص نفسها مع اختيار الطريقة الملائمة للقراءة وفق سيناريو العرض الذي تختارونه

أرقام البوابات

من أشهر البوابات التي تعبر عن خدمات إنترنت وهي عموماً خدمات تعتمد على بروتوكول النقل TCP، نذكر:

البوابة	البروتوكول	الخدمة
21	FTP	نقل الملفات
23	Telnet	فتح جلسة عن بعد
25	SMTP	نقل البريد الإلكتروني
80	Web	الوب، مشاركة الوثائق
110	POP-3	الوصول عن بعد إلى صندوق البريد الإلكتروني
119	NNTP	الأخبار

تُعرِّف العناوين الشبكية، الأجهزة –أو على نحو أدق– الواجهات الشبكية للأجهزة. ولا تُعرِّف إجراء خاص أو خدمة خاصة. لذا يوسع البروتوكولان TCP وUDP مفهوم العناوين IP اعتماداً على مفهوم "**البوابات**".

يجري التعبير عن البوابات بأرقام ممثلة على 16 بت تُضاف إلى العنوان الشبكي لتحديد قناة اتصال محددة. وتمتلك الخدمات مثل خدمة البريد الإلكتروني (email) وخدمة نقل الملفات (FTP) وخدمة الوب (web) بوابات معيارية عند تشغيلها على الإنترنت، حيث تمنع مختلف أنظمة التشغيل تعديل البوابات التي لها قيمة أصغر من 1024 من أجل مختلف البرامج والخدمات إلا إذا كان المستثمر هو مدير النظام. (طبعاً يقتصر المنع على تعديل رقم البوابة أما الاتصال بالبوابة فهو ممكن لأي مستثمر).

نشاطات

1. ابحث في نظام Windows الذي تعمل عليه على الملف المرجعي الذي يحتوي على أرقام البوابات المعيارية.

2. ما هي أرقام بوابات الخدمات التالية:
   i. TFTP
   ii. IMAP4
   iii. Finger
   iv. Telnet

الأجوبة:

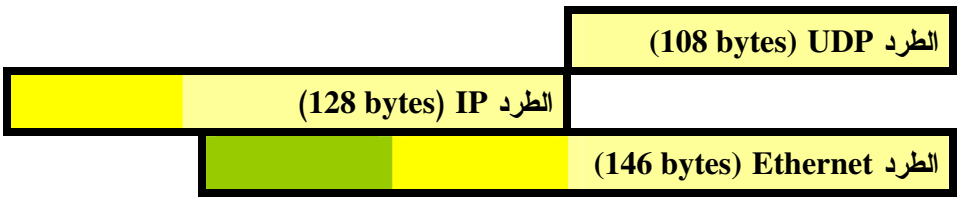
i. **TFTP (69)**
ii. **IMAP4 (110)**
iii. **Finger (79)**
iv. **Telnet (23)**

تغليف المعطيات

- تنتقل المعطيات في الشبكة على شكل "**طرود**" وهي قطع من المعطيات لها طول أعظمي تفرضه طبقة الارتباط. يتألف كل طرد من رأس ومن حِمل.
  - ندعو وحدة المعطيات الخاصة بطبقة الربط "**إطار**"
  - ندعو وحدة المعطيات الخاصة بالبروتوكول IP "**رسالة معطيات**"
  - ندعو وحدة المعطيات الخاصة بالبروتوكول TCP "**مقطعاً**"
  - نستخدم مصطلحاً عاماً هو " **الحزمة**" للدلالة على جميع هذه الحالات

- عند هبوط الحزمة، يعمل كل بروتوكول على إضافة معلومات خاصة به وإضافتها كرأس للحزمة الواردة من الطبقة الأعلى. ندعو هذه العملية بعملية "**التغليف**"، في حين ندعو العملية المعاكسة بعملية "**الترجمة**". يوضح المثال التالي مكونات مثل هذا النوع من الأطر

قيمة تحقق (CRC)	معطيات التطبيق	الرأس UDP	الرأس IP	الرأس Ethernet
4 bytes	100 bytes	8 bytes	20 bytes	14 bytes



- نستخدم مصطلح "بايت" (byte) للدلالة على مقطع من المعطيات مكوناً من 8 بت. ولكن نظراً لتحول مصطلح بايت إلى مصطلح عمومي، يجري حالياً في وثائق RFC استخدام مصطلح (octet) عوضاً عنه.

تنتقل المعطيات في الشبكة على شكل "**طرود**" وهي قطع من المعطيات لها طول أعظمي تفرضه طبقة الارتباط. يتألف كل طرد من رأس ومن حِمل. يتضمن الرأس معلومات عن مصدر الطرد وعن وجهته، بالإضافة إلى قيم تساعد في التحقق من صحة المعطيات ومعلومات خاصة بالبروتوكول. في حين يتضمن الحِمل المعطيات المُرسَلة إلى الوجهة.

يتعلق أسم وحدة المعطيات بطبقة البروتوكول. إذ ندعو، بشكلٍ عام، وحدة المعطيات الخاصة بطبقة الربط "**إطاراً**"، ولكن ندعو تجاوزاً وحدة المعطيات الخاصة بالبروتوكول IP "**رسالة معطيات** "، وندعو الوحدة الخاصة بالبروتوكول TCP "**مقطعاً**"، وتلك الخاصة بالبروتوكول UDP "**رسالة معطيات**" أيضاً. إلا أننا نستخدم مصطلحاً عاماً هو " **الحزمة**" للدلالة على جميع هذه الحالات.

عند هبوط الحزمة من طبقة إلى أخرى تمهيداً لإرسالها (من TCP أو UDP في طبقة النقل إلى IP ومن ثم إلى Ethernet باتجاه السلك أو الكابل الفيزيائي) يعمل كل بروتوكول على إضافة معلومات خاصة به وإضافتها كرأس للحزمة الواردة من الطبقة الأعلى. بالنتيجة، تصبح الحزمة الناتجة عن كل بروتوكول حِملاً لحزمة بروتوكول الطبقة **الأدنى**. ندعو هذه العملية بعملية **التغليف**. أما على الجهاز المستقبل فتتم عملية معاكسة لعملية التغليف السابقة عند صعود الحزمة من طبقة إلى الطبقة الأعلى ندعوها عملية "**الترجمة**".

فعلى سبيل المثال، تحتوي حزمة UDP مُرسلة عبر شبكة Ethernet على ثلاثة مغلفات مختلفة. فعلى طبقة Ethernet يجري "**تأطيرها**" باستخدام رأس بسيط يحتوي على العنوان الفيزيائي الخاص بالمصدر وبالجهاز المُستهدف بالإضافة إلى طول الإطار وقيمة التحقق من صحته. يكون حِمل الحزمة الخاصة بطبقة Ethernet مؤلفاً من حزمة IP، أما حِمل الحزمة IP فيحتوي على حزمة UDP، ويكون حِمل الحزمة UDP حاوياً على المعطيات التي يجري نقلها.

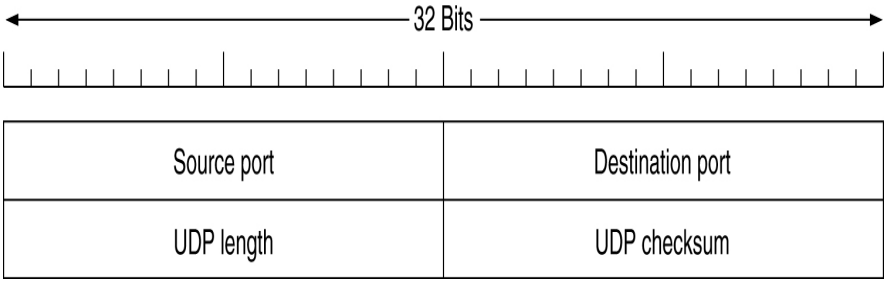
نستخدم مصطلح "بايت" (byte) للدلالة على مقطع من المعطيات مكوناً من 8 بت. ولكن نظراً لتحول مصطلح بايت إلى مصطلح عمومي، يجري حالياً في وثائق RFC استخدام مصطلح (octet) عوضاً عنه.

المقطع UDP

يتألف المقطع UDP من حزمة معطيات يسبقها رأس يجري فيه تحديد المعلومات التالية:

- البوابة المصدَر في الجهاز المُرسِل (Source Port)؛
- البوابة المُستهدفة في الجهاز المُستهدَف (Destination Port)؛
- طول المقطع UDP (UDP Length)؛
- قيمة تحقق من عدم حصول أخطاء في الطرد (UDP checksum).

يكون شكل رأس المقطع UDP كما يلي:



يتألف المقطع UDP من حزمة معطيات يسبقها رأس يجري فيه تحديد المعلومات التالية:

- البوابة المصدَر في الجهاز المُرسِل (Source Port)
- البوابة المُستهدفة في الجهاز المُستهدَف (Destination Port)
- طول المقطع UDP (UDP Length)

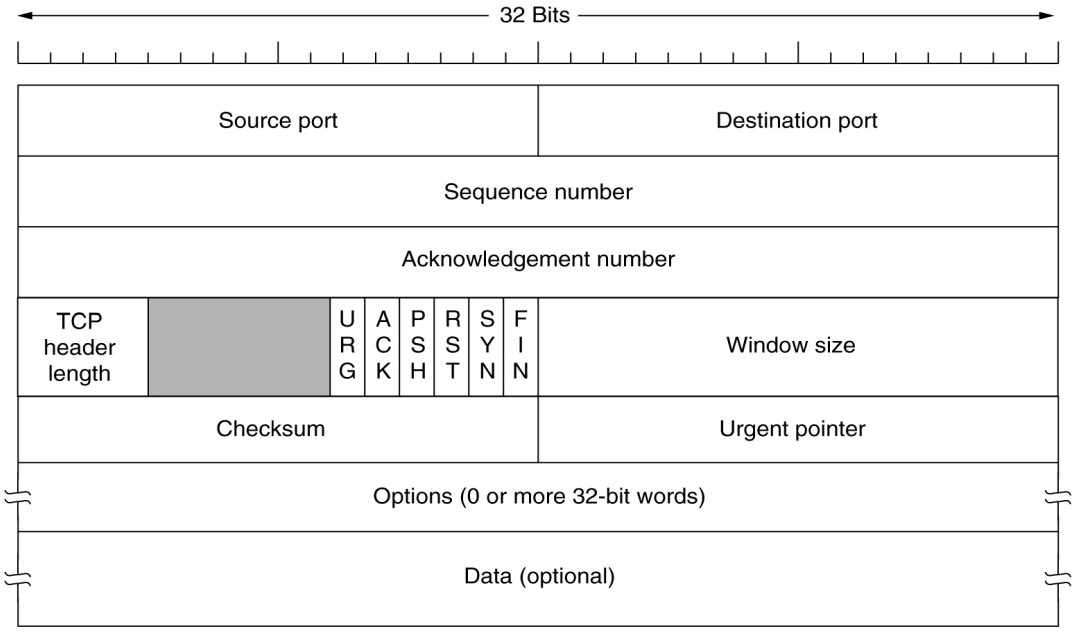
- قيمة تحقق من عدم حصول أخطاء في الطرد (UDP checksum)

المقطع TCP

يتألف المقطع TCP من حزمة معطيات يسبقها رأس يجري فيه تحديد مجموعة من المعلومات، نذكر منها:

- البوابة المصدَر في الجهاز المُرسِل (Source Port)
- البوابة المُستهدفة في الجهاز المُستهدَف (Destination Port)
- الرقم التسلسلي للطرد (Sequence Number - SEQ)
- الرقم الدال على رد في حال كان المقطع مُرسَل كرد على طردٍ سابق (Acknowledgement Number - ACK)
- طول رأس المقطع TCP (TCP Header Length)
- نمط المقطع المُرسَل (رد ACK، أو إيقاف FIN، أو مزامنة وإعلام SYN، أو طلب إعادة إرسال RST، ... وغيرها)
- حجم نافذة الإرسال المُعَبرة عن عدد مقاطع TCP المُرسَلة دفعة واحدة (قبل البدء بانتظار الأجوبة) (Window Size)
- قيمة تحقق من عدم حصول أخطاء في الطرد (TCP checksum)

يكون شكل رأس المقطع TCP كما يلي:

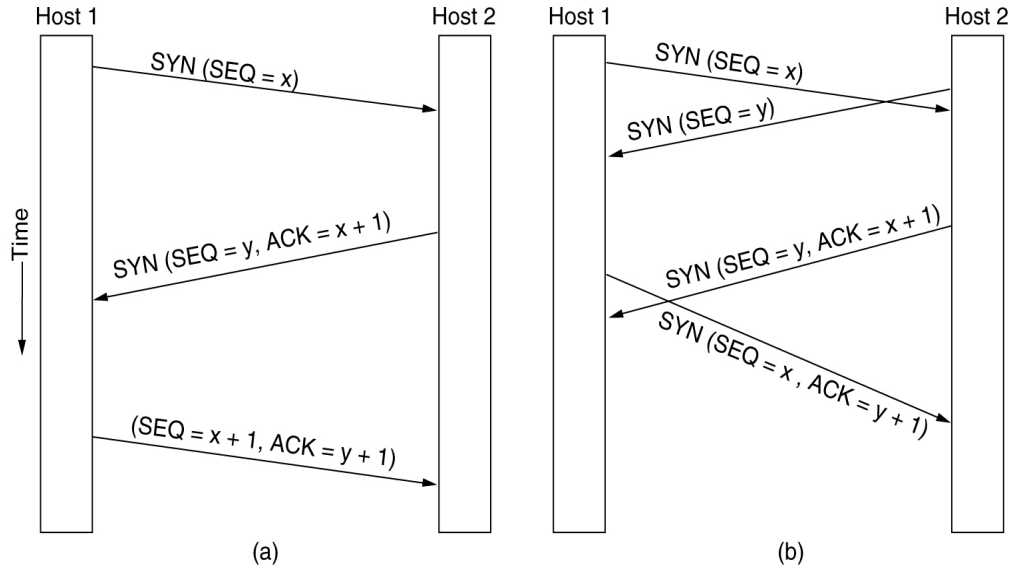


يتألف المقطع TCP من حزمة معطيات يسبقها رأس يجري فيه تحديد مجموعة من المعلومات، نذكر منها:

- البوابة المصدَر في الجهاز المُرسِل (Source Port)
- البوابة المُستهدفة في الجهاز المُستهدَف (Destination Port)
- الرقم التسلسلي للطرد (Sequence Number - SEQ)
- الرقم الدال على رد في حال كان المقطع مُرسَل كرد على طردٍ سابق (Acknowledgement Number - ACK)
- طول رأس المقطع TCP (TCP Header Length)
- نمط المقطع المُرسَل (رد ACK، أو إيقاف FIN، أو مزامنة وإعلام SYN، أو طلب إعادة إرسال RST، ... وغيرها)

- حجم نافذة الإرسال المُعبَرة عن عدد مقاطع TCP المُرسَلة دفعة واحدة (قبل البدء بانتظار الأجوبة) (Window Size)
- قيمة تحقق من عدم حصول أخطاء في الطرد (TCP checksum)

فتح اتصال TCP



a. فتح اتصال بدون تصادم

b. فتح اتصال مع تصادم

يجري إنشاء اتصال TCP على ثلاث مراحل، وتتم العملية كما يلي:

1. ينتظر مخدم على إحدى النقاط الشبكية مستمعاً إلى الاتصالات الشبكية من خلال إجرائيتين: LISTEN وACCEPT
2. يستخدم زبون على طرف آخر من الشبكة، الإجرائية CONNECT التي تأخذ المعاملات: عنوان المخدم ورقم بوابة الخدمة المطلوبة بالإضافة إلى معاملات أخرى، وتُرسِل مقطع TCP يحتوي على البت SYN مُفعَّلاً (يساوي 1) وعلى البت ACK غير مُفعَّل (يساوي 0). كما يمتلك المقطع رقماً تسلسلياً يجري تخزينه في SEQ
3. عند وصول المقطع إلى الجهاز المُستهدَف، تبحث الإجرائية LISTEN عن البوابة المطلوبة فإذا لم تجدها، تُرسل للمصدر مقطع TCP من النمط RST (أي يحتوي على بت RST مُفعلاً ومُساوياً للقيمة 1)، لتشير إلى أن الجهاز المُستقبِل قد رفض طلب الاتصال
4. أما إذا كانت الخدمة عاملة ومُفعَّلة، يجري إرسال المقطع إلى الخدمة، ويجري في حال قبوله على مستوى الخدمة، إرسال جواب على المقطع. يكون الجواب عبارة عن مقطع من النمط ACK له رقم تسلسلي خاص، ورقم جواب يساوي الرقم التسلسلي الخاص بالطلب الأصلي مُضافاً إليه واحد
5. للإشارة إلى إقامة الإتصال، يعيد الجهاز صاحب الطلب الأصلي، جواباً على الجواب السابق، مستخدماً الرقم التسلسلي للجواب السابق ومضيفاً إليه واحد
6. يُصبح الاتصال عندها مُفعَّلاً

ملاحظة:

في حال كان الطرفان يحاولان إنشاء اتصالين متعاكسين على نفس الخدمة (الأول باتجاه الثاني، والثاني باتجاه الأول)، تنشئ لدينا حالة ندعوها بحالة تصادم تنتج عن استخدام كل جهاز لنفس القناة (عنوان الجهاز، رقم الخدمة) في إنشائه لاتصال مع الآخر باتجاه نفس الخدمة.

إنهاء اتصال TCP

لإنهاء اتصال TCP، يمكن لأحد طرفي الاتصال أن يبدأ بطلب الإنهاء. تَعتبر الجهة التي أرسلت طرد الإنهاء، وتبعاً لموقعها، أن الإرسال أو الاستقبال قد انتهى عند إرسالها للطرد حتى ولو وردتها معطيات إضافية (في حال كانت جهة مُستقبِلة):

1. يبدأ الإنهاء مع إرسال طرد من النمط FIN (يكون فيه البت FIN مُفعَّلاً ومساوياً للواحد)
2. عند وصول الطرد FIN إلى الطرف الآخر يجري إرسال رد ACK على طلب الإنهاء مع طرد FIN للتأكيد على انتهاء العملية وعلى التوقف عن الإرسال أو الاستقبال، (يمكن أن يكون الطردان مندمجين في طرد واحد)
3. يرسل صاحب طلب الإنهاء الأصلي رد ACK على الطرد السابق

طبقة الربط

- تعتبر عملية إضافة رؤوس إلى الحزم وفصلها عن بعضها البعض من العمليات الأساسية لطبقة الربط
- ندعو إجراء إضافة بتات الفصل لتشكيل **الأطر**، بعملية "**التأطير**"
- تحدد المعايير والخيارات لمُختلف سرعات تقانة Ethernet (10Mb/s و100Mb/s و1Gb/s و10Gb/s) اعتماداً على المعايير IEEE

ملاحظة:

يمكن الرجوع إلى الموقع www.host.ots.utexas.edu/internet الذي يديره Charles Spurgeon للحصول على العديد من المراجع عن تقانة Ethernet.

تعتبر عملية إضافة رؤوس إلى الحزم وفصلها عن بعضها البعض من العمليات الأساسية لطبقة الربط. إذ تحتوي الرؤوس على معلومات العنونة الخاصة بحزم طبقة ربط المعطيات بالإضافة إلى قيم التحقق. أما الفواصل فتشير إلى نقطة انتهاء كل حزمة وبداية الحزمة التالية.

ندعو إجراء إضافة بتات الفصل لتشكيل **الأطر**، بعملية "**التأطير**". يُستخدم حالياً معيارين لعملية التأطير الخاصة بتقانة Ethernet: معيار Dix Ethernet II ومعيار IEEE 802.2LLC SNAP. تستخدم منصات Linux المعيار Ethernet II كحال معظم منصات UNIX وموجهات CISCO. أما Novell وشبكات IPX ومنصات Windows فتستخدم عادةً المعيار 802.2 الذي يختلف مع المعيار Ethernet II في بعض الحقول الخاصة برأس الإطار والتي لا تتعارض فيما بينها. يمكن للأجهزة المستقبِلة للأطر أن تحدد بدقة نوع الصيغة المستخدمة من قبل كل إطار ويمكن لها أن تفك ترميز الرؤوس بشكل صحيح مهما كان المعيار المُستَخدَم في بناء الإطار.

تحدد المعايير والخيارات لمُختلف سرعات تقانة Ethernet (10Mb/s و100Mb/s و1Gb/s و10Gb/s) اعتماداً على المعايير IEEE. يجري عادةً اعتبار كل نمط من أنماط الكابلات التي تمتد على مسافات قصيرة كتقانة جديدة قائمة بذاتها.

ملاحظة:

يمكن الرجوع إلى الموقع www.host.ots.utexas.edu/internet الذي يديره Charles Spurgeon للحصول على العديد من المراجع عن تقانة Ethernet.

وحدة النقل العظمى

- يكون حجم الطرود المنقولة على شبكة محدوداً بمواصفات العتاد الصلب وبمواصفات البروتوكول. ويرتبط الحجم ببروتوكول طبقة الإرتباط وندعو الحجم الأكبر الممكن "**وحدة النقل العظمى**" (MTU):

نمط الشبكة	وحدة النقل العظمى MTU
Ethernet	1500 بايت (1492 مع تأطير وفق 802.2)
وصلة مودم PPP	قابلة للإعداد وتكون غالباً 512 أو 576 بايت
وصلة بعيدة المدى نقطة لنقطة (T1, T3)	قابلة للإعداد وغالباً مساوية للقيمة 1500 بايت أو 4500 بايت

- تُقسِّم طبقة IP في سلسلة البروتوكولات TCP/IP الطرود إلى وحدات أصغر لتوافق قيمة وحدة النقل العظمى الخاصة بطبقة ربط الشبكة. ويمكن أن يعمل الموجه الذي يوجه الطرد على تقسيم هذا الطرد اعتماداً على إجراء ندعوه إجراء **التقطيع**

يكون حجم الطرود المنقولة على شبكة محدوداً بمواصفات العتاد الصلب وبمواصفات البروتوكول. فعلى سبيل المثال لا يمكن لحِمل إطار Ethernet معياري أن يتجاوز 1500 بايت. ويرتبط الحجم ببروتوكول طبقة الإرتباط وندعو الحجم الأكبر الممكن "**وحدة النقل العظمى**" (MTU) يعرض الجدول التالي بعض القيم النمطية للوحدة MTU:

نمط الشبكة	وحدة النقل العظمى MTU
Ethernet	1500 بايت (1492 مع تأطير وفق 802.2)
وصلة مودم PPP	قابلة للإعداد وتكون غالباً 512 أو 576 بايت
وصلة بعيدة المدى نقطة لنقطة (T1, T3)	قابلة للإعداد وغالباً مساوية للقيمة 1500 بايت أو 4500 بايت

تُقسِّم طبقة IP في سلسلة البروتوكولات TCP/IP الطرود إلى وحدات أصغر لتوافق قيمة وحدة النقل العظمى الخاصة بطبقة ربط الشبكة. وفي حال توجيه الطرد بين عدة شبكات، يمكن لشبكة وسيطة أن تمتلك وحدة النقل العظمى الأصغر مقارنةً ببقية الشبكات ومقارنةً بالشبكة التي أصدرت الطرد. في هذه الحالة، يعمل الموجه الذي يوجه الطرد باتجاه الشبكة ذات الوحدة الأصغر، على تقسيم هذا الطرد اعتماداً على إجراء ندعوه إجراء **التقطيع**.

يُعتبر إجراء التقطيع عملاً غير مرغوب فيه بالنسبة لموجه. في الحقيقة، يمكن للبروتوكول TCP أن يحدد الوحدة الأصغر على طول الطريق واختيار حجم الطرد على نحوٍ ملائم لهذه الوحدة منذ البداية، أما البروتوكول UDP فلا يمكنه تنفيذ عملية التقطيع مما يجعله يعتمد على البروتوكول IP من الطبقة الأدنى لتنفيذ هذا العمل.

نشاط

باستخدام تعليمة ping وباستخدام إحدى خياراتها، يمكنك إرسال حزمة بطول معين إلى منصة مقابلة وستنتاج وحدة النقل العظمى للشبكة المحلية التي تعمل عليها (لن يجري الإرسال قبل تحديد طول حزمة مقبول).

ما هو هذا الخيار، وما هو شكل تعليمة ping التي يجب أن نستخدمها، وما هي قيمة وحدة النقل العظمى على شبكتك؟

لاحظ أن القيمة التي تحصل عليها يمكن أن تكون القيمة الحقيقية مُضافاً إليها طول رأس الطرد (32 بايت) وهذا تبعاً لنظام التشغيل الذي تعمل عليه.

الجواب:

Ping –l *size* –f *target_address*

طبقة الإنترنت والبروتوكول IP (1)

يعتبر البروتوكول IP العنصر الأكثر أهمية في سلسلة بروتوكولات الإنترنت. فهو البروتوكول الوحيد الذي يقدم خدمات إيصال وحدات المعطيات إلى بروتوكولات طبقة النقل.

ندعو حزم البروتوكول IP **رسائل معطيات**. تُميز الخصائص الثلاث التالية خدمة إيصال رسالة معطيات:

- تعتمد الخدمة على مبدأ اتصال غير تأكيدي حيث يجري إيصال كل رسالة معطيات بشكل مستقل عن الرسائل الأخرى المُرسَلة سابقاً وتلك التي ستُرسل لاحقاً
- تكون الخدمة غير موثوقة فلا ضمان لوصول الرسائل
- تعتمد الخدمة على مبدأ عدم إدّخار أي جهد لتحقيق الهدف ولإيصال أي رسالة معطيات. غير أن إهمال الرسائل ممكن عندما يصبح من المستحيل إيصالها نتيجة نقصٍ الموارد اللازمة لإتمام المهمة أو نتيجة عطل أو نتيجة وجود تقانة غير كافية لإتمام العمل

من البديهي تصور البروتوكول IP وكأنه يعمل على إخفاء تنوع تقانات طبقات الربط المختلفة بحيث تتعامل هذه التقانات مع طبقة النقل وكأن الطبقات المختفية خلفها تشكل كتلة واحدة.

طبقة الإنترنت والبروتوكول IP (2)

يُعرِّف نموذج اتصال الإنترنت وسلسلة بروتوكولات الإنترنت نمطين من الطرفيات التي تعتمد في عملها على البروتوكول IP: منصات العمل والموجهات.

ندعو شبكة العقد المرتبطة ببعضها البعض عبر نفس وسيط البث (أو عبر مجموعة متصلة من وسائط البث) "**بمقطع شبكي**" ولاتكون هذه الشبكة بحاجة لموجهات أو لعملية توجيه.

تشكل عملية التوجيه الوظيفة الأكثر أهمية لطبقة الإنترنت. إذ تؤدي الموجهات عملها اعتماداً على طبقة الإنترنت ولا تحتاج لوجود طبقة التطبيقات ولا لوجود طبقة النقل.

تتصل الأجهزة التي أنتجتها جهات إنتاج مختلفة، بالاعتماد على البروتوكول IP استناداً إلى اتفاق مبدئي يعتمد على أسلوبين لترتيب البتات ضمن كل بايت والبايتات ضمن سلاسل البايتات.

- big-endian
- little-endian

ملاحظات:

1. في بدايات عمل IP أصطُلح على تسمية موجهات IP "عبَّارات". إذ تستخدم الوثيقة RFC 791 هذا التعبير. أما الآن فيُستخدم هذا التعبير على مستوى مكونات تعمل ضمن طبقتي التطبيقات والنقل في نموذج اتصال الإنترنت. ولا يقتصر استخدام هذا التعبير على كل حال، على نموذج اتصال الإنترنت.

2. إن وجود نفس مجتزآت طبقة ربط المعطيات في كلا المنصتين المتصلتين لا يعني بالضرورة عدم الحاجة لوجود موجه عند اتصالهما ببعضهما البعض. فإذا كانت هذه المنصات مرتبطة بوسائط بث مختلفة (كابلات مختلفة) تترابط فيما بينها بوساطة موجهات، يجري اتصال المنصات السابقة عبر الموجهات التي تربط وسائط البث.

يُعرِّف نموذج اتصال الإنترنت وسلسلة بروتوكولات الإنترنت نمطين من الطرفيات التي تعتمد في عملها على البروتوكول IP: منصات العمل والموجهات. نُعَرِف منصة عمل على أنها عقدة شبكية غير قادرة على تحويل خط سير عملية النقل. تتلقى منصة العمل المعطيات الموجهة إليها كوجهة نهائية فقط. على العكس من ذلك، تُعتَبر الموجهات عقداً وسيطة. فالمهمة الأولى لموجه تكمن في استقبال المعطيات وتوجيهها إلى وجهتها النهائية.

لا تحتاج كل شبكة لوجود موجه، في حال كانت المنصات متصلة ببعضها البعض باستخدام نفس وسيط البث (مبدلة أو مُجمع) فلا حاجة عندها لتبادل رسائل المعطيات IP عبر مجتزآت البروتوكول IP الموجودة في موجه. فإذا كانت المنصات تحتوي على نفس مجتزآت طبقة ربط المعطيات وكانت المنصات مرتبطة ببعضها البعض عبر نفس وسيط البث فإن هذه المنصات قادرة على تبادل رسائل المعطيات مباشرةً.

ندعو شبكة العقد المرتبطة ببعضها البعض عبر نفس وسيط البث (أو عبر مجموعة متصلة من وسائط البث) "**بمقطع شبكي**". ويُدعى هذا النمط في بعض الأحيان بـــ "**شبكات الطبقة الثانية**" وذلك نسبة إلى ترتيب طبقة ربط المعطيات في نموذج OSI. بنفس الطريقة، ندعو الشبكات المكوَنَة من مقاطع ترتبط فيما بينها باستخدام موجهات "**بشبكات الطبقة الثالثة**".

تشكل عملية التوجيه، في شبكات الطبقة الثالثة، الوظيفة الأكثر أهمية لطبقة الإنترنت. إذ تؤدي الموجهات عملها اعتماداً على طبقة الإنترنت ولا تحتاج لوجود طبقة التطبيقات ولا لوجود طبقة النقل لتنفيذ عملية التوجيه. رغم ذلك نلاحظ وجود المجتزآت التي تنتمي لطبقة النقل وطبقة التطبيقات في الموجهات وذلك لأهداف تتعلق بإدارة وصيانة هذه الموجهات.

تتصل الأجهزة التي أنتجتها جهات إنتاج مختلفة، بالاعتماد على البروتوكول IP استناداً إلى اتفاق مبدئي يعتمد على أسلوبين لترتيب البتات ضمن كل بايت والبايتات ضمن سلاسل البايتات. يعتمد الأسلوب الأول على وضع البت الأكبر أولاً ضمن كل بايت ووضع البايت الذي شكلته البتات الكبرى أولاً ضمن كل سلسلة. ندعو هذا الترتيب بـــ big-endian. أما الأسلوب الثاني فيستخدم ترتيباً مقلوباً بالنسبة للترتيب السابق يعتمد على وضع البت الأصغر أولاً ضمن كل بايت ووضع البايت الذي شكلته البتات الصغرى أولاً ضمن كل سلسلة. ندعو هذا الترتيب بـــ little-endian. يستخدم البروتوكول IP الأسلوب الأول إذ يُرسل أولاً البتات الكبرى والبايتات التي شكلتها هذه البتات.

عنونة الحزم

كحال رسائل البريد العادي ورسائل البريد الإلكتروني، تحتاج حزم الشبكة لعنونة تسمح لها بالوصول إلى وجهتها. يجري اســتخدام عدة مخططات عنونة:

- عناوين MAC (Medium Access Control) خاصة بالعتاد الصلب
- عناوين IP خاصة بالبرامج والخدمات
- أسماء مضيفين من أجل المستثمرين

تمتلك الواجهة الشبكية الخاصة بمضيف، عنوان MAC تابع لطبقة الربط يساعد على تفريقها عن بقية الأجهزة الموجودة على نفس المقطع الشبكي. أما العنوان IP فيُعرف الجهاز بالنسبة للشبكة الكلية. ويساعد اسم المُضيف المستخدم على تعريفه ضــمن الــشبكة الكلية.

العناوين MAC

تتأثر عنونة المستوى الأدنى بنوعية العتاد الصلب الشبكي المُستَخدَم:

- تمتلك أجهزة Ethernet عنوان مُرَمَّز على 6 بايت تضعه الجهة المصنعة
- تمتلك واجهات Token Ring عناوين مشابهة مُرمَزة على 6 بايت أيضاً

ينقسم عنوان Ethernet مُرَمَّز على 6 بايت إلى قسمين:

- تعرِّف البايتات الثلاث الأولى منها مُصنِّع العتاد الصلب
- تُعرِّف البايتات الثلاث المتبقية رقماً تسلسلياً وحيداً يقوم المُصنِّع بإسناده إلى الجهاز

ملاحظات:

- يمكن الحصول على الجدول الحالي لأرقام المُصنعِّين من الموقع:

http://www.iana.org/assignements/ethernet-numbers

- يكون عنوان Ethernet وحيد نظرياً على الأقل. فقد كانت شركة 3COM تكرر الأرقام بين البطاقات المنتمية إلى أنماط وصلات شبكية مختلفة. وقد كان الاعتقاد السائد يعتمد على أن الزبون سيقوم باستخدام نمط واحد من الوصلات وهو ما لم يحصل وخصوصاً في المواقع التي كانت تمر بمرحلة انتقال وتغيير لأنماط العتاد الصلب الشبكي مما سبب مشاكل عدة لشركة 3COM. طبعاً لا يمكن استخدام عناوين MAC متشابهة على نفس الشبكة الفيزيائية لكن لا شيئ يمنع من استخدامها على شبكات مفصولة بموجهات.

تتأثر عنونة المستوى الأدنى بنوعية العتاد الصلب الشبكي المُستخدم. فعلى سبيل المثال تمتلك أجهزة Ethernet عنوان مُرَمَّز على 6 بايت تضعه الجهة المُصنِعة. أما واجهات Token Ring فتمتلك عناوين مشابهة مُرمَّزة على 6 بايت أيضاً. بينما لا تحتاج بعض الشبكات العاملة بمبدأ الاتصال نقطة لنقطة (point to point networks) لعنونة العتاد الصلب إذ يتم تحديد هوية الواجهة عند إنشاء الاتصال.

ينقسم عنوان Ethernet مُرَمَّز على 6 بايت إلى قسمين: تعرِّف البايتات الثلاث الأولى منها مُصنِّع العتاد الصلب، بينما تُعرِّف البايتات الثلاث المتبقية رقماً تسلسلياً وحيداً يقوم المُصنِّع بإسناده إلى الجهاز. ويقوم مدير النظام بالتعرف على نوع الجهاز عبر التعرف على البايتات الثلاث المُعَرِّفة للمُصنِّع اعتباراً من جدول يحتوي على أرقام المُصنَعين.

جرت العادة على نشر المعلومات السابقة ضمن سلسلة وثائق RFC ولكن هذه العادة لم تعد دارجة وقد كانت الوثيقة RFC1700 لعام 1994 الوثيقة الأخيرة الخاصة بالأرقام المُسندة Assigned Numbers. وأضحى الموقع: www.iana.org/numbers.htm هو المكان الذي يمكن اعتباراً منه الحصول على هذه الأرقام.

من الضروري إسناد العناوين Ethernet الخاصة بالبنية الصلبة كعناوين دائمة وغير قابلة للتبديل. للأسف، تسمح بعض بطاقات الواجهات الشبكية للمستثمر بإسناد عناوين البنية الصلبة. وتعتبر البطاقات اللاسلكية الأكثر سماحية والأقل احتراماً للعناوين الدائمة. لذا من الضروري ألا يتم إسناد قيم من مجال العناوين متعددة الإسناد أو استخدام قيم خاصة.

العنونة IP

تُستخدم العنونة IP على المستوى الأعلى من مستوى البنية الصلبة، ويجري عادةً، إسناد عنوان IP مؤلف من 4 بايت (32 بت) لكل واجهة شبكية. وتكون العناوين IP العامة وحيدة ومستقلة عن البنية الصلبة للأجهزة.

يجري الربط بين العناوين IP وعناوين البنية الصلبة ضمن طبقة الربط في نموذج TCP/IP. ففي الشبكات التي تدعم عمليات البث (الشبكات التي تسمح للطرود بأن تكون موجهة إلى جميع المنصات على المقطع الشبكي)، يسمح البروتوكول ARP بالربط بين هذه العناوين عبر اكتشافها أوتوماتيكياً دون الحاجة لتدخل مدير النظام.

نظراً لطول العناوين IP ومحاكاتها لأرقام عشوائية، يصعب على الأشخاص تذكرها. تسمح أنظمة Linux أو أنظمة Windows لإسم محطة عمل أو لإسم عدة محطات أن ترتبط بعنوان IP بحيث يمكن للمستثمر أن يستخدم yahoo.com عوضاً عن 216.115.105.245. كما يمكن تثبيت عملية الربط السابقة بعدة طرق تتراوح بين الطريقة الثابتة والمعتمدة على استخدام الملف hosts وبين الطرق الديناميكية المعتمدة على DNS مروراً بقواعد المعطيات NIS. على كل حال علينا أن نتذكر دائماً أن الأسماء ليست إلا واجهات لعناوين IP. وسيجري الدخول في هذه التفاصيل في جلسات لاحقة.

