جامعة فلسطين التقنية
خضوري
Palestine Technical University
Kadoorei

الوحدة الأولى:
مقدمة للشبكات والانترنت

1

شبكات الحاسوب

14130340

أهداف الوحدة

- تعرف ماهية شبكات الحاسوب
- نفرق بين أنواع الشبكات
- تبين الفرق بين الانترنت والانترانت والاكسترانت
- تعرف أشكال وأنواع الكابلات المستخدمة لنقل البيانات

شبكات الحاسوب

- تعرف الشبكة على أنها مجموعة من الأجهزة المرتبطة مع بعضها بعضا بكيفية معينة قادرة على تبادل المعلومة فيما بينها.
- أدى استخدام الشبكات إلى توفير جهد كبير جداً كان يبذل في تداول المعلومات والبيانات بين أفراد منظومة أي نظام معلومات.
- Global Village العالم قرية صغيرة.
- بالسرعة الهائلة.
- تنظيم حياته الشخصية والعملية.

شبكات الحاسوب

4

- الشبكات نتيجة التطور السريع الحاصل في :
  - الحاسوب.
  - الاتصالات.
- التطور ساعد على زيادة انتشار الشبكات وتحسن عمله.
- وبسبب انتشار الشبكات أصبح هناك مشاركة في المعلومات والبرامج والموارد أمراً يسيراً جدا.
- إن جهاز الحاسوب انجاز عظيم ولكنه يزداد عظمة عندما يكون هناك اتصال مع حاسوب آخر من خلال الشبكات.
- الشبكات ساهمت في ثورة معلوماتية ضخمة.

نظرة عامة على الشبكات

- وفي العقدين السادس والسابع (1960-1970) أنظمة المعلومات لشركة معينة يتم إدارتها من خلال تخزينها على حاسوب مركزي (mainframe).
- العقد الثامن من القرن العشرين (1980) بدأ ظهور أجهزة الحاسوب الشخصية والتي تسببت في تغييرات كبيرة جداً في مجال الأعمال والصناعة.
- **الفرق بين الحاسوب الشخصي في بناء الشبكة و (mainframe):**
  - في شبكات الحاسوب عدد من الحواسيب الشخصية يمكن لها استخدام أو الحصول على ملفات من الخادم الرئيس (Server) وكل من هذه الحواسيب الشخصية يمتلك إمكانية تشغيل منفصلة عن الخادم الرئيس.
  - لكن في أنظمة الحاسوب المركزي (Main Frame) يوجد نهايات طرفية (Dummy Terminals) لا تمتلك أي إمكانية معالجة. وكل شيء محمل على الحاسوب المركزي.
  - وأيضاً في أنظمة الشبكات يتم تحقيق (Processing System Distribute) أي توزيع المهمات على الحواسيب المرتبطة بالشبكة.

الإدارة المركزية
CENTRALIZE MANAGEMENT

- لأن معظم الموارد موجودة بجانب الخادم.
- تصبح الإدارة سهلة.
- وعمليات استرجاع المعلومات سهلة.
- ولكن فيها مشكلة: عندما يحدث عطل في السيرفر ماذا يحدث؟؟؟

مكونات الشبكة

1. خادم Server.
2. محطات عمل Workstations.
3. بطاقة الشبكة Network Interface Card.
4. الكوابل Cables.
5. موارد المشاركة Shared Resources and Peripherals.

الخادم
SERVER

- هو ذلك الجهاز المنوط به أداء المهام التالية لكل محطة station ومن هذه المهام:
  1. تخزين الملفات.
  2. إدارة المستخدمين.
  3. ضبط أمن البيانات والمعلومات.
  4. الأوامر الخاصة بالشبكات.

محطات العمل
WORK STATIONS

- هو حاسوب مرتبط على الشبكة ويكون عضو بالشبكة ويسمي node أو station.
- تعمل بأي نوع من أنظمة التشغيل المختلفة windows , Linux.
- ممكن أن تملك وحدات تخزين ومعالجة وممكن أن لا تملك.
- في حال لا يوجد أقراص يتم تحميل نظام التشغيل من الخادم عن طريق كرت الشبكة.
- في حال محطات العمل التي لا تملك معالجة ولا وحدات تخزين تعتبر رخيصة مقارنة.

بطاقات الشبكة
NETWORK INTERFACE CARD

- يستخدم لربط الجهاز بالشبكة.
- تكون جزء أساسي من الجهاز build in أو عبارة عن كرت توصل بالجهاز.
- هناك أنواع مختلفة وكثير حسب الشركة المصنعة.

الكابلات
CABLES

- هي الأسلاك المستخدمة في ربط الخادم بالمحطة
- يوجد منها أنواع وهي:
  1. الأسلاك المحورية.
  2. الأسلاك المجدولة.
  3. الألياف الضوئية.

إشارات الإرسال
TRANSMISSION SIGNALS

- لكي يتمكن جهاز حاسوب من الاتصال بحاسوب أخر يجب:
  - أن تتم ترجمة البيانات إلى إشارات.
  - توفر قناة اتصال لإرسال واستقبال الإشارات.

- تستطيع الأجهزة استخدام الأنواع التالية من الإشارات للاتصال فيما بينها:
  - النبضات الكهربائية.
  - موجات الراديو.
  - موجات الميكروويف.
  - الأشعة تحت الحمراء.

- جميع هذه الإشارات تعتبر موجات كهرومغناطيسية.
- من الممكن تعديل الإشارة والتحكم بها باستخدام أشباه الموصلات.
- تستطيع تمثيل الإشارات التماثلية والرقمية.

لماذا نستخدم المقويات REPEATERS في الإشارات الرقمية

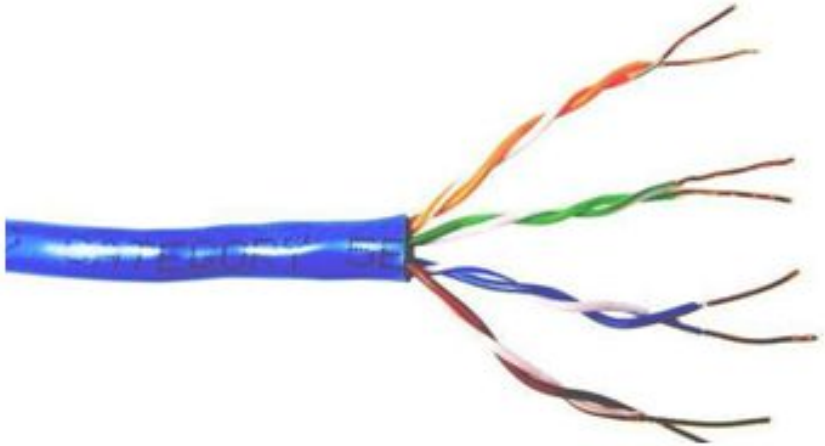
- لأنها لا تستطيع الانتقال لمسافات بعيدة نتيجة:
  1. وجود تشويش.
  2. تحمل سعة معينة.
  3. الاشارة معرضة للضعف والتلاشي.

- لذلك يستخدم الاشارات التناظرية في المسافات البعيدة لتلاشي تلك المشكلة.

الكابلات

- الأسلاك المحورية Coaxial Cable.
- الأسلاك المجدولة Twisted Pair.
- الألياف البصرية (الضوئية) Fiber Optic.

- Unshielded twisted pair (UTP)



- Shielded twisted pair (STP)

- Coaxial cable

- Fiber optic

خصائص الأسلاك المحورية

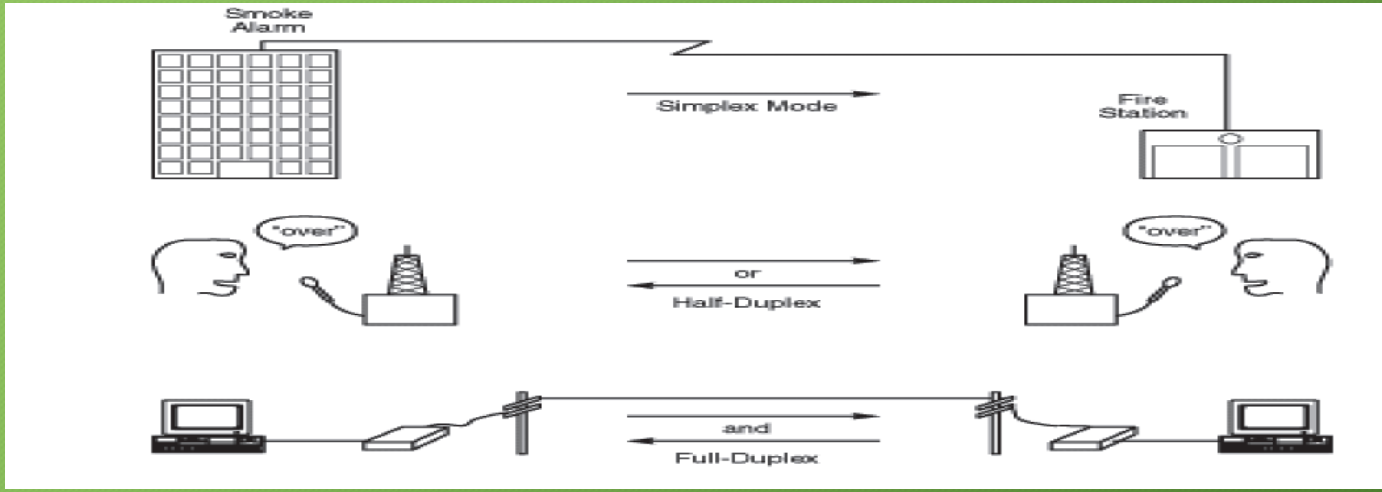
- يمكن أن تتأثر بأي تدخلات خارجية
- تلتقط تشويش خارجي من موجات الراديو والموجات الالكترونية.
- لها مشكلات مع التأثير الأرضي.
- تشع موجات خارجية يمكن أن تسرق من المتطفلين.
- منها نوعين: Thin و Thick.
- أقل الأنواع من حيث التكلفة.
- يعتبر محدود المسافة حوالي 100 متر.
- قابل للتأثير بأي تدخلات خارجية.