ملاحظة:
يمكن للواجهات الشبكية حالياً أن تمتلك أكثر من عنوان IP ولكن يبقى هذا الأسلوب، أسلوب إعداد خاص يُستخدم في ظروف خاصة. يمكن الاطلاع على فقرة العناوين الافتراضية لمزيد من المعلومات.

التوجيه

يُعَّرف التوجيه على أنه إجراء تحديد اتجاه طرد عبر سلسلة الشبكات الموجودة بين مصدر الطرد ووجهته. إذ تشبه عملية التوجيه في نظام TCP/IP.

تأخذ معلومات التوجيه TCP/IP شكل قواعد ندعوها "**طرق**". ويمكن أن تحتوي معلومات التوجيه على "**طرق تلقائية**" تحدد ما يجب عمله بالطرود المتجهة إلى شبكة لا يمتلك الموجه من أجلها طرقاً واضحة محددة.

يجري تخزين معلومات التوجيه في جدول ضمن النواة. ويمتلك كل قيد من قيود الجدول عدة معاملات بما فيها قناع الشبكة الخاص بالشبكات الموجودة ضمن الجدول.

تُستَخدم كلمة "توجيه" للدلالة على معنيين مختلفين:

- البحث عن عنوان شبكة في جدول التوجيه لتحويل الطرد عبرها باتجاه وجهته
- بناء جدول التوجيه في المكان الأول

يمكن إعداد جداول توجيه على نحو ثابت أو ديناميكي أو باستخدامين الأسلوبين معاً:

- يجري إدخال الطريق الثابت باستخدام تعليمات خاصة، فهي وسيلة توجيه سهلة وموثوقة، إلا أنها تتطلب تدخلاً من مدير النظام ومعرفةً جيدة بتبولوجيا الشبكة التي يجب أن تبقى ثايتة مع الزمن
- ويصبح التوجيه الديناميكي ضرورياً في الشبكات الأكثر تعقيداً. ويتم تنفيذ التوجيه الديناميكي إعتماداً على إجراء تخديم يحفظ ويعدل جدول التوجيه آلياً

يُعَّرف التوجيه على أنه إجراء تحديد اتجاه طرد عبر سلسلة الشبكات الموجودة بين مصدر الطرد ووجهته. إذ تشبه عملية التوجيه في نظام TCP/IP، السؤال عن وجهة غير معروفة في بلد غريب. فقد يوجهك الشخص الأول الذي تسأله باتجاه المدينة الصحيحة وعندما تقترب بعض الشيئ من وجهتك، قد تسأل شخصاً ثانياً يمكن أن يكون قادراً على تحديد الشارع الذي تتجه إليه بدقة أكبر. وعندما تصبح قريباً بما فيه الكفاية فإن أحدهم يكون قادراً على تحديد البناء الذي تبحث عنه.

تأخذ معلومات التوجيه TCP/IP شكل قواعد ندعوها "**طرق**" إذ تكون صيغة طريق على الشكل التالي: *"للبحث عن الشبكة A، أرسل طرداً عبر الجهاز C"*. كما يمكن أن تحتوي معلومات التوجيه على "**طرق تلقائية**" تحدد ما يجب عمله بالطرود المتجهة إلى شبكة لا يمتلك الموجه من أجلها طرقاً واضحة محددة.

يجري تخزين معلومات التوجيه في جدول ضمن النواة. ويمتلك كل قيد من قيود الجدول عدة معاملات بما فيها قناع الشبكة الخاص بالشبكات الموجودة ضمن الجدول. لتوجيه طرد نحو عنوان محدد، تقوم النواة بالبحث عن أكثر الطرق توافقاً مع وجهة الطرد. وفي حال لم تجد النواة طريقاً معقولاً ولم يكن لديها طريق تلقائي، تقوم بارجاع رسالة تشير بأنها *"غير قادرة على الوصول إلى الشبكة (network unreachable)* إلى المُرسِل.

تُستَخدم كلمة "توجيه" للدلالة على معنيين مختلفين:

- البحث عن عنوان شبكة في جدول التوجيه لتحويل الطرد عبرها باتجاه وجهته
- بناء جدول التوجيه في المكان الأول

يمكن إعداد جداول توجيه على نحو ثابت أو ديناميكي أو باستخدامين الأسلوبين معاً:

- يجري إدخال الطريق الثابت باستخدام تعليمات خاصة. وتبقى الطرق الثابتة في جدول التوجيه ما دام النظام يعمل ويتم تحميلها عند الإقلاع اعتماداً على برامج الإقلاع النصّية. وتوفر الطرق الثابتة حلاً فعالاً للشبكات المحلية المستقرة. فهي وسيلة توجيه سهلة وموثوقة، إلا أنها تتطلب تدخلاً من مدير النظام ومعرفةً جيدة بتبولوجيا الشبكة التي يجب أن تبقى ثايتة مع الزمن
- ويصبح التوجيه الديناميكي ضرورياً في الشبكات الأكثر تعقيداً. ويتم تنفيذ التوجيه الديناميكي إعتماداً على إجراء تخديم يحفظ ويعدل جدول التوجيه. وتتخاطب خدمات التوجيه على المحطات المضيفة المختلفة مع بعضها البعض لاكتشاف التبولوجيا الشبكية ولتحديد كيفية الوصول إلى الوجهات البعيدة

على كل حال ستجري مناقشة مُفصلة لعملية التوجيه في جلسات لاحقو مخصصة لشرح هذه العملية.

بروتوكول حلّ العناوين ARP (Address Resolution Protocol)

يعمل بروتوكول حلّ العناوين على اكتشاف العناوين الصلبة المرتبطة بعنوان IP محدد.

يبث ARP حزمة على الشبكة لها شكل السؤال *"هل هناك من يعلم بعنوان البنية الصلبة الخاص بالعنوان 128.138.116.4؟"*. يتعرف المضيف الذي نبحث عنه على عنوانه ويرد *"نعم، هذا هو العنوان IP الذي أملكه وعنوان Ethernet المقابل هو العنوان 8:0:20:0:fb:6a"*.

يحتوي السؤال الأصلي على العنوان IP وعلى العنوان Ethernet الخاص بالطالب لذا يمكن للجهاز الذي نسأله أن يرد دون الحاجة لإرسال طلب ARP. بالنتيجة يتلقن كلا الجهازين الثنائيات ARP خلال عملية تبادل وحيدة للحزم.
يتم الإعتماد على عناوين البنية الصلبة لنقل المعطيات عبر طبقة الربط في الشبكة. يعمل بروتوكول حلّ العناوين على اكتشاف العناوين الصلبة المرتبطة بعنوان IP محدد. ويمكن استخدامه على أي نوع من أنواع الشبكات شريطة دعمها لعملية البث. إلا أنه أكثر استخداماً على شبكات Ethernet.

عندما يريد المضيف A إرسال حزمة إلى المضيف B على نفس شبكة Ethernet فإنه يستدعي ARP لاكتشاف عنوان البنية الصلبة الخاص بالمضيف B. فإذا لم يكن B على نفس الشبكة التي يتوضع عليها A، يستخدم A نظام التوجيه لتحديد الموجه التالي على الطريق إلى B ومن ثم يستخدم ARP لإيجاد عنوان البنية الصلبة الخاص بالموجه. إلا أن استخدام ARP للبث الذي لا يعبر الشبكات يجعل مجال استخدامه محدوداً في إيجاد العناوين الصلبة الخاصة بالتجهيزات المتصلة مباشرةً إلى شبكة المضيف.

يحتفظ كل جهاز بجدول –في ذاكرة خبيئة خاصة بالبروتوكول ARP– يحتوي على نتائج المناقلات ARP الأخيرة التي قام بها البروتوكول. غالباً ما يتم استكشاف معظم عناوين المضيفين عند الإقلاع لذا لا يسبب ARP حركة مرور كبيرة ضمن الشبكة.

يبث ARP حزمة على الشبكة لها شكل السؤال *"هل هناك من يعلم بعنوان البنية الصلبة الخاص بالعنوان 128.138.116.4؟"*. يتعرف المضيف الذي نبحث عنه على عنوانه ويرد *"نعم، هذا هو العنوان IP الذي أملكه وعنوان Ethernet المقابل هو العنوان 8:0:20:0:fb:6a"*.

يحتوي السؤال الأصلي على العنوان IP وعلى العنوان Ethernet الخاص بالطالب، لذا يمكن للجهاز الذي نسأله أن يرد دون الحاجة لإرسال طلب ARP. بالنتيجة يتلقن كلا الجهازين، الثنائيات ARP خلال عملية تبادل وحيدة للحزم. أما الأجهزة الأخرى التي تتلقى الطلب الأصلي فيمكنها أيضاً الاحتفاظ بالثنائية الآتية من الجهاز الطالب مما يخفف من عمليات التبادل. تتفحص إجرائيات ARP الذاكرة الخبيئة ARP وتتعامل معها.

بروتوكول حلّ العناوين المعكوس
(RARP – Reverse Address Resolution Protocol)

تحتاج عناوين البنية الصلبة في بعض الأحيان لترجمتها بالطريقة المعاكسة إلى عناوين IP. إذ يحتاج الكثير من العتاد الصلب "العاجز" (مثل محطات العمل غير المالكة لأقراص صلبة والحواسيب الشبكية والطابعات) إلى تنفيذ عملية الترجمة خلال مرحلة الإقلاع عوضاً عن امتلاكها لعنوانIP مثبت فيها ضمن ملف إعداد، يمكن للجهاز أن يطلب هذا العنوان من مخدم مركزي. يكمل البروتوكول RARP عمل البروتوكول ARP لتغطية العملية السابقة.

على عكس ARP، يحتاج RARP لمخدم مركزي موجود على كل شبكة. ولا يعتبر بروتوكول ذاتي الإعداد إذ يجب تحديد ارتباط واضح بين العناوين IP والعناوين Ethernet. ندعو المخدم الآنف الذكر – في معظم الشبكات الداعمة للبروتوكول RARP– rarpd

جرى استبدال RARP في معظم الشبكات بالبروتوكول Bootp أولاً ومن ثم بالبروتوكول DHCP الذي سندرسه في جلسات لاحقة بالتفصيل.

نشاط

استخدم التعليمة arp مع الخيارات المرفقة بها، للبحث عن محتويات الذاكرة الخبيئة التي يجري فيها تخزين الثنائية (العنوان IP، العنوان MAC). يُفضَل البحث عن الثنائيات بعد تنفيذ عدة عمليات ping على منصات مختلفة.

الجواب:

التعليمة اللازمة هي:

arp –a

توجيهات ICMP
(ICMP redirects)

لا يعتمد البروتوكول IP على نفسه عند إدارة معلومات التوجيه بل يُعرِّف طرود إدارة خاصة ندعوها ICMP. فعندما يحوِّل موجه طرد إلى موجه على نفس الشبكة التي أتى منها الطرد، فهذا يعني أن شيئاً ما غير صحيح قد حدث.

إذ يمكن لموجه أن يستنتج أن جدول التوجيه الخاص بالمرسِل غير كامل أو غير صحيح. في هذه الحالة، يمكن للموجه أن يُعلم المُرسِل بالمشكلة باستخدام طرود توجيهات ICMP. في الحقيقة تُعلِم هذه الطرود المُرسِل بما يلي: *"يجب عدم إرسال الطرود الذاهبة إلى المضيف xxx باتجاهي؛ ويجب إرسالها إلى الموجه yyy عوضاً عن ذلك".*

يسمح البروتوكول ICMP بإرسال التوجيهات إلى الموجهات أو إلى المحطات المضيفة أو إلى شبكة بكاملها.

عند استقبال توجيه، يقوم المُرسِل (الساذج) بتعديل جدول توجيهه بحيث تأخذ الطرود التي ستتجه مستقبلاً إلى الوجهة التي تناولتها طرود التوجيه – طريقاً مباشراً.

لا يحتوي السيناريو ICMP على أي عملية تحقق. فعندما يتلقى موجه طرد توجيهات يدَّعي أنه وارد من موجه آخر فإن الموجه المتلقي سيصدقه وسيبدأ بتحويل إرساله. فهل يجب الاستماع إلى جميع هذه الطرود؟
يجب الانتباه إلى أن التوجيهات تولد مشكلة أمن لذا يتم اهمالها في نظام Linux (لأسباب متعلقة بالأمان) ومن قبل موجهات CISCO (لأنها هي نفسها موجهات). فمن غير المنطقي أن يساهم موجه غير موثوق (لم نتحقق من هويته) بتعديل جدول توجيه موجه آخر.

توجيهات ICMP
(ICMP redirects)

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

نشاط

1. كيف يمكن تبعاً لتوجيهات ICMP السماح لمستثمر غير مرخصّ بالتأثير على الشبكة؟
2. ما تعريف وحدة النقل العظمى MTU الخاصة بوصلة شبكة؟ ماذا يحدث إذا كان وحدة النقل العظمى الخاصة بوصلة، كبيرة جداً؟ وماذا يحدث إذا كانت صغيرة جداً؟
3. اعرض **بالتسلسل وبالتفصيل** (يمكن رسم مخطط تفصيلي) لجميع الخطوات التي نحتاجها لإرسال حزمة معطيات من مضيف إلى آخر اعتباراً من تطبيق (مثل المتصفح) على المضيف الأول باتجاه تطبيق (مخدم الوب) على المضيف الثاني. بفرض أن الأول مُعرَّف بالثنائية (IP1,MAC1) والثاني مُعرَّف بالثنائية (IP2, MAC2).

عنوان الموضوع:

العنونة IP

الكلمات المفتاحية:

أنظر معجم المصطلحات المرافق.

ملخص:

نستعرض في هذا الموضوع، أساليب إسناد واستخدام العناوين IP بالإضافة إلى أنواع هذه العناوين. نستعرض أيضاً مفهوم التقسيم إلى شبكات فرعية ومفهوم قناع الشبكة الفرعي الضروري في عملية التقسيم.

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- أنماط العناوين IP
- العنونة ذات الصفوف
- العنونة دون صفوف
- التقسيم إلى شبكات فرعية
- حجز العناوين
- العناوين الخصوصية
- ترجمة العناوين

مقدمة

يُعرَّف عنوان IP برقم ذي ترميزٍ ثنائي بطول 32 بت. ويمكن تصنيف العناوين IP على نوعين: "**عناوين وحيدة الإسناد**" أو "**عناوين متعددة الإسناد**".

يُقَسَّم عنوان IP وحيد الإسناد إلى قسمين: قسم يشير إلى الشبكة التي ينتمي إليها وندعوه بـــ "**مُعرِّف الشبكة**"، وقسم يشير إلى المُضيف الذي يعنونه وندعوه "**مُعَرِّف المضيف**".

يُعرَّف عنوان IP برقم ذي ترميزٍ ثنائي بطول 32 بت. ويمكن تصنيف العناوين IP على نوعين: "**عناوين وحيدة الإسناد**" أو "**عناوين متعددة الإسناد**".

تُستخدم العناوين وحيدة الإسناد لعنونة منصات العمل والمُضيفين والموجهات وتعريف واجهاتها الشبكية، بينما تُستخدم العناوين متعددة الإسناد لتعريف وعنونة مجموعة من المُضيفين التي ترغب باستقبال نمط خاص من الإرسال IP.

يُقَسَّم عنوان IP وحيد الإسناد إلى قسمين: قسم يشير إلى الشبكة التي ينتمي إليها وندعوه بـــ "**مُعرِّف الشبكة**"، وقسم يشير إلى المُضيف الذي يعنونه وندعوه "**مُعَرِّف المضيف**". يُحدد "مُعَرِّفْ الشبكة" المقطع الشبكي الذي يتواجد به المُضيف أما "مُعَرِّف المُضيف" فيُحدد الواجهة الشبكية التي تربط المُضيف بالمقطع الشبكي. يُفترض أن يكون لجميع الواجهات الشبكية المتصلة بنفس المقطع الشبكي معرِّف واحد للشبكة. أما معرِّف المُضيف فيكون وحيداً وخاصاً بكل مُضيف على حدى.

تكمن إحدى مساوئ العناوين وحيدة الإسناد في كونها تعرِّف الواجهة الشبكية لمُضيف وليس المُضيف نفسه. ففي فعند امتلاك مُضيف لأكثر من واجهة شبكية، يجري إسناد عنوان IP لكل واجهة، بينما لا يمتلك المُضيف نفسه أي تعريف IP ظاهر له.

ترميز العنوان IP

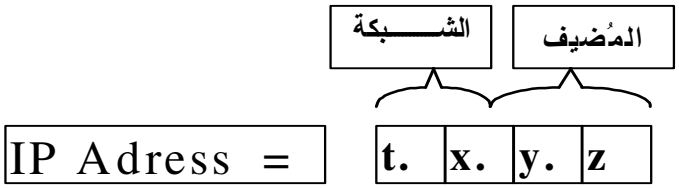
نظرياً، يجري ترميز العناوين IP ثنائياً بسلسلةً من 32 بت تحتوي كل منها على القيمة "0" أو "1".

يظهر العنوان المُمثل بالترميز الثنائي التالي:

00001010110000000011100000100101

على الشكل 10.192.56.37 في الترميز العشري.

يكون الرقم اليساري في العنوان هو الأكثر دلالة ويشكل دائماً جزءاً من مُعرِّف الشبكة.



عندما يكون الرقم الأول من عنوان IP مساوياً للقيمة 127، فإنه يشير عندها إلى "**شبكة راجعة**" ويشير العنوان 127.0.0.1 دائماً إلى المضيف نفسه ويدعى رمزياً "**المضيف المحلي**".

نظرياً، يجري ترميز العناوين IP ثنائياً بسلسلةً من 32 بت تحتوي كل منها على القيمة "0" أو "1". ونظراً لصعوبة قراءة هذا العبارة بشكلها الثنائي نتيجةً لطولها، فقد جرى اقتراح أسلوب ترميز أكثر وضوحاً يظهر فيه العنوان IP على شكل أربعة أرقام عشرية مفصولة بنقاط عن بعضها البعض بحيث يُمثل كل رقم منها 8 بت من العنوان IP.

يمثل الرقم الأول السلسلة الممتدة –من اليمين إلى اليسار– من البت رقم "0" حتى البت رقم "7"، بينما يمثل الرقم الثاني السلسلة الممتدة من البت رقم "8" إلى البت رقم "16" وهكذا دواليك. كمثال، يظهر العنوان المُمثل بالترميز الثنائي التالي: 00001010110000000011100000100101 على الشكل 10.192.56.37 في الترميز العشري. كما نكتب العنوان IP الخاص بواجهة شبكية ما على النحو التالي: 128.138.240.1، حيث يكون الرقم اليساري فيه هو الأكثر دلالة ويشكل دائماً جزءاً من عنوان الشبكة.

عندما يكون الرقم الأول من عنوان IP مساوياً للقيمة 127، فإنه يشير عندها إلى "**شبكة راجعة**" وهي عبارة عن شبكة تخيلية لا تمتلك أي عتاد صلب أو واجهات شبكية حقيقية. إذ يشير العنوان 127.0.0.1 دائماً إلى المضيف نفسه ويدعى رمزياً "**المضيف المحلي**".

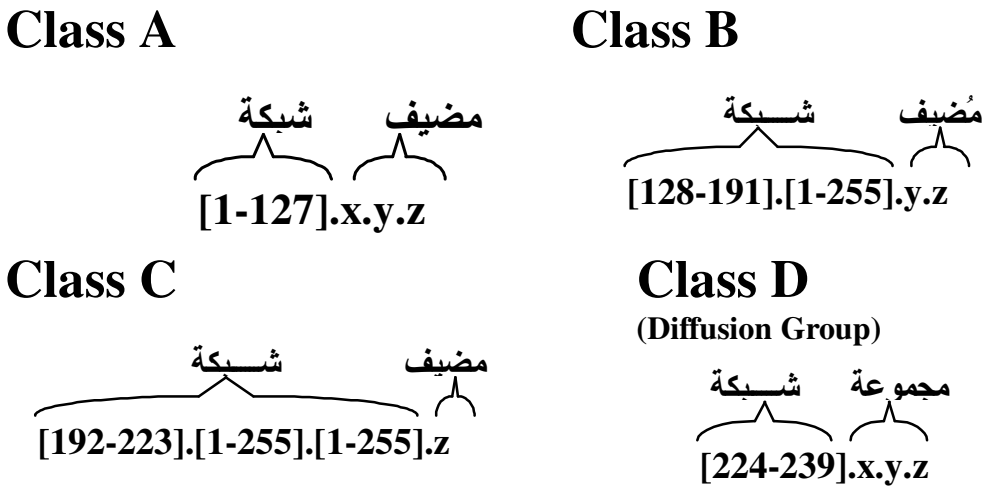
العنونة التقليدية ذات الصفوف

التقسيم إلى صفوف

يُقَسِّم أسلوب العنونة التقليدية فضاء العناوين إلى خمسة صفوف ندعوها صفوف الشبكة وهي: A، B، C، D، E.

تُعرِّف الصفوف A وB وC عناوين وحيدة الإسناد. أما الصف D فيُعرف عناوين متعددة الإسناد (أو "عناوين مجموعات" إذا صحَّ التعبير). ويُعرِّف الصف E مجموعة عناوين تجريبية.

يجري تحديد الصف اعتباراً من قيم البتات الأولى من العنوان IP.



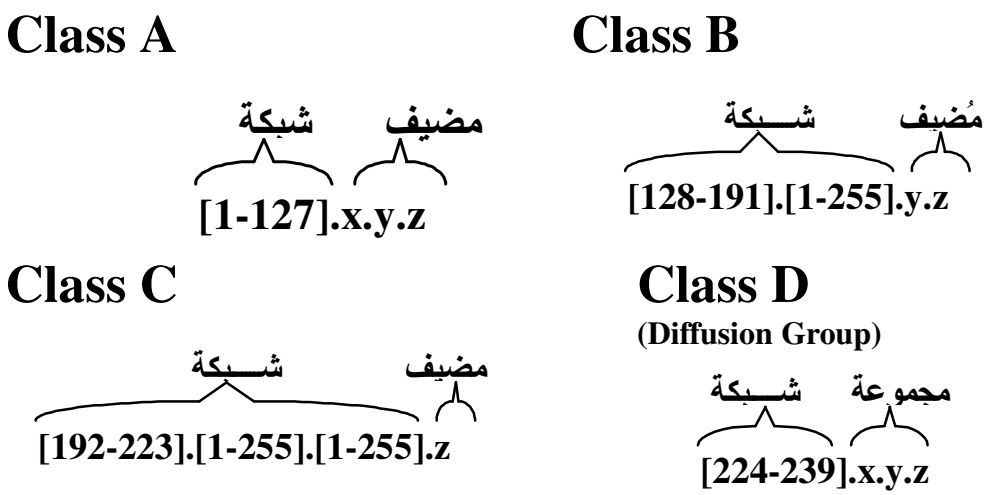
يُقَسِّم أسلوب العنونة التقليدية فضاء العناوين إلى خمسة صفوف ندعوها صفوف الشبكة وهي: A، B، C، D، E. يُعرِّف كل صف مجال عنونة خاص به لا يتقاطع مع مجالات العنونة التي تعرفها الصفوف الأخرى، بحيث ينتمي كل عنوان إلى صف واحد فقط لا غير.

تُعرِّف الصفوف A وB وC عناوين وحيدة الإسناد. ويتحدد انتماء العنوان إلى الصف، بأسلوب تشكيل العنوان من حيث عدد البتات التي تلعب دور معرِّف الشبكة وعدد البتات التي تلعب دور معرِّف المضيف. أما الصف D فيُعرف عناوين متعددة الإسناد (أو "عناوين مجموعات" إذا صحَّ التعبير). ويُعرِّف الصف E مجموعة عناوين تجريبية.

يجري تحديد الصف اعتباراً من قيم البتات الأولى من العنوان IP.

العنونة التقليدية ذات الصفوف

مجالات العنونة



الصف	البايت الأول	الصيغة	تعليق
A	1-126	N.H.H.H	شبكات محجوزة للـــDOD وتعتبـــر مـــن الشبكات الأولى
B	128-191	N.N.H.H.	مواقع واسعة مقسمة إلـــى شـــبكات فرعيـــة ويصعب الحصول عليها
C	192-233	N.N.N.H	متوفرة ويمكن الحصول عليها علـــى شـــكل مجموعات
D	224-239	–	عناوين متعددة الإسناد وغير مُسندة بشكل دائم
E	240-255	–	عناوين تجريبية

تهدف عملية توزيع العناوين ضمن الصفوف A وB وC إلى تعريف مجالات عنونة لشبكات حاوية على أعداد مختلفة من المُضيفين. إذ يدل عدد البتات المخصصة لمعرِّف المُضيف، في كل عنوان IP، على أكبر عدد من المُضيفين الذين يمكن أن يتواجدوا في مقطع الشبكة التي يُعرِفَها القسم الباقي من البتات والمخصص لمُعَرِّف الشبكة. وبما أن مجموعتي البتات، سواء تلك المخصصة لمعرِّف الشبكة، أو تلك المخصصة لمعرِّف المُضيف، تتقاسمان العنوان IP، يكون عدد الشبكات القادرة على تعريف عدد كبير من المنصات أقل من عدد الشبكات القادرة على تعريف عدد قليل منها.

لعنونة التقليدية ذات الصفوف

العناوين الخاصة

تخرج بعض العناوين التي تنتمي إلى مجالات العنونة السابقة، عن التصنيف الذي سبق ذكره، بحيث تُستَخدَم لأهدافٍ خاصة سنوضحها فيما يلي:

- يدل معِّرف الشبكة المؤلف بكامله من بتات مساوية للقيمة 0 فقط، على الشبكة الحالية التي يتواجد مضيف عليها
- يدل عنوان IP مؤلف بكامله من بتات مساوية للقيمة 0 فقط وله الترميز العشري 0.0.0.0 على المُضيف الحالي في الشبكة الحالية
- يدل العنوان IP المؤلف بكامله من بتات مساوية للقيمة 1 فقط وذو الترميز العشري 255.255.255 على "**عنوان بث محلي**"
- ندعو عنوان IP الحاو على مُعَرِّف مُضيف مؤلف بكامله من بتات مساوية للقيمة 1 فقط "**بعنوان البث ذي الوجهة**". مثال: العنوان 20.255.255.255
- ندعو عنوان IP حاوٍ على مُعِّرف مُضيف مؤلف بكامله من بتات مساوية للقيمة 0 فقط، "**بعنوان شبكة**". مثال: 20.0.0.0
- ندعو أي عنوان IP يكون البايت الأول فيه مساوي عشرياً للقيمة 127 "**بالعنوان الحلقي الراجع**" ويدل على المُضيف نفسه الذي يستخدمه

تخرج بعض العناوين التي تنتمي إلى مجالات العنونة السابقة، عن التصنيف الذي سبق ذكره، بحيث تُستَخدَم لأهدافٍ خاصة سنوضحها فيما يلي:

- يدل معِّرف الشبكة المؤلف بكامله من بتات مساوية للقيمة 0 فقط، على الشبكة الحالية التي يتواجد مضيف عليها. إذ يمكن استخدام عنوان IP حاوي على مُعرِّف شبكة مؤلف من أصفار، كعنوان IP لمصدر الإرسال فقط.
- يدل عنوان IP مؤلف بكامله من بتات مساوية للقيمة 0 فقط وله الترميز العشري 0.0.0.0 على المُضيف الحالي في الشبكة الحالية، ويمكن استخدامه كعنوان IP لمصدر الإرسال فقط. تستخدم هذه العناوين بالإضافة للعناوين التي لها مُعِّرف شبكة مؤلف من بتات مساوية للقيمة 0، في منصات العمل التي لا تملك معلومات عن الشبكة التي تنتمي إليها أوعن مُعرِّفاتها الخاصة مما يجعلها تستخدم هذه العناوين بشكل مؤقت للحصول على عناوينها النظامية الحقيقية.
- ندعو يدل العنوان IP المؤلف بكامله من بتات مساوية للقيمة 1 فقط وذو الترميز العشري 255.255.255 على "**عنوان بث محلي**". ويمكن استخدام هذا النمط من العناوين، كعناوين لمصدر الإرسال فقط بحيث تؤشر إلى جميع المضيفين الموجودين على مقطع شبكي.
- ندعو عنوان IP الحاو على مُعَرِّف مُضيف مؤلف بكامله من بتات مساوية للقيمة 1 فقط "**بعنوان البث ذي الوجهة**". يمكن استخدام هذا النمط من العناوين كعنوان وجهة إرسال فقط بحيث يشير إلى جميع المُضيفين الموجودين على الشبكة التي يحُددها مُعِّرف الشبكة الموجود في عنوان البث. يكون البث في هذه الحالة اتجاه هذه الشبكة. مثال: العنوان 20.255.255.255
- ندعو عنوان IP حاوٍ على مُعِّرف مُضيف مؤلف بكامله من بتات مساوية للقيمة 0 فقط، "**بعنوان شبكة**". يُستخدم عنوان الشبكة في الإشارة إلى مقطع شبكي. ولا يمكن استخدامه لا كعنوان مصدر إرسال ولا كعنوان وجهة إرسال. مثال: 20.0.0.0
- ندعو أي عنوان IP يكون البايت الأول فيه مساوي عشرياً للقيمة 127 "**بالعنوان الحلقي الراجع**" ويدل على المُضيف نفسه الذي يستخدمه. يُستعمل هذا العنوان داخلياً فقط ولا تحمله أية حزمة لا كعنوان مَصدَر إرسال ولا كعنوان وجهة إرسال فهو لا يُستَخدَم خارج المُضيف. يُستخدم هذا العنوان عادةً لأغراض التحقق من صحة وسلامة تطبيق شبكي في حال عدم وجود شبكة فعلية.

العنونة التقليدية ذات الصفوف

حجوم الشبكات

لنحسب عدد الشبكات وعدد المنصات التي تعرفها الصفوف A وB وC:

- يسمح الصف A بإنشاء (2 - 2^7) أو 127 عنوان شبكة يمكن لكل منها أن يسمح بتعريف (2 - 2^{24}) أو 16.777.214 مُضيف. ويشير الصف A إلى مجال عناوين الشبكات المحصورة 1.0.0.0 و126.0.0.0
- يسمح الصف B بإنشاء (2 - 2^{14}) أو 16383 عنوان شبكة يمكن لكل منها أن يسمح بتعريف (2 - 2^{16}) أو 65534 مُضيف. ويشير الصف B إلى مجال عناوين الشبكات المحصورة بين 128.0.0.0 و191.255.0.0
- يسمح الصف C بإنشاء (2 - 2^{21}) أو 2097151 عنوان شبكة يمكن لكل منها أن يسمح بتعريف (2 - 2^8) أو 254 مُضيف. ويشير الصف C إلى مجال عناوين الشبكات المحصورة بين 192.0.0.0 و223.255.255.0

عند النظر لأسلوب العنونة المعتمدة على تجزئة العناوين إلى صفوف، نلحظ أن الصف C هو الصف الوحيد الذي يُعرِّف عدداً معقولاً من المُضيفين (254 منصة). إذ تبدو أعداد المُضيفين التي يمكن تعريفها اعتباراً من شبكات تنتمي إلى إحدى الصفوف A وB غير منطقية وخاصةً عندما نتذكر أنه يفترض بهذه العناوين أن تعنون مقاطع شبكية.

العناوين متعددة الإسناد

تسهل عملية العنونة متعددة الاسناد عمل بعض التطبيقات الخاصة كتطبيقات المؤتمرات الفيديوية والتي تحتاج لإرسال نفس مجموعة الحزم إلى جميع المشتركين. وتساعد تطبيقات الصوت والصورة التي يزداد انتشارها في السوق على انتشار هذا النمط من العناوين.

تبدأ العناوين متعددة الإسناد ببايت أول تتراوح قيمته بين 224 و239 (قيمة الثمانية الأولى من البتات المتوزعة من اليمين إلى اليسار بين البت رقم 0 والبت رقم 7).

يدير البروتوكول IGMP (Internet Gatway Multicast Protocol) مجموعة المُضيفين التي تمتلك عناوين متعددة الإسناد، ويتعامل البروتوكول مع مجموعة المضيفين التي تمتلك نفس العنوان متعدد الإسناد، كمُضيف واحد يتجه إليه الإرسال.

التقسيم إلى شبكات فرعية

من النادر أن تمتلك شبكة واحدة أكثر من 100 حاسب متصل بها بآن واحد. بالنتيجة، يعتبر صفا العناوين A،B، صفان واسعان.

تستخدم المواقع التي لها مثل هذه العناوين أسلوباً في تشذيب حجم هذه الشبكات ندعوه "**التقسيم إلى شبكات فرعية**"،

يسمح تعريف الشبكات الفرعية بتقسيم القسم المخصص لمعرِّف المُضيف، في عنوان IP، إلى قسمين: الأول يدعى "**معرِّف الشبكة الفرعية**" والثاني يدعى "**معرِّف المُضيف**".

مثال:

يكون لعنوان من الصف B عادةً الشكل N.N.H.H، (حيث تشير N إلى رقم تابع لعنوان شبكة، وتشير H إلى رقم تابع لعنوان مُضيف)، لكن يمكن استخدام التقسيم إلى شبكات فرعية عبر استخدام البايت الثالث كجزء من عنوان الشبكة وليس كجزء من عنوان المضيف ويصبح العنوان من الشكل N.N.N.H. يساعد هذا التقسيم في تحويل عنوان الشبكة من الصف B إلى 256 عناوين لعدة شبكات من النمط C، حيث يمكن لكل عنوان من العناوين الشبكية الأخيرة أن يحمل 254 منصة.

من النادر أن تمتلك شبكة واحدة أكثر من 100 حاسب متصل بها بآن واحد. بالنتيجة، يعتبر صفا العناوين A،B، صفان واسعان (إذ يسمحان بما يعادل 16777214 و65534 مضيف لكل شبكة على الترتيب). فعلى سبيل المثال، تستهلك شبكات الصف A أكثر من نصف العناوين المتوفرة.

بالنتيجة، تستخدم المواقع التي لها مثل هذه العناوين أسلوباً في تشذيب حجم هذه الشبكات ندعوه "**التقسيم إلى شبكات فرعية**"، بحيث نستخدم فيه جزءاً من القسم المخصص لعنوان المضيف لتوسيع القسم الخاص بعنوان الشبكة. إذ يسمح تعريف الشبكات الفرعية بتقسيم القسم المخصص لمعرِّف المُضيف، في عنوان IP، إلى قسمين: الأول يدعى "**معرِّف الشبكة الفرعية**" والثاني يدعى "**معرِّف المُضيف**". يدل مُعرِّف الشبكة الفرعية على مقطع من الشبكة أما "معرِّف المُضيف" الجديد الناتج عن عملية التقسيم فهو يُعرِّف كالسابق، واجهة منصة عمل متصلة بالمقطع.

بالنتيجة، تعتبر عملية تعريف شبكات فرعية تعديلاً على مبدأ العنونة ذات الصفوف بهدف حل المشكلة الناجمة عن وجود عدد ثابت من عناوين المنصات في عنوان شبكة منتمٍ إلى إحدى الصفوف السابقة.

التقسيم إلى شبكات فرعية:
قناع الشبكة الفرعية

يجري تطبيق التقسيم إلى شبكات فرعية بتحديد "**قناع الشبكة الفرعية**" إضافةً للعنوان IP.

يُرمَّز قناع الشبكة الفرعية ثنائياً على 32 بت.

مثال:

يشير العنوان 10.15.3.154 المصحوب بقناع شبكة فرعية 255.255.255.0 إلى شبكة مُعَرَّفة بالعنوان 10 وإلى شبكة فرعية معرَّفة بالعنوان 15.3 وإلى مُضيف مُعَرَّف بالعنوان 154.

مثال:

	ترميز عشري	ترميز ثنائي
IP Address	200.20.16.5	1101000 00010100 00001000 00000101
Subnet Mask	255.255.255.0	1111111 11111111 11111111 00000000
Network	200.20.16.0	1101000 00010100 00001000 00000000

ملاحظة:

لا يشكل قناع الشبكة الفرعية جزءاً من العنوان IP فهو ليس إلا وسيلة إدارية يجري تطبيقها على العنوان IP بهدف تقسيمه إلى مُعَرِّف شبكة فرعية ومعرِّف مُضيف.

تعيد عملية تقسيم الشبكة إلى شبكات فرعية صياغة معنى ومفهوم "معرِّف الشبكة". إذ يشير معرِّف الشبكة هنا إلى مجموعة من الشبكات الواقعة تحت نفس السلطة الإدارية. ويجري تطبيق عملية التقسيم إلى شبكات فرعية بتحديد "**قناع الشبكة الفرعية**" إضافةً للعنوان IP.

يُرمَّز قناع الشبكة الفرعية ثنائياً على 32 بت بحيث يدل كل بت مُثبَتْ فيه (له القيمة "1") على أن البت المقابل له في العنوان IP ينتمي إلى معرِّف الشبكة الفرعية، بينما يدل كل بت ممسوح (له القيمة "0") على أن البت المقابل له في العنوان IP ينتمي إلى معرِّف المُضيف. يُستخدم الترميز الشعري المنقط أيضاً لتمثيل قناع الشبكة الفرعية.

تمارين

1. يتألف العنوان IP من قسمين، ..... و.....:
   i. قسم لتعريف الشبكة، وقسم لتعريف مُضيف
   ii. قسم لتعريف مُضيف، وقسم لتعريف عنوان MAC
   iii. قسم لتعريف شبكة، وقسم لتعريف شبكة فرعية
   iv. قسم لتعريف مُضيف، وقسم لتعريف شبكة فرعية

2. كم عدد بتات عنوان IP:
   i. 16 بت
   ii. 32 بت
   iii. 48 بت
   iv. 64 بت

3. في الصف B، ما هي أقسام العنوان التي يجري تحديدها محلياً كعنوان مُضيف (العدّ من اليسار إلى اليمين طبعاً):
   i. الأول
   ii. الرابع
   iii. الأول والثاني
   iv. الثالث والرابع

4. إلى أي صف ينتمي العنوان 172.16.10.10:
   i. A
   ii. B
   iii. C
   iv. D
   v. E

5. أي العبارات التالية الخاصة بعنوان بث محلي، صحيحة:
   i. يتألف من 32 بت تساوي كل منها 0
   ii. يتألف من 32 بت تساوي كل منها 1
   iii. يتألف مُعرِّف الشبكة من 16 بت تساوي كل منها 1
   iv. يتألف مُعرِّف المُضيف من 16 بت تساوي كل منها 1

6. أي من العناوين التالية تُعتبر عناوين ذات أهداف خاصة:
   i. 10.200.10.30
   ii. 172.16.20.20
   iii. 255.10.10.2
   iv. 0.10.10.3

7. ماهي نسبة العناوين IP من الصف A بالنسبة للعدد الكلي من العناوين IP:
   i. 25%
   ii. 50%
   iii. 12.5%
   iv. 75%

التقسيم إلى شبكات فرعية
صياغة قناع الشبكة الفرعية (1)

لا تتطلب طريقة تعريف قناع شبكة فرعية وضع البتات ذات القيمة 1 بشكل متجاور. فما مدى إمكانية استخدام مثل هذا القناع عملياً؟

يساعد وجود قناع شبكة –تكون فيه البتات ذات القيمة 1 والبتات ذات القيمة 0 متجاورة– في تقسيم العنوان وبشكلٍ واضح إلى معرِّف للشبكة ومعرِّف للشبكة الفرعية ومعرِّف للمُضيف. بينما يجري تقسيم العنوان، باستخدام القناع الذي تتناوب فيه البتات ذات القيمة 0 والبتات ذات القيمة 1 إلى معرِّف شبكة ومعرِّفيّ شبكة فرعية غير متجاورين ومعرِّفيّ مُضيف غير متجاورين.

مثال:

في حال إسناد العنوان 10.192.3.63 إلى واجهة أحد المُضيفين مع قناع شبكة فرعية بقيمة 255.240.255.192 يكون عنوان المُضيف التالي الذي يمكن استخدامه هو العنوان 10.193.3.0 وهو عنوان غير مناسب لمُضيف حسب قواعد التعريف.

لا تتطلب طريقة تعريف قناع شبكة فرعية وضع البتات ذات القيمة 1 بشكل متجاور. إذ يمكننا نظرياً تعريف قناع شبكة فرعية يتناوب فيه ظهور البتات ذات القيمة 0 والبتات ذات القيمة 1 كالقناع 255.240.255.0 لكن السؤال الذي يطرح نفسه هو: ما مدى إمكانية استخدام مثل هذا القناع عملياً؟

يساعد وجود قناع شبكة –تكون فيه البتات ذات القيمة 1 والبتات ذات القيمة 0 متجاورة– في تقسيم العنوان وبشكلٍ واضح إلى معرِّف للشبكة ومعرِّف للشبكة الفرعية ومعرِّف للمُضيف. بينما يجري تقسيم العنوان، باستخدام القناع الذي تتناوب فيه البتات ذات القيمة 0 والبتات ذات القيمة 1 إلى معرِّف شبكة ومعرِّفيّ شبكة فرعية غير متجاورين ومعرِّفيّ مُضيف غير متجاورين.

التقسيم إلى شبكات فرعية
صياغة قناع الشبكة الفرعية (2)

من البديهي أن نلاحظ مدى صعوبة واستحالة إدارة الشبكة باستخدام الأقنعة التي ندعوها بالأقنعة "**ذات القيم المتناوبة**" (تتناوب فيها القيم "0" و"1") مقارنة بالأقنعة "**ذات القيم المستمرة**". إذ يؤدي هذا الاستخدام إلى تعقيد عملية توزيع العناوين بالإضافة إلى تعقيد عملية التوجيه.

لذا يجري استخدام أقنعة ندعوها "**بأقنعة تلقائية**" عندما لا يتم تحديد أقنعة شبكة فرعية بشكل مباشر. ترتبط هذه الأقنعة التلقائية بصفوف الشبكة. فلجميع عناوين الصف A القناع التلقائي 255.0.0.0 ولجميع عناوين الصف B القناع التلقائي 255.255.0.0 ولجميع عناوين الصف C القناع التلقائي 255.255.255.0. إلا أن استخدام الأقنعة التلقائية لا يؤدي للتعدي على البتات المخصصة لعناوين المُضيفين، إذ تحافظ الأقنعة التلقائية على التوزيع الأصلي للعناوين في صفوف وبالشكل الأساسي المؤلف من مُعَرِّف الشبكة ومُعَرِّف المُضيف.

التقسيم إلى شبكات فرعية

صياغة قناع الشبكة الفرعية (3)

يجري التعبير عن الأقنعة التي لا تنتهي عند حدود انتهاء بايت (ضمن عنوان IP) بالشكل XX/ حيث يشير XX إلى عدد البتات المكونة للقسم الخاص بالشبكة من العنوان. وندعو هذا القسم في بعض الأحيان CIDR (classless Inter-Domain Routing).

مثال:

يشير عنوان الشبكة 128.138.243.0/26 إلى الشبكة الأولى من الشبكات الأربع التي يكون القسم الخاص بالشبكة من عنوانها هو 128.138.243، أما الشبكات الثلاث المتبقية فتمثلك عناوين هي 128.138.243.64 و128.138.243.128 و128.138.243.192.

يكون قناع الشبكات الفرعية المرتبط بهذه الشبكات هو 255.255.255.192؛ ويُمثل ثنائياً بسلسة من ستة وعشرين بتاً لكلٍ منها القيمة 1 متبوعة بستة بتات لكل منها القيمة، 0. يوضح الجدول التالي العلاقة بين هذه الأعداد بالتفصيل.

عنوان الشبكة	**0**	**243.**	**138.**	**128.**
القناع بالصيغة العشرية	**192**	**255.**	**255.**	**255.**
القناع بالصيغة الثنائية	**1100 0000**	**11111111**	**11111111**	**11111111**

يكون للشبكة 26/، ستة بتات (6=26-32) لترقيم المحطات المضيفة. وبما أن $64=2^6$، يكون لهذه الشبكة 64 عنوان ممكن لعنونة المحطات المضيفة. على كل حال، يمكن استخدام 62 عنوان فقط لأن العناوين المؤلفة من سلسلة من البتات 0 أو سلسلة من البتات 1 تكون محجوزة (تشير إلى عنوان الشبكة وعنوان البث على الترتيب).

حساب الشبكات الفرعية (1)

من الصعب تنفيذ هذه العمليات ذهنياً لذا يمكننا استخدام بعض الطرائق البسيطة لتنفيذ هذه الحسابات ولنأخذ الشبكة 128.138.234.0/26 كمثال:

1. نستنتج من 26/ أن هناك 6 بتات متوفرة لعنونة المضيفين:

$$Number\_of\_bits = 32-26=6 \text{ bits}$$

2. يكون حجم الشبكة (Network Size) النظري (عدد المضيفين) يساوي 64

$$Network\_Size = 2^{Number\_of\_bits} = 2^6 = 64$$

3. يساوي البايت الأخير من قناع الشبكة الفرعية، 256 ناقص حجم الشبكة:

$$Last\_Octet = 256 - Network\ Size = 256-64=192$$

4. بالنتيجة يكون قناع الشبكة الفرعية هو: 255.255.255.192، ويكون له الشكل:

عنوان الشبكة	**0**	**243.**	**138.**	**128.**
القناع بالـــصيغة العشرية	**192**	**255.**	**255.**	**255.**
القناع بالـــصيغة الثنائية	**1100 0000**	**11111111**	**11111111**	**11111111**

5. نستنتج مما سبق، أن لدينا بتان، وهما البتان الملونان في الجدول، يشيران إلى عدة شبكات فرعية (عدد البتان هو 2 وبالتالي يمكن أن يمثلا 4 شبكات فرعية). يأخذ هذان البتان الإضافيان اللذان قمنا بإدخالهما إلى عنوان الشبكة القـيم 00 و01 و10 و11 مما يؤدي لتقسيم الشبكة 128.138.234.0/26 إلى 4 شبكات 26/ وهي:
   - **128.138.243.0/26 (128.138.243.00000000)**
   - **128.138.243.64/26 (128.138.243.01000000)**
   - **128.138.243.128/26 (128.138.243.10000000)**
   - **128.138.243.192/26 (128.138.243.11000000)**

6. يكون البتان المكتوبان بالخط الملون منتميان إلى القسم الخاص بالشبكة.

حساب الشبكات الفرعية (2)

لا تسمح وثيقة RFC التي تتناول التقسيم إلى شبكات فرعية (RFC950) باستخدام الشبكة الفرعية الأولى أو الأخير (المؤلفـــة مـــن سلسلة بتات مساوية للصفر أو الواحد).

يمكننا اعتبار وثيقة RFC خاطئة، بالرغم من نواياها الحسنة. وقد نجم المنع الحاصل على الشبكات الفرعية 0 من اعتقاد المصممين أن هذه الشبكات ستؤدي للخلط بين عنوان شبكة فرعية وعنوان شبكة عادية غير مقسمة.

بالنتيجة، يجري حجز عنوانين من عناوين المضيفين في كل شبكة فرعية:

1. عنوان الشبكة؛
2. عنوان البث.

ويكون عدد المضيفين مساوياً لحجم الشبكة الفرعية النظري ناقصاً 2.

مثال:

اعتماداً على مثالنا السابق يكون لدينا عناوين البث عناوين الشبكات التالية:

عنوان الشبكة الفرعية	عنوان الشبكة	عنوان البث
128.138.243.0/26	**128.138.243.0**	**128.138.243.63**
128.138.243.64/26	**128.138.243.64**	**128.138.243.127**
128.138.243.128/26	**128.138.243.128**	**128.138.243.191**
128.138.243.192/26	**128.138.243.192**	**128.138.243.255**

لا تسمح وثيقة RFC التي تتناول التقسيم إلى شبكات فرعية (RFC950) باستخدام الشبكة الفرعية الأولى أو الأخير (المؤلفة من سلسلة بتات مساوية للصفر أو الواحد). ففي مثالنا يجري وفقاً للقاعدة السابقة حذف نصف الشبكات الفرعية وهي: الشبكة الفرعية 0 والشبكة الفرعية 192.

يمكننا اعتبار وثيقة RFC خاطئة، بالرغم من نواياها الحسنة. وقد نجم المنع الحاصل على الشبكات الفرعية 0 من اعتقاد المصممين أن هذه الشبكات ستؤدي للخلط بين عنوان شبكة فرعية وعنوان شبكة عادية غير مقسمة، لكن الواقع أثبت عدم صحة هذا الإعتقاد والدليل على ذلك هو استخدام الشبكات الفرعية المؤلفة من سلاسل من البتات مساوية للقيمة 1 أو سلاسل من البتات مساوية للقيمة 0. وثبت أنه من الضروري تطبيق القاعدة السابقة على القسم الخاص بعنوان المنصة فقط).

بالنتيجة، يجري حجز عنوانين من عناوين المضيفين في كل شبكة فرعية:

3. الأول ندعوه عنوان الشبكة وهو العنوان الناجم عن اسناد 0 إلى جميع البتات المخصصة للمضيف؛
4. والثاني ندعوه عنوان البث وهو العنوان الناجم عن اسناد 0 إلى جميع البتات المخصصة للمضيف.

لذا يكون عدد المضيفين مساوياً لحجم الشبكة الفرعية النظري ناقصاً 2. وتكون أصغر شبكة فرعية ممكنة هي تلك التي تحتوي على أربعة منصات مضيفة: اثنتان حقيقيتان بالإضافة إلى عنوان الشبكة وعنوان البث.

تمارين

8. ما هو الهدف من استخدام قناع شبكة فرعية:
   i. تحديد جزء العنوان IP المخصص للشبكة، وجزء العنوان IP المخصص للمُضيف
   ii. للتفريق بين الشبكات الخارجية واللشبكات الداخلية
   iii. لتحديد عدد الشبكات الفرعية التي يمكن توليدها
   iv. لتحديد عدد المُضيفين ضمن شبكة فرعية

9. حدد العدد الأصغر من البتات التي يمكن تخصيصها عملياً لتوليد شبكات فرعية اعتباراً من شبكة ما:
   i. 1 بت
   ii. 2 بت
   iii. 3 بت
   iv. 4 بت

10. حدد عدد المُضيفين التي يمكن لشبكة من الصف C عنونته:
   i. 253
   ii. 254
   iii. 255
   iv. 256

11. حدد العدد الأكبر من البتات التي يمكن تخصيصها عملياً لتوليد شبكات فرعية اعتباراً من شبكة من الصف C:

i. 2
ii. 6
iii. 4
iv. 8

12. حدد عدد العناوين التي يوفرها العنوان IP التالي 206.15.8.0/20:

i. 4094
ii. 4088
iii. 4098
iv. 4096

13. إذا كان من الضروري حجز 4 بت لتوليد قناع شبكة فرعية من أجل عنوان من الصف B، فما هو القناع الذي ستولده:

i. 255.255.240.0
ii. 255.255.224.0
iii. 255.255.0.0
iv. 255.255.255.64

14. حدد عدد الشبكات الفرعية التي يمكن توليدها عند حجز 6 بتات لذلك:

i. 32
ii. 64
iii. 48
iv. 128

نشاط

نريد دراسة عدة حالات تقسيم إلى شبكات فرعية' والمطلوب، أنشئ من أجل كل شبكة من الشبكات التالية:

1- X.Y.Z.T/26
2- X.Y.Z.T/27
3- X.Y.Z.T/28
4- X.Y.Z.T/33
5- X.Y.Z.T/34

الجدول التالي:

الشبكة الفرعية	عدد المضيفين	عنوان الشبكة	عنوان البث	عنوان المُضيف الأول	عنوان المُضيف الأخير

بحيث تحدد:

1- الشبكات الفرعية

2- من أجل كل شبكة فرعية ناتجة، عنوان البث وعنوان الشبكة الخاصة بها

3- من أجل كل شبكة فرعية ناتجة، عنوان المُضيف الأول في الشبكة الفرعية، وعنوان المُضيف الأخير بالترتيب

توجيه: يجب أن يكون عدد الشبكات الفرعية في كل حالة كمايلي:

1- X.Y.Z.T/26 عدد الشبكات الفرعية: 4

2- X.Y.Z.T/27 عدد الشبكات الفرعية: 8

3- X.Y.Z.T/28 عدد الشبكات الفرعية: 16

4- X.Y.Z.T/33 عدد الشبكات الفرعية: 32

5- X.Y.Z.T/34 عدد الشبكات الفرعية: 64

العنونة دون صفوف أو العنونة CIDR

أدت عمليات التطوير المتتالية التي أُدخلت على أسلوب تصميم العنونة IP إلى الوصول إلى شكل للعناوين ندعوه بـــ "**العناوين IP دون صفوف**".

يمكن لأي عنوان IP أن يُقسم عشوائياً إلى "**بادئة الشبكة**" (network prefix) (أو "بادئة شبكة") وإلى "**مُعَرِّف مُضيف**".

تتألف كلا القيمتين من سلسلة مترابطة من البتات لا انفصال بينها وتسبق بادئة الشبكة في ترتيب القراءة القسم المدعو مُعَرِّف المُضيف.

تُعطى إحدى أكثر التمثيلات شيوعاً للبادئة المُعَرِّفة للشبكة على الشكل: 10.10.0.0/16 حيث يحدد الرقم الموجود بعد الخط الفاصل طول البادئة المُعرَّفة للشبكة بالبتات، وهو يحدد بالتالي عدد المضيفين الذي تسمح به الشبكة.

العلاقة بين طول البادئة المُعرِّفة للشبكة وعدد المُضيفين التي تسمح بها.

عدد المُضيفين	طول البادئة	قناع الشبكة الفرعية الموافق
1	/32	255.255.255.255
أكثر من 2	/30	255.255.255.252
أكثر من 6	/29	255.255.255.248
أكثر من 14	/28	255.255.255.240
أكثر من 30	/27	255.255.255.224
أكثر من 62	/26	255.255.255.192
أكثر من 126	/25	255.255.255.128
أكثر من 254	/24	255.255.255.0
أكثر من 510	/23	255.255.254.0
أكثر من 1022	/22	255.255.252.0
أكثر من 2046	/21	255.255.248.0

ملاحظة:

جرى اشتقاق أسلوب تعريف القيم السابقة اعتباراً من عناوين الشبكات المصحوبة بأقنعة شبكات فرعية ذات بتات متتالية لها القيمة 1. إذ يجري إعطاء طول سلسلة البتات عوضاً عن إعطاء القناع بشكلٍ يحدد طول البادئة المعرِّفة للشبكة مما يشير إلى علاقة الأقنعة بطول البادئة المعرِّفة للشبكة. وغالباً ما تُعرَّف هذه القيم بالأسلوب القديم بتحديد عنوان IP تكون فيه قيمة البتات المخصصة لمعرِّف المنصة مساوية للصفر، متبوعاً بقناع شبكة فرعية. فالمثال المعطى فيما سبق يُكتب بالأسلوب القديم على الشكل التالي: 10.10.0.0 255.255.0.0.

أدت عمليات التطوير المتتالية التي أُدخلت على أسلوب تصميم العنونة IP إلى الوصول إلى شكل للعناوين ندعوه بـــ "**العناوين IP دون صفوف**".

يضع هذا الأسلوب في العنونة، حداً لاستخدام صفوف العناوين A وB وC، بحيث لا يبقى للشكل الذي تأخذه البتات الأولى من العنوان أي تأثير في التعريف المُسبق لمعرِّف الشبكة ومعرِّف المُضيف. إذ يمكن لأي عنوان IP أن يُقسم عشوائياً إلى "**بادئة الشبكة**" (network prefix) (أو "بادئة شبكة") وإلى "**مُعَرِّف مُضيف**".

تتألف كلا القيمتين من سلسلة مترابطة من البتات لا انفصال بينها وتسبق بادئة الشبكة في ترتيب القراءة القسم المدعو مُعَرِّف المُضيف. تكتمل عملية تقسيم العنوان إلى بادئة شبكة وإلى معرِّف مُضيف بتحديد طول البادئة المُعرِّفة للشبكة.

تُعرِّف هذه البادئة، كما هو حال معرِّف الشبكة أو معرِّف الشبكة الفرعية، مقطعاً من الشبكة. أما معرِّف المُضيف فيُعرِّف واجهة شبكية تعمل على وصل مُضيف إلى المقطع. ويكون لكل واجهة شبكية متصلة بالمقطع مُعرِّف مُضيف وحيد بينما يكون لجميع الواجهات المتصلة بالمقطع نفس البادئة المُعَرِّفة للشبكة. وتُعطى إحدى أكثر التمثيلات شيوعاً للبادئة المُعَرِّفة للشبكة على الشكل: 10.10.0.0/16 حيث يحدد الرقم الموجود بعد الخط الفاصل طول البادئة المُعرَّفة للشبكة بالبتات، وهو يحدد بالتالي عدد المضيفين الذ تسمح به الشبكة.

ملاحظة:

جرى اشتقاق أسلوب تعريف القيم السابقة اعتباراً من عناوين الشبكات المصحوبة بأقنعة شبكات فرعية ذات بتات متتالية لها القيمة 1. إذ يجري إعطاء طول سلسلة البتات عوضاً عن إعطاء القناع بشكلٍ يحدد طول البادئة المعرِّفة للشبكة مما يشير إلى علاقة الأقنعة بطول البادئة المعرِّفة للشبكة. وغالباً ما تُعرَّف هذه القيم بالأسلوب القديم بتحديد عنوان IP تكون فيه قيمة البتات المخصصة لمعرِّف المنصة مساوية للصفر، متبوعاً بقناع شبكة فرعية. فالمثال المعطى فيما سبق يُكتب بالأسلوب القديم على الشكل التالي: 10.10.0.0 255.255.0.0.

العناوين IP الخصوصية

يمتاز كل عنوان IP مُستخدَم وظاهر على الإنترنت بأنه عنوان وحيد.

تأخذ المواقع عناوينها، اعتماداً على نظام العنونة CIDR، من مزودي الخدمة. فإذا رغب أحد المواقع بتغيير مزود الخدمة كلفه ذلك تغيير وإعادة عنونة شبكته.

يمكن استخدام العناوين الداخلية الخاصة التي لا علاقة لها بمزود الخدمة ومن ثم تنفيذ عملية ترجمة اعتماداً على الموجه للخروج إلى الإنترنت.

توضح الوثيقة RFC1918 شبكة من الصف A و16 شبكة من الصف B و256 شبكة من الصف B يمكن استخدامها لعنونة الشبكات داخلياً.

يوضح الجدول العناوين الشبكية المحجوزة كعناوين خاصة. يمكن للمواقع أن تختار من مجموعة العناوين الآنفة الذكر تلك التي يتناسب حجمها مع تنظيمها.

العنوان IP	من	إلى	المجال CIDR
الصف A	10.0.0.0	10.255.255.255	10.0.0.0/8
الصف B	172.16.0.0	172.31.255.255	172.16.0.0/12
الصف C	192.168.0.0	192.168.255.255	192.168.0.0/16

يمتاز كل عنوان IP مُستخدَم وظاهر على الإنترنت بأنه عنوان وحيد. ويجري الحصول عليه من جهة رسمية تَضمن عدم وجود عناوين مكررة على هذه الشبكة' فتكرار عنوان، في حال حدوثه، يجعل من بعض منصات العمل معزولةً وهو ما يتنافى مع مبدأ الانفتاح على الجميع الذي قامت عليه الإنترنت.

تأخذ المواقع عناوينها، اعتماداً على نظام العنونة CIDR، من مزودي الخدمة. فإذا رغب أحد المواقع بتغيير مزود الخدمة كلفه ذلك تغيير وإعادة عنونة شبكته، إذ يوفر مزود الخدمة للشبكة عناوين طالما كانت هذه الشبكة زبوناً من زبائنه، أما في حال أراد المسؤولون عن الموقع الاعتماد على مزود خدمة آخر، فمن الصعب إقناع مزود الخدمة القديم بتوجيه الطرود الواردة إلى عناوين الزبون باتجاه مزود الخدمة الجديد واعتبار العناوين السابقة كعناوين خاصة بمزود الخدمة الجديد. لذا يتوجب عادةً إعادة ترقيم الشبكات من جديد.

عموماً، يكمن الحلّ لهذه المشكلة في استخدام العناوين الداخلية الخاصة التي لا علاقة لها بمزود الخدمة ومن ثم تنفيذ عملية ترجمة اعتماداً على الموجه للخروج إلى الإنترنت. توضح الوثيقة RFC1918 شبكة من الصف A و16 شبكة من الصف B و256 شبكة من الصف B يمكن استخدامها لعنونة الشبكات داخلياً. حيث لا يمكن لطرد خارج من منصة تعمل بعنوان من العناوين الخاصة السابقة، الخروج إلى الإنترنت إذ تتم عملية ترشيح الطرود على الموجه الحدودي للتأكد من عدم خروجهم.

يوضح الجدول العناوين الشبكية المحجوزة كعناوين خاصة. يمكن للمواقع أن تختار من مجموعة العناوين الآنفة الذكر تلك التي يتناسب حجمها مع تنظيمها.

ترجمة العناوين الشبكية

تستخدم الموجهات الحدودية نظام ترجمة العناوين NAT.

يمكن للموجهات الحدودية أيضاً أن تحتفظ بجداول لمقابلة العناوين الداخلية الخاصة بعناوين خارجية حقيقية والبوابات الداخلية ببوابات خارجية

في حال اختار المسؤولون عن موقع تغيير مزود الخدمة سيحتاجون لتغيير إعدادات الموجه الحدودي وإعدادات NAT عليه، أما إعدادات المحطات المضيفة فتبقى على حالها.

تقدم عدة شركات منتجة للموجهات، بما فيها CISCO، نظام NAT على موجهاتها.

كما يمكن أن نستخدم أنظمةWindows Server و Linux لتنفيذ NAT.

يسمح NAT بإخفاء البنية الداخلية ويظهر كأنه ميزة أمان.

تستخدم الموجهات الحدودية نظام ترجمة العناوين NAT (Network Address Translation) لتمكين المنصات المضيفة، التي تستخدم عناوين خاصة، من الاتصال بالإنترنت.
يتلقى نظام NAT الحزم المعنونة بهذه العناوين الداخلية الخاصة ويقوم بتعديل عنوان المصدر في هذه الحزم ووضع عناوين حقيقية، كما يمكن لها أن تقوم بتعديل رقم البوابة في بعض الأحيان.
يمكن لهذه الموجهات أيضاً أن تحتفظ بجداول لمقابلة العناوين الداخلية الخاصة بعناوين خارجية حقيقية والبوابات الداخلية ببوابات خارجية. تساعد هذه الجداول في عملية الترجمة وخصوصاً عند ورود إجابات من الشبكات الخارجية والحاجة لتحويل هذه الإجابات إلى المحطات المضيفة الداخلية.
يستخدم NAT عملية مقابلة لأرقام البوابات تسمح بإقامة حوار بين الشبكات الخارجية والشبكة الداخلية عبر عنوان IP خارجي وحيد ومشترك بين المحطات المضيفة الداخلية. ففي بعض الأحيان يكون للموقع بكامله عنوان خارجي وحيد.
يحتاج الموقع الذي يستخدم عناوين خاصة داخلية لمزود خدمة يوفر له فضاء عنونة يستخدمه في معاملاته الخارجية. إلا أن الموقع يستخدم معظم العناوين التي يحصل عليها من مزود الخدمة في عملية الترجمة حيث يقابلها بعناوين داخلية يجري إسنادها إلى المحطات المضيفة. وفي حال اختار المسؤولون عن الموقع تغيير مزود الخدمة فسيحتاجون لتغيير إعدادات الموجه الحدودي وإعدادات NAT عليه، أما إعدادات المحطات المضيفة فتبقى على حالها.
تقدم عدة شركات منتجة للموجهات، بما فيها CISCO، نظام NAT على موجهاتها. كما يمكن أن نستخدم أنظمة Windows Server و Linux لتنفيذ NAT بالرغم من أن عدداً كبيراً من المواقع تفضل توكيل هذه المهمة لموجهاتها أو للأجهزة التي تصلها بالإنترنت.
يسمح NAT بإخفاء البنية الداخلية ويظهر كأنه ميزة أمان إضافية ولكن المهتمون بمسألة الأمن يعتبرون أن NAT لا يساعد فعلياً في زيادة الأمن ولا يُغني عن استخدام جدران النار. كما لا يسمح بالقياس الفعلي لحجم الشبكة الإنترنت.

1أزمة العناوين IP

توصل جمهور الإنترنت في عام 1992 إلى تحديد ثلاث مشاكل خاصة بالنموذج الأصلي لحجز العناوين:

1. استنفاذ عناوين الصفوف؛
2. تحول جداول التوجيه وهي الأدوات المفصلية على الأنترنت، إلى جداول ضخمة لا يمكن لذواكر الموجهات أن تستوعبها.
3. حجز العناوين IP وفقاً لمبدأ "تخديم الذي يصل أولاً" دون أي مرجعية .

لحلّ هذه المشكلة، جرى اقتراح الحلين التاليين معاً:

- الأول، ويُعتبر حل ضمن المدى المنظور آنذاك، وكان في تبنّي التوجيه البيني المعتمد على العنونة (CIDR-Classless Inter-Domain Routing)
- الثاني، ويُعتبر حلّ بعيد المدى، وكان في تبني IPV6

توصل جمهور الإنترنت في عام 1992 إلى تحديد ثلاث مشاكل خاصة بالنموذج الأصلي لحجز العناوين:

4. استنفاذ عناوين الصفوف وخصوصاً الصف B– وهي العناوين المرغوبة من قبل المنظمات والهيئات الكبيرة – في منتصف عام 1995؛
5. تحول جداول التوجيه وهي الأدوات المفصلية على الأنترنت، إلى جداول ضخمة لا يمكن لذواكر الموجهات أن تستوعبها.
6. حجز العناوين IP وفقاً لمبدأ "تخديم الذي يصل أولاً" دون أي مرجعية جغرافية مما يعني أن هناك عناوين متسلسلة ستكون تابعة لهيئة أو شركة متوضعة في عدة قارات وستتوزع على هذه القارات. طبعاً، يمكننا أن نتخيل الغموض الذي سيحصل في حال لم يكن لدينا رموز للنداء الآلي الخاصة بكل من بلدان العالم وكان توزيع الأرقام الهاتفية عشوائياً.

لحلّ هذه المشكلة، جرى اقتراح الحلين التاليين معاً:

- الأول، ويُعتبر حل ضمن المدى المنظور آنذاك، وكان في تبنّي التوجيه البيني المعتمد على العنونة (CIDR-Classless Inter-Domain Routing). إذ يوفر هذا الحلّ أسلوباً مختلفاً لإدارة العناوين IP المؤلفة من 4 بايت، ويستخدم العناوين على نحو أكثر فعالية بحيث يسمح بتبسيط جداول التوجيه عبر استخدام أسلوب عدّ البتات المتجاورة والاحتفاظ بعددها عوضاً عن الاحتفاظ بها كاملة
- الثاني، ويُعتبر حلّ بعيد المدى، وكان في تبني IPV6 الذي يعتبر نسخة معدلة من البروتوكول IP بحيث يجري توسيع فضاء العنونة باستخدام عناوين ممثلة على 16 بايت بحيث يستفيد المصممون من الدروس التي تعلموها من استخدام IP خلال السنوات الخمس والعشرين السابقة. وتعتمد هذه النسخة على حذف عدة خصائص قليلة الأهمية خاصة بالبروتوكول IP لجعله أكثر سرعة وأسهل من ناحية التطوير البرمجي. كما تتضمن النسخة الجديد عوامل أمان وتلغي عمليات التقطيع التي تجريها الموجهات البينية عند نقل الطرود

ما زالت النسخة IPV6 في طور التجريب والنشر الأولي، أما CIDR فقد أصبح في طور التشغيل الكامل منذ عدة سنوات، كما يُستخدم CIDR في الانترنت ومن قبل مطوري تجهيزات التوجيه.

حجز العناوين

اعتمدت المواقع على مركز معلومات شبكة الإنترنت (InterNIC) للحصول على عناوين في بدايات الإنترنت. أما في يومنا هذا فقد حلت ARIN محل InterNIC في القارة الأميركية.

إدارياً، قامت هيئة الإنترنت المسؤولة عن توزيع الأسماء والأرقام:
(The Internet Corporation for Assigned Names, & Addresses) ICANN
بتقسيم العناوين إلى ثلاث سجلات مناطقية وتوكيل إدارة هذه السجلات إلى سلطة خاصة بكل منطقة.

الأسم	عنوان موقع الوب	المنطقة التي يغطيها
ARIN	www.arin.net	شمال وجنوب القارة الأميركية وجنوب الصحراء الأفريقية
APNIC	www.apnic.net	منطقة آسيا والباسيفيك
RIPE	www.ripe.net	منطقة أوروبا والمناطق المحيطة بها

سمح توكيل عملية الإدارة من قبل ICANN إلى ARIN وRIPE وAPNIC ومن ثم إلى مزودي الخدمة المحليين في كل بلد أو في كل منطقة، بتجميع ودمج جداول التوجيه المفصلية الأساسية التي تدير الإنترنت.

اعتمدت المواقع على مركز معلومات شبكة الإنترنت (InterNIC) للحصول على عناوين في بدايات الإنترنت. أما في يومنا هذا فقد حلت ARIN محل InterNIC في القارة الأميركية.

يجري توزيع أرقام الشبكات؛ بحيث يقوم كل موقع بتعريف أرقام المحطات المضيفة التي يملكها. كما يمكننا تقسيم فضاء العناوين الذي نحصل إليه إلى شبكات فرعية بالطريقة التي نراها مناسبة.

إدارياً، قامت هيئة الإنترنت المسؤولة عن توزيع الأسماء والأرقام:
(The Internet Corporation for Assigned Names, & Addresses) ICANN
بتقسيم العناوين إلى ثلاث سجلات مناطقية وتوكيل إدارة هذه السجلات إلى سلطة خاصة بكل منطقة. عملت هذه السلطات المحلية على توزيع حصصها على مزودي الخدمة في المنطقة التي ترعاها، كما هو محدد في الجدول حيث يقوم مزودي الخدمة الآنفي الذكر بدورهم، بتقسيم العناوين وتوزيعها على زبائنهم بحيث يتعامل مزودي الخدمة الكبار فقط مع السجلات التي توزعها ICANN.

سمح توكيل عملية الإدارة من قبل ICANN إلى ARIN وRIPE وAPNIC ومن ثم إلى مزودي الخدمة المحليين في كل بلد أو في كل منطقة، بتجميع ودمج جداول التوجيه المفصلية الأساسية التي تدير الإنترنت إذ لا يحتاج الزبائن الحاصلون على عنوان من مزود خدمة لأن يكون عنوانهم مرئياً في جدول توجيه مفصلي أساسي، حيث يكفي وجود قيد واحد خاص بمقطع العناوين المخصص لمزود الخدمة الآنف الذكر.

نشاط 1.9-10-11.23

1. اشرح مفهوم التقسيم إلى شبكات فرعية واشرح فائدته.

2. ما معنى أقنعة الشبكات الفرعية؟ وكيف تساعد هذه الأقنعة على تحديد الأقسام الخاصة بالشبكة وبالمضيف في عنوان IP؟

3. ليكن لدينا الشبكة 134.122.0.0/16:
   i. كم عدد الشبكات 19/ هنا؟ اذكرهم واذكر أقنعتهم
   ii. كم عدد المضيفين على كل شبكة فرعية؟
   iii. حدد الشبكة التي ينتمي لها العنوان 134.122.64.124
   iv. ما هو عنوان البث الخاص بكل شبكة

الفصل الثاني عشر والثالث عشر

عنوان الموضوع:

مبادئ التوجيه IP

الكلمات المفتاحية:

أنظر الملف Glossary المُرافق.

ملخص:

سنناقش في هذه الجلسة أسلوب إيصال رزم المعطيات IP عبر محيط مؤلف من عدة شبكات متصلة ببعضها البعض، وسنستعرض أسس ومبادئ عملية بالتوجيه، وستشرح بالتفصيل التقنيات والمكونات التي تستخدمها الموجهات في تنفيذ عملية التوجيه تلك.

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- الموجه IP ومكوناته
- خوارزميات التوجيه وجداول التوجيه
- التوجيه الثابت، والتوجيه الديناميكي
- بروتوكولات التوجيه الداخلية، وبروتوكولات التوجيه الخارجية
- رسائل التحكم بأخطاؤ الموجهات

1.12-13.1 مقدمة

- نُعرِّف التوجيه بأنها عملية مسؤولة عن تحديد اتجاه حزم المعطيات عبر سلسلة المقاطع والشبكات الموجودة بين مصدر الرزمة ووجهتها، وعن إيصال هذه الحزم إلى وجهتها

- تصبح عملية التوجيه معقدة في حال وجود عدد كبير من الشبكات والمقاطع المرتبطة ببعضها البعض عبر عدة موجهات.

نُعرِّف التوجيه بأنها عملية مسؤولة عن تحديد اتجاه حزم المعطيات عبر سلسلة الشبكات الموجودة بين مصدر الرزمة ووجهتها، وعن إيصال هذه الحزم إلى وجهتها. تشبه عملية التوجيه السؤال عن وجهة غير معروفة في بلد غريب. فقد يوجهك الشخص الأول الذي تسأله باتجاه المدينة الصحيحة وعندما تقترب بعض الشيء من وجهتك، قد تسأل شخصاً ثانياً يمكن أن يكون قادراً على تحديد الشارع الذي تتجه إليه بدقة أكبر. وعندما تصبح قريباً بما فيه الكفاية فإن أحدهم سيكون قادراً على تحديد البناء الذي تبحث عنه.
تأخذ معلومات التوجيه شكل قواعد ندعوها "**طرق**" مثل "**للبحث عن الشبكة A، أرسل طرداً عبر الجهاز C**". كما يمكن أن تحتوي معلومات التوجيه على "**طرق تلقائية**" تحدد ما يجب عمله بالطرود المتجهة إلى شبكة لا يمتلك الموجه من أجلها طرقاً واضحة محددة.