خصائص الألياف الضوئية

- تستخدم بكثرة في الربط بين شبكات المتباعدة.
- سعره أعلى.
- يعطي مسافات أطول.
- سرعة النقل عالية.
- لا يشع موجات خارجية وبالتالي درجة عالية في الأمان.
- قوي ولا يتأثر بالعوامل الجوية.

كيف يتم بناء الشبكة وإشكال الاتصال

- يتم بناء الشبكات من خلال بطاقات الاتصال.
- أشكال الاتصال:
  - أحادي الاتجاه Simple-Dublex، مثل: الإذاعة.
  - ثنائي الاتجاه Half-Dublex، في وقت غير متزامن، مثل: السيناو.
  - ثنائي الاتجاه Full-Dublex، بنفس الوقت، مثل: الهاتف.



معايير تحديد نوع وسيلة الاتصال

1. سرعة الإرسال ونقل المعلومات.
2. أقصى طول للكابل بدون مقوي الإشارة Repeater.
3. التكلفة المطلوبة.
4. كمية الكابلات للمبني.
5. أسلوب حماية الكابلات من التداخل.
6. درجة الأمان للمعلومات المنقولة.
7. السعر.

الخلاصة

- أهمية الشبكات وخلفياتها التاريخية.
- الهيكل العام للشبكات.
- الإشارات الرقمية والتناظرية.
- أنواع الأسلاك المستخدمة في الاتصال.

انتهت الوحدة الأولى

مع تمنياتي لكم بالتوفيق

جامعة فلسطين التقنية
خضوري
Palestine Technical University
Kadoorei

الوحدة الثانية:
تراسل البيانات والشبكات

1

شبكات الحاسوب

14130340

أهداف الوحدة

- أهمية الشبكات وبرمجياتها والبرتوكولات.
- الطبقات الرئيسية في الشبكات .
- الفروق في الشبكات.
- ضبط الأخطاء في الإرسال والاستقبال.
- مرور الرسائل في الشبكة.

الانترنت والاتصالات

- الاتصالات Communication أقدم من الحوسبة.
- التلغراف ،....
- تطورت وسائل الاتصال السلكية و اللاسلكية و من ثم الاعتماد على الألياف الضوئية.
- النقل الرقمي يعتبر النقلة النوعية في وسائل الاتصالات

الانترنت
INTERNET

- أكبر شبكة اتصالات (شبكة الشبكات)
- الإنترنت شبكة غير تجارية.
- مكونة من عدة شبكات فردية وجماعية وحواسيب موزعة في جميع أنحاء العالم، مرتبطة معا بدون شكل محدد.
- مملوكة لكل الأفراد و المؤسسات و ليست مملوكة لطرف بعينه.
- ARPAnet (1969 - 1960): Advanced Research Projects Agency شبكة لأغراض الأبحاث العسكرية.
- 1989 تم وقف الأربانت، و إنشاء الإنترنت.
- كلمة إنترنت مشتقة من اسم بروتوكول الإنترنت.
- مستخدم الحاسوب يمكنه الوصول إلى المعلومات و الأنظمة و التشارك مع الآخرين في نفس الوقت.
- الاتصال في الإنترنت غير محدد بمسار ثابت.

الانترنت
INTERNET

- عدة شبكات اتصالية فردية وجماعية ومجموعة حاسبات متناثرة وموزعة في جميع أرجاء العالم مرتبطة معاً في كتلة لم يتبلور لها شكل معين حتى الآن.
- فقد ظهرت الإنترنت إلى الوجود كثمرة لمشروع حكومي أمريكي بدأ تنفيذه كلفت) -ARPAnetعام 1960وتحقق وجوده النهائي عام 1969وقد سمي)الاربانت
- في عام 1989قررت الحكومة الأمريكية وقف تمويل الأربانت ووضعت خططاً لإنشاء خلف تجاري لها في شكل شبكة تقرر تسميتها الإنترنت وقد اشتق الاسم من اسم البروتوكول الأساسي للاتصالات وظل أغلب مشتركي الإنترنت من بين العلماء داخل الجامعات والشركات العاملة في صناعة الحاسوب واستخدموها لتبادل البريد الإلكتروني.

الانترنت
الميزات التقنية

- توفير قواعد تبادل النصوص والملفات.
- توفير نموذج مالي مقبول (وسيلة اتصال دائمة بسعر ثابت بدلا من الحساب على أساس المدة). Leased Line
- يعتمد على بروتوكول (ضبط الإرسال /بروتوكول الإنترنت TCP/IP (Transmission Control Protocol / Internet Protocol
- السعة النطاقية : Bandwidthسرعة نقل البيانات عبر الشبكة ، وتتنوع السرعة بناء طبيعة وسيلة الاتصال ووسيط النقل) (. Analog, Digital
- نقل البيانات في الإنترنت لا يكون بمعدل ثابت -يتحكم به الازدحام.

الانترنت
الميزات التقنية

- نموذج يتيح الخروج من مأزق الكلف الباهظة مقابل استغلال شبكات الاتصال التي تؤدي بدلات استخدامها تبعاً لوقت الاستعمال والمسافة.
- إن الوضع المتفرد للإنترنت ينشأ عن عدة عناصر:

1. أولها :برمجيات أو بروتوكولات الاتصال ؛ وهي مجموعة قواعد برمجية تحدد الطريق التي تتصل بها آلة بأخرى،
2. والبروتوكول الرئيس للإنترنت هو ما يعرف ببرتوكولات ضبط الإرسال/بروتوكول الإنترنت tcp/ip

الانترانت
INTRANET

- الإنترانت عبارة عن شبكة حاسوب خاصة بمؤسسة ما تستعمل البروتوكولات والقواعد التي بني عليها الإنترنت.
- وذلك كي تمكن الأفراد والعاملين من الاتصال ببعضهم البعض.
- والوصول إلى المعلومات بطريقة أسرع وأفضل وأكثر كفاءة وأقل كلفة من الأساليب التقليدية المعتادة.

الانترانت
INTRANET

- شبكة حاسوب خاصة بمؤسسة تستعمل بروتوكولات الإنترنت.
- عبارة عن نسخة مصغرة من الإنترنت.
- البيانات تكون محدد حسب طبيعة عمل المؤسسة ويستطيع
- الوصول إليها العاملون في المؤسسة فقط.
- يمكن الولوج من الإنترانت للإنترنت وليس العكس عدا المسجلين فيها (Firewall).
- نموذج مطور من نظام (Client/Server).

مبدأ عمل الانترانت

- يختلف مبدأ شبكات INTRANET عن مبدأ شبكة الإنترنت. فتوجه الإنترانت إلى المستوى الخاص، وليس إلى المستوى العام.
- ويعني ذلك أن المعلومات في الإنترانت هي معلومات خاصة، لا يسمح باستخدامها أو تبادلها، إلا من قبل مجموعة خاصة من المستخدمين.
- المدى الجغرافي للإنترانت يمتد من المحلى حتى الموسع.
- تأخذ طابع الظاهرية.
- يمكن وصلها بالإنترنت مع الحفاظ على خصوصيتها (الجدار الناري).

بناء الانترانت

1. تحليل ودراسة الجدوى:
   - حاجة العاملين للخدمات الإلكترونية.
   - الموارد و التطبيقات المشتركة بين العاملين.
   - تحديد آليات الوصول و الصلاحيات للمستخدمين.

2. اختيار أدوات العمل:
   - برامج التصميم و التطوير بحيث تتناسب مع الميزانية المحددة.
   - تحديد مصادر محتوى الموقع الداخلي و اختيار القائمين عليه.
   - تعيين فريق العمل (مصممين و مطورين).

بناء الانترانت

3. إصدار نسخة تجريبية Pilot Version لدراسة ما يلي :
   - قياس مدى قبول المستخدمين للحلول الجديدة.
   - الزمن الذي تم توفيره و سرعة إنجاز العمل.
   - تحديد مدى صحة و كفاية محتوى الموقع الداخلي على الإنترانت.
   - التأكد من إجراءات الصيانة الوقائية Preventive Maintenance و النسخ الاحتياطي Backup لمحتويات البيانات.

4. تنفيذ المشروع.
5. المتابعة و الصيانة.

الحاجة لوجود شبكة الانترانت

1. تقليص التكاليف Centralized Database - دليل الهاتف - طلبات الصيانة - الأجهزة تكون متواضعة للموظفين.
2. توفير الوقت: مثل البوابة الأكاديمية والإدارية التي تضمن وصول المعلومة استخدام نماذج معيارية حيث تلبي متطلبات ضمان الجودة Quality Assurance وتوفر دقة في التحكم بالجودة Quality Control.
3. الاستقلالية والمرونة: الربط بين أجهزة من عائلات وبيئات مختلفة، يتم النفاذ للموارد من خلال المستكشف Browser.
4. تسخير خدمات الإنترنت: خدمات Web باستخدام HTTP:
   - خدمات الاتصال و نقل المعلومات، مثل: البريد الالكتروني
   - خدمات التعرف على الموارد و مشاركتها.
   - خدمات البحث عن المعلومات.

الحاجة لوجود شبكة الانترانت

4. خدمات الاتصال: email، video conference، Network News(NNTP).
5. خدمات الموارد المعلوماتية:
   - تقنية الملفات المحمولة Portable Electronic Document.
   - خدمات البحث عن المعلومات و التعامل معها، مثال Gopher, Web Page.

متطلبات شبكة الانترانت

1. قنوات التوصيل و أجهزة الاتصال.
2. أنظمة الخادم Servers.
3. أنظمة العملاء Clients.
4. أنظمة أمن و خصوصية الشبكة FireWalls.

سرعات شبكة الانترانت

- تعتمد سرعة نقل البيانات على الهيكلية التي تعتمدها الشبكة.
- تقاس سرعة الإنترانت حسب الهيكلية التي تعتمدها.
- في حال كانت الإنترانت مبنية على شبكة محلية تصل السرعة لـ: 10Mbps - 100Mbps
- في حال كان اتصال بعض العقد بالإنترانت من خلال الإنترنت فإن سرعة الإنترانت ستعتمد على سرعة الإنترنت .
- في حال اعتماد الإنترانت على خدمة هاتفية محددة(Frame Relay مثلاً) تكون السرعة معتمدة على سرعة الخدمة.

فوائد الانترانت

1. تسهيل الاتصال بين المستخدمين والتعامل فيما بينهم بكفاءة وفاعلية.
2. توفير الخدمات على المستوى الخاص، مثل: خدمة الاتصال وخدمة الموارد المعلوماتية، وخدمة البحث عن المعلومات.
3. يمكن التوصيل بين المؤسسات الحكومية عن طريق الانترنت ولاستفادة من ربط هذه الخدمات مع بعضها البعض.

الفرق بين الإنترنت والانترانت

1. الإنترنت غير مملوك لأي أحد، ويمكن لأي شخص الوصول إليه من أي مكان أو موقع.
2. الإنترنت يحتوي على العديد من الصفحات المتضمنة معلومات غير لائقة أو سخيفة.
3. الإنترانت ملك المؤسسة التي تستضيفه وبذلك لا يمكن لأي شخص الوصول إليه إلا الذين سمح لهم.
4. الإنترانت يحتوي على المواضيع والمعلومات التي أنت توافق عليها. وتعمل فقط في موقع واحد على الأغلب.

بيئات الانترانت
INTRANET PLATFORMS

- بيئة ويندوز Windows NT Platforms:
  Intel Based، Alpha Based، Risc Based، Power PC Based
- بيئة يونكس Unix Platforms:
  Sun Solaris، IBM R6000، Alpha Unix.
- Novel: Netware based platforms.

- عناصر تقييم البيئة المناسبة لشبكة الإنترانت :
  1. سهولة التركيب و تشغيل الشبكة Ease of setup/configuration.
  2. الوظائف و العمليات المتاحة Functionality.
  3. الدمج مع الملفات و الخدمات المتوفرة Integration.
  4. قابلية التوسع و النمو Scalability.
  5. توفير الأدوات من شركات أخرى Third Party Tools.

بروتوكولات الشبكة وطبقاتها

- هي مجموعة من القوانين والإجراءات البرمجية التي تستخدم للاتصال، مهمتها تحديد القوانين والإجراءات التي تتحكم بالاتصال والتفاعل بين أجهزة الحاسوب المختلفة على الشبكة.

- بعض الأمور التي تتعلق بالبروتوكولات:
  1. اختلاف الكثير منها في عملها ووظيفتها.
  2. من الممكن أن تعمل عدة بروتوكولات معاً لتنفيذ عمل ما.
  3. لكل بروتوكول مزاياه وعيوبه.

بروتوكولات الشبكة وطبقاتها

- البروتوكولات (Protocols):
  - مجموعة من القوانين والإجراءات البرمجية التي تستخدم للاتصال والتحكم به بين أجهزة الحاسوب المختلفة.
  - تختلف البروتوكولات في وظيفتها وطبيعة عملها.
  - كل بروتوكول له مزايا وعيوب.

- Protocol Stack: مجموعة البروتوكلات التي تعمل سوياً.
- Layering: عملية تنظيم المهام بين البروتوكولات.
- Binding: الطريقة التي يتم بها ربط البروتوكلات وترتيبها.
- Routing & Routing Protocols.

المرسل والمستقبل

- مهام البروتوكلات في الجهاز المرسل:
  1. تقسيم البيانات إلى حزم.
  2. إضافة معلومات العنونة إلى الحزم.
  3. تحضير البيانات للإرسال.

- مهام البروتوكولات في الجهاز المستقبل:
  1. التقاط حزم البيانات من وسط الاتصال.
  2. إدخال حزم البيانات إلى داخل الحاسوب عبر بطاقة الشبكة Net Card.
  3. تجميع كل حزم البيانات المرسلة وقراءة معلومات التحكم المضافة إلى هذه الحزم.
  4. نسخ البيانات من الحزم إلى ذاكرة مؤقتة لإعادة تجميعها.
  5. تمرير البيانات المعاد تجميعها إلى البرامج في صورة مفهومة قابلة للاستخدام.

أنواع البروتوكولات

1. Connection Oriented protocols

- يحقق هذا الاتصال المباشر موثوقية عالية لتسليم البيانات.
- قد يؤدي إلى بطئ في عمل وأداء الشبكة.
- مثال: TCP (Transmission Control Protocol).

2. Connectionless protocols

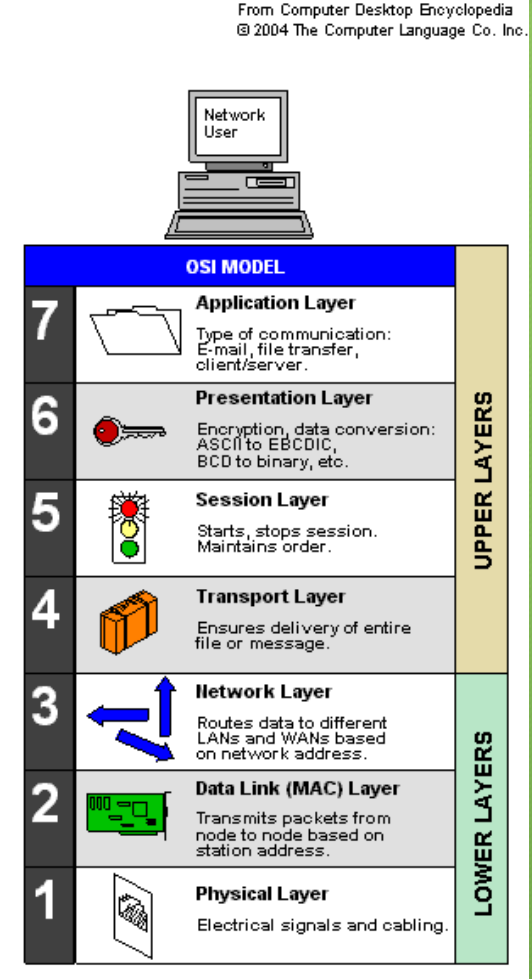
- لا توفر اتصال مباشر مع الحاسوب المستقبل قبل إرسال البيانات.
- تنتقل البيانات بسرعة، مما يحسن أداء الشبكة.
- ليست تامة الموثوقية بحيث لا تعرف بالأخطاء الواقعة أثناء الإرسال.
- مثل: IP, UDP.