تحتاج منصة العمل لأن تكون على درايةٍ تامة ــ بطريقةٍ ما ــ بوجود الموجه الذي يربط بين مقاطع الشبكة المختلفة حتى تتمكن من استخدامه خلال تعاملاتها عبر المقاطع.

تصبح العملية معقدة في حال وجود عدة مقاطع مرتبطة ببعضها البعض عبر عدة موجهات. إذ لايكفي عندها أن تكون منصات العمل على درايةٍ بوجود الموجهات بل تحتاج الموجهات أيضاً أن تكون على دراية ببعضها بعضاً وعلى علمٍ بالمقاطع المرتبطة بكل موجه.

تشرح الشرائح التالية وبالتفصيل التقنيات والمكونات التي تستخدمها الموجهات في تنفيذ عملية التوجيه ضمن محيط مؤلفة من عدة شبكات متصلة ببعضها البعض.

التوجيه البسيط المنطقي

إذا كانت الشبكة مؤلفة من مقطع واحد، وكانت عناوين المنصات لاتنتمي إلى نفس الشبكة، يجري اختيار منصة لتلعب دور الموجه (الذي ندعوه عبّارة عندها)، بحيث تمتلك المنصة عدة عناوين كل منها ينتمي إلى شبكة من هذه الشبكات. عندها يجب أن يكون المُضيف على درايةٍ تامة ــ بطريقةٍ ما ــ بوجود هذه العبارة.

يجري إعلام كل مُضيف بوجود هذه العبارة اعتماداً على عنوان **العبّارة** التي يجري إسنادها كجزء من الإعدادات الشبكية للمُضيف.

عندما يرغب المُضيف بإرسال رزمة إلى مُضيف آخر، يُجري عملية حساب منطقية باستخدم AND منطقية بين عنوان المُضيف المُرسِل وقناعه، وبين عنوان المُضيف الوجهة وقناع المُضيف المُرسِل، فإذا كانت النتيجتان متساويتين، جرى إرسال الرزمة مباشرةً إلى الوجهة (على اعتبار أن التساوي يعني تواجد المُرسِل والمُستقبِل على شبكة واحدة)، وإلا جرى إرسالها للعبّارة (الموجه) التي تتولى توجيهها تبعاً لجداول وخوارزميات التي تعمل وفقها.

نشاط

بفرض لدينا الحالات التالية التي يريد فيها المُضيف الوجهة إرسال رزمة إلى وجهة ما (بالرغم من أن بعض هذه الحالات هي حالات نظرية لا تُستَخدَم في تقسيم الشبكات واقعياً)، حدد بالحساب فيما إذا كان المُرسِل والمُستقبِل يقعان على شبكة واحدة ولا يحتاج المُرسل إلى توجيه الرزمة باتجاه الموجه:

الجواب: على نفس الشبكة؟	عنوان المُستقبِل	قناع المُرسِل	عنوان المُرسِل
كلا	20.20.20.3	255.255.255.1	20.20.20.2
نعم	20.20.20.4	25.255.255.1	20.20.20.2
كلا	200.200.128.0	255.255.64.0	200.200.65.24
نعم	200.200.129.128	255.255.128.0	200.200.128.24

موجهات IP

- تتكون موجهات IP من مجموعة مكونات شبكية عاملة على شبكات IP تهتم بتحويل الحزم من مقطع شبكي إلى آخر لحين إيصالها إلى وجهة إرسالها النهائية
- يحتوي مكدس البروتوكولات في موجهات IP، على كتل برمجية تابعة لطبقة الارتباط ولطبقة الإنترنت لتنفيذ عمليات التحويل والنقل
- نُعرِّف الواجهات الشبكية بأنها كيانات منتمية إلى طبقة الارتباط تهدف إلى ربط الموجهات أو المنصات بالمقاطع الشبكية
- يجب التفريق بين "**واجهة الدخل**"، و"**واجهة الخرج**"، حيث يجري استقبال الحزم عبر واجهة الدخل ويجري إرسالها عبر واجهة الخرج.
- نُعرِّف موجه **IP** على أنه جهاز شبكي وسيط يقوم باستقبال حزم المعطيات على واجهات الدخل ويقوم بإرسالها إلى وجهتها اعتباراً من واجهات الخرج

ملاحظة:

نستخدم مصطلح "**موجه IP**" عندما نريد الإشارة إلى أن جميع الاعتبارات هي اعتبارات قابلة للتطبيق على موجهات عاملة بالبروتوكول IP فقط وليس على موجهات عاملة ببروتوكولات أخرى مثل موجهات IPX، AppletalK ... الخ. في حين، يمكننا استخدام مصطلح "**موجه**" دون إلحاقه بكلمة **"IP"** عندما لا يسبب استخدام المصطلح الأخير غموضاً وتناقضاً.

تتكون موجهات IP من مجموعة مكونات شبكية عاملة على شبكات IP تهتم بتحويل الحزم من مقطع شبكي إلى آخر لحين إيصالها إلى وجهة إرسالها النهائية.

يحتوي مكدس البروتوكولات في موجهات IP، على كتل برمجية تابعة بشكل أساسي لطبقة الارتباط ولطبقة الإنترنت لتنفيذ عمليات التحويل والنقل، وتُعتبر هذه الكتل البرمجية رئيسية وضرورية ضمن الموجهات، في حين تبقى كتل طبقات أخرى مثل طبقة التطبيقات اختيارية وغير ضرورية.

لتعريف طرق وأساليب اتخاذ قرارات التحويل والتوجيه سنبدأ بتعريف نظري لموجه IP لنعتمد عليه فيما بعد في شرح أساليب التوجيه.

نحتاج أولاً لتعريف ما نعنيه بالواجهات الشبكية، إذ يمكننا اعتبار هذه الواجهات كيانات منتمية إلى طبقة الارتباط تهدف إلى ربط الموجهات أو المضيفين بالمقاطع الشبكية. من منظور IP يمكن اعتبار الواجهة الشبكية مزيجاً من بطاقة الشبكة وسواقتها. وبهدف تعريف موجه IP بشكل نظري بحت يجب أن نُفرِّق بين ما ندعوه "**واجهة الدخل**"، و"**واجهة الخرج**"، حيث يجري استقبال الحزم عبر واجهة الدخل ويجري إرسالها عبر واجهة الخرج. يمكن لنفس الواجهة أن تكون واجهة دخل وواجهة خرج بآن واحد.

نُعرِّف **موجه IP** على أنه جهاز شبكي وسيط يقوم باستقبال حزم المعطيات على واجهات الدخل ويقوم بإرسالها إلى وجهتها اعتباراً من واجهات الخرج.

المكونات الرئيسية لموجه

لموجه ثلاثة مكونات من منظور عملية التوجيه IP: مجموعة من **واجهات الدخل والخرج**، وبنية معطيات تُدعى "**جدول التوجيه**"، بالإضافة إلى "**محرك توجيه**".

- سبق وذكرنا أنه يجري استقبال الحزم عبر واجهة الدخل ويجري إرسالها عبر واجهة الخرج بحيث يمكن لنفس الواجهة أن تكون واجهة دخل وواجهة خرج بآن واحد

- نُعرِّف جدول التوجيه بأنه بنية معطية حاوية على معلومات تشير إلى عناوين الشبكات (المرتبطة بكل واجهة خرج) والتي تديرها وتتعامل معها الكتل البرمجية المُختصّة (التي ندعوها الكتل IP)

- نُعرِّف محرك التوجيه بأنه مزيج من المكونات الصلبة والمكونات البرمجية في موجه، يتلقى حزم المعطيات من واجهات الدخل، ويعالجها لاتخاذ القرار المناسب الذي يهدف إلى إرسالها نحو وجهتها

ملاحظة:

لا توجد بنية معطيات محددة ومُعرَّفة مسبقاً لجدول توجيه، فلكل جهة إنتاج حرية إنجاز هذه البنية بما يتوافق مع أسلوب إنجازها لكتل IP البرمجية. إلا أن بعض المكونات التي تؤلف هذه البنية تتواجد في أي شكلٍ من أشكال جداول التوجيه كونها مكونات تساعد على التواصل مع الغير وسيجري لاحقاً شرح هذه المكونات بالتفصيل.

يمتلك الموجه – من منظور عملية التوجيه IP– ثلاثة مكونات: مجموعة من **واجهات الدخل والخرج**، وبنية معطيات تُدعى "**جدول التوجيه**"، بالإضافة إلى "**محرك توجيه**".

سبق وذكرنا أنه يجري استقبال الحزم عبر واجهة الدخل ويجري إرسالها عبر واجهة الخرج بحيث يمكن لنفس الواجهة أن تكون واجهة دخل وواجهة خرج بآنٍ واحد.

نُعرِّف جدول التوجيه بأنه بنية معطية حاوية على معلومات تشير إلى عناوين الشبكات (المرتبطة بكل واجهة خرج) والتي تديرها وتتعامل معها الكتل البرمجية المُختصّة (التي ندعوها كتل IP البرمجية).

نُعرِّف محرك التوجيه على أنه مزيج من المكونات الصلبة والمكونات البرمجية في موجه. يتلقى المحرك حزم المعطيات من واجهات الدخل، ويعالج هذه المعطيات اعتماداً على كلٍ من: عنوان الإرسال وجهة الإرسال الموجودين في حزم المعطيات، بالإضافة إلى جدول التوجيه، بحيث يجري اتخاذ القرار المناسب الذي يهدف إلى إرسال حزم المعطيات خارجاً، نحو وجهتها، عبر واجهة الخرج المناسبة.
يستخدم محرك التوجيه خوارزميات توجيه تساعده على اتخاذ القرارات بشأن عملية التوجيه. وتساعد هذه الخوارزميات المحرك على اتخاذ القرار المناسب الذي يحدد فيما إذا كان من الواجب إرسال رزمة المعطيات إلى عقدة أخرى أو إهمالها في حال تعذر وجود وجهة صالحة لها.

جداول التوجيه

يجري تخزين معلومات التوجيه في جدول ضمن النواة. يتكون جدول التوجيه من قيود بحيث يتألف كل قيد من ثلاثة حقول:

- يحتوي الأول على عنوان شبكة (بادئة شبكة) تدل على الشبكة "الوجهة"
- يشير الثاني إلى واجهة الخرج التي يمكن عبرها الوصول إلى الشبكة المحددة بالعنوان السابق (البادئة السابقة)
- يحتوي الثالث على عنوان الموجه التالي الذي يُعتَبَر الوجهة المقبلة للمعطيات المتجهة إلى الشبكة "الوجهة" التي عرفناها بالعنوان الأول (البادئة الأولى)

ندعو التشكيلة المؤلفة من الحقول الثلاثة المكونة لقيد من قيود جدول التوجيه بـــ "**طريق**".

لتوجيه رزمة نحو عنوان محدد، تبحث النواة عن أكثر الطرق توافقاً مع وجهة الرزمة (الطريق ذو القناع الأطول).

يجري تخزين معلومات التوجيه في جدول ضمن النواة. يتكون جدول التوجيه من قيود بحيث يتألف كل قيد من ثلاثة حقول: يحتوي الأول على عنوان شبكة (بادئة شبكة) تدل على الشبكة "الوجهة"، ويشير الثاني إلى واجهة الخرج التي يمكن عبرها الوصول إلى الشبكة المحددة بالعنوان السابق (البادئة السابقة)، ويحتوي الثالث على عنوان الموجه التالي الذي يُعتَبَر الوجهة المقبلة للمعطيات المتجهة إلى الشبكة "الوجهة" التي عرفناها بالعنوان الأول (البادئة الأولى). فإذا كان بالإمكان الوصول مباشرة إلى الشبكة عبر إحدى واجهات المواجه يكون عنوان الموجه التالي والمُعطى في الحقل الأخير، فارغاً.

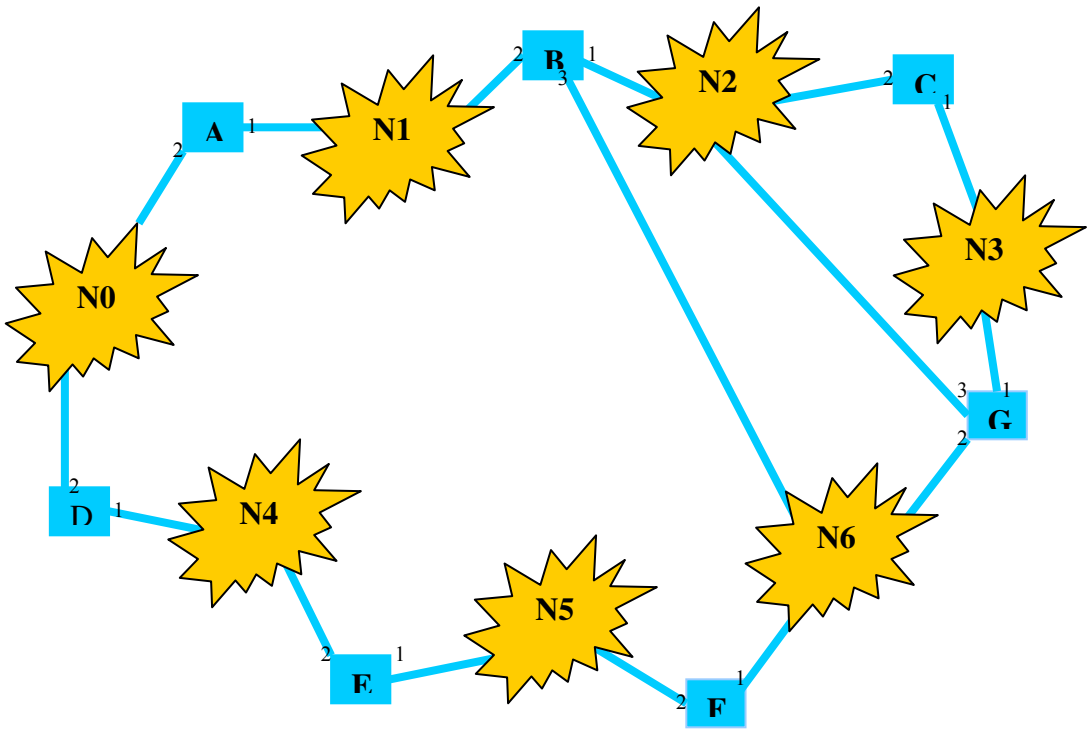
يمكن لجدول التوجيه أن يحتوي على عدة قيود تشير جميعها إلى نفس عنوان (بادئة) الشبكة على أن يكون محتوى بقية الحقول وحيداً في كل قيد منها سواءاً كان ذلك الحقل هو حقل واجهة الخرج أو الحقل الحاوي على عنوان الموجه التالي.

ندعو التشكيلة المؤلفة من الحقول الثلاثة المكونة لقيد من قيود جدول التوجيه بـــ "**طريق**". بحيث نقول أن جدول التوجيه يحدد طرقاً، ونقول أن الطريق "**يؤشر**" إلى واجهة الخرج المحددة في تشكيلته. وفي حال احتوى الطريق على عنوان الموجه التالي، نقول أن الطريق "**يؤشر**" إلى عنوان الموجه التالي.

لتوجيه رزمة نحو عنوان محدد، تبحث النواة عن أكثر الطرق توافقاً مع وجهة الرزمة (الطريق ذو القناع الأطول). في حال لم تجد النواة طريقاً معقولاً ولم يكن لديها طريق تلقائي، تقوم بإرجاع رسالة ICMP إلى المُرسل تفيد بأنها "**غير قادرة على الوصول إلى الشبكة**" **(network unreachable)**.

نشاط

بفرض أن لدينا الشبكة التالية:



بفرض N1,N2, ... مجموعة من الشبكات المرتبطة بموجهات A,B,C, ... بحيث يكون كل موجه مرتبط بعدة شبكات، بحيث يرتبط الموجه بالشبكة اعتباراً من إحدى واجهاته المُرقمة 1، 2، ... الخ.

بفرض أنك مدير الشبكة السابقة، حدد يدوياً (طرق ثابتة) من أجل كل موجه من الموجهات الظاهرة في الشكل السابق، جدول التوجيه الذي يسمح للموجه بتحويل الرزم التي تصل إليه من أي شبكة من الشبكات التي يرتبط بها إلى إحدى الشبكات الظاهرة في الشكل السابق. طبعاً سنفترض أن جدول التوجيه تقريبي وله الشكل:

جدول توجيه الموجه E:

وجهة الطرد	الموجه التالي	الواجهة	عدد الموجهات التي يجب تجاوزها للوصول إلى الوجهة
N3	F	1	2
N3	D	2	4
...	...		...
...			

ترى هل سيكون لديك الصبر الكافي لوضع جداول التوجيه الكاملة لجميع الموجهات على هذه الشبكة والتي تقتصر فقط على قيود التوجيه ضمن الشبكة !!!

تصور ما الذي سيحدث لو أن جداول توجيه موجهات الإنترنت تُدار بالشكل السابق !!!

خوارزميات التوجيه

سبق وأشرنا إلى وجود نوعين من العنونة IP: العنونة ذات الصفوف، والعنونة دون صفوف. وقد سبق ووضحنا الفرق بين أسلوبي العنونة.

يؤدي هذا الاختلاف إلى وجود نوعين من خوارزميات التوجيه. خوارزميات التوجيه المعتمدة على العنونة ذات الصفوف وخوارزميات التوجيه المعتمدة على العنونة دون صفوف.

تستخدم كلا الخوارزميتين إجرائية مشتركة: المقارنة بين عنوان الوجهة وبادئة الشبكة.

تجدر الإشارة إلى وجود غموض في أسلوب تنفيذ هذه المقارنة. لذا، وقبل الخوض في تفاصيل خوارزميات التوجيه، من الضروري البدء بتوضيح أسلوب المقارنة.

خوارزميات التوجيه: القواعد المتبعة في إجرائية المقارنة

ندعو سلسلة بتات بادئة الشبكة المحصورة بين البت الأول (من اليسار) والبت ذي الترتيب المساوي لطول البادئة ناقصاً 1 (من اليسار) "**سلسلة البتات ذات الدلالة**".

تجري المقارنة بتاً، بتاً وحسب نفس الترتيب بين السلسلة ذات الدلالة وعنوان الوجهة.

يوضح الشكل المرافق عملية المقارنة بين العنوان 10.35.63.45 وبادئة الشبكة 10.32.0.0/14.

IP Address=10.35.63.45	**00001010**	**00100011**	00111111	00101101
	↓	↓		
Network = 10.32.0.0./14	**00001010**	**00100000**	00000000	00000000

ملاحظة:

من الضروري، في بعض الأحيان، مقارنة بادئتي شبكتين بنفس أسلوب مقارنة بادئة شبكة وعنوان IP. في هذه الحالة، نعتبر أن البادئتين متطابقتان إذا كان لهما نفس الطول وكانت قيمة كل بت من سلسلة البتات ذات الدلالة في البادئة الأولى، مساوية لقيمة البت المقابل من سلسلة البتات ذات الدلالة في البادئة الثانية.

ندعو سلسلة بتات بادئة الشبكة المحصورة بين البت الأول (من اليسار إلى اليمين) والبت ذي الترتيب المساوي لطول البادئة ناقصاً 1 (اعتباراً من اليسار إلى اليمين) "**سلسلة البتات ذات الدلالة**". وتجري المقارنة بتاً، بتاً وحسب نفس الترتيب بين السلسلة ذات الدلالة وعنوان الوجهة.

نعتبر أن عنوان الوجهة موافقاً لبادئة الشبكة إذا كانت قيمة كل بت في "سلسلة البتات ذات الدلالة" مساوية لقيمة البت المقابل في عنوان الوجهة.

يوضح الشكل المرافق عملية المقارنة بين العنوان 10.35.63.45 وبادئة الشبكة 10.32.0.0/14. نلاحظ أن العنوان يطابق بادئة الشبكة حسب المقارنة التي وضحناها فيما سبق. إذ تتوافق البادئة المُعَرِّفة للشبكة 10.32.0.0/14 مع العنوان 10.35.63.45 لأن قيمة كل بت في "السلسلة ذات الدلالة" تكون مساوية لقيمة البت المقابل في عنوان الوجهة.

خوارزمية التوجيه المعتمدة على عنونة دون صفوف
Classless routing Algorithm

لا تضع هذه الخوارزمية أية فرضيات متعلقة بطريقة تعريف العنوان IP.

تتكون هذه الخوارزمية من مرحلتين أساسيتين.

تأخذ هذه الخوارزمية كلاً من العنوان IP وجدول التوجيه كمعاملات وتقوم بإرجاع صفر أو واحد أو عدة قيود من جدول التوجيه.

نوضح فيما يلي المراحل المؤلفة لخوارزمية التوجيه المعتمدة على عنونة دون صفوف:

- ← **المقارنة الأساسية:** تجري في هذه المرحلة مقارنة عنوان الوجهة مع بادئات الشبكات الموجودة في قيود جدول التوجيه.
- ← **المقارنة المُعَمَقة:** يجري فيها اختيار القيد الحاوي على طول البادئة الأكبر من ضمن مجموعة القيود الناتجة عن المرحلة السابقة.
- ← تتوقف الخوارزمية عن العمل في حال لم ينتج عن إحدى المراحل السابقة أي قيد من قيود جدول التوجيه.

مثال:

لتوضيح مراحل الخوارزمية السابقة بشكلٍ أفضل سنقوم بعرض عدة أمثلة. لنفترض أن لدينا موجه حاوي على جدول التوجيه المعروض في الجدول التالي:

رقم القيد	بادئة الشبكة	واجهة الخرج	الموجه التالي
1	8.0.0.0/5	Ethernet0	192.168.1.1
2	10.1.0.0/16	TokenRing0	192.168.2.1
3	172.0.0.0/8	Serial0	172.16.1.1
4	10.32.0.0/14	Ethernet1	10.32.1.10
5	10.32.1.0/24	Ethernet1	-
6	10.32.0.0/14	Ethernet1	10.32.1.11
7	192.168.1.0/24	Ethernet0	-
8	192.168.2.0/24	TokenRing0	-
9	172.16.1.0/30	Serial0	-

نلاحظ أن للقيدين 4 و6 نفس قيمة حقل بادئة الشبكة ونفس قيمة حقل الواجهة الخارجية، إلا أنهما يختلفان بعنوان الموجه التالي اللذان يؤشران إليه. طبعاً يجعل الاختلاف الأخير من وجودهما ممكناً ضمن نفس جدول التوجيه وإلا فلا معنى لتكرار نفس القيد في نفس الجدول.

لنفترض الآن أن الموجه قد تلقى رزمة معطيات موجهة للعنوان 10.35.45. سنحاول فيما يلي تتبع خطوات الخوارزمية حسب المراحل التي ذكرناها سابقاً.

← ستتمخض المرحلة الأولى، وهي مرحلة المقارنة الأساسية، عن الاحتفاظ بالقيود 1 و2 و4 و6 وإهمال القيود 3 و5 و7 و8 و9.

← أما المرحلة الثانية فستؤدي للاحتفاظ بالقيدين 4 و6 لاحتوائهما على الطول الأكبر لبادئة الشبكة.

← بالنتيجة، تقوم الخوارزمية بإرجاع القيدين 4 و6 من جدول التوجيه لاحتوائهما على البادئة ذات الطول الأكبر.

لنفترض الآن وصول رسالة المعطيات الموجهة إلى العنوان 10.255.5.1، سيجري تطبيق مراحل الخوارزمية الثلاث بالشكل التالي:

← ينتج عن مرحلة المقارنة الأساسية القيد رقم 1 من جدول التوجيه.

← تحتفظ المرحلة الثانية بالقيد رقم 1.

← بالنتيجة يجري إرسال رسالة المعطيات عبر الواجهة Elhernet0 للموجه التالي ذات العنوان 192.168.1.1.

في مثالنا الأخير سنفترض وصول رسالة معطيات موجهة للعنوان 9.1.1.1. تكون خطوات الخوارزمية على الشكل التالي:

← ينتج عن المرحلة الأولى القيد رقم 1 من جدول التوجيه.

← تحتفظ المرحلة الثانية بالقيد رقم 1.

← وكما هو الحال في المثال السابق، يجري إرسال رسالة المعطيات عبر الواجهة Elhernet0 للموجه التالي ذي العنوان 192.168.1.1.

لا تضع هذه الخوارزمية أية فرضيات متعلقة بطريقة تعريف العنوان IP. بمعنى آخر لا يوجد فيها أية إشارة أو اعتبار لصفوف الشبكة A و B و C.

تتكون هذه الخوارزمية من ثلاثة مراحل بحيث يمكن اعتبار المرحلة الثالثة اختيارية.

تأخذ هذه الخوارزمية كلاً من العنوان IP وجدول التوجيه كمعاملات وتقوم بإرجاع صفر أو واحد أو عدة قيود من جدول التوجيه حاوية على تفاصيل الوجهات المحتملة لحزم المعطيات. وفي حال عدم إرجاع أي قيد من قيود جدول التوجيه، يجري إهمال رزمة المعطيات المعنية على اعتبار أن لائحة التوجيه لا تملك ما يكفي من المعلومات لإتمام عملية توجيه رسالة المعطيات.

نوضح فيما يلي المراحل الثلاثة المؤلفة لخوارزمية التوجيه المعتمدة على عنونة دون صفوف:

← **المقارنة الأساسية:** تجري في هذه المرحلة مقارنة عنوان الوجهة مع بادئات الشبكة الموجودة في قيود جدول التوجيه. ويجري إهمال جميع البادئات التي لا تتوافق مع هذا العنوان. وينتج عن هذه المرحلة مجموعة من القيود الحاوية على بادئات شبكات متوافقة مع عنوان الوجهة.

← **المقارنة المُعَمَقة:** يجري فيها اختيار القيد الحاوي على طول البادئة الأكبر من ضمن مجموعة القيود الناتجة عن المرحلة السابقة. ويمكن الاحتفاظ بأكثر من قيد في هذه المرحلة إذا كانت تحتوي على بادئات بنفس الطول.

← تتوقف الخوارزمية عن العمل في حال لم ينتج عن إحدى المراحل السابقة أي قيد من قيود جدول التوجيه.

خوارزميات التوجيه المعتمدة على عنونة ذات صفوف
Classfull Routing Algorithm

على عكس خوارزميات التوجيه المعتمدة على عنونة ذات صفوف، تفترض الخوارزميات التي نحن بصددها في هذه الفقرة ما يلي:

- هناك صفوف عناوين وحيدة الإسناد وينتمي كل عنوان IP إلى واحدة من هذه الصفوف.
- هناك استمرارية في قيم العناوين المحجوزة من أجل المضيفين ضمن شبكة معنونة بعناوين ذات صفوف.

كحال خوارزميات التوجيه المعتمدة على عنونة دون صفوف تتألف خوارزميات التوجيه المعتمدة على عنونة ذات صفوف بشكل أساسي من مرحلتي المقارنة الأساسية والمقارنة المُعَمَقة.

على عكس خوارزميات التوجيه المعتمدة على عنونة ذات صفوف، تفترض الخوارزميات التي نحن بصددها في هذه الفقرة ما يلي:

- هناك صفوف عناوين وحيدة الإسناد وينتمي كل عنوان IP إلى واحدة من هذه الصفوف.
- هناك استمرارية في قيم العناوين المحجوزة من أجل المضيفين ضمن شبكة معنونة بعناوين ذات صفوف. بمعنى آخر وفي حال استخدام العنونة ذات الصفوف، لا يمكن فصل مضيفين لهما نفس عنوان الشبكة، بمقاطع شبكية، دون أن تكون هذه المقاطع مُعنونة بنفس عنوان الشبكة السابق.

  فإذا كان المضيفان H1 وH2 منتميين إلى مقطعين S1 وS2 على الترتيب، ومُعَنونين بعنوان الشبكة 10.0.0.0/8 (المنتمي للصف A). وإذا كان المقطعان S1 وS2 مفصولين بالمقطع الشبكي S3 المعنون بعنوان الشبكة 172.16.0.0/16 (المنتمي للصف B)، فإن المضيفين H1 وH2 لن يستطيعا إجراء الاتصال فيما بينهما إذا استخدم موجها المقطعين S1 وS2 وهما R1 وR2 على الترتيب، خوارزميات التوجيه المعتمدة على عنونة ذات صفوف.

كحال خوارزميات التوجيه المعتمدة على عنونة دون صفوف تتألف خوارزميات التوجيه المعتمدة على عنونة ذات صفوف بشكل أساسي من مرحلتي المقارنة الأساسية والمقارنة المُعَمَقة. وكحال الخوارزميات السابقة، تأخذ خوارزمية التوجيه المعتمدة على عنونة ذات صفوف كلاً من عنوان الوجهة وجدول التوجيه كمعاملات وتقوم بإرجاع صفر أو قيد أو عدة قيود من جدول التوجيه لاستخدامها في توجيه حزم المعطيات.

بعد الانتهاء من تنفيذ خوارزمية التوجيه

بعد الانتهاء من تنفيذ خوارزمية التوجيه ــ سواء كانت معتمدة على عنونة ذات صفوف أو عنونة دون تصنيف ــ يحتاج الموجه لتحويل رسالة المعطيات أو إهمالها.

يجري إهمال الرسالة في حال عدم إرجاع الخوارزمية لأي طريق توجيه ممكن للمعطيات. أما في حال أرجعت الخوارزمية قيوداً من جدول التوجيه فهناك حالتين:

- **أن نحصل على طريق توجيه واحد:** في هذه الحالة يكون تصرف محرك التوجيه بديهياً إذا يقوم باستخدام واجهة الخرج والعنوان IP الممثل للموجه التالي لإرسال رسالة المعطيات إلى هذا الأخير.
- **أن نحصل على عدة طرق توجيه:** في هذه الحالة يكون تعامل محرك التوجيه مع عدة طرق ممكنة تابعاً لأسلوب تصميم الموجه إذ يمكن للمصمم أن يُطور الموجه بحيث يجري اختيار الطريق الأول من عدة طرق ممكنة، أو أن يجري استخدام الطريق الأفضل، أو أن يجري استخدام جميع الطرق أو عدة طرق. طبعاً لن يجري استخدام الطرق، في الحالة الأخيرة، بنفس الوقت لإرسال رزمة معطيات واحدة، ولكن لإرسال مجموعات جزئية من رسائل المعطيات المتجهة إلى نفس الوجهة. ندعو هذه العملية بعملية "**توزيع الحِمْل**".

ملاحظة:

يختلف مفهوم الطريق الأفضل تبعاً لتصميم وإعداد الموجه، فقد يعني الطريق الأقصر عدد الموجهات التالية التي يجب أن تمر بها الرزمة، وقد يعني عرض الرزمة بين الموجهات.

توزيع الحِمْل

هناك أسلوبين لتنفيذ هذه العملية:

- "توزيع الحمل عبر توزيع الرزم" (per-packet load balancing)
- "توزيع الحِمْل تبعاً للمُضيف الوجهة" (per-destination load balancing)

هناك أسلوبين لتنفيذ هذه العملية:

- يعتمد الأول على إرسال رزم المعطيات الموجهة أصلاً إلى نفس بادئة الشبكة والتي أرجعت خوارزمية التوجيه عدة طرق ممكنة لها، باستخدام جميع هذه الطرق. يجري ذلك عبر إرسال الرزم باستخدام التعاقب الدوراني. ندعو هذا الأسلوب "**بتوزيع الحمل عبر توزيع الرزم**" (per-packet load balancing).
- أما الأسلوب الثاني فيجري فيه الاختيار طريق الرزمة الأولى المتجهة إلى عنوان IP لمُضيف ينتمي للشبكة ذات البادئة، عشوائياً. تسلك جميع الرسائل الموجهة إلى نفس البادئة نفس الطريق السابق إذا كانت وجهتها هو العنوان IP الذي توجهت إليه الرسالة الأولى. بمعنى آخر، يجري "توزيع الحِمْل تبعاً للمُضيف الوجهة" (per-destination load balancing) وهو الأسلوب المُفَضَل في حال جرى بناء الموجه ليقوم بتوزيع الحمل.

إنشاء الطرق في جدول التوجيه

تحتاج جداول التوجيه الموجودة في الموجهات لعمليات تساعد على إغنائها وإنشاء الطرق المكونة لها.

يجري بناء قيد يمثل طريق ضمن جدول التوجيه بإسناد عنوان IP مع طول بادئة شبكة إلى واجهة من واجهات الموجه. ندعو الطريق الناتج "**طريق اتصال مباشر**".

يجري تغيير القيد في حال تغيرت المعلومات المتعلقة بعنوان بادئة الشبكة المرتبطة بواجهة الخرج:

- يمكن توليد وتغيير وحذف قيود جدول التوجيه يدوياً "**الطرق الثابتة**"
- يمكن توليد وتغيير وحذف قيود جدول التوجيه باستخدام بروتوكولات مساعدة ندعوها "**بروتوكولات التوجيه**". ندعو طرق التوجيه الناشئة عن البروتوكولات السابقة "**الطرق الديناميكية**"

تحتاج جداول التوجيه الموجودة في الموجهات لعمليات تساعد على إغنائها وإنشاء الطرق المكونة لها. كما تحتاج هذه الجداول لعمليات حذف وتغيير في هذه الطرق نظراً لتغير معلومات التوجيه تبعاً للظروف المحيطة.

يجري بناء قيد يمثل طريق ضمن جدول التوجيه بإسناد عنوان IP مع طول بادئة شبكة إلى واجهة من واجهات الموجه. يحتوي هذا القيد على بادئة الشبكة المطلوبة ويؤشر إلى واجهة الخرج المطلوبة. يبقى القسم الممثل للموجه التالي فارغاً ضمن القيد السابق. ندعو الطريق الناتج "**طريق اتصال مباشر**".

يجري تغيير القيد في حال تغيرت المعلومات المتعلقة بعنوان بادئة الشبكة المرتبطة بواجهة الخرج. كما يجري حذف القيد في حال توقفت واجهة الخرج عن العمل وأصبحت غير صالحة.

- يمكن توليد وتغيير وحذف قيود جدول التوجيه يدوياً (عبر عمليات إدارية). ندعو الحقول المولّدة يدوياً بالحقول الثابتة وندعو الطرق المرتبطة بها بالطرق الثابتة
- يمكن توليد وتغيير وحذف قيود جدول التوجيه باستخدام بروتوكولات مساعدة ندعوها "**بروتوكولات التوجيه**". كما يمكن لموجه واحد أن يستخدم عدة بروتوكولات توجيه. ندعو طرق التوجيه الناشئة عن البروتوكولات السابقة "**الطرق الديناميكية**"

إشكاليات متعلقة بإضافة طرق جديدة إلى جدول التوجيه

تظهر بعض الحالات الإشكالية عند إضافة قيود جديدة إلى جدول التوجيه، وذلك:

- عندما تحاول عدة مصادر لمعلومات التوجيه إضافة قيود من أجل نفس بادئة الشبكة
- عند إضافة طرق جديدة من أجل بادئة شبكة لها قيد موجود أصلاً في جدول التوجيه

يجري حل هذه الإشكاليات بوضع نظام أفضليات لمصادر المعلومات بحيث يحتفظ مصدر المعلومات الذي له الأفضلية الأكبر بالأولوية في عملية الإضافة على جدول التوجيه ويجري إهمال المصادر الأخرى المتعارضة معه.

يجري اكتشاف الإشكالات السابقة بمقارنة حقول بادئات الشبكة في الطرق التي تكون في وضع تنافسي ويهمل الحقلين الآخرين ـــأي حقل واجهة الخرج وحقل عنوان الموجه التالي في قيد جدول التوجيه.

أفضليات الطرق

ندعو الأفضلية التي تميز طريق عن آخر في جدول توجيه "**بالمسافة الإدارية**" الخاصة بمصادر معلومات التوجيه.
تُعطى قيم المسافات الإدارية ضمن مجال يتراوح بين 0 و255 حيث تدل القيمة صفر على أفضلية أكبر لمصدر المعلومات حيث تكون الطريق مباشرة (متصلة بالموجه مباشرةً).

يحتفظ الموجه عادةً بقيم المسافات الإدارية بالاستعانة بحقل خاص ضمن كل قيد من قيود جدول التوجيه يجري فيه وضع قيمة المسافة الإدارية الخاصة بمصدر المعلومات الذي قام بإضافة هذا القيد مما يساعد الموجه على مقارنة المسافات الإدارية لمصادر القيود في حال حدوث إشكالات عند إضافة قيود جديدة. لذا فمن المتعارف عليه التحدث عن "المسافة "**المسافة الإدارية لطريق**".

مثال:

لنفترض على سبيل المثال أن لموجه ما جدول التوجيه المعطى فيما يلي:

رقم القيد	بادئة الشبكة	واجهة الخرج	الموجه التالي	المسافة الإدارية
1	8.0.0.0/5	Ethernet0	192.168.1.1	100
2	10.1.0.0/16	TokenRing0	192.168.2.1	150
3	172.0.0.0/8	Serial0	172.168.1.1	150
4	10.32.0.0/14	Ethernet1	10.32.1.10	200
5	10.32.1.0/24	Ethernet1	-	0
6	10.32.0.0/14	Ethernet1	10.32.1.11	100
7	192.168.1.0/24	Ethernet0	-	0
8	192.168.2.0/24	TokenRing0	-	0
9	172.16.1.0/30	Serial0	-	0

لنفترض أن مصدراً لمعلومات التوجيه حاول إضافة قيد جديد، ولنفترض أن لهذا المصدر مسافة إدارية لها القيمة 1. لنفترض أن الطريق يتجه لبادئة الشبكة 10.32.1.0/28.

يضيف الموجه هذا القيد نظراً لعدم احتواء جدول التوجيه على أي قيد من أجل هذه البادئة. تجدر الإشارة هنا إلى أن تشابه بادئة الشبكة 10.32.1.0/24 الموجودة في القيد الخامس مع البادئة السابقة لا يجعلهما متساويتين كون الطول المعطى للبادئة الأخيرة هو 24 بينما الطول المعطى للبادئة المضافة هو 28.

لنفترض الآن أن مصدر للمعلومات الذي يمتلك مسافة إدارية مقدرة بالقيمة 150، حاول إضافة سطر جديد مرتبط بالبادئة 8.0.0.0/5، سنلحظ أن هذه الإضافة لن تتم كون الحقل الأول مرتبط ببادئة مماثلة ولكنه يتميز بمسافة إدارية (لمصدر معلوماته) مقدرة بالقيمة 100 وهي مسافة أصغر وذات أفضلية أعلى.

بروتوكولات التوجيه الداخلية وبروتوكولات التوجيه الخارجية

تُعتبر بروتوكولات التوجيه الطريقة الأكثر استخداماً لملئ جداول توجيه الموجهات بمعلومات التوجيه:

- تساعد هذه البروتوكولات في تقليل الجهد الإداري
- تسهل التفاعل مع التغييرات التي تطرأ على طبولوجيا الشبكة
- تساعد على تغيير معلومات التوجيه بشكل أسرع

ندعو مجموعة الشبكات الحاوية على موجهات تعمل باستخدام نفس بروتوكول التوجيه، "**مجال توجيه**" البروتوكول.

ندعو مجموعة الشبكات العاملة تحت نفس السلطة الإدارية "**نظم توجيه مستقلة**".

ندعو البروتوكولات المستخدمة لتبادل معلومات التوجيه ضمن الأنظمة المستقلة "**بروتوكولات العبّارات الداخلية**".

ندعو البروتوكولات المستخدمة لتبادل المعلومات بين النظم المستقلة "**برتوكولات العبّارات الخارجية**".

تعتبر بروتوكولات التوجيه الطريقة الأكثر استخداماً لملئ جداول توجيه الموجهات بمعلومات التوجيه. ويُفضل عادةً استخدام هذه البروتوكولات مقارنة بطريقة التوجيه الثابتة لعدة أسباب:

- لأنها تساعد في تقليل الجهد الإداري المرتبط بأسلوب التوجيه الثابت والضروري لعمليات الصيانة المختلفة المطبقة على الجداول
- لأنها تسهل التفاعل مع التغييرات التي تطرأ على طبولوجيا الشبكة مما يقلل من احتمال ظهور أخطاء ناتجة عن معلومات توجيه خائطة
- لأنها تساعد على تغيير معلومات التوجيه بشكل أسرع مما لو كان التغيير سيحصل عبر تدخل مدير الشبكة

تنفذ بروتوكولات التوجيه عملها عبر تبادل معلومات التوجيه، وتتواجد الموجهات التي تعمل باستخدام نفس بروتوكول التوجيه على نفس المقطع الشبكي مما يجعلها قادرة على تبادل معلومات التوجيه باستخدام البروتوكول. ندعو مجموعة الشبكات الحاوية على موجهات تعمل باستخدام نفس بروتوكول التوجيه، "**بمجال توجيه**" البروتوكول.

ندعو مجموعة الشبكات العاملة تحت نفس السلطة الإدارية بـــ "**نظم توجيه مستقلة**". وتحتاج النظم المستقلة عند ربطها بالإنترنت للتعريف عن نفسها عبر تقديم معلومات مترابطة تساعد على الوصول للوجهات المتواجدة ضمنها. وتعتبر شبكات المؤسسات الضخمة وشبكات الجامعات وشبكات مخدمي الإنترنت أمثلة نموذجية عن نظم توجيه مستقلة.
يمكن للنظم المستقلة توظيف عدة بروتوكولات توجيه لتبادل معلومات التوجيه. ندعو البروتوكولات المستخدمة لتبادل معلومات التوجيه ضمن الأنظمة المستقلة بـــ "**بروتوكولات العبّارات الداخلية**". ولا يتعدى نطاق عمل مثل هذا النوع من البروتوكولات نظام مستقل. أما البروتوكولات المستخدمة لتبادل المعلومات بين النظم المستقلة فندعوها "**برتوكولات العبّارات الخارجية**". ويشمل مجال عملها عدة أنظمة مستقلة. ويمكن لنظام مستقل مرتبط بالإنترنت أن يستخدم برتوكول من النمط الخارجي يشمل مجاله الإنترنت بأكملها.

التوجيه بين المجالات المعتمد على عنونة دون صفوف
Classless Inter-Domain Routing (CIDR)

أدى التوسع الهائل للإنترنت وما نتج عنه من متطلبات عنونة IP، إلى الاعتماد على أسلوب عنونة دون صفوف. وبات من الواضح أن استخدام العناوين وحيدة الإسناد بات غير كافٍ نتيجة الحاجة لعدد متزايد من العناوين لربط الشبكات الجديدة المُستحدثة بالإنترنت.

لذا ظهرت طريقة جديدة لحجز العناوين IP لتنفيذ عملية التوجيه عبر الإنترنت تلت ظهور العناوين دون صفوف ودعيت CIDR.

تعتمد طرق CIDR بشكل أساسي على بروتوكولات EGP. ويعتبر مجال هذه البروتوكولات واسعاً ومعقداً ويحتاج لكتاب كامل مستقل لشرحها لذا فإننا سنبتعد عن مناقشة هذا الجانب وجميع التقنيات المتعلقة ولمزيد من المعلومات عن CIDR يمكن مراجعة الوثيقة RFC 1519 ذات العنوان:

"Classless Inter-Domain Routing (CIDR): An address Assignment and Aggregation Strategy"

والوثيقة رقم RFC 1518 ذات العنوان:

"Architecture for IP Address Allocation With CIDR"

بالإضافة للوثيقة رقم RFC 1812 التي تعطي مقدمة جيدة عن CIDR.

الترشيح

تُعتبر عملية ترشيح المعلومات المارة عبر موجه إحدى الإجرائيات النمطية للموجهات الحديثة. إذ يقرر الموجه فيما إذا كان سيقوم بإرسال رزم المعطيات الواردة باتجاه وجهتها أو إهمالها تبعاً لعوامل إدارية يتم تحديدها وتعريفها في الموجهات.

تجري عملية الترشيح عادةً بتعريف لائحة ترشيح ندعوها **لائحة ولوج** ونستخدمها كمرشح للمعلومات المتنقلة. تتكون لوائح الولوج من تعبيرات منطقية توصِّف عوامل الترشيح.

ملاحظة حول المضيفين

تحتوي كتل IP البرمجية في المضيفين على العناصر الثلاثة اللازمة لعمل الموجه:

- واجهات الشبكة
- جدول التوجيه
- محرك التوجيه

إلا أن هذه العناصر تكون أقل تعقيداً في مُضيف عنها في موجه.

يحتوي المضيغ عادةً على واجهة شبكية وحيدة بعكس الموجهات. يمتلك جدول التوجيه في مُضيف نفس بنية جدول التوجيه في موجه لكن لا يمتلك محرك التوجيه في المنصات فعالية محركات توجيه الموجهات.

يعتمد التشكيل النمطي في المضيفين على مفهوم "**العبّارة التلقائية**".

ندعو الطريق المرتبط بالعنوان التلقائي "بالطريق التلقائي".

لكل من المُضيفين والموجهات متطلبات وحاجات مختلفة. وتوصِّف الوثيقة RFC 1122 ذات العنوان:
"Requirements for Internet Hosts Communication Layer"
متطلبات المنصات بينما نجد توصيف المتطلبات الخاصة بالموجهات في الوثيقة ذات الرقم RFC 1812.

تحتوي كتل IP البرمجية في المضيفين على العناصر الثلاثة اللازمة لعمل الموجه:

- واجهات الشبكة
- جدول التوجيه
- محرك التوجيه

إلا أن هذه العناصر تكون أقل تعقيداً في مُضيف عنها في موجه.

يحتوي المضيغ عادةً على واجهة شبكية وحيدة بعكس الموجهات. يمتلك جدول التوجيه في مُضيف نفس بنية جدول التوجيه في موجه مع ملاحظة احتواء جدول التوجيه في موجه على حقول إضافية خاصة بالمُصنِّع والتي يمكن أن تحدد وبشكل كبير، نوعية التوجيه ومستوى الموجه. كما لا يمتلك محرك التوجيه في المنصات فعالية محركات توجيه الموجهات.

يشكل IP جزءاً من نظام التشغيل الموجود في مُضيف بينما يشكل المكون الرئيسي الذي يتحمل عبء العمل الأساسي ضمن موجه.

يعتمد التشكيل النمطي في المضيفين على مفهوم "**العبّارة التلقائية**". وتُعَرَّف العبّارة التلقائية على أنها عنوان موجه يستقبل ما يُحوله له المُضيف من معطيات متوجهة لمقاطع شبكية مختلفة عن المقطع الذي تتواجد فيه المنصة نفسها.

يتألف جدول التوجيه في مُضيف من قيدين. يدل الأول على طريق مباشر ويرتبط ببادئة الشبكة الممثلة للمقطع الشبكي الذي تتواجد فيه المنصة ويدل الثاني على العنوان التلقائي 0.0.0.0/0.

ندعو الطريق المرتبط بالعنوان التلقائي "بالطريق التلقائي".

لكل من المُضيفين والموجهات متطلبات وحاجات مختلفة. وتوصِّف الوثيقة RFC 1122 ذات العنوان:
"Requirements for Internet Hosts Communication Layer"
متطلبات المنصات بينما نجد توصيف المتطلبات الخاصة بالموجهات في الوثيقة ذات الرقم RFC 1812.

نشاط

استخدم تعليمة route وبالتحديد route PRINT على جهازك (العامل بنظام Windows 2000 أو WindowsXP لرية الطرق التلقائية والمباشرة الموجودة)

يمكن لتعليمة route أن تساعد في إضافة طرق جديدة

بروتوكول التحكم برسائل الخطأ في طبقة الإنترنت
Internet Control Message Protocol (ICMP)

يُعرِف البروتوكول ICMP على أنه بروتوكول مساعد يُستخدَم لجمع الأخطاء التي تظهر في طبقة الإنترنت ولإرسال رسائل تحكم مفهومة من قبل طبقة الإنترنت. ندعو وحدة المعطيات المستخدمة من قبل هذا البروتوكول بـــ "**خطأ**" أو "**رسالة تحكم**" حيث يمكن أن تحمل رسالة التحكم إعلاماً بخطأ أو معلومة تحكم.

يجري تغليف رسائل ICMP ضمن رزم معطيات IP. بمعنى آخر، يستخدم ICMP خدمة إرسال رزم المعطيات IP. وبالرغم من تموضع ICMP في طبقة الإنترنت وتواجده كجزء مكمل للبروتوكول IP إلا أنه يُعتبر بروتوكولاً مستقلاً.

ملاحظة:
يمكن النظر إلى ICMP كجزء من IP وليس كبروتوكول مستقل. في هذه الحالة، يجب اعتبار الرسائل ICMP كتكملة لرأس رسالة معطيات IP. يمكن اعتبار هذه النظرة تقيداً بنموذج الاتصال متعدد الطبقات دون أن يكون لها أي هدف آخر.

رسائل التحكم ICMP

يتموضع البروتوكول ICMP في طبقة الإنترنت.

عند استخدام ICMP للإعلام عن خطأ، يجري إرسال رسالة ICMP إلى العنوان IP الذي يظهر كعنوان مصدر المعلومات في رأس رزمة المعطيات المسببة للخطأ..

عندما تتلقى الكتل البرمجية الخاصة بالبروتوكول IP التابعة للجهاز المصدر رسالة الخطأ ICMP تقوم باتباع خطوات محددة لإعلام بروتوكولات الطبقة الأعلى بظروف الخطأ.

لجميع رسائل التحكم ICMP قسم مشترك مؤلف من ثلاثة حقول متوضعة في بداية الرسالة ICMP.

هذه الحقول الثلاثة هي التالية:

- حقل النمط (Type)
- حقل الرماز وهو (Code)
- حقل التحقق (Checksum)

بالإضافة لما سبق، تتضمن رسائل ICMP التي تقوم بالإعلام عن الأخطاء رأس رسالة المعطيات المسببة للخطأ بالإضافة إلى القسم الأول من حِمْل رزمة المعطيات السابقة والذي يبلغ طوله 64 بت.

يمكن الحصول على المعلومات التفصيلية من الوثيقة رقم RFC 792 بعنوان:

"Internet Control Message Protocol"

والوثيقة رقم RFC 1700 بعنوان:

"Assigned Numbers"

وهي آخر الوثائق المكتوبة عن هذا الموضوع.

يتموضع البروتوكول ICMP في طبقة الإنترنت مما يعني أن إرسال رسائل التحكم ICMP هو إرسال غير موثوق، حيث يمكن لهذه الرسائل أن تضيع أو أن تحمل هي نفسها أخطاء ناتجة عن عملية النقل.

عند استخدام ICMP للإعلام عن خطأ، يجري إرسال رسالة ICMP إلى العنوان IP الذي يظهر كعنوان مصدر المعلومات في رأس رزمة المعطيات المسببة للخطأ. ولا تُرسل أي رسالة خطأ إلى عنوان وجهة رسالة المعطيات.

عندما تتلقى الكتل البرمجية الخاصة بالبروتوكول IP التابعة للجهاز المصدر رسالة الخطأ ICMP تقوم باتباع خطوات محددة لإعلام بروتوكولات الطبقة الأعلى بظروف الخطأ. تجدر الإشارة إلى أن العقدة المولدة لرسالة الخطأ لا تحاول إصلاح الخطأ أو إيجاد حل للمشكلة.

لكل رسالة تحكم ICMP شكلها وهيأتها الخاصة إلا أن لجميع رسائل التحكم ICMP قسم مشترك مؤلف من ثلاثة حقول متوضعة في بداية الرسالة ICMP.

هذه الحقول الثلاثة هي التالية:

- حقل النمط (Type) وهو حقل مؤلف من 8 بت ويدل على نمط الرسالة
- حقل الرماز وهو (Code) حقل مؤلف من 8 بت يعطي معلومات إضافية عن الرسالة
- حقل التحقق (Checksum) وهو حقل مؤلف من 16 بت يُستخدم للتحقق من تكامل المعطيات المؤلفة للرسالة

بالإضافة لما سبق، تتضمن رسائل ICMP التي تقوم بالإعلام عن الأخطاء رأس رسالة المعطيات المسببة للخطأ بالإضافة إلى القسم الأول من حِمْل رسالة المعطيات السابقة والذي يبلغ طوله 64 بت.

يمكن الحصول على المعلومات التفصيلية من الوثيقة رقم RFC 792 بعنوان:

"Internet Control Message Protocol"

والوثيقة رقم RFC 1700 بعنوان:

"Assigned Numbers"

وهي آخر الوثائق المكتوبة عن هذا الموضوع.

الفصل الرابع عشر والخامس عشر

عنوان الموضوع:

خدمات أساسية في شبكات TCP/IP

الكلمات المفتاحية:

أنظر الملف Glossary المُرافق.

ملخص:

نستعرض في هذا القسم بعض الخدمات التي تنتمي إلى طبقة التطبيقات في النموذج المرجعي TCP/IP والتي تُعتبر من خدمات وتطبيقات الإنترنت. نركز في هذا القسم على خدمتين إداريتين أساسيتين في إدارة شبكات TCP/IP: خدمة الإعداد الديناميكي للمضيف، وخدمة حلّ أسماء النطاقات.

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- خدمة إعداد المضيف ديناميكياً
- خدمة حلّ أسماء النطاقات

1.14-15.1 خدمات وتطبيقات

سنركز في هذا القسم على نوعيين من الخدمات التي تحتل طبقة التطبيقات في عائلة البروتوكولات TCP/IP:

- خدمات إدارية تساعد في إدارة شبكات TCP/IP مثل خدمة الإعداد الديناميكي للمضيف وخدمة حلّ أسماء النطاقات؛
- وخدمات تطبيقية تكون عادةً موجهة للمستخدمين مثل خدمة الوب، وخدمة نقل الملفات وخدمة البريد الإلكتروني.

ملاحظة:

نُذكِّر أن استخدامنا اللاحق لكلمة بروتوكول عند إشارتنا لخدمة من الخدمات السابقة، هو استخدامٌ مبني على مفهوم البروتوكول الذي عرفناه في أقسام سابقة، والذي يدل على لغة تواصل مشتركة بين طبقتين متناظرتين من سلسلة الطبقات المكونة لنموذج شبكي طبقي. من هنا نعني ببروتوكول –في حالة أي خدمة من الخدمات السابقة– بروتوكول تطبيقي.

بروتوكول إعداد المُضيف ديناميكياً
DHCP

يُعرف البروتوكول DHCP في الوثائق RFC2131 وRFC2132، ويعتبر توسيعاً للبروتوكول BootP الذي تم تصميمه أصلاً للسماح لمحطات UNIX التي لا تمتلك أقراص صلبة بالإقلاع عن بعد.

يحمل BootP للزبون الذي يرغب بالإقلاع: العنوان IP، وقناع الشبكة، والعبّارة الإفتراضية والمعلومات اللازمة لخدمة نقل الملفات TFTP التي تلزمه لتنفيذ عملية نقل المعطيات الخاصة بنظام تشغيله من المخدم إلى ذاكرته ليتسنى له استكمال الإقلاع. يدعم البروتوكول DHCP هذه المعاملات، ويضيف إليها مفهوم "**الحجز**".

بروتوكول إعداد المُضيف ديناميكياً:
خطوات العمل

1. يبدأ زبون DHCP تعاطيه مع المخدم بإرسال بث يحمل رسالة "النجدة! من أنا؟"
2. في حال وجود مخدم DHCP على الشبكة المحلية، يقوم هذا الأخير بالتفاوض مع الزبون لحجز عنوان IP خاص به وتوفير المعاملات الشبكية الأخرى (قناع الشبكة ومعلومات عن مخدم الأسماء بالإضافة إلى العبّارة الافتراضية)
3. اما في حال عدم وجود مخدم DHCP على الشبكة المحلية، فيمكن للمخدمات الموجودة على شبكات فرعية أخرى أن تتلقى البث المُرسل من الزبون من خلال وكيل ندعوه "**عميل إيصال طلبات DHCP**" يكون مثبتاً على الشبكة المحلية للزبون
4. يبدأ الزبون بالعمل اعتماداً على المعاملات الشبكية التي تلقاها من المخدم. وبعد مرور فترة زمنية مساوية لنصف فترة حجز المعاملات الآنفة الذكر، يطلب تجديد الحجز. يكون الطلب هذه المرة معتمد على اسلوب اتصال نقطة لنقطة، وليس على البث، فالزبون والمخدم يملكان إعدادات شبكية كاملة؛ بالتالي، يكون المخدم مجبراً على الاحتفاظ بالعناوين التي قام بحجزها وبالزبائن التي حجز لهم هذه العناوين بحيث تبقى هذه المعلومات ثابتة عند إعادة إقلاع المخدم طالما أنها ضمن فترة الحجز
5. في حال كان المخدم موجوداً، يجري تجديد الحجز لفترة زمنية مساوية لفترة الحجز

6. أما في حال وجود عطل، أو توقُف طارئ للمخدم، يستمر الزبون في عمله دون تجديد ويعاود إرسال طلب تجديد الحجز بعد مرور فترة زمنية مساوية لأكثر من ثلاثة أرباع فترة حجز المعاملات التي يعمل بها
7. في حال كان المخدم قد عاد للعمل، يجري تجديد الحجز لفترة زمنية مساوية لفترة الحجز
8. أما في حال استمرار التوقف، يستمر الزبون في العمل حتى انتهاء فترة الحجز، ويتخلى عندها عن إعداداته، ويعيد إرسال بث يحمل رسالة "النجدة! من أنا؟" بحثاً عن مخدم جديد DHCP (عودة للبند الأول)

بروتوكول إعداد المُضيف ديناميكياً:

ملاحظات

1. يتعامل مخدم DHCP بشكل مباشر مع الزبائن المتواجدين على نفس مقطعه الشبكي. ويحتاج الزبائن المتواجدون على مقطع شبكي آخر لوكيل DHCP متصل بالمقطعين لإيصال طلباتهم. يعود السبب في ذلك إلى استخدام أسلوب البث –كما لاحظنا في خطوات العمل– في بداية إقلاع الزبون عندما يفتقد لأي إعدادات شبكية، وإلى عدم إمكانية تمرير البث عبر الموجهات التي تصل بين عدة مقاطع شبكية.
2. يسمح البروتوكول لزبون DHCP بحجز معاملات شبكية إدارية اعتباراً من مخدم مركزي مسموح له بالعمل ومسموح له بتوزيع هذه المعاملات. ويناسب إجراء الحجز عمل الحواسب الشخصية التي لا تعمل بشكل دائم، أو مزودي الخدمة الذين يتعاملون مع زبائن يتصلون بهم مؤقتاً عبر اتصال هاتفي. تتضمن المعاملات القابلة للحجز:
   a. العناوين IP وأقنعة الشبكات الفرعية
   b. العبّارات (طرق تلقائية)
   c. مخدمات الأسماء (DNS)
   d. بالإضافة إلى العديد من المعاملات الأخرى (يمكن الإطلاع على الوثيقة RFC2132).
3. يبدأ زبائن DHCP بمفاوضات مع مخدم DHCP باستخدام عنوان عمومي للبث تكون جميع البتات فيه مساوية للواحد إذ لا يكون عندها الزبون على علم بشبكة أو بأقنعة الشبكات الفرعية لذلك لا يمكن له استخدام عناوين البث الشبكية.
4. يمتلك مخدم DHCP ميزة إجراء حجز معاملات IP بشكل دائم من أجل عنوان MAC (عنوان بطاقة شبكية خاصة بعقدة شبكية). يؤدي هذا الحجز إلى جعل العقدة تحصل على نفس العنوان دائماً، وإلى عدم حصول أي عقدة أخرى على هذا العنوان.
5. من المفضل استخدام الإعدادات الشبكية الديناميكية مع المُضيفين والإبقاء على إعدادات المخدمات يدوية (حتى ولو كان بإمكاننا حجز عنوان على نحو دائم).
6. لا يسبب الاعتماد على مخدم DHCP لتوزيع العناوين عبأً كبيراً على الشبكة نظراً لصغر حجم الرزم المتبادلة.

نشاط

خطوات إعداد مخدم DHCP على نظام Windows

يحتاج هذا النشاط للعمل على نظام Windows 2000 Server أو Windows 2003 Server حتى يتسنى تثبيت مخدم DHCP المرافق لنظام تشغيل Windows.

1. اذهب إلى Control Panel
2. اضغط على أيقونة Add Remove Software
3. اذهب إلى زر Add Remove Windows Component
4. اذهب إلى Networking Services
5. اختر Dynamic Host Configuration Protocol واطلب تثبيته
6. عند الانتهاء من التثبيت ستظهر أيقونته في الـ Administrative Tools
7. شغِّل الأداة
8. اضغط بالزر اليميني على Local Host وأضف مجال عناوين جديد ضمن النافذة التي تظهر؛ تتضمن المعاملات: مجال العناوين، القناع، المجال الزمني للحجز. يمكن (تبعاً لنسخة Windows Server المُستخدمة) أن يظهر مُساعد يطلب المعاملات بالتدريج عوضاً عن ظهور النافذة؛ ضع المعاملات التي تناسب شبكتك
9. لاحظ أنه بإمكانك عزل مجال جزئي من مجال العناوين الذي اخترته للتوزيع بحيث لا يوزعه المخدم
10. ابحث عن نافذة إضافة عملية حجز Reservation وحدد عنوان IP من المجال واربطه بشكل دائم بعنوان MAC من عناوين البطاقات الشبكية التي تستخدمها على أحد حواسبك
11. ابحث عن النافذة التي تسمح لك بتحديد مخدم DNS (سندرسه لاحقاً) لشبكتك أو أي نوع من المخدمات الأخرى (إذا لم يكن المساعد قد طلب منك هذا الطلب أثناء مساعدتك في إعداد المخدم تدريجياً، إذ يتعلق الأمر بنسخة Windows Server المُستَخدَمة)
12. عليك الآن أن تنهي إعداداتك بجعل المضيفين يعتمدون على هذا المخدم. يتم ذلك اعتباراً من الإعدادات الشبكية لكل حاسب من الحواسب؛ اجعل الحواسب تعتمد على مخدم DHCP وذلك بتعديل واجهة الإعدادات الشبكية التي تصلها اعتباراً من لوحة التحكم Control Panel، ومن ثم Network Connections، تليها Local Area Network وأخيراً TCP/IP.
13. أعد إقلاع أحد المضيفين بعد إعداده ليتلقى عناوينه من مخدم DHCP
14. افتح نافذة Command Prompt ونفذ التعليمة التالية:

```
ipconfig /all
```

15. اقرأ النتائج، ستلاحظ أن المضيف قد أخذ معاملات من المخدم DHCP الذي أعددته سابقاً
16. نفذ التعليمة:

```
ipconfig /release
```

من ثم أعد تنفيذ التعليمة:

```
ipconfig /all
```

ستلاحظ أن الإعدادات قد ذهبت وأن المضيف يمتلك الآن العنوان 0.0.0.0.

17. نفذ التعليمة:

```
ipconfig /renew
```

من ثم أعد تنفيذ التعليمة:

```
ipconfig /all
```

ستلاحظ أن المضيف قد حصل على إعدادات جديدة.

18. أخيراً، برأيك، ماهي فوائد استخدام مخدم DHCP لإعداد المضيفين عوضاً عن اعتماد الإعدادات اليدوية؟

نظام أسماء المجالات (النطاقات)

إن وجود المليارات من المضيفين المتصلين بالإنترنت يجعلنا نطرح سؤالاً مهماً عن كيفية الاحتفاظ بأثر عنهم رغم انتمائهم إلى بلدان مختلفة وإلى شبكات وسلطات إدارية متنوعة!

يتلخص الجواب على السؤال السابق في نظامين مفتاحيين: نظام أسماء المجالات الذي يحتفظ بأثر عن هوية المضيفين ونظام توجيه الإنترنت الذي يحتفظ بأثر عن أسلوب وصلهم.

يتمحور هذا الجزء حول نظام DNS. فبالرغم من أن DNS قد أُنشأ ليحقق عدة أهداف إلا أن هدفه الأول يتلخص في تثبيت العلاقة بين أسماء المضيفين والعناوين IP. ففي الوقت الذي يستخدم فيه المستثمر وبرامجه أسماء المنصات، تعتمد البرمجيات في المستوى الأخفض على العناوين IP للدلالة على الأجهزة. بالنتيجة، يقدم DNS ما يلزم لتشغيل كلا المستويين. كما يلعب دوراً مهماً في عملية توجيه البريد الإلكتروني وفي عمليات الوصول إلى مخدمات الويب.

يعتبر نظام DNS، نظام قواعد معطيات موزعة. وتعني كلمة "**موزعة**" بأن يقوم كل موقع بتخزين المعطيات عن حواسبه وبأن تقوم المواقع بالتعاون أوتوماتيكياً والمشاركة في المعطيات عندما تحتاج إحدى المواقع للبحث عن معطيات تنتمي لموقع آخر.

تاريخ نظام DNS

- كانت عملية الربط بين أسماء المضيفين والعناوين تجري سابقاً اعتماداً على ملف نصي يُدار على نحو مركزي
- أتى DNS كحل للمشاكل الناجمة عن الملف النصي الثابت عبر استخدامه لمفهومين أساسيين: أسماء هرمية للمضيفين ومسؤولية موزعة
- قام Paul Mackapetris بتوصيف DNS على نحو صوري في الوثيقة RFC 882 وفي الوثيقة RFC 883 في عام 1983، كما قام Paul بالتحقيق البرمجي لنسخة NS
- جرى تنفيذ العمل الأصلي تحت نظام UNIX في عام 1984 من قبل أربعة طلاب كانوا يحضرون لشهادة الدكتوراه في جامعة Berkeley
- في عام 1985 نفذ أحد مهندسي شركة DEC وهو Kevin Dunlap نسخة BIND (Berkeley Internet Name Damain System)
- نفذت شركة Nortel مع ISC نسخة BIND على Windows وبات لنظام BIND نسخته التي لا تخص UNIX والتي لها أسم DNS
- قدمت Microsoft أيضاً مخدم DNS مع نظام Windows 2000 ولكن نسخة Microsoft تمتلك خصوصية واختلافات.
- يوجد أكثر من 30 وثيقة RFC أخرى تتناول نسخ متعددة من البروتوكول بالإضافة إلى توصيفها لصيغ المعطيات التي يديرها البروتوكول

كانت عملية الربط بين أسماء المضيفين والعناوين تجري سابقاً اعتماداً على ملف نصي يُدار على نحو مركزي وبحيث يجري توزيعه على جميع المضيفين في شبكة ARPANET.

لم تكن أسماء المضيفين ذات بنية هرمية، وكانت إجرائية تسمية حاسوب تتضمن التحقق من عدم وجود هذا الاسم في مكان آخر من الشبكة، كما كانت الملفات بحاجة للتحديث على نحو مستمر.

لقد بات واضحاً في تلك الفترة أنه وبالرغم من أن الجدول الثابت الخاص بالمضيفين يعتبر حلاً معقولاً بالنسبة للشبكات الصغيرة، إلا أنه حل غير مناسب لشبكة ARPANET التي كانت في طور التطور والتوسع. وقد أتى DNS كحل للمشاكل الناجمة عن الجدول الثابت عبر استخدامه لمفهومين أساسيين: أسماء هرمية للمضيفين ومسؤولية موزعة.

قام Paul Mackapetris بتوصيف DNS على نحو صوري في الوثيقة RFC 882 وفي الوثيقة RFC 883 في عام 1983، وتم تعديل التوصيف في عام 1987 بالوثيقتين RFC 1034 وRFC 1035 كما قام Paul بالتحقيق البرمجي لنسخة DNS ولكن النسخة لم تكن تخص نظام UNIX.

جرى تنفيذ العمل الأصلي تحت نظام UNIX في عام 1984 من قبل أربعة طلاب كانوا يحضرون لشهادة الدكتوراه في جامعة Berkeley وهم: Douglas Terry ، وMark Painter، و David Riggle ، وSongnian Zhou. وجرت إضافته إلى نظام BSD من قبل Ralph Campbell الباحث في مجموعة الأبحاث الخاصة بأنظمة الحواسيب في جامعة Berkeley.

في عام 1985 نفذ أحد مهندسي شركة DEC وهو Kevin Dunlap نسخة BIND (Berkeley Internet Name Damain System) وجرت إدارتها لعدة سنوات من قبل Mike Karels وPhil Almquist وPaul Vixie. كما أُضيف BIND لمعظم أنظمة UNIX وLINUX وهو يتوفر على الموقع www.isc.org، وهو موقع التجمع الخاص ببرمجيات الإنترنت ISC (Internet Software Consortium) والذي يمثل الهيئة التي تدير العديد من برمجيات الإنترنت الأساسية بما في ذلك BIND.
وقد طورت ISC عدة أنظمة BIND9 بمساعدة العديد من المنتجين ومن الهيئات الحكومية وغيرها. كما توفر ISC عدة أنماط من الدعم لهذه المنتجات بما في ذلك المساعدة على إعدادها بالإضافة إلى عمليات البرمجة التي تخص بعض أجزاء الأنظمة التي تجري ملاءمتها مع حاجات المستثمرين. ويجري تقديم هذه الخدمات للمواقع التي لها اتصال مع الهيئة وتستخدم الدعم الذي تقدمه عبر البرمجيات ذات الرماز المفتوح الخاص بالهيئة.

نفذت شركة Nortel مع ISC نسخة BIND على Windows وبات لنظام BIND نسخته التي لا تخص UNIX والتي لها أسم DNS والتي تتميز بتوافقها الكامل مع أنظمة BIND على UNIX بفضل تقييس البروتوكول DNS. تُشغل الكثير من المواقع أنظمة UINX لتوفير خدمة DNS لحواسب Windows وتعمل هذه الخدمة على نحو جيد دون مشاكل. وقد قدمت Microsoft أيضاً مخدم DNS مع نظام Windows 2000 ولكن نسخة Microsoft تمتلك خصوصية واختلافات فهي تتعامل مع BIND ولكنها تملئ الشبكة بطرود غير ضرورية أو غير متوافقة مع الأشكال المعيارية للطرود.

ماتزال الوثائق RFC 1034 وRFC 1035 تشكل الأساس في توصيف نظام DNS ولكن يوجد أكثر من 30 وثيقة RFC أخرى تتناول نسخ متعددة من البروتوكول بالإضافة إلى توصيفها لصيغ المعطيات التي يديرها البروتوكول، وقد ظهرت هذه الوثائق في العقد الأخير.

نشاط

ابحث عن الملف hosts أو مايكافئه على نظام التشغيل الذي تعمل عليه.
(إذا كنت تعمل على Windows 2000 يكون الملف موجوداً في مجلد %SystemRoot%\System32\drivers\etc أما على أنظمة Linux فهو موجود في مجلد etc/).

انظر إلى محتوى الملف، وأضف أسماء مضيفين على الشبكة ونفذ عملية التحقق من الاتصال بهم عبر الأسم باستخدام تعليمة Ping.

من يحتاج لنظام DNS؟

يُعرِّف نظام DNS:

- فضاء أسماء هرمي خاص بالمضيفين وبالعناوين IP
- جدول بالمضيفين منجز على شكل قاعدة معطيات موزعة
- مكتبة إجرائيات حل "resolver" للاستعلام والاستفهام من قاعدة المعطيات
- عملية توجيه للبريد الإلكتروني
- آلية استكشاف خدمات شبكية
- بروتوكول لتبادل المعلومات الخاصة بالأسماء

تحتاج المواقع الموطنة على نحو كامل في الإنترنت لنظام DNS.

يحتفظ كل موقع بقطعة أو بعدة قطع من قاعدة المعطيات الموزعة التي تشكل قاعدة معطيات نظام DNS العالمي.

يعتمد نظام DNS في عمله على مبدأ زبون/ مخدم.

في حال كانت المؤسسة صغيرة (عدة مضيفين على شبكة وحيدة)، يمكن تشغيل المخدم على أحد المضيفين أو توجيه طلب إلى مزود الخدمة لتوفير خدمة DNS عوضاً عن المؤسسة.

أما المواقع ذات الحجوم المتوسطة مع عدة شبكات فرعية فتحتاج لتشغيل عدة مخدمات DNS لتخفيض عدد الاستفهامات على مخدم واحد .

أما المواقع الكبيرة فيمكن تقسيم المجال DNS الخاص بها إلى مجالات فرعية وتشغيل عدة مخدمات من أجل كل مجال فرعي.

يُعرِّف نظام DNS:

- فضاء أسماء هرمي خاص بالمضيفين وبالعناوين IP
- جدول بالمضيفين منجز على شكل قاعدة معطيات موزعة
- مكتبة إجرائيات حل "resolver" للاستعلام والاستفهام من قاعدة المعطيات
- عملية توجيه للبريد الإلكتروني
- آلية استكشاف خدمات شبكية
- بروتوكول لتبادل المعلومات الخاصة بالأسماء

تحتاج المواقع الموطنة على نحو كامل في الإنترنت لنظام DNS فإدارة ملف /etc/hosts لتنجيز عملية ربط أسماء المضيفين بالعناوين IP ليس كافياً لمن يريد الاتصال بغيره عبر الإنترنت.

يحتفظ كل موقع بقطعة أو بعدة قطع من قاعدة المعطيات الموزعة التي تشكل قاعدة معطيات نظام DNS العالمي.

- تتألف القطعة التي تخص موقع ما من ملفين نصيين أو أكثر يحتويان على تسجيلات لكل مضيف من المضيفين.
- يتكون كل تسجيل من سطر وحيد يتألف من اسم (عادةً، اسم مضيف) ومن نمط تسجيل، وبعض قيم المعطيات.