نظام الوصل المفتوح
OPEN SYSTEM INTERCONNECT (OSI)

7	Application Layer	طبقة التطبيقات
6	Presentation Layer	طبقة التمثيل
5	Session Layer	طبقة الجلسة
4	Transport Layer	طبقة النقل
3	Network Layer	طبقة الشبكة
2	Data Link Layer	طبقة ربط البيانات
1	Physical Layer	الطبقة المادية

طبقات نظام الوصل المفتوح

نظام الوصل المفتوح
OPEN SYSTEM INTERCONNECT (OSI)



7. طبقة التطبيقات: وهي الطبقة التي تحتوي على التطبيقات مثل المستعرضات الانترنت والبريد والالكتروني وغيرها والتي تساعد على الاتصال من المستخدم للشبكة للحصول على المطلوب

6. طبقة التقديم: وهي الطبقة مسؤولة عن التشفير وضغط البيانات وكذلك مسؤولة عن ترميز الأبجدية

5. طبقة الجلسة: وهي الطبقة عن تأسيس الاتصال بين المرسل والمستقبل ومراقبة هذا الاتصال وكمية البيانات المرسلة ويتحقق أحيانا من كلمات المرور.

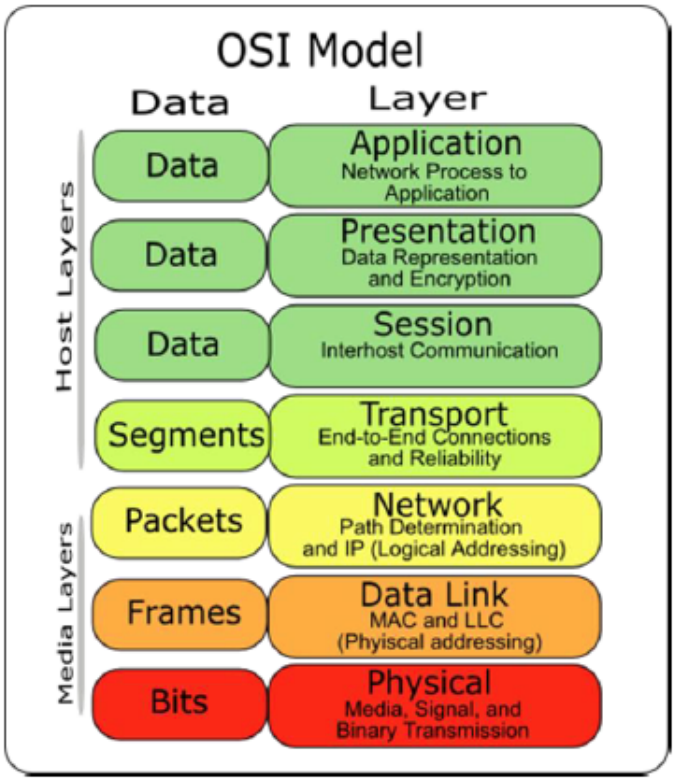
4. طبقة النقل: وهي الطبقة التي تكون مسؤولة عن نقل البيانات وتسليمها خالية من الأخطاء ويقسم المعلومات إلى أجزاء صغيرة ويستلم ويتأكد من استلام الشحنة.

3. طبقة الشبكة: مسؤولة عن اختيار أفضل طريق للإرسال حسب الازدحام على الشبكة والتوجيه على العنوان الصحيح.

2. طبقة الارتباط: تقوم هذه الطبقة بتنسيق الرزم المقدمة للشبكة الفيزيائية والتحكم في التدفق الحاصل على الشبكة وإعادة إرسال البيانات التي تعرضت للتلف.

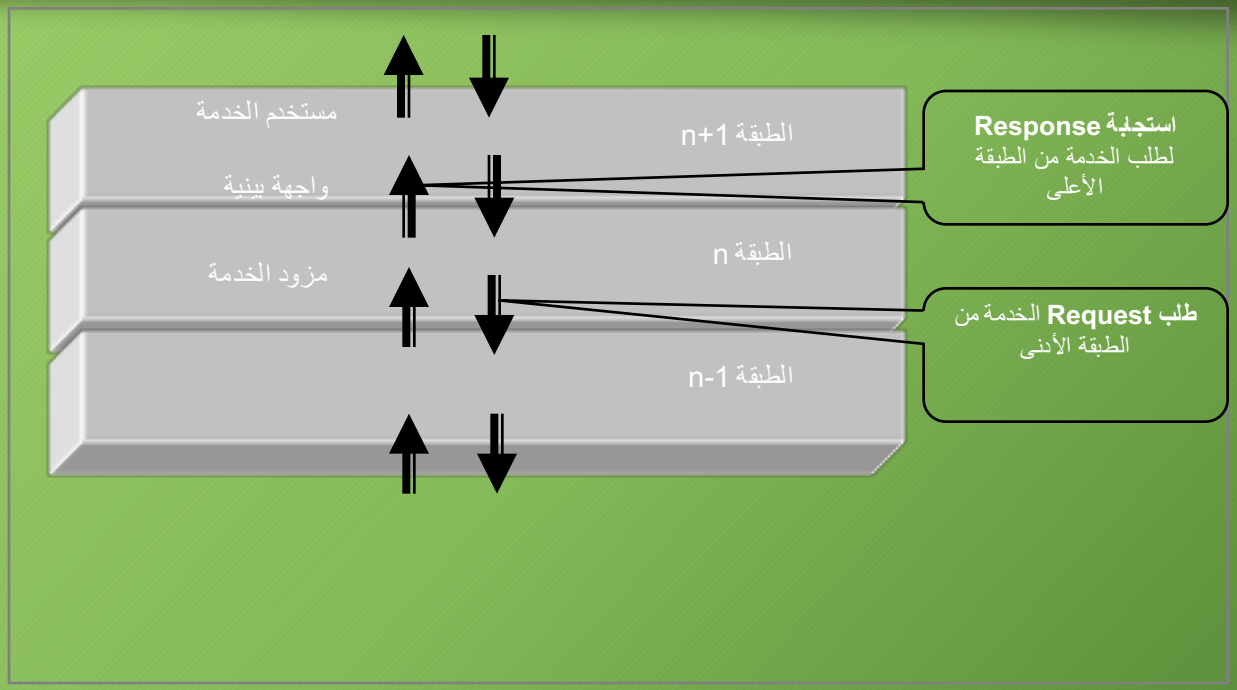
1. الطبقة الفيزيائية: تحويل البيانات من متوازي إلى تسلسلي وتوضع على السلك.

نظام الوصل المفتوح
OPEN SYSTEM INTERCONNECT (OSI)



- طبقة التطبيق.
- طبقة التقديم.
- طبقة الجلسة.
- طبقة النقل.
- طبقة الشبكة.
- طبقة الارتباط.
- الطبقة الفيزيائية.

SERVICE ACCESS POINTS SAP



الواجهة البينية Interface: هي واجهة اتصال طبقتين متجاورتين، و من خلالها يحدث تبادل البيانات عبر نقاط ولوج الخدمة Service Access Points SAP.

ويندوز سيرفر 2003

- يدعم ويندوز سيرفر 2003 ثلاثة برتوكولات:
  1. AppleTalk: للاتصال بين أجهزة ابل ماكنتوش القديمة.
  2. IPX/SPX: للاتصال بين شبكات Novell Netware.
  3. TCP/IP: للاتصال بمعظم الأنظمة الحديثة.

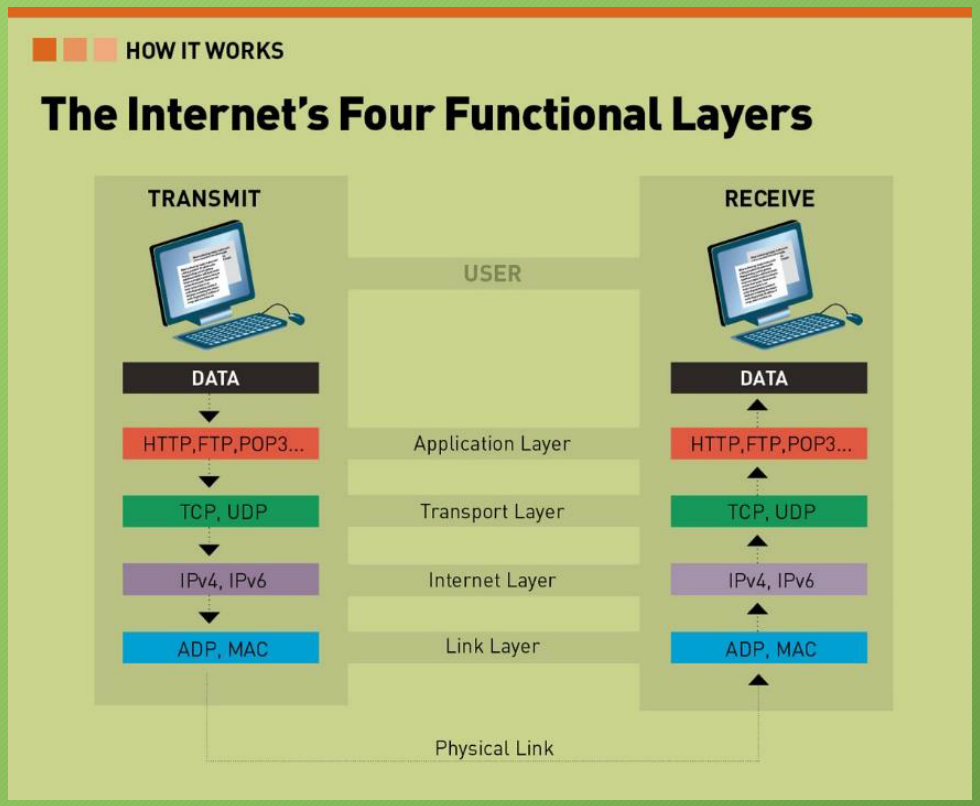
بروتوكول APPLE TALK

- ظهر مع ظهور نظام ماكنتوش.
- عمل مع شبكات Local Talk.
- حُسّن للعمل مع شبكات Token Ring, FDDI, Ethernet.
- صمم لمجموعات العمل الصغيرة المحلية (غير قابل للتوجيه).

بروتوكول IPX/SPX
INTERNET WORK PACKET EXCHANGE /SEQUENCED EXCHANGE

- بروتوكول ربط شبكات من إنتاج Novell Netware.
- بروتوكول قابل للتوجيه.
- يعمل IPX في طبقة الشبكة في نموذج OSI، بحيث يتحكم في تجميع حزم البيانات وتوفير خدمة التوجيه.
- يعمل SPX في طبقة النقل Transport.
- يقوم SPX بـ:
  - تأسيس الاتصال مع وحد شبكة فرعية أخرى.
  - إخبار IPX ببدء تجميع حزم البيانات ونقلها.
  - تجميع البيانات في حزم يصل جمها لـ 64KB.
  - إضافة التروسية Header وحجمها 30Byte، بحيث تحتوي على: مصدر البيانات Source، وعنوان الوجهة Destination، ومعلومات التحكم Control Data.

بروتوكول TCP/IP

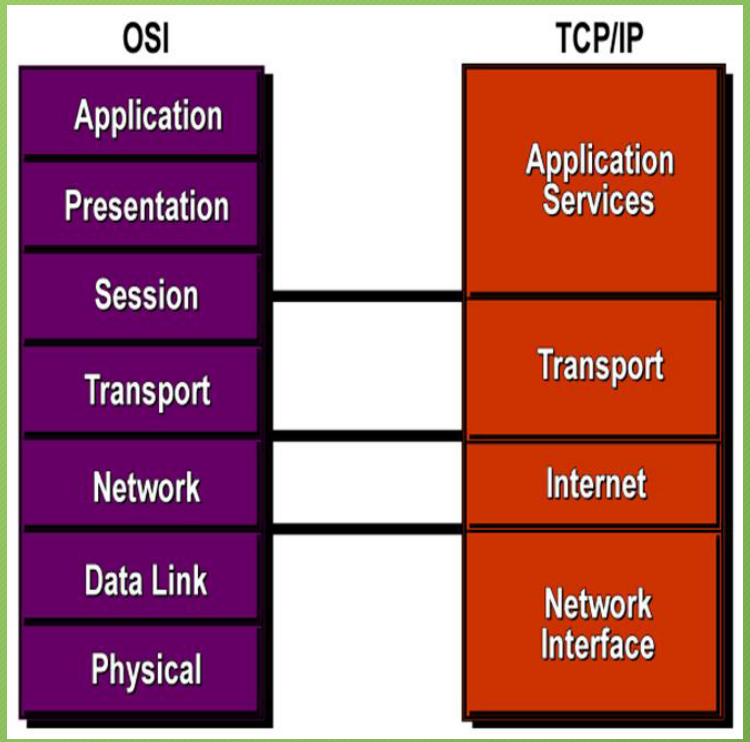


- مجموعة من البروتوكولات ذات المعايير الصناعية.
- ذات موثوقية و فاعلية كبيرة.
- في بداياتها كانت عبارة عن بروتوكولات WAN للأغراض العسكرية.
- بعد ذلك استخدمت كأساس للإنترنت.

مميزات بروتوكول TCP/IP

- ليس تابعاً أو مملوكاً لشركة محددة، ومقرّ من IETF.
- أبطأ في التطور من بروتوكولات تابعة لشركات خاصة.
- لا يعتمد على نظام التشغيل في عملية التوصيل، مثل: FTP.
- تحقيق بنية قياسية لا تتعلق بنوع الحاسوب (وضعية Client\Server).
- إمكانية الدخول إلى الإنترنت: حيث يعتبر هو البروتوكول الرئيس للدخول للإنترنت

بروتوكول TCP/IP
الطبقات الأربعة



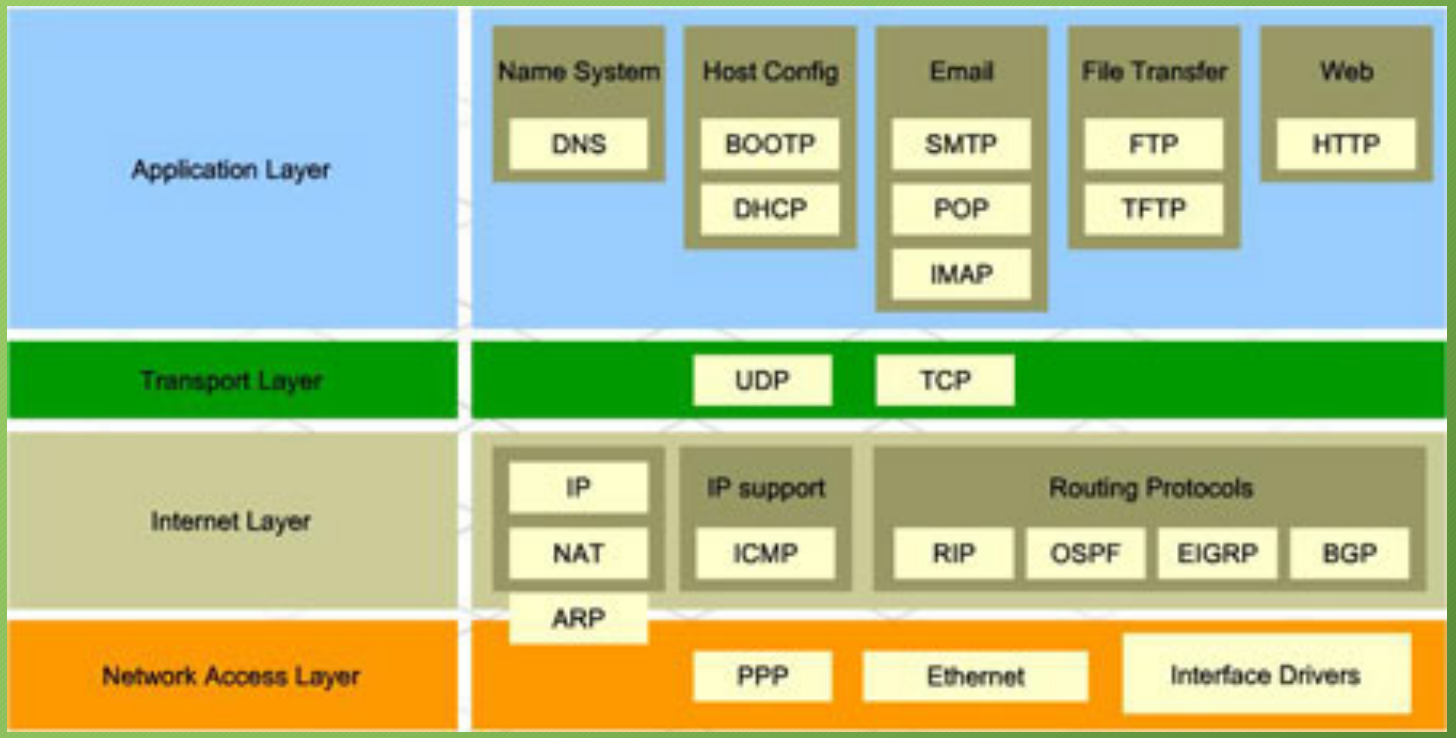
طبقة التطبيقات: مسؤولة عن جميع النشاطات التي تحدث في طبقة جلسة العمل وطبقة التمثيل وطبقة التطبيقات وقد تم كتابة العديد من البروتوكولات من اجل هذه الطبقة

طبقة النقل: نفس الطبقة في OSI وتعمل على تأمين الاتصال بين الحواسيب ويمكن ان يكون الاتصال موثوق مثل TCP أو غير موثوق مثل UDP