يعتمد نظام DNS في عمله على مبدأ زبون/ مخدم. تقوم المخدمات (مخدمات الأسماء) بتحميل المعطيات من ملفات DNS إلى الذاكرة وتقوم باستخدامها في الرد على استفهامات الزبائن الداخليين أو المخدمات الأخرى الموجودة على الإنترنت. كما يجب على جميع المضيفين أن يمتلكوا زبائن DNS في حين لا نحتاج إلا إلى عدد ضئيل من المخدمات DNS.

في حال كانت المؤسسة صغيرة (عدة مضيفين على شبكة وحيدة)، يمكن تشغيل المخدم على أحد المضيفين أو توجيه طلب إلى مزود الخدمة لتوفير خدمة DNS عوضاً عن المؤسسة. أما المواقع ذات الحجوم المتوسطة مع عدة شبكات فرعية فتحتاج لتشغيل عدة مخدمات DNS لتخفيض عدد الاستفهامات على مخدم واحد والتي تؤدي لخفض أدائه. أما المواقع الكبيرة فيمكن تقسيم المجال DNS الخاص بها إلى مجالات فرعية وتشغيل عدة مخدمات من أجل كل مجال فرعي.

ما الجديد في نظام DNS؟

هناك عدة تغييرات ذات معنى جرى تحقيقها على DNS في السنوات الأخيرة. يعرض الجدول التالي بعض التغييرات والخصائص الجديدة لنظامي DNS وBIND.

وثيقة RFC	الميزة
2052	تسجيلات SRV لتحديد مواقع الخدمات.
-	تسجيلات A6 لتمثيل عناوين IPV6.
2672-3	تسجيلات DName لعمليات البحث وإعادة التحويل IPV6.
-	إجرائيات الحل الخاصة بعناوين IPV6.
2136	تعديلات ديناميكية (للمواقع التي تستخدم DHCP).
2535-51	DNSSEC، التحقق والأمان الخاص بمعطيات منطقة.
2845	TSIG/TKET توقيع المبادلات وتبادل المفاتيح.

يدعم BIND9 أقسام IPV6 التي جرى تقييسها ولكن يبدو أن نشر IPV6 على نحو واسع لن يكون قريباً.

أما القياس DNSSEC فيسعى لإضافة عملية تحقق على قاعدة معطيات DNS وعلى مخدماتها.

يعتبر DNS مقدمة لمجال أسماء عالمي سيسمح للبلدان التي لا تستخدم الإنكليزية بتعريف أسماء اعتماداً على حروفها الأبجدية ولغتها الخاصة.

تزيد كلٌ من هذه المشاكل الثلاث (IPV6 وDNSSEC والتدويل) من حجم تسجيلات المعطيات الخاصة بنظام DNS وتجعلها غير قادرة على البقاء محدودة في إطار حجوم الطرود UDP.

هناك عدة تغييرات ذات معنى جرى تحقيقها على DNS في السنوات الأخيرة. إذ يجري تعديل كل من نظامي DNS وBIND باستمرار حيث بات DNS يمتلك عدة أنماط جديدة من التسجيلات وعدة خصائص بالإضافة إلى عدة تغييرات متعلقة بالبروتوكول. وقد جرت إعادة تصميم BIND وجرت إعادة صياغته بحيث بات يمتلك دعماً لأنظمة التشغيل متعددة الإجراءات ومتعددة المسالك. على كل حال، تعتبر بعض هذه الميزات بمثابة مشاريع ضخمة خاصة بهيئة IETF ولم تنتهي منها بعد.

يدعم BIND9 أقسام IPV6 التي جرى تقييسها ولكن يبدو أن نشر IPV6 على نحو واسع لن يكون قريباً.

أما القياس DNSSEC فيسعى لإضافة عملية تحقق على قاعدة معطيات DNS وعلى مخدماتها. يستخدم DNSSEC مفتاح تشفير عام للتحقق من مصدر وصحة معطيات DNS ويستخدم DNS لتوزيع المفاتيح ومعطيات المضيف.
لقد جرى إدخال آلية تحقق بسيطة تعتمد على مبدأ "السر المشترك". على كل حال، يجب أن يكون "السر المشترك" موزعاً على كل زوج من المخدمات التي تود القيام بتحقق متبادل. بالرغم من أن هذا ممكن في موقع محلي فإنه يستحيل توسيعه على مستوى الإنترنت. يقدم BIND9 تنجيزاً لنظام المفتاح العام DNSSEC ولنظام السر المشترك وتوقيع المبادلات TSIG (Transaction Signature).

كما يعتبر DNS مقدمة لمجال أسماء عالمي سيسمح للبلدان التي لا تستخدم الإنكليزية بتعريف أسماء اعتماداً على حروفها الأبجدية ولغتها الخاصة.

وتزيد كلٌ من هذه المشاكل الثلاث (IPV6 وDNSSEC والتدويل) من حجم تسجيلات المعطيات الخاصة بنظام DNS وتجعلها غير قادرة على البقاء محدودة في إطار حجوم الطرود UDP.

فضاء الأسماء DNS

يُعرَّف فضاء الأسماء DNS على أنه شجرة من "المجالات" (domains). يمثل كل مجال، قسماً من فضاء الأسماء وتتم إدارته من قبل كيان إداري وحيد.

ندعو جذر شجرة الأسماء بالنقطة أو "."، ولكل شجرة أسماء فرعينك

- يقوم الأول بربط أسماء المضيفين إلى عناوين IP، ويدعى بفرع "**الربط المباشر**" وندعو ملفاته "**بملفات المنطقة المباشرة**"
- في حين يقوم الفرع بربط عناوين IP عكسياً بأسماء مضيفين ويُدعى فرع "**الربط المعكوس**" وندعو ملفاته "**بملفات المنطقة المعكوسة**"

ندعو مجالات المستوى الأعلى **مجالات المستوى الأول العمومية** GTLDs (Generic Top-Level Domains). في الجدول التالي، تعبر المجالات الموجودة في العمود اليميني عن المجالات الأصلية التي تعود إلى عام 1988 بينما يعرض العمود اليساري المجالات الحديثة المضافة عام 2001.

المجال	مخصص لـــ	المجال	مخصص لـــ
com	الشركات التجارية	aero	صناعة النقل الجوي
edu	المعاهد التدريسية	biz	التجارة والأعمال
gov	المكاتب الحكومية	coop	التعاونيات
mil	المكاتب العسكرية الأمريكية	info	استخدام غير محدد
net	مزودي الشبكات	museum	المتاحف
org	هيئات غير ربحية	name	الأشخاص
int	هيئات دولية	Pro	محاسبون، محامون.... الخ
arpa	الهيئة المعتمدة لشجرة العناوين IP		

تبني بعض البلدان خارج الولايات المتحدة بنية تنظيمية هرمية بمستوى ثان من المجالات. ويتغير اصطلاح التسمية:

الرمز	البلد	الرمز	البلد	الرمز	البلد
au	أستراليا	Fi	فلندا	hk	هونغ كونغ
ca	كندا	Fr	فرنسا	Ch	سويسرا
br	البرازيل	Jp	اليابان	mx	المكسيك
de	ألمانيا	Se	السويد	hu	هنغاريا

تكون أسماء المجالات غير حساسة لشكل الأحرف (كبيرة أو صغيرة) فاسم "SVU" مطابق لإسم "svu" ولإسم "Svu" في نظام DNS.

يتشكل **اسم كامل ومؤهل** خاص بمضيف (Fully Qualified) من اسم المجال مدموجاً مع اسم المضيف الأصلي. فعلى سبيل المثال، يكون mail.svuonline.org اسماً كاملاً مؤهلاً للمضيف mail في الجامعة الإفتراضية.

من الشائع أن يمتلك مضيف أكثر من اسم. إذ يمكن أن يكون المضيف Host.svuonline.org أن يكون معروفاً باسم mail.svuonline.org أو www.svuonline.org إذا أردنا جعل الاسم يعكس الخدمات التي يقدمها المضيف.

يُعرَّف فضاء الأسماء DNS على أنه شجرة من "المجالات" (domains). يمثل كل مجال، قسماً من فضاء الأسماء وتتم إدارته من قبل كيان إداري وحيد.

ندعو جذر شجرة الأسماء بالنقطة أو ".". يتوضع هذا الجذر في مستوى المجالات الأعلى (مستوى الجذر أو root-level). وقد جرى تثبيت مجالات المستوى الأعلى تاريخياً إلا أن ICANN (وهي مجلس الإنترنت المؤهل لإسناد العناوين والأسماء) وافقت على إدخال سبعة مجالات جديدة في عام 2001 وهم: biz، info، name، museum، aero وcoop.

لكل شجرة أسماء فرعين، يقوم الأول بربط أسماء المضيفين إلى عناوين IP في حين يقوم الفرع الثاني بالعملية المعاكسة ويربط عناوين IP عكسياً بأسماء مضيفين. ندعو الفرع الأول بفرع "**الربط المباشر**" وندعو ملفات المعطيات الحاوية على ثنائيات الربط (أسم، عنوان) "**بملفات المنطقة المباشرة**"، في حين ندعو الفرع الثاني بفرع "**الربط المعكوس**" وندعو ملفاته "**بملفات المنطقة المعكوسة**".

يُستخدم نمطان من أسماء المجالات الخاصة بالمستوى الأعلى حالياً. ففي الولايات المتحدة، تعبر مجالات المستوى الأعلى عن بنى تنظيمية وسياسية وجرى إعطاؤها أسماء مؤلفة من ثلاثة حروف مثل com وedu. وتُستخدم بعض هذه المجالات (مثل com، org وnet) خارج الولايات المتحدة الأمريكية أيضاً، وندعو هذه المجالات **مجالات المستوى الأول العمومية** (Generic Top- GTLDs Level Domains).

يُستخدم رمز مؤلف من حرفين ويدل على البلد من أجل جميع المجالات الموجودة خارج الولايات المتحدة. تتعايش أسماء مجالات المستويات العليا الجغرافية والتنظيمية سوياً ضمن نفس فضاء الأسماء العام.

تبني بعض البلدان خارج الولايات المتحدة بنية تنظيمية هرمية بمستوى ثان من المجالات. ويتغير اصطلاح التسمية. فعلى سبيل المثال، يمكن لمعهد تدريسي أكاديمي أن يكون ضمن المجال edu في الولايات المتحدة أو ضمن المجال JP في اليابان.

قام العديد من المرتزقة بشراء فضاءات أسماء كاملة خاصة بدول أو بغيرها. فعلى سبيل المثال، جرى تسويق مجال Moldovia "md" وبيعه لأطباء وسكان ولاية Maryland، (MD) الأمريكية. ولم يقتصر الأمر على هذا بل تعداه إلى بلدان أخرى مثل Tonga التي لها الرمز "to".

كما كانت عمليات السطو على أسماء المجالات، عمليات دارجة: إذ قام العديد من المهتمين بتسجيل أسماء كانوا يعتقدون بأنها ستكون مطلوبة في المستقبل ومن ثم كانوا يقومون بإعادة بيعها لأشخاص آخرين لهم علاقة بالمجال محققين أرباحاً من عمليات البيع. إذ يمكن أن تصل قيمة اسم جيد في المجال com إلى عدة آلاف أو عدة ملايين من الدولارات حيث جرى بيع business.com بمبلغ $3.5M.

تكون أسماء المجالات غير حساسة لشكل الأحرف (كبيرة أو صغيرة) فاسم "SVU" مطابق لإسم "svu" ولإسم "Svu" في نظام DNS. كما يقوم نظام DNS بإهمال الفرق بين الحروف الكبيرة والصغيرة إلا أنه يقوم بنشرها على حالها في حال وجودها. ففي الماضي، كان استخدام الحروف الكبيرة شائعاً في مجالات المستويات العليا واستخدام الحرف الأول كحرف كبير في مجالات المستويات الثانية. أما في أيامنا هذه فقد بات من المتعارف عليه استخدام الأحرف الصغيرة.

يتشكل **اسم كامل ومؤهل** خاص بمضيف (Fully Qualified) من اسم المجال مدموجاً مع اسم المضيف الأصلي. فعلى سبيل المثال، يكون mail.svuonline.org اسماً كاملاً مؤهلاً للمضيف mail في الجامعة الإفتراضية. يمكن لمواقع أخرى أن تستخدم اسم المضيف mail دون تعارض مع الاسم السابق وذلك لاختلاف الاسمين الكاملين المؤهلين. وتنتهي الأسماء الكاملة المؤهلة ضمن نظام DNS، بنقطة مثل .mail.svuonline.org. ويشير اختفاء النقطة الأخيرة إلى عنوان نسبي. إذ قد نحتاج لإضافة مكونات إضافية تبعاً للسياق الذي يجري فيه استخدام العنوان النسبي.

من الشائع أن يمتلك مضيف أكثر من اسم. إذ يمكن أن يكون المضيف Host.svuonline.org أن يكون معروفاً باسم mail.svuonline.org أو www.svuonline.org إذا أردنا جعل الاسم يعكس الخدمات التي يقدمها المضيف. وفي الحقيقة، تعتبر هذه العملية جيدة وخصوصاً أنها تجعل الخدمات مثل www، والبريد الإلكتروني mail خدمات متحركة تسمح بتحريك الخدمة من جهاز إلى آخر دون تغيير الاسم الأصلي للجهاز. يتم إسناد أسماء إضافية اعتماداً على تسجيل مُعرِّف يدعى CNAME ضمن نظام DNS.

يجب تحقيق التنسيق مع مدراء المجال الأعلى عند إنشاء مجال جزئي جديد لتأمين إحادية هذا المجال الجزئي. وتقوم القيود الموجودة في ملفات الإعداد الخاصة بالمجال الأب بتوكيل سلطة إدارة فضاء أسماء المجال الجزئي لمدراء المجال الجزئي.

إدارة المجالات

جرت سابقاً عملية إدارة مجالات المستوى الأعلى com وorg وnet وedu من قبل Network Solutions بتوكيل من National Science Foundation.

جرى حالياً السماح لمنظمات أخرى بتسجيل أسماء مجالات في المستوى gTLDs.

يوفر مزودو الخدمة خدمة مباشرة لتسجيل الأسماء.

بالرغم من إمكانية دفع مبلغ أصغر عبر التعامل المباشر مع القائمين على عملية التسجيل لتشغيل مخدم DNS، إلا أن الاعتماد على مزود الخدمة يجعل الزبون يفقد السيطرة والتحكم على مجاله. وحتى لو قرر الزبون إدارة خدمة DNS الخاصة به، فإنه يحتاج للتنسيق مع مزود الخدمة الذي يمر عبره إلى الإنترنت.

يجب أن تعتمد مجالات DNS على مخدمين على الأقل (انظر الوثيقة RFC 1219) وتتمثل إحدى الحلول في إدارة مخدم DNS الأساسي من قبل المؤسسة نفسها وترك مزود الخدمة يدير مخدماً احتياطياً.

كما يجب عدم وضع جميع مخدمات DNS على نفس الشبكة، فعندما يتوقف DNS عن العمل، تتوقف الشبكة فعلياً بالنسبة للمستثمرين.

جرت سابقاً عملية إدارة مجالات المستوى الأعلى com وorg وnet وedu من قبل Network Solutions بتوكيل من National Science Foundation. إلا أن هذا الحل الاحتكاري قد تغير حالياً وجرى السماح لمنظمات أخرى بتسجيل أسماء مجالات في المستوى gTLDs. أما مجالات المستويات العليا الأخرى مثل المجالات الخاصة بالبلدان فتتم إدارتها من قبل منظمات محلية.

هناك العديد من الاقتراحات التي تسمح للشركات الخاصة بإدارة مجالات المستويات العليا الخاصة بها. ومن المرجح أن تتوفر مجالات إضافية في المجالات العليا في المستقبل القريب. يمكن لهذا الغرض مراجعة www.cann.org للحصول على آخر المعلومات عن هذا الموضوع.

يوفر مزودو الخدمة خدمة مباشرة لتسجيل الأسماء. ويتعامل مزودو الخدمة مع سلطة إدارة المجال الأعلى على نحو شفاف بحيث يجري تأهيل مخدمات DNS للتعامل مع عمليات البحث عن الأسماء ضمن كل المجالات. وبالرغم من إمكانية دفع مبلغ أصغر عبر التعامل المباشر مع القائمين على عملية التسجيل لتشغيل مخدم DNS، إلا أن الاعتماد على مزود الخدمة يجعل الزبون يفقد السيطرة والتحكم على مجاله. لذا تلجأ إلى هذا الحل المؤسسات الصغيرة التي لاتملك الكادر الكافي لإدارة مخدمها. على كل حال، حتى لو قرر الزبون إدارة خدمة DNS الخاصة به، فإنه يحتاج للتنسيق مع مزود الخدمة الذي يمر عبره إلى الإنترنت.

يجب أن تعتمد مجالات DNS على مخدمين على الأقل (انظر الوثيقة RFC 1219) وتتمثل إحدى الحلول في إدارة مخدم DNS الأساسي من قبل المؤسسة نفسها وترك مزود الخدمة يدير مخدماً احتياطياً. فبعد إعداد النظام تقوم مخدمات مزود الخدمة بتحميل الإعدادات أوتوماتيكياً من مخدم الزبون الأساسي. ويتم عكس التغييرات التي تتم في المخدم الأساسي أوتوماتيكياً على المخدم الاحتياطي.

كما يجب عدم وضع جميع مخدمات DNS على نفس الشبكة، فعندما يتوقف DNS عن العمل، تتوقف الشبكة فعلياً بالنسبة للمستثمرين.

اختيار اسم مجال

تعتبر بعض الأسماء ممنوعة كحال الأسماء المستخدمة من قبل الآخرين والمسجلة كأسماء مملوكة. وقد تم السماح لأسماء كانت تعتبر ممنوعة سابقاً مثل أسماء مؤلفة من تشكيل لأسماء مجالات في المستوى الأعلى edu.com.

عادةً، ننصح باستخدام أسماء قصيرة سهلة الإدخال وتُعرِّف بشكل جيد عن مؤسستك. على كل حال، تكمن المشكلة في أيامنا هذه في أن جميع الأسماء الجيدة والقصيرة والمعبرة قد تم حجزها وخصوصاً في المجال com.

تنصح الوثيقة RFC 1032 بألا تكون أسماء المستوى الثاني أطول من 12 حرف. إلا أن خدمة DNS تسمح حالياً باستخدام أسماء بطول يتراوح بين 63 حرف إلى 255 حرف من أجل كل مكون من مكونات الاسم الكامل. على كل حال، يعود السبب الأساسي في احترام نصيحة الوثيقة إلى ضرورة وضع أسماء سهلة الإدخال.

المجالات غير المُنَظَمة

جرى تصميم DNS لربط اسم مجال يخص هيئة إلى اسم مخدم تملكه هذه الهيئة. وكنا بالتالي نحتاج لتوسيع الخدمة لتشمل المؤسسات والهيئات العالمية. إلا أن التوسع الهائل الذي شهدته الإنترنت جعل استخدام مجالات الأسماء يتوسع ليشمل المنتجات والأفلام والأحداث الرياضية... الخ. فاسم مجال مثل Twinkies.com لا يتعلق باسم المؤسسة التي تصنع المنتج، بل يُستخدم للإعلان عن المنتج نفسه لا أكثر.

بالنتيجة يصعب علينا أن نتوقع فيما إذا كانت أسماء المجالات قادرة على التوسع بهذا الأسلوب. فشجرة الأسماء DNS تكون فعالة إذا كان هناك نوع من الهرمية فيها وتفقد فعاليتها شيئاً فشيئاً مع فقدانها لهرميتها.

لقد قامت شركة Sony بوضع جميع منتجاتها على شكل مجالات جزئية من مجالها Sony.com وهي عملية مناسبة جداً لأسلوب عمل DNS.

إنشاء المجالات الفرعية الخاصة

تشبه إجرائية إنشاء مجال فرعي تلك التي تساعد على إنشاء مجال المستوى الثاني إلا أن السلطة الإدارية في حالة المجال الفرعي تكون محلية (ضمن مؤسسة الزبون الخاصة).

تكون الخطوات على النحو التالي:

- اختيار اسم وحيد ضمن المجال المحلي
- تعريف مضيفين اثنين أو أكثر لتخديم المجال الجديد
- التنسيق مع مدير المجال الأعلى

يتوجب على المجالات الأعلى التحقق من أن مخدمات الأسماء الخاصة بالمجالات الأدنى، تعمل على نحو صحيح قبل توكيلها بإدارة المجالات الأدنى.

نسخ BIND

هناك ثلاثة نسخ أساسية من BIND: BIND4 وBIND8 وBIND9. ظهر BIND4 منذ نهاية الثمانينيات (النسخة الموثقة في الوثائق RFC رقم 1034 و1035). أما BIND8 فقد جرى إصداره عام 1997 وجرى إصدار BIND9 في منتصف عام 2000.

لا توجد نسخ باسم BIND5 أو BIND6 أو BIND7، فقد كان BIND8 عبارة عن تعديل هام جداً، شعر المطور أنه يحتاج إلى رقم نسخة يساوي ضعف رقم النسخة السابقة. حقيقةً، جرى إصدار BIND8 مع BSD4.4 حيث تم رفع جميع أرقام النسخ الخاصة بهذا النظام إلى 8. فقد جرى ترقيم نسخة Sendmail بالرقم 8 بعد تجاوز رقم النسخة بعدة أرقام رقم النسخة السابقة.
يحتوي BIND8 على عدد من التطويرات التقنية التي أثبتت فعاليتها، كالمتانة والأمان. كما يرفع BIND9 هذا المستوى بتقديمه دعماً لوجود عدة معالجات في الجهاز دعماً لتأمين عمليات الإجراءات بالإضافة إلى وجود عناصر أمان حقيقية (مفتاح تشفير عام)، ودعم للبروتوكول IPV6، وعملية نقل منطقة بأسلوب متزايد بالإضافة إلى العديد من الخواص التي يمكن أن يتمتع بها المضيف.

كما جرى اعتماد بنى معطيات جديدة (بالنسبة لبرمجية BIND) شجرية لتخزين معطيات المنطقة في الذاكرة. على كل حال، يمكن اعتبار BIND9 وكأنه برمجية مصممة ومطورة من جديد. إذ يقوم بفصل قسم الرماز الخاص بالتعامل مع نظام الاستثمار بحيث يجعل من السهل نقل BIND إلى أنظمة مختلفة عن نظام UNIX.

تختلف البنية الداخلية لمختلف نسخ BIND9 عن بعضها البعض إلا أنها تمتاز بنفس الإعدادات أما BIND4 فسيتم التوقف عن استخدامه قريباً، بعد أن تستقر نسخة BIND9 لمدة سنتين أو ثلاثة في الاستثمار بحيث سيجري إيقاف العمل بنسخة BIND8 كذلك.

مكونات BIND

- إجراء تخديمي يدعى named يقوم بالإجابة على الاستعلامات، حيث ندعو إجراء تخديمي مثل named (أو الجهاز الذي يعمل عليه) بمخدم الأسماء (name Server).
- مكتبة إجرائيات تقوم بحل الاستعلامات الواردة بخصوص المضيفين عبر اتصالها بقاعدة المعطيات الموزعة الخاصة بمخدم DNS، ندعو الرماز الزبون الذي يقوم بالاتصال بالمخدم بمحلل الأسماء (Resolver)
- واجهة لإدخال أسطر التعليمات الخاصة بنظام DNS مثل: nslookup، وdig، وhost.

المخدمات العودية والمخدمات غير العودية

تكون مخدمات الأسماء إما مخدمات عودية أو مخدمات غير عودية.

المخدمات غير العودية:

- إذا كانت المخدمات غير العودية تمتلك جواباً لاستعلام مخزن من مناقلة سابقة أو جواباً رسمياً عن المجال الذي يسأل الاستعلام عنه، فإن المخدم يقدم جواباً مناسباً
- وإلا، فإن المخدم وعوضاً عن تقديمه لجواب حقيقي، يقوم بإرجاع مؤشر إلى مخدمات رسمية خاصة بمجال آخر يمكن أن تكون أقرب للجواب
- وعليه، يجب أن يكون زبون المخدم غير العودي مهيأ لقبول والتصرف مع هذه المراجع
- بالرغم من أن المخدمات غير العودية تبدو كسولة إلا أنها محقة في عدم أخذها لأعباء عمل كبيرة. فالمخدمات الرئيسية التي تعمل على مستوى المجالات الأعلى تكون جميعها غير عودية إلا أن بإمكاننا تفهم عدم اعتمادهم للأسلوب العودي إذا عملنا أن مثل هذه المخدمات تعالج حوالي 10,000 استعلام في الثانية

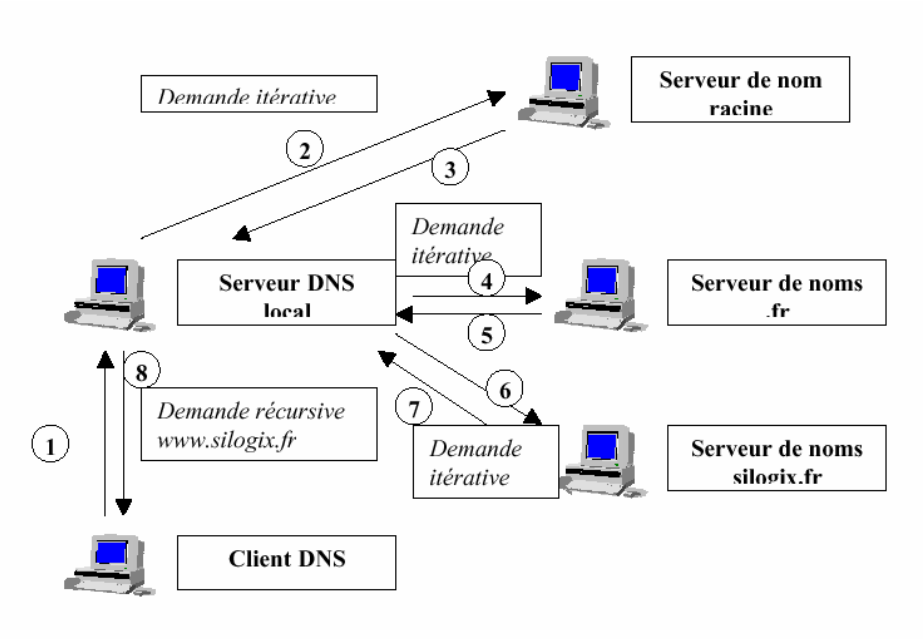
المخدم العودي:

- يعيد المخدم العودي أجوبة حقيقية فقط أو رسائل خطأ
- يقوم هذا المخدم بتتبع المراجع بنفسه عبر التوكل بهذه المهمة عن الزبون نفسه. أما إجرائية الحل فتبقى نفسها ويكمن الفرق الوحيد فيها في معالجة المخدمات للاستعلامات وطرح الاستعلامات على المخدمات الأخرى لحيز الوصول إلى جواب نهائي لتقوم بإرساله إلى الزبون

ملاحظات:

- لا تفهم المكتبات الإجرائية الخاصة بالمحللات التي تستخدمها زبائن DNS، المؤشرات المرجعية التي تشير إلى مخدمات لذا يجب أن يكون مخدم الأسماء المحلي مخدماً عودياً يمكن الاعتماد عليه للقيام بهذه المهمة
- يسمح التخزين بالاستفادة من عمليات الحل السابقة لسماء المضيفين. في حين لا تفيد هذه العملية في المجالات العليا مثل bin أو com أو edu لعدم حاجتنا لحفظ معلومات عن مضيف قد يكون على عمق عدة مجالات فرعية منها

كيف يعمل DNS



يرجى رسم المخطط التالي مع تعديل الجمل وفق الترجمة التالية:

الجدول الملحق	
Client DNS	زبون DNS
Demande Recursive www.silogix.fr	طلب عودي للعنوان المخدم mail.svuonline.org
Serveur DNS Local	المخدم DNS المحلي (ns.mydomain.com)
Demande itérative	طلب تكراري غير عودي
Serveur Racine	المخدم الجذر
Serveur de nom .fr	مخدم الأسماء org.
Serveur de nom silogix.fr	مخدم الأسماء svuonline.org

يُعتبر كل مضيف DNS عبارة عن زبون للنظام أو زبون ومخدم بآن واحد. تكون جميع مخدمات الأسماء على علم بالمخدمات الرئيسية. كما تمتلك المخدمات الرئيسية ما يكفي من المعلومات عن المجالات ذات المستويات العليا مثل com وedu وorg وfr وde... الخ. كما يكون المجال org على معرفة كاملة بالمجال svuonline.org. ويكون com على معرفة تامة بالمجال admin.com وهكذا دواليك، حيث يمكن لكل منطقة أن تقوم بتوكيل السلطة على مجالاتها الفرعية لمخدمات أخرى.

لنفترض أننا نريد البحث عن عنوان الجهاز mail.svuonline.org اعتباراً من الجهاز host1.mydomain.com يتوجه الجهاز host1 بالسؤال لمخدم الأسماء المحلي وهو ns.mydomain.org للبحث عن جواب.

لا يمتلك مخدم الأسماء المحلي أية معلومات عن العنوان، كما لا يمتلك أية معلومات عن mail.svuonline.org أو عن svuonline.org أو حتى عن org. إلا أنه يعلم بوجود عدة مخدمات من أجل المجال الرئيسي (الجذر). بالنتيجة، ونظراً لكونه مخدم عودي، فإنه يقوم بالاستعلام من المخدم الجذر عن mail.svuonline.org.

تُستخدم المخدمات الرئيسية (الجذر) لحفظ معلومات عن مخدمات المناطق الخاصة بالمجالات gTLDs إلا أن هذه المجالات (مثل com وnet وorg) تمتلك مخدماتها الخاصة. وعليه، يمتلك المجال org مخدماته الخاصة لذا سنفترض في مثالنا هذا أننا سنحصل على مؤشرات مرجعية إلى مخدمات مستقلة خاصة بالمجال org كجواب عن الاستعلام الموجه إلى المخدم الرئيسي والذي يسأل عن mail.svuonline.org.

يقوم مخدم الأسماء المحلي بإرسال استعلامه إلى المخدم org (ليسأله عن mail.svuonline.org) وليحصل بالمقابل على مؤشر مرجعي إلى المخدمات الخاصة بالمجال svuonline.org. يكون المخدم الخاص بالمجال svuonline.org، مخدماً رسمياً للمعلومات المطلوبة لذا يقوم هذا المخدم بإعادة العنوان المطلوب. عند رجوع العنوان يقوم ns.mydomain.com بتخزين لائحة المخدمات الخاصة بالمجالات org وsvuonline.org.

تخزين نتائج الاستعلامات وفعالية النظام

ترفع عملية التخزين من فعالية البحث: فالجواب المخزن يكون عادة متوفر وصحيح، لأن علاقات الأسماء بالعناوين لا تتبدل بكثرة.

كانت عملية التخزين مطبقةٌ سابقاً ولفترة طويلة على الإجابات الإيجابية.

في عام 1998، جرى وضع تصور مُعدل لتخزين الإجابات السلبية في الوثيقة RFC 2308 وقد جرى تحقيقها في BIND8.2 كخاصة اختيارية وأضحت إجبارية في BIND9.

تقوم عملية تخزين الإجابات السلبية، بتخزين إجابات من الأنماط التالية:

- لا يوجد اسم مضيف أو اسم مجال يتوافق مع الاسم المحدد في الاستعلام

- لا يوجد نمط المعطيات المطلوبة من أجل هذا المضيف
- لا توجد إجابة من المخدم المطلوب
- لا يمكن الوصول إلى المخدم بسبب مشاكل في الشبكة

يتبع BIND هذه الخطوط العريضة الموثقة في وثائق RFC أما أنظمة Windows فتقوم بتنجيز زمن بقاء الأجوبة بشكل اختياري.

ترفع عملية التخزين من فعالية البحث: فالجواب المخزن يكون عادة متوفر وصحيح، لأن علاقات الأسماء بالعناوين لا تتبدل بكثرة.

تتعلق معظم الاستعلامات عادة بمضيفين محليين لذا يكون حلها سريع. كما يكرر المستخدمون استعلاماتهم على نحو ضمني فبعد الجزء الأول من الاستعلام والذي يخص مضيف، يكون الجزء المتبقي والذي يخص مجال، مكرراً على الأغلب.

كانت عملية التخزين مطبقةٌ سابقاً ولفترة طويلة على الإجابات الإيجابية. فإذا لم يكن بالإمكان الحصول على اسم المضيف أو عنوانه كانت الإجابة السلبية تُرسل لمن طلبها دون أن يجري تخزينها. وقد جرى وضع تصور لعملية تخزين الاستعلامات DNS ذات الإجابات السلبية في الوثيقة RFC 1034 ولكن هذا التصور كان ناقصاً ولم يجر تحقيقه في نسخ BIND.

في عام 1998، جرى وضع تصور مُعدل لتخزين الإجابات السلبية في الوثيقة RFC 2308 وقد جرى بتحقيقها في BIND8.2 كخاصة اختيارية وأضحت إجبارية في BIND9.

لقد أظهرت عملية قياس جرت على المخدم الرئيسي RIPE في أوربا أن 60% من الاستعلامات تخص معطيات غير موجودة (كانت العديد من الاستعلامات موجهة لخدمات Microsoft مُعبَّر عنها بأسماء مضفين). وقد ساعد تخزين الإجابات السلبية على تخفيض عمليات البحث في شجرة DNS على نحو كبير جداً وخفف من حمل المخدمات الرئيسية.

تقوم عملية تخزين الإجابات السلبية، بتخزين إجابات من الأنماط التالية:
- لا يوجد اسم مضيف أو اسم مجال يتوافق مع الاسم المحدد في الاستعلام.
- لا يوجد نمط المعطيات المطلوبة من أجل هذا المضيف.
- لا توجد إجابة من المخدم المطلوب.
- لا يمكن الوصول إلى المخدم بسبب مشاكل في الشبكة.

يتبع BIND هذه الخطوط العريضة الموثقة في وثائق RFC أما أنظمة Windows فتقوم بتنجيز زمن بقاء الأجوبة بشكل اختياري وخصوصاً بالنسبة للتخزين الخاص بالأجوبة السلبية. إذ تستخدم هذه الأنظمة القيمة الدنيا الموجودة في التسجيلات التي تُعرِّف المجال الأصلي (المدعوة تسجيلات SOA أو Start-Of-Authority) في المرة الأولى التي يعود فيها الاستعلام NXDOMAIN (أي لا يوجد مجال بهذا الاسم). ومن ثم يتم إعادة تثبيت زمن البقاء على 15 دقيقة بحيث يُسمح له بالعد اعتباراً من لحظة التغيير.

مخدمات حل الأسماء ديناميكياً

بشكل عام، يجري استخدام مخدمات DNS لحل أسماء المخدمات مثل مخدمات البريد الإلكتروني التي نعطيها أسم mail في كثير من الأحيان، أو مخدمات الوب التي نعطيها أسم WWW دائماً (كإسم أو لقب أي alias إضافي على أسمها الأصلي).

غالباً ما تكون هذه المخدمات ذات عناوين ثابتة، إذ يجري تثبيت عناوينها يدوياً ولا يجر استخدام مخدمات DHCP لتوزيع إعداداتها إلا في حالات خاصة تكون مُعَدَّة على نحو يضمن بقاء العنوان ثابتاً.

أما في حالة المضيفين العاديين، فيمكن تعريفهم أيضاً ضمن مجالات الأسماء وإعطاؤهم أسماء محددة، ولكن وجود مخدم DHCP يوزع الإعدادات الشبكية على نحو ديناميكي، سيجعل هؤلاء المضيفين يمتلكون عناوين متغيرة مع كل إقلاع، مما سيتعارض مع مبدأ تثبيت أسماء لهم في مخدم DNS مرتبطة بعناوين ثابتة.

لحلّ هذه المشكلة، جرى تطوير النسخ الحديثة من DNS لجعلها ديناميكية. في هذه النسخ، يمكن إعداد المجال بحيث يستقبل عناوين المضيفين عند الإقلاع على نحو ديناميكي، مما يعني أن تسجيل المضيف يجري بعد إقلاعه وأخذه لإعداداته من مخدم DHCP، بحيث يجري التسجيل ضمن المخدم المجال اللذان يجري تحديدهما من قبل مخدم DHCP.

نشاط

خطوات إعداد مخدم أسماء DNS محلي بسيط تحت نظام Windows 2000

يحتاج هذا النشاط للعمل على نظام Windows 2000 Server أو Windows 2003 Server حتى يتسنى تثبيت مخدم DNS المرافق لنظام تشغيل Windows.

1. اذهب إلى Control Panel
2. اضغط على أيقونة Add Remove Software
3. اذهب إلى زر Add Remove Windows Component
4. اذهب إلى Networking Services
5. اختر Domain Name Service واطلب تثبيته
6. عند الانتهاء من التثبيت ستظهر أيقونته في الـ Administrative Tools
7. شغِّل الأداة
8. اضغط بالزر اليميني على لائحة المخدمات وأضف مخدمك كمخدم حلّ أسماء
9. اضغط بالزر اليميني على المخدم وأضف منطقة حل أسماء New Zone
10. ستكون مضطراً لإضافة اسم المنطقة ومعلومات عنها مما سيؤدي لتوليد ملف نصي بإسم المطقة
11. عند الانتهاء من تعريف المنطقة، ستظهر مجموعة تسجيلات أهمها التسجيل SOA أو Start-Of-Authority والذي يشكل سجل تعريف المنطقة
12. اعتباراً من هذه المرحلة، يمكن إضافة تسجيلات تدل على مضيفين ضمن المجال، بالضغط بالزر اليميني على أسم المجال، وإضافة تسجيلات أخرى كتسجيلات خاصة عن مضيفين (Host)، أو تسجيلات عن مخدمات بريد إلكتروني (MX)
13. بالضغط بالزر اليميني على أسم المجال، واختيار Properties، يمكننا إعداد المجال بجعله مجالاً ديناميكياً مثلاً (مما يعني أنه يستقبل عناوين المضيفين عند إقلاعهم ولايجر تثبيت عناوينهم بشكل ثابت)

14. إذهب إلى مكان إعداد المخدمات العليا (Forwarders) وضع عنوان المخدم الأعلى الذي سيعتمد عليه المخدم DNS المحلي الذي تقوم بإعداده
15. يجب إعداد المخدم وإعداد جميع المضيفين بحيث يعتمدون على هذا المخدم. يمكن تنفيذ ذلك اعتباراً من الإعدادات الشبكية لكل جهاز بحيث يجري تحديد عنوان المخدم DNS المحلي ضمن هذه الإعدادات. (يمكن أن تكون الإعدادات الشبكية الخاصة بالمضيفين ناتجة عن مخدم DHCP، عندها يجب تعديل إعدادات مخدم DHCP بحيث يقوم بتوزيع عنوان المخدم DNS مع عناوين المضيفين كجزء من الإعدادات)
16. افتح نافذة Command Prompt أو استخدم ملفات المساعدة في Windows للبحث عن التعليمة التالية: nslookup ، ستلاحظ أن تنفيذ هذه التعليمة على أي مضيف سيعطي مخدم DNS الذي يستخدمه هذا المضيف

عنوان الموضوع:

مبادئ أمن المنظومات الشبكية

الكلمات المفتاحية:

أنظر الملف Glossary المُرافق.

ملخص:

نستعرض في هذا القسم المبادئ الأساسية لأمن المنظومات الشبكية سواء على عدة مستويات: مستوى البرمجيات، ومستوى أنظمة التشغيل ومستوى الشبكة. كما نهتم باستعراض أسس الوقاية، والمخاطر الرئيسية التي تحيق بمنظومة شبكية وأساليب مقاومتها.

أهداف تعليمية:

يتعرف الطالب في هذا الفصل على:

- تعريف أمن نظام معلومات مرتبط بمنظومة شبكية
- مبادئ الوقاية
- مخاطر أساسية وطرق مقاومتها: فيروسات، برامج متنقلة، أبواب خلفية، اختراقات شبكية، ... الخ

مقدمة

لم يعد بإمكاننا التحدّث عن الحواسب المستخدمة في حياتنا اليوميّة دون أن نأخذ بعين الاعتبار قدراتها الكبيرة في مجال الاتصالات. فقد أخذت الأنظمة المعلوماتيّة الخاصة بالمؤسسات، والمتصلة بالإنترنت، تنتشر بسرعةٍ كبيرةٍ وأضحت أغلب الشركات العالمية تعتمد بشكل أساسي على النظام المعلوماتي للتواصل مع فروعها المختلفة، مما جعلها تدرك الأهمية الكبيرة لحماية شبكاتها وجعلها تبدأ في تعريف سياسة أمنية تساعد على وضع ضوابط لبناء الأنظمة المعلوماتية واستخدامها.

لقد أخذ أمن النظم المعلوماتية أهمية متزايدة مع تطور الشبكات العاملة بعائلة بروتوكولات الإنترنت المعروفة باسم TCP/IP. فبالرغم من أن هذه البروتوكولات قد أوجدت تلبيةً لاحتياجات الجيش الأمريكي إلا أنها تحوي الكثير من نقاط الضعف من الناحية الأمنية. وقد حرَّض حجم الاستثمارات الهائل في مجال تطوير الأنظمة المعلوماتية، وتقدم التقنيات المستخدمة فيها والازدياد المطّرد للأجهزة الواجب حمايتها، بالإضافة إلى انتشار تهديدات جديدة (الفيروسات، طرق القرصنة المختلفة...)، الكثير من المؤسسات، على وضع سياسة أمنية صارمة للحفاظ على مصالحها الاستراتيجية من الأخطار التي باتت تهددها نتيجة الاختراق المحتمل لأنظمتها.

الأخطار التي تهدد المؤسسات

تُعرّف الأخطار المتعلقة بالأمن المعلوماتي للمؤسسات وفقاً لأهميّة الأنظمة المعلوماتية وطبيعة دورها في المؤسسة.

الأخطار الاستراتيجية:

حفظ "*حياة*" المؤسسة ضمن نظامها المعلوماتي يجعلها مضطرة لضمان سلامة العتاد الذي يحفظ المعلومات من جهة، ويحفظ سلامة المعلومات وسريتها من جهة أخرى.

بالإضافة إلى مشكلة الإتلاف أو التخريب، تعاني المؤسسات الكبرى من معضلة التجسس الصناعي.

الأخطار اليومية:

يمكننا أن نحدد نوعين من الأهداف: مواقع التجارة الإلكترونية ومواقع الويب الدعائية الخاصة بالمؤسسات الضخمة.

تصبح هذه المخاطر استراتيجية عندما يكون نشاط الشركة مقتصراً على عمليات تجارية عن طريق الإنترنت.

تُعرّف الأخطار المتعلقة بالأمن المعلوماتي للمؤسسات وفقاً لأهميّة الأنظمة المعلوماتية وطبيعة دورها في المؤسسة. يمكن أن نميّز نوعين من الأخطار التي تواجهها المؤسسة بحسب الأنظمة المُستهدفة. يقودنا هذا التصنيف للحديث عن أخطارٍ استراتيجية وعن مشاكل أقل خطورة.

الأخطار الاستراتيجية:

تطبّق الكثير من المؤسسات والشركات العالمية سياسة (صفر ورقة - Zero Paper). ولكن حفظ "*حياة*" المؤسسة ضمن نظامها المعلوماتي يجعلها مضطرة لضمان سلامة العتاد الذي يحفظ المعلومات من جهة، ويحفظ سلامة المعلومات وسريتها من جهة أخرى. كما تقتضي الأهمية المتزايدة لتبادل المعلومات، وجود أنظمةٍ ذات وثوقية عالية تضمن استمرار العمل حتى في حال حدوث عطل أو خطأ طارئ في المنظومة.

تشكل سرقة أو إتلاف أو تخريب المعطيات، خطراً كبيراً على وضع المؤسسة. فعلى سبيل المثال، خصصت شركة بوينغ الأميريكية، عام 1998، 570000 دولار أمريكي للتأكد من سلامة وصحة معطياتها بعد أن لاحظت اختراق مجموعة من الطلاب الجامعيين لنظامها المعلوماتي. فقد يشكل تعديل بسيط في معطيات المؤسسة، خطراً كبيراً على عملها ويؤدي إلى كوارث من مختلف الأنواع.

بالإضافة إلى مشكلة الإتلاف أو التخريب، تعاني المؤسسات الكبرى من معضلة التجسس الصناعي. فقد أضحت بعض المعطيات الاستراتيجية كالمشاريع الاستراتيجية البعيدة الأمد أو المبادلات التجارية أو الاختراعات غير المسجلة، هدفاً للقرصنة والسرقة خصوصاً بعد وصل منظومات المؤسسات بالإنترنت لتسهيل التواصل بين فروعها. فقد أكدت مجموعة المحامين الأمريكيين Gartner William Malik أن أحد زبائنها قد خسر، عام 1999، أكثر من 90 مليون دولار أميريكي نتيجة قرصنة نفذها عدد من منافسيه على مشاريعه.

الأخطار اليومية:

يمكننا أن نحدد نوعين من الأهداف: مواقع التجارة الإلكترونية ومواقع الويب الدعائية الخاصة بالمؤسسات الضخمة.

ننوه، إلى أن هذه المخاطر تصبح استراتيجية عندما يكون نشاط الشركة مقتصراً على عمليات تجارية عن طريق الإنترنت. يحيق الخطر عادةً، في مواقع التجارة الإلكترونية،

بالمبادلات التجارية وبالمناقلات التي تعتمد على أرقام البطاقات المصرفية. فنقطة الضعف الأساسية في هذه العمليات ليست عمليات الإرسال التي أصبحت تعتمد تقنيات تشفير عالية، وإنما أنظمة تخزين المعلومات التي تكون الهدف الرئيسي لعمليات القرصنة. فقد تمكن القرصان الأميريكي Kevin Mitchnick من سرقة 17000 رقم بطاقة مصرفية خاصة بزبائن مزود الخدمة Internet Netcom في ولاية كاليفورنيا الأمريكية قبل أن يتم إيقافه. وقد نفذ ذلك بعد أن تمكن من الولوج إلى قاعدة المعطيات التي يحتفظ فيها مزود الخدمة، بهذه الأرقام.

تشكل قرصنة مواقع الوب العادية الخاصة بالمؤسسات أحد هذه الأهداف أيضاً. إذ تكون هذه المواقع عادةً غير محمية بشكل جيد نظراً لعدم أهميتها الاستراتيجية، مما يعرضها للاختراق ويعرض المؤسسة للدعاية المضادة كما يُعرّض صورة المؤسسة التي تقوم باستضافة الموقع لدعايةٍ مضادةٍ أيضاً. يكون لمثل هذه الأعمال هدفين: إما قرصان يطمح للشهرة أو قرصان تابع لمجموعات تجارية منافسة، وهو ما جرى مع شركة الفرو العالمية Kriegsmann التي كانت ضحية لقرصنة من إحدى الشركات المنافسة.

الأخطار التي تهدد الأفراد

لا تختلف كثيراً عناصر حماية حاسوب منزلي شخصي عن تلك المستخدمة في حماية الحاسوب المُستعمل في موقع العمل.

السؤال الأول الذي ينبغي أن يطرحه المستخدم العادي على نفسه: هل يمكن تحسس محاولة اختراق الحاسوب الشخصي، سواء نجحت هذه المحاولة أم لا؟ وفي حال نجاحها، هل يمكن حصر ما جرى أثناء هذا الاختراق؟

للإجابة على الأسئلة السابقة ينبغي أن يطرح المستخدم على نفسه بعض الأسئلة الأخرى:

- من ذا الذي يهتم بحاسوب منزلي متواضع؟
- هل يسهل اختراقه؟
- ما هي الأخطار المحيقة به وهل هي أخطار ناجمة عن الاتصال بالإنترنت أم أن هناك أخطار لا علاقة لها بالاتصال بالعالم الخارجي؟
- وهل يمكن حصر أساليب الوقاية من مثل هذه الأخطار؟
- هل هناك لائحة بالملفات والمجلدات وبمختلف البطاقات والتجهيزات المثبتة على الجهاز؟
- هل جرى حصر التطبيقات التي تعمل على الحاسوب؟
- هل يمكن تحديد فيما إذا كان الحاسب يعمل بشكلٍ طبيعي أم لا؟
- وأخيراً، هل المستخدم نفسه على درايةٍ بأهمية طرح التساؤلات السابقة؟

لا تختلف كثيراً عناصر حماية حاسوب منزلي شخصي عن تلك المستخدمة في حماية الحاسوب المُستعمل في موقع العمل. إذ يبدأ مشوار الألف ميل عادةً بخطوة، فما بالنا إذا كان بإمكان المُستخدم العادي اجتياز أكثر من نصف المسافة عبر مجموعة من الإجراءات البسيطة التي تكفل مستوى حماية متميز للحواسب المنزلية.

المهم في الموضوع، هو أن يستطيع المستخدم العادي استيعاب الأخطار وفهم أسبابها ومنطلقاتها، حتى يستطيع فهم تقنياتها وآليات تنفيذها، للوصول أخيراً إلى تحقيق ما يضمن حماية نفسه منها. ولعل أكثر ما يثير العجب في هذا المجال، هو أن جزءاً مهماً من نظام الأمن والحماية الخاص بنظام معلوماتي، يرتكز على قواعد سلوكية وإجراءات بسيطة يمكن لأي شخص، مهما كانت معلوماته التقنية بسيطة، أن يطبقها بسهولة. فالسؤال الأول الذي ينبغي أن يطرحه المستخدم العادي على نفسه: هل يمكن تحسس محاولة اختراق الحاسوب الشخصي، سواء نجحت هذه المحاولة أم لا؟ وفي حال نجاحها، هل يمكن حصر ما جرى أثناء هذا الاختراق؟

للإجابة على الأسئلة السابقة ينبغي أن يطرح المستخدم على نفسه بعض الأسئلة الأخرى:

- من ذا الذي يهتم بحاسوب منزلي متواضع؟
- هل يسهل اختراقه؟
- ما هي الأخطار المحيقة به وهل هي أخطار ناجمة عن الاتصال بالإنترنت أم أن هناك أخطار لا علاقة لها بالاتصال بالعالم الخارجي؟

- وهل يمكن حصر أساليب الوقاية من مثل هذه الأخطار؟
- هل هناك لائحة بالملفات والمجلدات وبمختلف البطاقات والتجهيزات المثبتة على الجهاز؟
- هل جرى حصر التطبيقات التي تعمل على الحاسوب؟
- هل يمكن تحديد فيما إذا كان الحاسب يعمل بشكلٍ طبيعي أم لا؟
- وأخيراً، هل المستخدم نفسه على درايةٍ بأهمية طرح التساؤلات السابقة؟

من يريد اختراق حاسوب منزلي؟

قد لا يهتم الدخيل بمعرفة هوية الشخص الذي ينفذ عملية الاختراق ضده، فقد يكون جلّ ما يحتاجه، هو التحكم بحاسوبه الشخصي لكي يتمكن من استخدامه كمنصةٍ لاختراق أنظمةٍ حاسوبيةٍ أخرى.

بالنتيجة، يشكِّل حاسوب منزلي متواضع، هدفاً محتملاً حتى ولو كان الاتصال بالإنترنت يقتصر على تصفح مواقع ألعاب أو على إرسال واستقبال البريد الإلكتروني.

ومن الخطأ الاعتقاد بأن الأمن هو حاجة خاصة بحاسوب أو بشبكة مؤسساتية أو حكومية وليس حاجة ملحة لحاسوب شخصي منزلي يُستخدم للاتصال بالإنترنت.

قد لا يهتم الدخيل بمعرفة هوية الشخص الذي ينفذ عملية الاختراق ضده، فقد يكون جلّ ما يحتاجه، هو التحكم بحاسوبه الشخصي لكي يتمكن من استخدامه كمنصةٍ لاختراق أنظمةٍ حاسوبيةٍ أخرى. إذ سيتمكن الدخيل، عبر تحكمه بحاسوب طرفٍ ثالث، من إخفاء مكانه وموقعه الحقيقي وسيتمكن من مهاجمة أنظمة شبكية وحاسوبية تحتوي على معلومات حساسة (مالية، حكومية ... الخ)، دون أن يكون بإمكان أنظمة الحماية الخاصة بالمواقع الآنفة الذكر تحديد موقعه الحقيقي بسهولةٍ وبدقة.

بطبيعة الحال، يمكن لمن يخترق حاسوب شخصي (إذا افترضنا أنه يسعى للتخريب أو أنه فضوليّ، لا أكثر)، أن يراقب الأعمال التي تجري عليه على نحوٍ كامل، كما يمكنه تغيير المعطيات الموجودة على حاسب الضحية أو تعطيل نظام التشغيل أو أي برنامجٍ آخر.

بالنتيجة، يشكِّل حاسوب منزلي متواضع، هدفاً محتملاً حتى ولو كان الاتصال بالإنترنت يقتصر على تصفح مواقع ألعاب أو على إرسال واستقبال البريد الإلكتروني. ومن الخطأ الاعتقاد بأن الأمن هو حاجة خاصة بحاسوب أو بشبكة مؤسساتية أو حكومية وليس حاجة ملحة لحاسوب شخصي منزلي يُستخدم للاتصال بالإنترنت. فالمستخدم العادي لايرغب، على الأرجح، من أن يتمكن أحد الغرباء من الاطلاع على وثائقه المهمة أو العبث بها. ومن المؤكد أن المستخدم العادي يرغب بالحفاظ على أداءٍ عالٍ لحاسوبه المنزلي حتى ولو كان استخدامه يقتصر على الاتصال بالإنترنت وتصفح المواقع. وهو لا يريد، بطبيعة الحال، أن يستخدم أحدهم عنوان بريده الإلكتروني لإرسال رسائل إلى الآخرين. ومن المؤكد أنه يرغب باستخدام معالج النصوص المثبت على الحاسوب في أي وقت دون مواجهة أعطالٍ طارئةٍ تعيق استخدامه وتضطره لإعادة تثبيته.

تعريف

تعريف الأمن: يهدف الأمن إلى حماية الممتلكات والأشخاص، ويتعلق مستوى الأمن المطلوب عادةً بحساسية وقيمة العناصر المحمية.

يمكن تصنيف الأمن إلى ثلاثة مستويات:

- الوقاية من المخاطر؛
- تحسس الاختراق الأمني أو المشكلة الأمنية؛
- رد الفعل تجاه الخطر.

ويمكن النظر إلى متطلبات أمن الشبكات (أو نظام المعلومات بشكل عام) وفق ثلاثة محاور:

- **السرية:** وهي منع الكشف عن المعلومة الخاصة غير القابلة للنشر؛
- **الصحة:** وهي منع تعديل المعلومات من قبل أشخاص غير مسموح لهم بذلك؛
- **التوفر:** وهي منع إيقاف أو تعطيل خدمة أو عمل من قبل أشخاص غير مسموح لهم بذلك.

السرية

لفترة طويلة تم اعتبار السرية، الهدف الرئيسي لأمن المعلومات:

- اعتماداً على كون الهدف من أمن المعلومات يتمثل في مكافحة التجسس ومكافحة نشر المعلومات الحساسة.

تعني سريّة معلومة، منع المستثمر غير المخوَّل، من الوصول إلى المعلومة واستخدامها:

- يمكن أن يكون محتوى ملف ما علنياً؛
- لكن عدد مستثمري الملف قد يكون سرياً؛
- مثال: في مواقع البيع الإلكتروني قد يكون عدد المشترين رقماً سرياً استراتيجياً لا يحق إلا لأشخاص محددين الاطلاع عليه لأسباب تتعلق باستراتيجية الموقع التسويقية.

الصحة

ترتبط السرية بفعل **القراءة** بينما ترتبط صحة المعلومات بفعل **التعديل**؛

تُعرَّف **صحة المعلومة** بأنها تطابق النسخة الحالية من المعلومة مع النسخة المصدرية بهدف البرهان على أنها لم تتعرض للتعديل بشكل عرضي أو مقصود؛

يكون لهذا المفهوم –في مجال الاتصالات– معنى موسعّ: إذ يُعرَّف بأنه اكتشاف وتصحيح كل عملية تغيير أو إضافة أو مسح أو تبديل جرى تنفيذه على المعلومات المُرسَلة سواء كانت العمليات السابقة قد نتجت عن أخطاء أو عن تدخل طرف ثالث بشكل مقصود.

التوفر

تُعرَّف بأنها إمكانية الوصول للمعلومة أو الخدمة واستثمارها دون الانتظار طويلاً؛

تتلخص إحدى أهم اختراقات الشبكات المعلوماتية في عملية منع الوصول للخدمة، أو ما ندعوه إيقاف الخدمة (DOS: Deny Of Service)، وهي تُعتبر من أكثر أنواع الاختراقات التي يصعب احتواؤها وردها.

مثال: قد يكلف إيقاف مخدمات الوب التي تستضيف موقع تجارة إلكترونية مثل الموقع www.amazon.com ملايين الدولارات. فإذا علمنا أن حجم أعمال هذا الموقع يبلغ 4 بلايين دولار سنوياً يمكننا أن نتخيل حجم الخسائر التي سيتعرض لها في حال توقفت مخدماته عن العمل لثلاثة أيام متتالية. حصل هذا الأمر مع الموقع في عام 1998 ونتيجة اختراق عبر الإنترنت بإسلوب DOS.

الوقاية: الدعامة الأساسية لسياسة الأمن المعلوماتي

كي تكون فعالة، تتحدد سياسة الأمن المعلوماتي لمؤسسة وفق أسسٍ نظرية يتم تطبيقها على المؤسسة بأسرها. تتحدد هذه القواعد في الكثير من الحالات، في مركز المؤسسة ثم يتم تعديلها قليلاً لتتوافق مع احتياجات الفروع.

تتضمن الوقاية، بشكل رئيسي، وضع خطّة انتشار المنظومة المعلوماتية (حواسيب، مخدمات، شبكة، قواعد معطيات، وغيرها) وفق قواعد محددة. ويؤدي وضع خطة الانتشار إلى تحقيق المعادلة الصعبة التي تسعى للتوفيق بين رفع سوية أمن المنظومة من جهة، وتوفير الحد الأقصى من الإمكانيات لمستخدميها، من جهةٍ أخرى. تتضمن الخطة الآنفة الذكر العمليات التالية:

1. تصنيف المعلومات؛
2. تمييز الغرض من كلّ حاسوب وتوثيق الهدف من استعماله؛
3. تحديد الخدمات الشبكية التي يقدمها كل حاسوب؛
4. تعريف مجموعات المستخدمين التي لها صلاحيات استخدام الحاسوب؛
5. تحديد الامتيازات التي تملكها كل مجموعة مستثمرين؛
6. فرض استراتيجية محددة للوصول إلى مصادر المعلومات وإلى موارد المنظومة؛
7. تطوير آليات مساعدة على تحسس الاختراق الأمني؛
8. تحديد الأساليب التي تكفل استمرار خدمات المنظومة في العمل عند الأعطال، وكيفية استعادة هذه الخدمات؛
9. التركيز على القواعد السلوكية؛
10. تحديد المشاكل الأمنية التي ترتبط بالإدارة اليومية للحواسيب.

وسائل وأدوات الوقاية

يعتمد أمن المعلومات على العديد من وسائل الوقاية والحماية التي يعالج كل منها جانب أو عدة جوانب من موضوع الأمن:

- التشفير
- التحقق من الهوية ومراقبة عمليات الولوج
- توزيع الصلاحيات والسماحيات
- توفير حد أدنى من سماحية التعرض للأخطاء
- اتباع نهج التخزين الدوري
- وضع خطة للإستعادة بعد الكوارث

يعتمد أمن المعلومات على العديد من وسائل الوقاية والحماية التي يعالج كل منها جانب أو عدة جوانب من موضوع الأمن:

- **التشفير:** عند تخزين أو نقل المعلومة لضمان حمايتها من السرقة. مثال: استخدام بروتوكولات مشفرة لتبادل البريد الإلكتروني، أو لتنفيذ عمليات بيع وشراء على الإنترنت مع مواقع تجارة إلكترونية؛
- **التحقق من الهوية ومراقبة عمليات الولوج:** للتأكد من وصول العناصر المسموح لها بالولوج إلى المنظومة، إلى الأغراض التي تخصها أو المسموح لها بمعالجتها. مثال: إجبار المستخدمين على إدخال اسم وكلمة مرور عند استخدامهم لنظام تشغيل مثبت على حاسب. تسمح عمليتا التحقق والمراقبة أيضاً بتحسس أي اختراق أمني قد يحصل؛
- **توزيع الصلاحيات والسماحيات:** لإعطاء العناصر الفعالة (كالمستخدمين) صلاحيات محددة كصلاحية تعريف المستخدمين، أو صلاحية تنفيذ التخزين الاحتياطي؛ وإسناد سماحيات دخول إلى الأغراض والموارد المختلفة كالملفات والطابعات والخدمات، لتحديد شروط استخدام عنصر ما لمورد. مثال: تحديد صلاحية مدير نظام تشغيل، وصلاحية مدير شبكة، وإسناد سماحيات الإدارة والتشغيل والاستخدام إلى طابعة أو إلى خدمة الوب؛
- **توفير حد أدنى من سماحية التعرض للأخطاء:** للتمكن من الاستمرار في العمل مع حدوث أعطال. يمكن أن يجري ذلك من خلال تأمين العتاديات المناسبة (مثل المخدمات ذات البنى العنقودية، أو الأقراص الصلبة المتعددة التي تعمل على التوازي، وغيرها)؛
- **اتباع نهج التخزين الدوري:** لضمان وجود نسخ احتياطية من المعطيات في حال حدوث أعطال أو تخريب متعمد؛
- **وضع خطة للإستعادة بعد الكوارث:** لاستعادة العمل والخدمات والمعطيات الضائعة حتى مع حدوث كوارث كالحرائق والزلازل. يمكن أن يجري ذلك عبر توزيع الخدمات والنسخ الاحتياطية على عدة مواقع جغرافية.

مصادر الخطر

1- أخطاء الأنظمة البرمجية التجارية والأبواب الخلفية الموجودة فيها
2- أحصنة طروادة
3- أدوات إدارة حاسوب عن بعد بصورة غير شرعية
4- البرامج المتنقلة
5- الفيروسات
6- ملحقات مخفية لأسماء الملفات
7- اختراقات شبكية: تنصت، إغراق، ... الخ

تزداد سهولة اختراق الأنظمة الحاسوبية والشبكات بشكلٍ مطرِّد مع ازدياد الثغرات والأخطاء الموجودة في الأنظمة البرمجية المُستخدمة، ومع السماح بعمليات التثبيت الأوتوماتيكي لبرمجيات مختلفة، أثناء تصفح المواقع الموجودة على الإنترنت.

كما تأتي اختراقات أخرى نتيجة استقبال بعض أنواع البريد الإلكتروني، أو نتيجة التحميل العشوائي للملفات دون مراجعة دقيقة لمحتواها. لذا، نحتاج قبل تنفيذ إجراءات الحماية، أن نتعرف على المخاطر المحتملة.

فيما يلي سرد لبعض الأساليب التي يستخدمها الدخلاء للوصول إلى نظام معلومات:

1- أخطاء الأنظمة البرمجية التجارية والأبواب الخلفية الموجودة فيها
2- أحصنة طروادة
3- أدوات إدارة حاسوب عن بعد بصورة غير شرعية
4- البرامج المتنقلة
5- الفيروسات
6- ملحقات مخفية لأسماء الملفات
7- اختراقات شبكية من تنصت وإغراق وغيرها

أخطاء الأنظمة البرمجية وثغراتها

للأسف يستطيع القراصنة دائماً اكتشاف نقاط ضعف جديدة "قابلة للاستثمار" في البرامج الحاسوبية. فتعقيد البرمجيات يجعل من اختبارها على نحوٍ كامل، أمراً صعباً جداً.

لذا يحاول مطورو الأنظمة البرمجية، عند اكتشاف ثغرات ضمن الأنظمة التي يسوقونها، تطوير وتسويق نسخ مُحدَّثة من هذه البرامج أو تطوير برامج تصحيحية (Patches) تساعد على إصلاح هذه الثغرات والأخطاء. كما يحاول المطورون توزيع الأنظمة المُحدَّثة أو البرامج التصحيحية على نحوٍ واسع يضمن حلّ المشاكل على أوسع نطاق.

لذا يتحتم على المستخدم متابعة آخر عمليات التحديث التي تطرأ على الأنظمة والبرمجيات التي يستخدمها، وذلك للاستعلام عن مثل هذه المشاكل وتصحيحها في الوقت المناسب. فعلى سبيل المثال، تضمن شركة Microsoft لزبائنها، بشكل مجاني اعتباراً من موقعها على شبكة الإنترنت، الحصول على برامج خاصة تساعد على تصحيح أخطاء أنظمة التشغيل التي تسوقها (أنظمة windows) وعلى تصحيح أخطاء أنظمتها البرمجية المختلفة (مجموعة Office، أو أداة تصفح المواقع Internet Explorer، ... الخ) وعلى نحو مؤتمت في كثيرٍ من الأحيان (Live Update) كما تقدم آخر النصائح في مجال تحصين الأنظمة والبرامج التي تطورها وتوزعها الشركة.

بالنتيجة، يحتاج المستخدم لملاحقة مثل هذه التعديلات بهدف تطبيقها مباشرةً عن ظهورها.

أحصنة طروادة

يعرَّف حصان طروادة على أنه برنامج له مظهر برئ، ووظيفة ظاهرة تساعد على إغراء المستخدمين باستعماله، إلا أنه يحتوي أيضاً على وظائف خفية تساعد من صممه على استغلال امتيازات المستخدم الذي يقوم بتشغيله، لتحقيق أهدافٍ أخرى.

كيف يجري تثبيت أحصنة طروادة ؟

تعتمد أحصنة طروادة، أساساً، على قيام المستخدم بتثبيتها بنفسه على حاسوبه بعد أن تخدعه وظيفتها المُعلَنة.

ما الآثار التي يمكن أن تنجم عن أحصنة طروادة؟

- حذف أي ملف يحق للمستخدم حذفه
- إرسال أي ملف يمكن للمستخدم قراءته، إلى الدخيل
- تعديل أي ملف يحق للمستخدم تعديله
- إمكانيات اختراق حواسب أخرى موجودة على نفس شبكة المستخدم
- تثبيت فيروسات
- استخدام الحاسوب الضحية كمنصة للهجوم على حواسب أو شبكات أخرى

ما هي الحلول الممكنة؟

يعتبر تجنب هذا النوع من البرامج الحلّ الأمثل لمواجهتها:

- التأكد من أن البرامج التي نقوم بتثبيتها، صادرة عن مصادر موثوقة
- عدم تنفيذ أيّ برنامج تم الحصول عليه عبر البريد الإلكتروني
- توخي الحذر عند استعمال متصفح الويب
- تطبيق مبدأ استخدام الحدّ الأدنى من الامتيازات عند استخدام الحاسوب
- إذا وقع المستخدم ضحيّة برنامج من نمط حصان طروادة، يمكن لبعض البرامج المضادة أن تزيل البرنامج وأن تعالج الضرر الذي يتسبب به

يعرَّف حصان طروادة على أنه برنامج له مظهر برئ، ووظيفة ظاهرة تساعد على إغراء المستخدمين باستعماله، إلا أنه يحتوي أيضاً على وظائف خفية تساعد من صممه على استغلال امتيازات المستخدم الذي يقوم بتشغيله، لتحقيق أهدافٍ أخرى.

كيف يجري تثبيت أحصنة طروادة ؟

تعتمد أحصنة طروادة، أساساً، على قيام المستخدم بتثبيتها بنفسه على حاسوبه بعد أن تخدعه وظيفتها المُعلَنة. فعلى سبيل المثال، قد يصل البرنامج عبر البريد الإلكتروني على شكل لعبة حاسوبية جديدة ومجانية. عندما يستلم المستخدم بريده، تغريه الرسالة بتثبيت اللعبة الجديدة لتجريبها. في الحقيقة، يكون البرنامج عبارة عن لعبة حقيقية إلا أنه يمتلك بنفس الوقت وظائف أخرى تعمل في الخفاء عند التثبيت وتقوم بأعمال من نمط حذف ملفات أو حذف رسائل إلكترونية أو تثبيت برامج أخرى للتحكم بالحاسوب عن بعد.

يمكن أيضاً للدخيل أن يدَّعي عبر رسالة إلكترونية، بأن الرسالة مُرسَلة من إحدى الهيئات العالمية المسؤولة عن محاربة القراصنة كهيئة CERT (www.cert.org)، لإقناع المستخدم بتثبيت برنامج تصحيح يساعد على تدعيم أمن النظام أو تدعيم إحدى البرامج.
قد يصل الأمر في بعض الأحيان إلى تلقي اتصال هاتفي أو رسالة إلكترونية من شخص يدعي بأنه ممثل مزود الخدمة الخاص بالمستخدم، لكي يطلب منه تشغيل برامج معينة أو تثبيت برامج اعتباراً من مواقع محددة.

ما الآثار التي يمكن أن تنجم عن أحصنة طروادة؟

يمكن لحصان طروادة أن ينفذ أي عمل يستطيع مستخدم الحاسوب تنفيذه:

- حذف أي ملف يحق للمستخدم حذفه
- إرسال أي ملف يمكن للمستخدم قراءته، إلى الدخيل
- تعديل أي ملف يحق للمستخدم تعديله
- تثبيت برامج أخرى (تبعاً لصلاحيات المستخدم)، توفر إمكانيات اختراق لحواسب أخرى موجودة على نفس شبكة المستخدم؛
- تثبيت فيروسات
- استخدام الحاسوب الضحية كمنصة للهجوم على حواسب أو شبكات أخرى

ما هي الحلول الممكنة؟

يعتبر تجنب هذا النوع من البرامج الحلّ الأمثل لمواجهتها:

- التأكد من أن البرامج التي نقوم بتثبيتها، صادرة عن مصادر موثوقة ولم يجر العبث بها أو تعديلها عند نقلها
- عدم تنفيذ أيّ برنامج تم الحصول عليه عبر البريد الإلكتروني
- توخي الحذر عند استعمال متصفح الويب بسبب تشغيله الآلي لبريمجات Java، و Javascript، وActiveX التي يقوم بتحميلها اعتباراً من صفحات الويب. لذا، من الأفضل إعداد المتصفح لتعطيل التشغيل الآلي لهذه البرامج
- تطبيق مبدأ استخدام الحدّ الأدنى من الامتيازات عند استخدام الحاسوب في النشاط اليومي العادي (تصفح مواقع الويب، استخدام معالج نصوص، استخدام برامج رسم، ... الخ). فمن الأفضل عدم استخدام امتيازات لا حاجة للمستخدم بها حتى ولو كان المستخدم يعمل على حاسوبه الشخصي
- إذا وقع المستخدم ضحيّة برنامج من نمط حصان طروادة، يمكن لبعض البرامج المضادة أن تزيل البرنامج وأن تعالج الضرر الذي يتسبب به. إلا أنه من المفضل، عند اكتشاف مثل هذه البرامج، فصل النظام عن الشبكة (في حال اتصاله بشبكة محلية) وإعادة بناء النظام وتثبيت البرامج، وتطبيق برامج التصحيح الخاصة بنظام التشغيل وبالبرامج الاستثمارية

إدارة الحاسوب عن بعد بصورة غير شرعية

توجد، على أنظمة Windows، عدة أدوات يستعملها الدخلاء للتمكن من إدارة حاسوب عن بعد، نذكر منها: Backorifice، وNetbus، وSubSeven.

ما هي أساليب الحماية الممكنة؟

يستطيع الدخيل بعد تثبيته لمثل هذا النوع من البرامج، تعديل نظام التشغيل على نحوٍ كامل. لذا، يجب إعادة بناء نسخة كاملة من النظام المُخترَق لتحليلها من قبل المستخدم أو من قبل أحد المختصين، من خلال:

- البحث عن التعديلات التي جرت على خدمات النظام وملفات إعداده
- البحث عن التعديلات التي جرت على بيانات المستخدم
- البحث عن أدوات وبيانات تركها الدخيل خلفه
- مراجعة ملفات التسجيل الخاصة بنظام التشغيل
- البحث عن أدوات تنصت شبكية
- فحص أنظمة أخرى على الشبكة
- إعادة تثبيت نظام التشغيل اعتباراً من قرص مُدمج
- إعادة النظر في الخدمات العاملة على الحاسوب وتعطيل الخدمات غير الضرورية
- تثبيت برامج تصحيح الأنظمة والأدوات
- الانتباه عند استعادة معطيات من وسائط التخزين، فقد يكون الدخيل قد عبث بالمعطيات قبل تخزينها
- تغيير كلمات السر المُستخدَمة

توجد، على أنظمة Windows، عدة أدوات يستعملها الدخلاء للتمكن من إدارة حاسوب عن بعد، نذكر منها: Backorifice، وNetbus، وSubSeven. تسمح هذه البرامج، في حال تثبيتها، بوصول الدخلاء إلى الحاسب وبسيطرتهم عليه.

يمكن أن تصل هذه البرامج إلى حاسوب عبر أحصنة طروادة. إذ غالباً ما تكون هذه البرامج مؤلفة من قسمين: برنامج مخدم صغير الحجم، يتم تمريره إلى الحاسوب عبر أحد أحصنة طروادة وبحيث يصبح جزءاً من نظام التشغيل ويصبح بإمكانه الإقلاع مع إقلاع الحاسب. وبرنامج زبون يبقى على حاسب الدخيل، ويتيح له التحكم بحاسب الضحية.