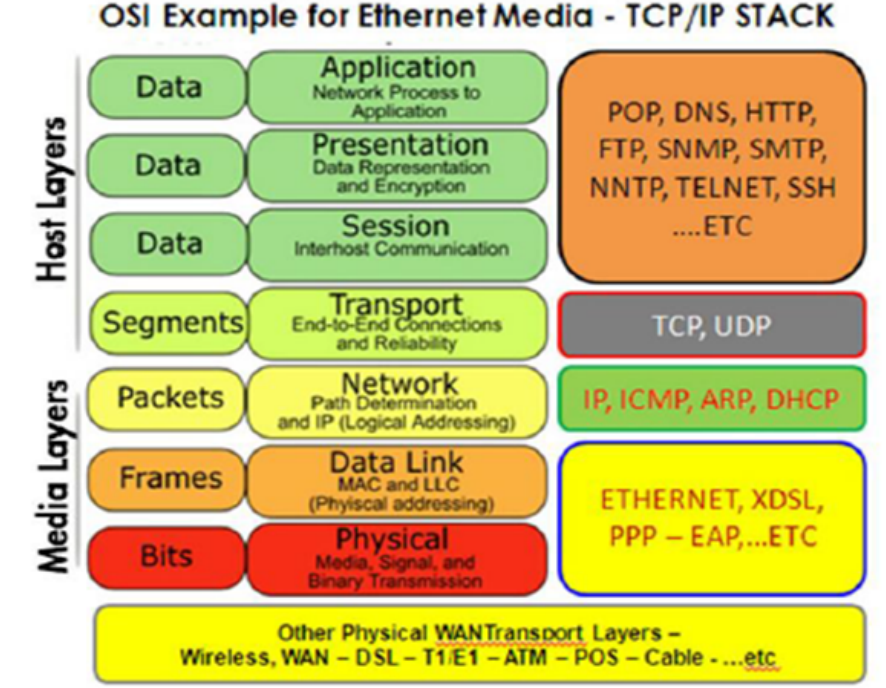
طبقة الانترنت: مسؤولة عن الاتصال مباشرة مع طبقة الشبكة وهي تقوم بعمليات توجيه وإيصال الرزم بواسطة بروتوكول IP وهناك العديد من البروتوكولات لهذه الشبكة

طبقة الشبكة: مسؤولة عن الاتصال مباشرة مع الشبكة

بروتوكول TCP/IP
الطبقات الأربعة



بروتوكول TCP/IP
الطبقات الأربعة



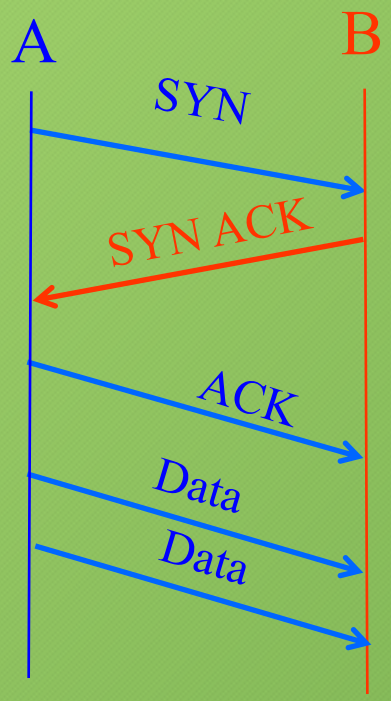
مواضيع هامة في TCP

- المنافذ Ports:
  - 1 - 1023 تسمى المنافذ المعيارية Well Know Ports، وتكون محجوزة من قبل Internet Assigned Numbers Authority.
  - المقبس Socket: عبارة عن عنوان IP بالإضافة للمنفذ Port.
- الاتصال الموثوق:
  - Connected Based, Connection Oriented Protocol.
- مكونات الإطار Frame.
- المصافحة الثلاثية Three Way Handshake.
- النوافذ المنزلقة (حجمها 8KB):
  - إرسال رزم متعددة واستقبالها بدون النظر للترتيب.

المنافذ والمقابس
Ports & Sockets

- نظراً لكثرة عدد للتطبيقات؛ لابد من وسيلة للتميز بينها.
- تم وضع منفذ لكل تطبيق، حيث أن هناك الكثير من التطبيقات، ويتم تمييز التطبيق حسب المنفذ.
- تم تعين 1 - 1023 منفذ من قبل شركة IANA.
- يمكن استخدام منافذ غير المحجوزة لتطبيقات أخرى.
- المقبس Socket = عنوان IP + المنفذ Port.

المصافحة الثلاثية
TCP THREE-WAY HANDSHAKE



- Three-way handshake to establish connection:
  1. حاسوب A يرسل SYN إلى الحاسوب B يطلب عملية تزامن مع النظام
  2. حاسوب B يرسل **SYN ACK** إلى الحاسوب A دلالة على انه جاهز ومستعد لتلقي المعطيات.
  3. حاسوب A يرسل ACK إلى الحاسوب B عرف أن B جاهز للاستقبال و هنا تبدأ عملية إرسال البيانات.

النوافذ المنزلقة
SLIDING WINDOW

- يستخدم لنقل المعطيات بين الحواسيب.
- كل حاسوب له نافذة إرسال ونافذة استقبال لتخزين المعطيات.
- تعمل النوافذ على تحسين عملية الاتصال.
- تسمح للمرسل أن يقوم بإرسال معطيات النافذة دون انتظار مصادقة على كل رزمة مفردة.
- تسمح للمتلقي استلام الرزم دون ترتيب أثناء الانتظار للرزم المتبقية.
- تسمح بنقل كميات من البيانات.

انتهت الوحدة الثانية

مع تمنياتي لكم بالتوفيق

الوحدة الثالثة

تصميم شبكات الخادم الزبون

أهداف الوحدة

- توضيح دور كل من الخادم والزبون
- تختار الأدوات المناسبة التي تعمد على جودة الاتصال بين الخادم والزبون
- تصمم تطبيقا بسيطا على شبكة الخادم الزبون

أصل نموذج الخادم الزبون وغرضه

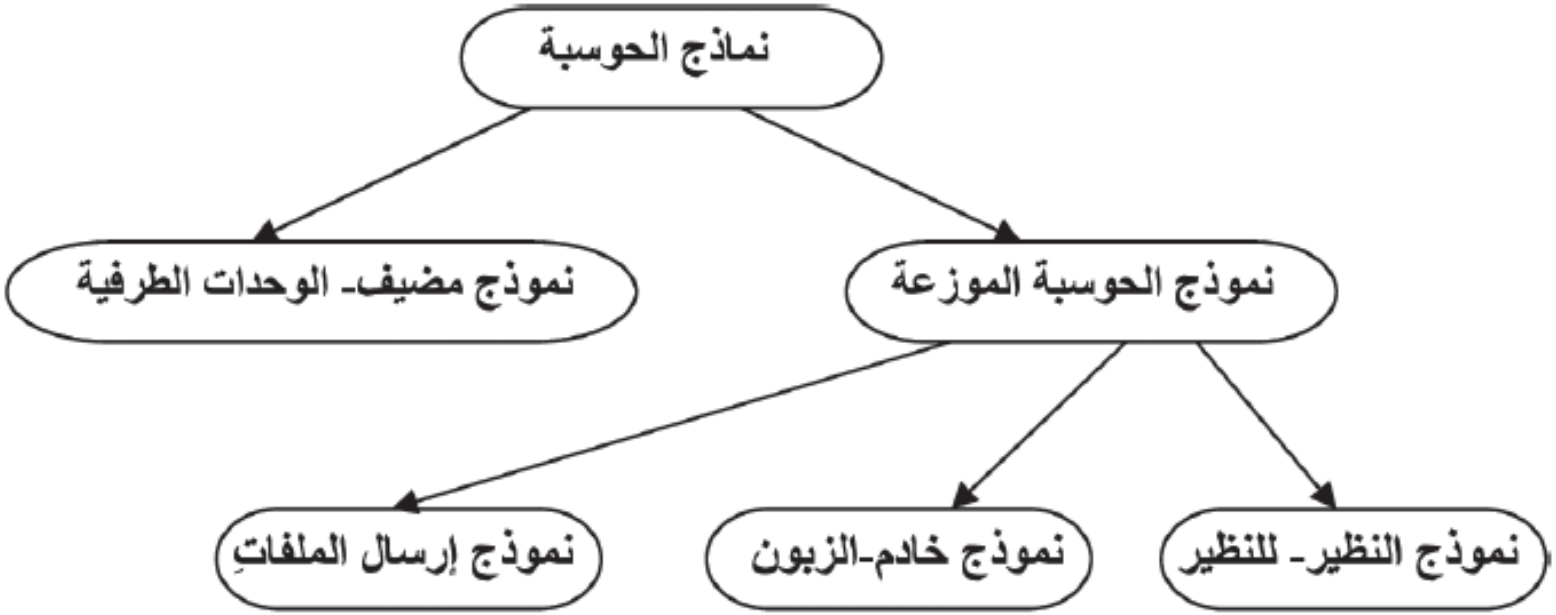
كَانتْ سنوات السبعينيات والثمانينات من القرن الماضي، عزيزي الدارس، عصرَ استعمال الحوسبة المركزية Centralized Computing وحواسيب الآي بي إمِ الكبرى IBM mainframeوالتي احتلَّت 70 % مِنْ عمل حواسيب العالم. نحن الآن في مرحلة حوسبة نموذج خادم-الزبون وهو مفهوم وتقنية مختلفة كلياً عن عمل الحواسيب الكبرى.

الحوسبة المركزية

الحوسبة الموزعة DCS

أي نظام حوسبة مُوَزَّعة (DCS) هو مجموعة من الحواسيب المستقلة ذاتياً ربطتْ من خلال شبكة اتصالِ لانْجاز وظائفِ العملِ. تقنياً، الحواسيب لا تَشتركُ في الذاكرةِ الرئيسةِ لذا لا يمكن تبادل المعلومات خلال المتغيّراتِ العالميةِ Global Values. وإنما يتم تبادلها فقط من خلال رسائل على شبكة الاتصال.

الحوسبة الموزعة ونموذج خادم زبون



الشكل (1): نموذج خادم- الزبون حالة خاصّة مِنْ نموذج الحوسبة المُوَزَّعة.

نموذج إرسال الملفات FILE TRANSFER

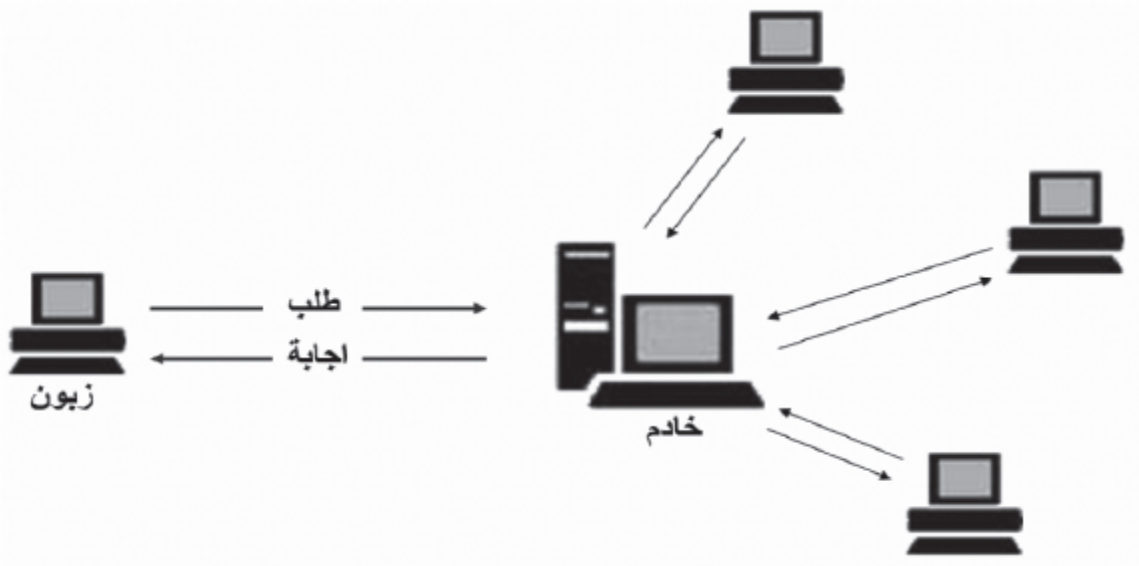
- وهو قديم في الحوسبة الموزعة
- تتصل الحواسيب مع بعضها بإرسال الملفات والبريد وهو حالة خاصة من إرسال الملفات
- ما يزال هذا النموذج يستعمل رغم قدمه
- مثال على ذلك : تبادل مواد إعلامية وإخبارية مثل اليوتيوب وغيرها.
- ويستعمل البريد الالكتروني لهذا الصدد بتخزين الملفات البريد عليه.

نموذج النظير للنظير PEER TO PEER

- يسمح للعمليات في المواقع المختلفة باستحضار بعضها البعض
- بحيث ممكن أي جهاز يكون خادم أو زبون أو كليهما حسب المهمة
- مثال عليه Workgroup

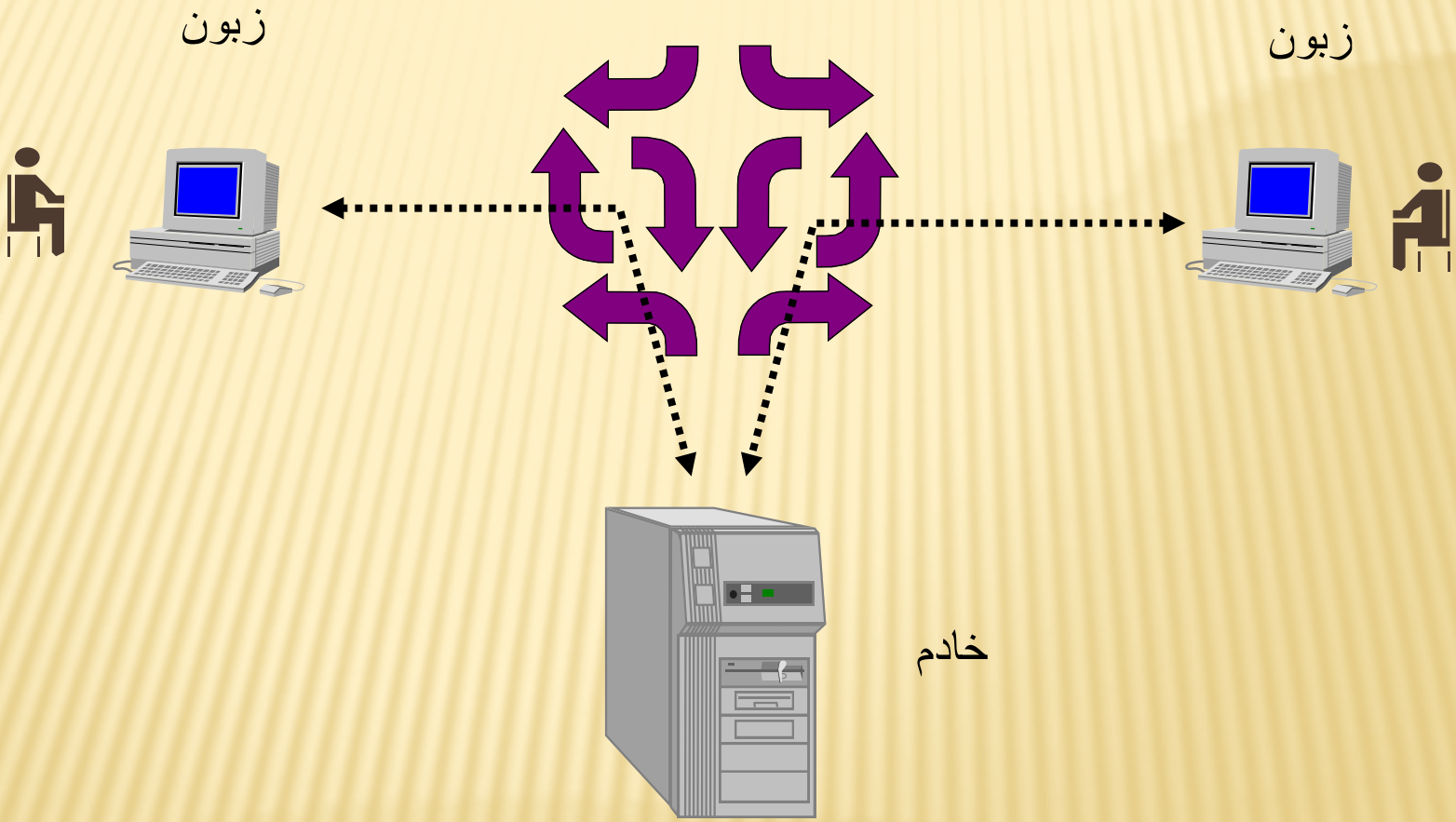
نموذج خادم زبون
CLIENT – SERVER

الصورة العامة نموذج خادم زبون



- يتكون من :
  - الخادم - الزبون - الوسيط

شکل آخر



مكونات نظام الخادم الزبون

- الزبون Client
- الخادم Server
- الوسيط Middleware

الزبون CLIENT

- يتولى إدارة البرنامج الخاص بالواجهة المستخدمGUI
- تقيم مدخلات وطلبات المستخدم وإرسالها إلي الخادم
- المستخدم في الزبون لا يرى سوى الطرف الأمامي للتطبيق
- العمليات تتولى إدارة المصادر المحلية التي يتعامل معها المستخدم مثل الشاشة ولوحة المفاتيح

الخادم SERVER

- يلبي طلبات الزبون ويسترجع البيانات ويحافظ على سلامة المعلومات وصتها وتلبية طلب الزبون
- يعمل كمحرك للبرمجيات ويدير المصادر المشتركة مثل الطابعة وقاعدة البيانات
- ابسط مثال على ذلك خادم الملفات وخادم الاقراص
- المثال المتقدم هو قاعدة البيانات والتطبيقات