ما هي أساليب الحماية الممكنة؟

يستطيع الدخيل بعد تثبيته لمثل هذا النوع من البرامج، تعديل نظام التشغيل على نحوٍ كامل. لذا، قد لا ينفع حذف البرنامج ونزعه من على نظام التشغيل، بل يجب إعادة بناء نسخة كاملة من النظام المُخترَق لتحليلها من قبل المستخدم أو من قبل أحد المختصين، من خلال:

- البحث عن التعديلات التي جرت على خدمات النظام وملفات إعداده
- البحث عن التعديلات التي جرت على بيانات المستخدم
- البحث عن أدوات وبيانات تركها الدخيل خلفه
- مراجعة ملفات التسجيل الخاصة بنظام التشغيل
- البحث عن أدوات تنصت شبكية
- فحص أنظمة أخرى على الشبكة
- إعادة تثبيت نظام التشغيل اعتباراً من قرص مدمج (عدم الاعتماد على صور سابقة لنظام التشغيل، لأنها قد تكون مصابة بنفس البرنامج)
- إعادة النظر في الخدمات العاملة على الحاسوب وتعطيل الخدمات غير الضرورية

- تثبيت برامج تصحيح الأنظمة والأدوات
- الانتباه عند استعادة معطيات من وسائط التخزين، فقد يكون الدخيل قد عبث بالمعطيات قبل تخزينها
- تغيير كلمات السر المُستخدَمة

البرامج المتنقلة (Applet Java / Javascript / ActiveX / Macros)

هي عبارة عن برامج، يمكن لها أن ترتبط بكل ما يتناقله مستخدم خدمات وتطبيقات الإنترنت مع المخدمات (وب، بريد إلكتروني، وغيرها)، بحيث يجري تنفيذ العديد من البرامج على حاسب المستخدم ودون علمه.

- عند ملئ استمارة على موقع وب
- عند فتح رسائل بريد إلكتروني
- فتح ملفات ملحقة (attached files) برسائل واردة عبر البريد الإلكتروني

ماذا يمكن للبرامج غير البريئة، أن تفعل؟

- التقاط كلمات مرور يُطلب إليك إدخالها
- التعرض لأجزاء محدودة من الشبكة التي تعمل عليها
- يمكن للماكروز المرافقة لملفات office أن تقوم بعمليات حذف على ملفات، وعمليات تثبيت ملفات، وعمليات تشغيل برامج

كيف نتجنّب المشكلة؟

يتلخص الأسلوب الأمثل، لتجنب مثل هذه البرامج، بتعطيل تشغيل كلّ أنماط البرامج المتنقلة التي يمكن أن تعمل على الحاسوب.

هي عبارة عن برامج، يمكن لها أن ترتبط بكل ما يتناقله مستخدم خدمات وتطبيقات الإنترنت مع المخدمات (وب، بريد إلكتروني، وغيرها)، بحيث يجري تنفيذ العديد من البرامج على حاسب المستخدم ودون علمه. فمن بين الطرق التي يتعرض فيها مستخدم الإنترنت لمثل هذه البرامج:

- **عند ملئ استمارة على موقع وب** فعندما يقوم المستخدم بزيارة موقع وب يطلب منه ملئ استمارة معينة، فإن صفحة الموقع التي يفتحها المتصفح تحتوي في أغلب الأحيان، على برنامج متنقل يجري تنفيذه من قبل المتصفح، ويهدف لتنفيذ عمليات تحقق نمطية على بعض المعلومات التي يدخلها المستخدم قبل إرسالها. فعلى سبيل المثال، إذا كان المطلوب إدخال رقم هاتف، يسعى البرنامج المرافق للصفحة، إلى التحقق من أن سلسلة المحارف التي أدخلها المستثمر، مؤلفة من أرقام فقط. إذ لا داعي لإرسال الصفحة إلى مخدم الوب للتحقق من صحة عمليات إدخال نمطية، من النوع الآنف الذكر، تجنباً لحالات ذهاب وإياب متكررة بين المتصفح والمخدم
- **عند فتح رسائل بريد إلكتروني** تحمل معها مثل هذا النوع من البرامج، وبحيث يجري تشغيل البرامج حال فتح الرسالة في بعض الأحيان
- **فتح ملفات ملحقة (attached files) برسائل واردة عبر البريد الإلكتروني.** إذ تملك مجموعة الأدوات المكتبية Microsoft Office، على سبيل المثال، أدوات برمجية تسمح بكتابة برامج مرافقة للنصوص أو الملفات، ندعوها Macros، بلغة برمجية خاصة تدعى VBA (Visual Basic application). يمكن اعتماداً على هذه الآلية تطوير برامج متنقلة مرتبطة بملفات office، يتم تفعيلها عند فتح الملف أو إغلاقه أو القيام بأي عملية عليه

ماذا يمكن للبرامج غير البريئة، أن تفعل؟

- التقاط كلمات مرور يُطلب إليك إدخالها، أو أي معلومات أخرى تعتقد أنها معلومات محمية
- يمكن أن تُستخدم هذه البرامج للتعرض لأجزاء محدودة من الشبكة التي تعمل عليها
- يمكن للماكروز المرافقة لملفات office أن تقوم بعمليات حذف على ملفات، وعمليات تثبيت ملفات، وعمليات تشغيل برامج

كيف نتجنّب المشكلة؟

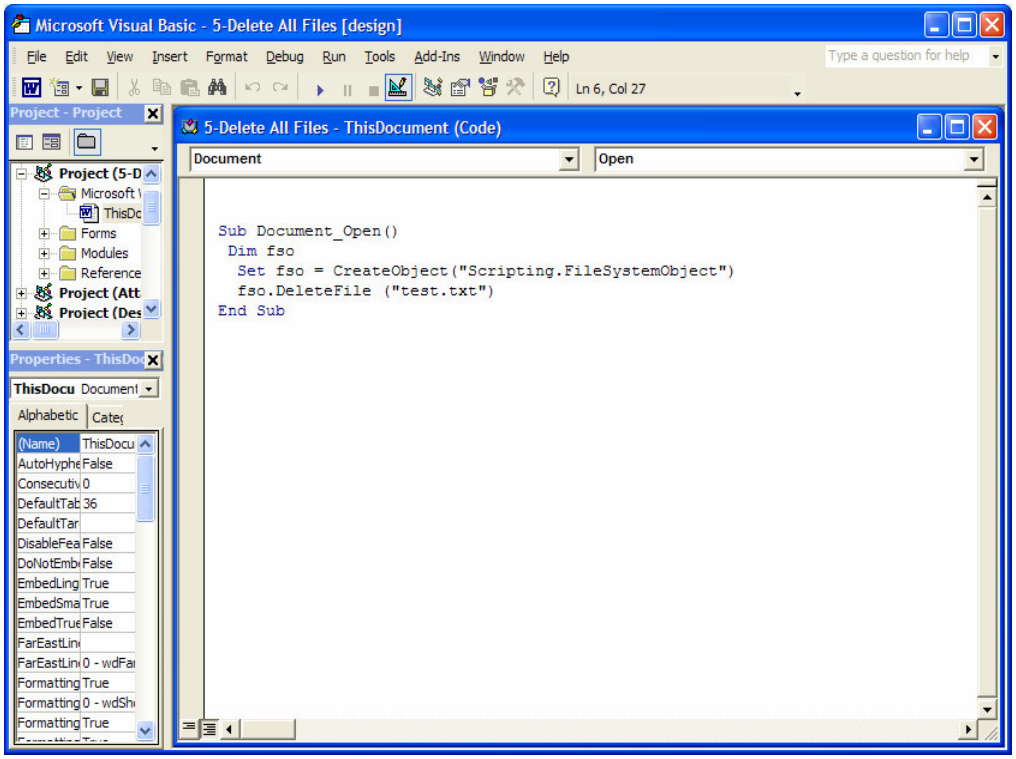
يتلخص الأسلوب الأمثل، لتجنب مثل هذه البرامج، بتعطيل تشغيل كلّ أنماط البرامج المتنقلة التي يمكن أن تعمل على الحاسوب. على كل حال، لا يمنع الإجراء السابق بعض أنواع البرامج المتنقلة من الاستمرار في العمل.

نشاطات

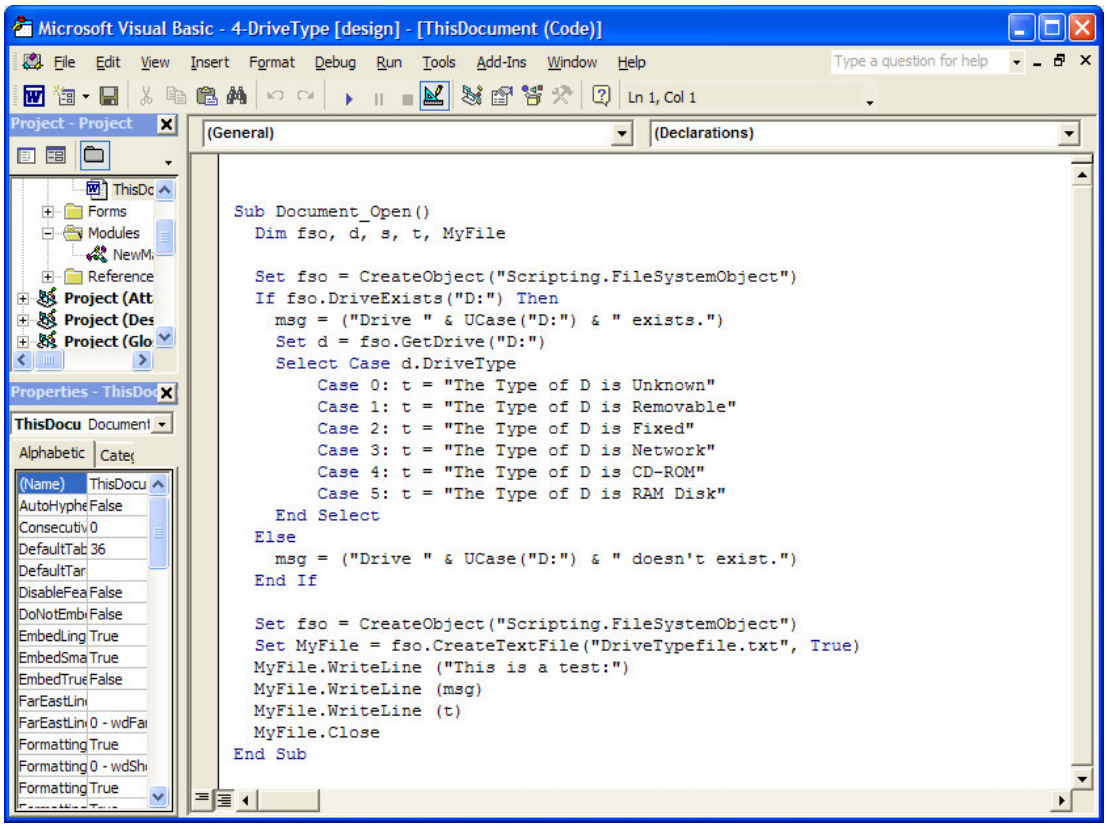
التعرف على الماكروز:

في حال أراد الطالب التعرف على هذه الآلية وعلى أدواتها التي دعاها البعض (Microsoft Virus Builder) أي "معمل Microsoft لبناء الفيروسات" يمكنه فتح ملف Word، والذهاب إلى قائمة أدوات (Tools)، واختيار ماكرو (Macros) وفتح محرر Visual Basic (Visual Basic Editor) والإطلاع عبر تعليمات المساعدة (help) على إمكانيات هذه الأداة !!

مثال عن ماكرو مرتبط بملف Word ويسمح بحذف الملف test.txt المتواجد في نفس المجلد الذي يتواجد به الملف Word المعني:



مثال عن ماكرو مرتبط بملف Word ويسمح بحذف الملف test.txt المتواجد في نفس المجلد الذي يتواجد به الملف Word المعني.



حلول للمشاكل المتعلقة بالماكروز

بالنسبة للماكروز المرافقين لملفات office، قدمت Microsoft حلاً للمشكلة عبر إلغاء التشغيل الأوتوماتيكي للماكروز، وذلك اعتباراً من سلسلة Office 2000. للتأكد راجع قائمة أدوات (Tools) في الأداة Word واختر أمان (Security)، يظهر لك بالنتيجة مستوى الأمان المتعلق بالتشغيل الآلي للماكروز.

حلول لبعض المشاكل المتعلقة بالبرامج المتنقلة مع صفحات الوب

أما بالنسبة لمتصفحات الإنترنت، فإننا نورد فيما يلي بعض الخطوات الضرورية لتغيير خيارات متصفح الويب من نوع Internet Explorer 5.0 (النسخة 5.0 أو النسخ أعلى).

- اختر من قائمة الأدوات (Tools) خيارات الإنترنت (Internet Options) ومن ثم صندوق حوار خيارات الإنترنت
- اختر استمارة الأمن (Security). ستظهر خيارات الأمن أمامك
- إنقر على منطقة الإنترنت (Internet) لإختيارها
- إختر الخيار العالي من القائمة الخاصة بـ مستويات الأمن (Security Levels)
- إذا أردت تشكيل مستويات الأمن يدوياً، انقر على زر اختيار المستويات (Custom Level) فتظهر لك قائمة بالخيارات المتاحة. تحتاج الآن لتصفّح قائمة الخيارات لتنفيذ التغييرات التي ترغب بها. قد ترغب بإلغاء تفعيل عمل كافة أنواع البرامج المتنقلة، أو إجبار المتصفح على إرسال طلب سماح بتشغيلها في كل مرة يحتاج فيها لتحميل وتشغيل مثل هذه البرامج، أو قد ترغب بتفعيلها جميعاً!

- بالعودة إلى خيارات الإنترنت (Internet Options)، إنقر استمارة الخيارات المتقدّمة (Advanced)
- تأكّد من تفعيل الزر الذي يجعل المتصفح يرسل تحذيراً في حال حدث تغيير بين حالة آمنة وحالة غير آمنة، والموجود تحت فقرة الأمن (security)

الفيروسات

تنتشر الفيروسات والأنواع الأخرى من البرامج الضارة، في أغلب الأحيان، كملحقات لرسائل البريد الإلكتروني. لذا وقبل فتح أيّ ملفات ملحقة، يجب التأكد من مصدر الملحقات إذ لا يكفي أن يكون عنوان الرسالة معروفاً. فقد انتشر فيروس Melissa بسرعة لأنه كان يبدو آتياً من عنوان مألوف بالنسبة للمستثمر.

تستعمل العديد من الفيروسات والعديد من مروجيها أساليب أذكى. فقد يجري توزيع البرامج الضارة أيضاً مع البرامج المسلية كبرامج الألعاب وبرامج الخدمات المختلفة. كما يمكن التحايل على القواعد السلوكية للمستخدم والسعي لاستخدام أساليب خداع أو إغراء.

على كل حال يجب تجنب تشغيل أي برنامج لم نستعلم، على نحو كافٍ، عن مصدره، وعن الشخص أو المؤسسة التي طورته. كما يجب تجنب إرسال برامج مجهولة الأصل، للأشخاص المحيطين بنا فقد تكون هذه البرامج بمثابة أحصنة طروادة الحاملة لمختلف أنواع المفاجآت غير السارة.

مواصفات الفيروس:

- برنامج ضيف يتطفل على برنامج آخر يسمى المضيف
- يستطيع تكرار نفسه بحيث يحقق انتشاراً أوسع
- خطورته تبدأ من المعدومة إلى المدمرة
- يهاجم برامج محددة
- يغير البيانات الخاصة بالبرامج المهاجَمة
- يقوم بعملية التكاثر لإنتاج برامج إضافية متضررة
- تصيب معظم الفيروسات البرنامج مرة واحدة
- تعمل معظم البرامج المُصابة بشكل مقبول لفترة معينة من الزمن
- تتغير بعض الفيروسات وتتبدل لمنع كشفها

متى نقول عن برنامج أنه فيروس؟

- أن يكون قادراً على استنساخ نفسه
- أن يتطفل على برنامج بدمج نفسه فيه
- ألا يقتصر على برنامج واحد
- أن يكون قادراً على عدم إصابة نفسه
- أن يعلم إن كان برنامج معين مصاباً أو لا
- ألا يصيب البرنامج المصاب مرة أخرى

أجزاء الفيروس:

- مُكرِر – Replicator: يحوي هذا الجزء على معلومات التكاثر
- حامي – Protector: يهتم هذا الجزء بحماية الفيروس من الكشف عن طريق التشفير والتبدل
- قادح – Trigger: يهتم هذا الجزء بانتظار الحدث الذي يبدأ عنده الفيروس بتنفيذ المهمة الموكلة إليه
- حِمل – Payload: يحتوي هذا الجزء على المهمة الموكلة للفيروس والتي غالباً ما تكون مؤذية

المناطق التي يهاجمها الفيروس:

- قطاع الإقلاع: يصيب هذا النوع من الفيروسات قطاع الاقلاع في الجهاز، وقد يمنع هذا النوع من الفيروسات المستخدم من الوصول الى النظام ويمنعه من اقلاع الجهاز.
- الملفات التنفيذية
- الملفات النصيّة: تصيب الفيروسات برامج Office مثل Word وExcel. إذ تنتشر هذه الفيروسات انتشاراً واسعاً جدا وتُقدر نسبتها بـــ 75% من عدد الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير محتويات المستندات. فقد تجد بعض التصرفات غير المنطقية في بعض الاحيان مثل طلب كلمة مرور لفتح ملف تعرف انك لم تضع عليه كلمة مرور.

أنواع الفيروسات:

- الفيروسات الشبكية: وهي تنتقل عبر الشبكة عن طريق مشاركة المجلدات والملفات.
- الديدان: تنتقل الدودة عبر الحواسب الموصولة بالشبكة بشكل اوتوماتيكي، ومن غير تدخل الانسان، ويجعلها هذا الامر تنتشر بشكل اوسع وأسرع من الفيروسات. لا تقوم الديدان بحذف او تغيير الملفات بل تقوم باستهلاك موارد الجهاز واستخدام الذاكرة بشكل كبير مما يؤدي الى بطء ملحوظ جدا للجهاز' لذا من المهم تحديث نسخ نظام التشغيل المستخدمة بشكل مستمر كي يتم تجنب الديدان.
- الفيروسات متعددة الأقسام: وهي الفيروسات التي تكون لها عدة أشكال من الأشكال السابقة وتكون مدمرة في كثير من الاحيان اذا لم يجر الوقاية منها.

متى نشك بوجود الفيروسات:

- بطء الجهاز الشديد، بما لا يتناسب مع عدد البرامج التي تعمل في نفس الوقت
- امتلاء القرص بما لا يتناسب مع عدد وحجم الملفات الموجودة عليه
- ظهور مربّعات حوار غريبة اثناء العمل على الجهاز
- اضاءة لمبة القرص الصلب أو القرص المرن، دون أن تقوم بعملية فتح أو حفظ ملف

الآليات المستخدمة للتعرف على الفيروسات:

- البحث عن توقيع الفيروس: من خلال مطابقة محتوى الملفات مع تواقيع فيروسات سابقة مخزنة ضمن قواعد بيانات يمتلكها مضاد الفيروسات (لكل فيروس توقيع يستخدمه حتى لايصيب نفسه أو يصيب ملفات سبق له وأصابها).
- ملاحظة التغييرات المفاجئة وغير المتوقعة على الملفات
- البحث عما يشبه عمل الفيروسات ولو لم يكن هذا الفيروس معروف سابقاً

نصائح عامة للوقاية من الفيروسات:

- النسخ الاحتياطي الدوري للملفات
- استخدام مضادات الفيروسات وتحديثها باستمرار
- عدم فتح الملفات المرفقة مع الرسائل الالكترونية دون وجود مضاد فيروسات
- فحص الأقراص المتنقلة بشكل دائم قبل استخدامها
- تعطيل ميزة تشغيل الماكرو في البرامج المكتبية
- استخدم خاصية فحص الفيروسات المدمجة مع الـــ BIOS لفحص فيروسات الإقلاع
- منع المستخدمين من تنصيب برامج غير مرخصة من قبل المؤسسة التي يعملون بها

اللواحق المخفية لأسماء الملفات

تحتوي أنظمة التشغيل Windows على خيارا لإخفاء لواحق أسماء الملفات ذات الأنماط غير المعروفة". يكون الخيار مفعّلاً بشكل تلقائي. لكن يمكن للمستخدم أن يعطل هذا الخيار لكي يتم عرض لواحق أسماء الملفات.

تستغل الفيروسات المنقولة عن طريق البريد الإلكتروني اللواحق المخفية لأسماء الملفات. وقد كان الهجوم الذي شنته الدودة LoveLetter الأول من نوعه الذي استغل هذه اللواحق بحيث كانت الدودة محتواة ضمن ملف ملحق برسالة بريد إلكتروني بعنوان: "LOVE-LETTER-FOR-YOU.TXT.vbs" (لاحظ أن اللاحقة الأولى الكاذبة والظاهرة هي TXT في حين تكون اللاحقة الحقيقية vbs مخفية).

بطبيعة الحال تكون أيقونة الملف متوافقة مع اللاحقة الكاذبة. إذ يمكن لأيٍ كان وبسهولة تغيير شكل أيقونة أي ملف بعد إنشائه بحيث تظهر بالشكل المطلوب.

تبدو البرامج المُعتمِدة على مثل هذه الآليات وكأنها نصوص غير مؤذية من نمط (txt)، أو (jpg)، أو (avi) أو أي نوع من أنواع الملفات الأخرى. إلا أنها تحتوي حقيقةً على رماز غير برئ قابل للتّنفيذ (من نمط vbs أو exe على سبيل المثال).

لمقاومتها، نحتاج لتفعيل عملية إظهار لواحق أسماء الملفات.

نشاطات

تغيير شكل أيقونة ملف:

يمكن تغيير شكل أيقونة ملف تنفيذي وجعله يبدو كملف نصيّ، اعتماداً على قائمة أدوات (Tools) الخاصة بنافذة من نوافذ النظام، وباختيار خيارات المجلد (Folder Option)، وتعديل شكل الأيقونة في استمارة أنماط الملفات (Files Type).

إلغاء تفعيل عملية إخفاء اللواحق:

يمكن إلغاء تفعيل عملية إخفاء اللواحق اعتباراً من قائمة أدوات (Tools) الخاصة بنافذة من نوافذ النظام، وباختيار خيارات المجلد (Folder Option)، وبالبحث ضمن الاستمارة الخاصة بشكل الملفات المجلدات (Views) عن السطر المسؤول عن إخفاء اللواحق الخاصة بأسماء الملفات (Hide extensions).

التنصت

كما هو الحال في الشبكات الهاتفية، يمكن تنفيذ عملية تنصت ضمن شبكة داخلية لمراقبة الاتصالات التي تتم بين مختلف عقد الشبكة.

العملية:

- من أجل تنفيذ عملية التنصت، يجب أن يمتلك الدخيل حساب مدير نظام على الحاسب المُستخدم كمنصة تصنت. لذلك يجري التنصت عادةً عن طريق استخدام حاسب شخصي محمول موصول على الشبكة، أو عن طريق زرع برنامج تنصت على الحاسب المعني. (70% من حالات الاختراق تحصُل من الداخل)
- يُضاعِف من حجم المشكلة وجود عدد كبير من أنظمة التنصت المجانية السهلة الاستخدام التي تعمل تحت نظم الاستثمار المفتوحة Windows وUnix
- يستخدم الدخيل حالة PROMISCUOUS لبطاقة الشبكة التي تسمح لها بالتقاط كل ما يمر عبر الشبكة بغض النظر عن البروتوكول المغلف ضمن وحدة المعلومات IP الملتقطة
- عموماً يجب استخدام أدوات مراقبة للشبكة تساعدنا على ملاحظة إجرائيات في حالة تنفيذ على الأجهزة من أمثال Sniff winsniff أو أي إجرائية غير معروفة

مقاومة التنصت:

- الإقلال قدر المستطاع من السماح لأجهزة محمولة من الارتباط بالشبكة ومنع المستخدمين من استخدام الأجهزة المتصلة بالشبكة كمدير نظام
- استخدام Switch عوضاً عن Hubs. طبعاً، لايحلّ استخدام Switch لا يشكل حلاً كاملاً لمشكلة التنصت إذا يمكن للقرصان وضع أداة تنصت على جهاز بعد اختراقه بأساليب أخرى مما يسمح له بمراقبة جميع الاتصالات التي يقوم بها هذا الجهاز المخترق مع الأجهزة الأخرى
- عدم استخدام تطبيقات تعتمد على إرسال كلمات المرور عبر الشبكة بدون حماية

الإغراق

العملية:

- وهي عملية اختراق تهدف إلى تعطيل الخدمة Deny of Service، تقوم على مبدأ قصف الجهاز الضحية بعدد كبير من طرود من أنماط مختلفة كالطرود من نمط ICMP Echo (مثل طرود تعليمة Ping) من أجل زيادة حمله، وذلك بعد انتحال عنوان جهاز آخر حتى تصل ردود الطرود إليه.

- تخصص الضحية وقتها للرد على الطرود مما يؤثر على خدماتها الأخرى الطبيعية، وتزداد فعالية هذا الهجوم كلما كانت سرعة الوسط الفيزيائي بين الجهازين عالية
- يمكن لهذا الهجوم إيصال الموجهات أيضاً إلى حالات إشباع لا تصبح بعدها قادرة على أداء عملها، بالنتيجة يتم وضع خدمات الشبكة وعناصرها في حالة توقف عن الخدمة وتسبيب عمليات ازدحام واختنا قات في الشبكة
- يمكن لهذا أن يؤثر اقتصادياً على وضع الشركات التي تدير المخدمات وخصوصاً تلك التي تقوم بعمليات التجارة الإلكترونية عبر الانترنت، فقد سببت عملية من هذا النوع لشركة (Amazon) خسارة قُدرت بعشرات الملايين من الدولارات خلال 3 أيام

مقاومة الإغراق:

- يمكن ملاحظة المشكلة بملاحظة نوعية الخدمة التي تصبح بطيئة جداً بالإضافة إلى بطئ عمل الشبكة بشكل عام
- لا يعتبر منع مرور بعض أنواع الطرود كالطرود من نمط ICMP echo عبر الموجهات حلاً، إذ يعطل مثل هذا الحلّ عمل أدوات مراقبة وإدارة الشبكة
- في حال طرود ICMP Echo يجب مراقبة مستوى كثافة هذه الطرود وليس منعها تماماً بمراقبة ملفات التسجيل المستمر على الموجهات وذلك بهدف الانتباه إلى حصول ارتفاع كبير في مستواها

لمحة عن التشفير

مبادئ التشفير:

- تشبه عملية التشفير بشكل عام أسلوب اغلاق أو فتح قفل الباب:
  - لفتح أو لقفل الباب نحتاج إلى مفتاح
  - تختلف المفاتيح والأقفال بحجمها وتعقيدها
  - بعضها سهل الاختراق
  - الآخر صعب يحتاج لـــ Brut Force لكسرها
- لا تعتمد أساليب التشفير الحديثة على سرية الخوارزميات:
  - المفتاح هو العنصر السري الوحيد فهو سهل التبديل لذا يصعب كشفه
  - الخوارزمية صعبة التبديل وسهلة الكشف
  - إن عملية نشر خوارزميات التشفير أنتجت عملية "اصطفاء طبيعي" فالأقوى هو القادر على البقاء
  - ظهرت الكثير من خوارزميات التشفير التي يجري تعديلها بشكل مستمر للاحتفاظ بالأفضل وجعلها خوارزميات قياسية
- تعتبر عملية إدارة مفاتيح التشفير أساس عملية التشفير، لذا يحتاج المطورون لتحديد:
  - أين يتم توليد المفاتيح؟
  - كيف يتم توليد المفاتيح؟
  - كيف يتم تخزين المفاتيح؟
  - كيف يتم وصول المفاتيح إلى الأطراف التي تستخدمها؟

- أين تُستخدَم المفاتيح؟
- كيف يتم تبديل المفاتيح؟

- عند تبادل معلومات سرية يحتاج الطرفان لإيجاد مفاتيح مشتركة، نتكلم عندها عن بروتوكول تبادل مفاتيح. هناك عدة بروتوكولات:
  - Deffie-Hellman
  - Public Key Exchange Protocol

خوارزميات التشفير:

- من أجل رسالة M ومفتاح تشفير K_C يكون لدينا تابع تشفير C بحيث : $C[K_C](M)= M_E$
- من أجل رسالة مشفرة M_E ومفتاح فك تشفير K_D يكون لدينا تابع فك تشفير D بحيث: $D[K_D](M_E)=M$
- نقول عن خوارزمية التشفير أنها متناظرة في حال $K_C=K_D$
  - ندعوها بالخوازميات ذات المفاتيح السرية
  - ندعو المفتاح السري K_{AB}
  - خوارزميات: DES, IDEA
- نقول عن خوارزمية التشفير أنها غير متناظرة في حال أختلف K_C عن K_D
  - ندعوها بالخوازميات ذات المفاتيح العامة
  - يكون مفتاح التشفير عاماً K_{pub} يمكن تبادله، بينما يكون مفتاح فك التشفير خاصاً Kprv
  - يتم تبادل المفاتيح العامة بحيث يقوم كل طرف بالتشفير باستخدام المفتاح العام للطرف الآخر
  - ترتبط المفاتيح خوارزمياً ببعضها البعض دون أن يجعل ذلك بالإمكان استنتاج أحدهما من الآخر
  - خوارزميات: RSA, El Gamal

استخدام التشفير:

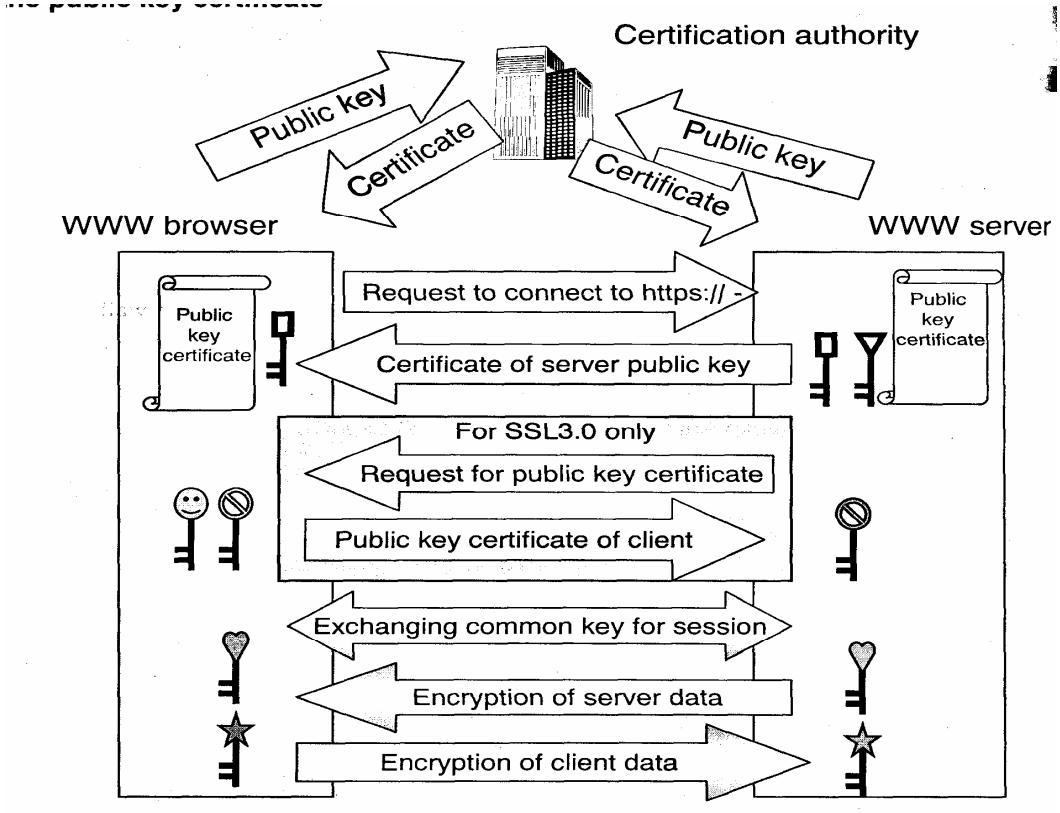
- الخوارزميات غير المتناظرة أبطأ من الخوارزميات المتناظرة (من 1000 إلى 10000 مرة)
- تستخدم الخوارزميات المتناظرة لتشفير الحجوم الكبيرة
- تستخدم الخوارزميات غير المتناظرة لتشفير حجوم صغيرة مع عمليات إدارة مفاتيح مثل عمليات التحقق من الهوية بتبادل كلمات سر مشفرة
- حسب ما سبق، تجري عملية دمج للطريقتين ضمن بروتوكول تشفير واحد يجري فيه استخدام خوارزميات ذات مفاتيح سرية متناظرة ولكن يجري تبادل هذه المفاتيح باستخدام خوارزميات غير متناظرة ذات مفاتيح عامة
- صلابة الخوارزمية وتحملها للكسر تعتمد على طول المفتاح بشكل أساسي وليس على التوابع.

شهادات الوثوقية الرقمية

- تفترض الأساليب السابقة التحقق من هوية مُرسل المفاتيح. إذ يجب أن نتأكد أن مُرسل المفاتيح هو الشخص الذي نريد التعامل معه وخصوصاً في حالات التجارة الإلكترونية

- لهذا الغرض، يجري استخدام شهادة وثوقية (أو ثقة) رقمية Numerical Certificate عند التشفير بهدف التأكد من هوية من يتعامل معنا
- تُعرَّف شهادة الوثوقيةبأنها مجموعة من المعلومات التي تسمح بتوصيف كامل لعنصرما:
  - يجري إصدارها من قبل سلطة خاصة مستقلة ندعوها سلطة إصدار شهادات الوثوقية وتمتلك إمكانيات التحققمن صحة هوية العنصر المعني بالشهادة
  - تتضمن هذه المعلومات:
    - مفتاح التشفير العام لهذا العنصر وخوارزمية التشفير العام مما يسمح بالتأكد من توقيعه الإلكتروني
    - فترة صلاحية الشهادة
- تكمن أهمية السلطة المسؤولة عن اصدار شهادة وثوقية في استقلالها وفي إصدارها لشهادات ذات مدة محددة
- يمكن للسلطة التي أصدرت شهادة الوثوقية أن توقعها (Root CA) أو أن تطلب من سلطة أخرى التوقيع على شهادة الوثوقية. عندها يجب تحديد سلسلة الموقعين على الشهادة

SSL (Secure Socket Layer)



الجدول المُلحق (الترجمة):

Public Key	مفتاح عام
Certificate	شهادة وثوقية
Request to connect to: https://...	طلب اتصال https
Certificate of Server Public Key	شهادة الوثوقية الحاوية على المفتاح العام للمخدم
Public Key Certificate	شهادة خاصة بمفتاح عام
WWW browser	متصفح الوب
WWW Server	مخدم الوب
For SSL3 Only	نسخة SSL3 فقط
Request for public key Certificate	طلب شهادة الوثوقية الحاوية على المفتاح العام
Public Key Certificate of Client	شهادة الوثوقية الحاوية على المفتاح العام الخاص بالزبون
Exchanging Common Key for session	تبادل مفتاح الجلسة
Encryption of Server Data	تشفير معطيات المخدم
Encryption of Client Data	تشفير معطيات الزبون
Certification Authority	سلطة إصدار شهادات الوثوقية

ملاحظات:

- تقوم خدمة إدارة المفاتيح بتوليد ملف طلب لشهادة وثوقية وإرسالها بشكل مباشر من أجل الحصول على شهادة وثوقية. .عند الحصول عليها يجري تثبيتها من قبل خدمة إدارة المفاتيح
- نحتاج لمخدم يولد شهادات وثوقية من أجل إقامة اتصال من نمط SSL
- يستخدم مخدم الوب شهادة الوثوقية تلك للتأكيد على صحة هويته
- نحتاج لاستخدام مخدم توليد شهادات وثوقية خارجي عمومي على الإنترنت في حال وجود مخدم الوب على الإنترنت
- في حال كانت الحاجة داخلية (إنترانت) يمكن تشكيل هيئة توليد شهادات الوثوقية داخلياً باستخدام أدوات مثل Certificate Server

إقامة جلسة SSL :

- يقوم الزبون (المتصفح) بإقامة اتصال مع مخدم الوب؛
- يقوم المخدم بالرد على المتصفح بإرسال شهادة الوثوقية الخاصة به مع مفتاحه العام. تدل شهادة الوثوقية على كون مخدم الوب هو مخدم موثوق وليس مخدم مُدَعي
- يتحاور المتصفح مع المخدم عن مستوى التشفير (40بت، 128بت ...)

- يقوم المتصفح بتوليد مفتاح خاص بالجلسة ويقوم بتشفيره باستخدام المفتاح العام الذي يخص مخدم الوب ويرسلها إلى المخدم بشكل آمن
- يستخدم المخدم مفتاحه الخاص لفك تشفير مفتاح الجلسة ويستخدم هذا المفتاح الناتج (مفتاح الجلسة) لإقامة قناة اتصال آمنة مع المتصفح للتراسل فيما بينهما عبر تشفير المعطيات المرسلة بمفتاح الجلسة