الوسيط MIDDLEWARE

- يساعد التطبيقات بالاتصال بشفافية بغض النظر عن موقعها.
- العنصر الأهم في الوسيط هو نظام التشغيل الداعم للشبكات الذي يوفر التوزيع والتراسل والإدارة للشبكة
- يتعمد هذا النظام على بروتوكولات الاتصال.
- ينفذ البروتوكول قبل طلب الزبون الدخول على الشبكة

تعريفات : تصميم البرنامج مقابل الشبكة

- لفهم حوسبة خادم – زبون هي القدرة على التميز بين نموذجين:
  - معمارية تصميم الشبكة
  - معمارية تصميم البرامج

معمارية تصميم الشبكة

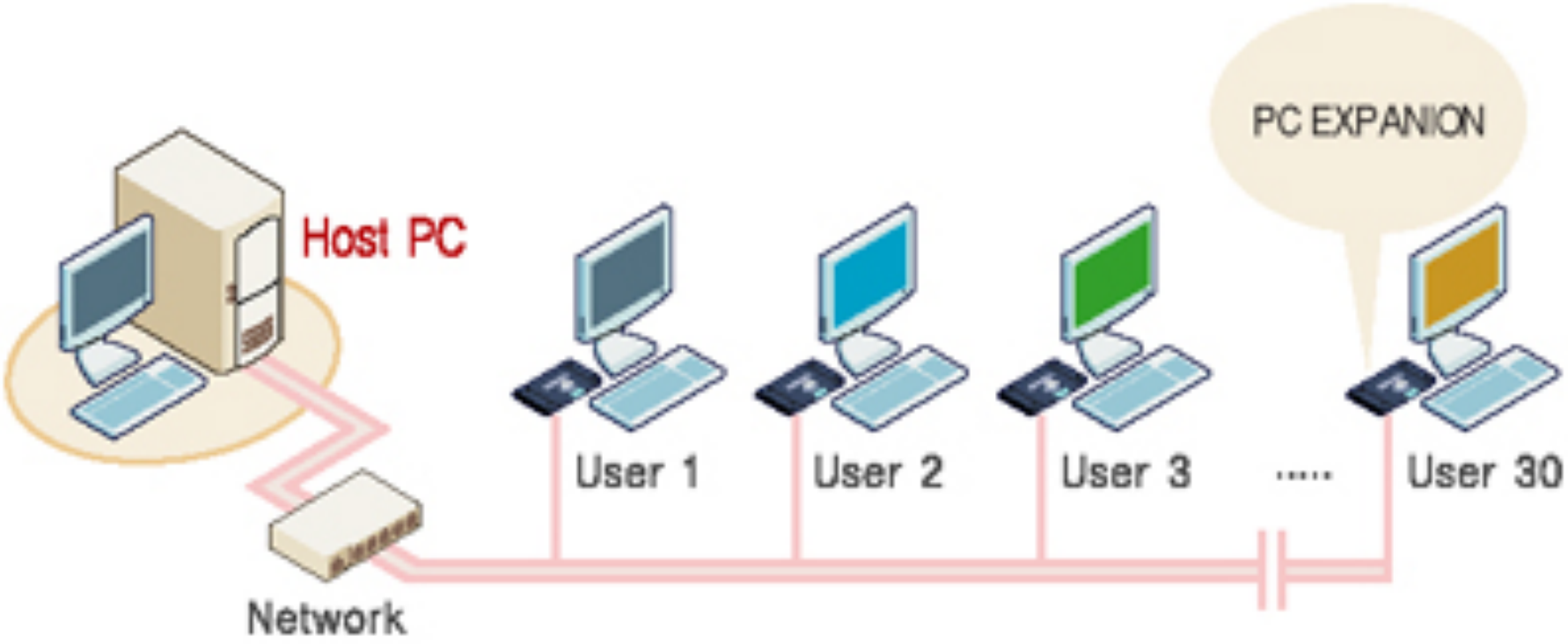
ضمن سياق تصميمِ الشبكةِ، يصف التعبير «معمارية تصميمِ خادم-الزبون» يَصِفُ نموذجاً لتَوزيع «عملِ» المهامِ الحاسوبية على مختلف الحواسيب المربَوطة بالشبكةِ. بهذا المعنى، فإن التعبير « معمارية تصميمِ خادم-الزبون» هو تعبير يُستَعملُ لوَصْف أحد النماذجِ الأساسيةِ الثلاث مِنْ ربطِ الشبكات:

- معمارية مضيف – طرف
- معمارية خادم – زبون
- معمارية النظير – للنظير
- معمارية الحاسبات الكبرى
- معمارية تشارك الملفات

معمارية مضيف طرف - HOST TERMINAL

- يصف نوع الشبكة الذي فيه حاسوب مركزي (مضيف)
- موصول إلى عدد من المحطات العمل الفرعية
- كل المعالجات تجرى على المضيف
- المحطات الطرفية تستعمل لإدخال البيانات ومراجعة التقارير
- المحطات الطرفية خرساء لا تشارك المعالجة
- تناسب الشبكات الكبيرة والصغيرة
- مميزاتها مركزية الادارة

معمارية مضيف طرف - HOST TERMINAL



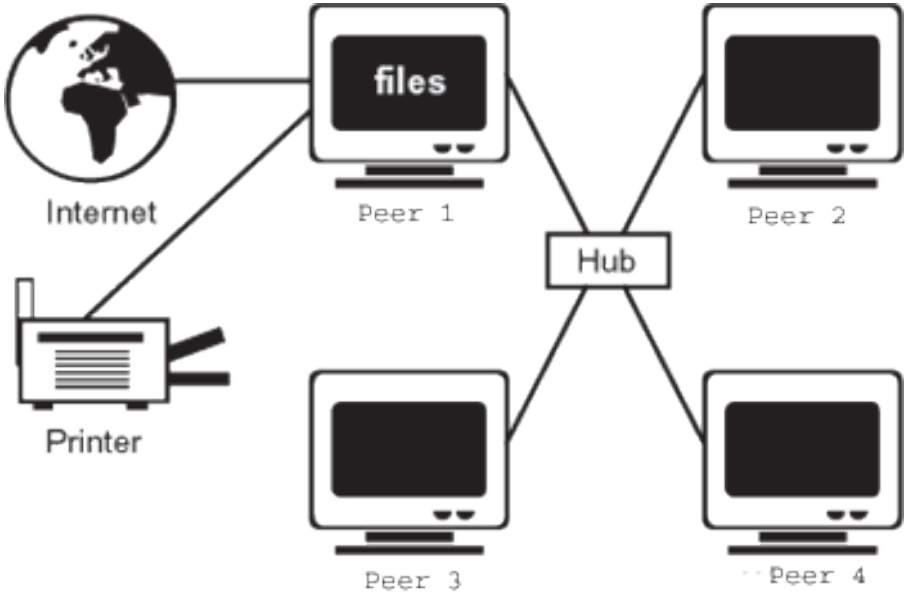
معمارية خادم – زبون CLIENT SERVER

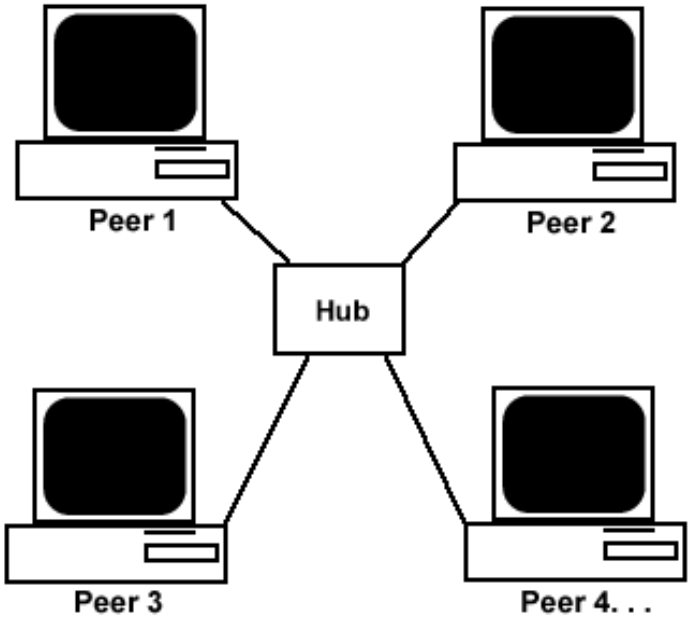
- كل حاسوب يتولى جزء من المعالجة
- الخادم يكرس لتقديم الخدمات (تخزين – معالجة – تنظيم موارد الشبكة – طباعة)
- يمكن استعمالها في أي حجم شبكة
- مميزاتها تشارك المعالجة والمشاركة في العمل

معمارية النظير ـ للنظير

- محطات العمل مرتبطة سويا ولا يوجد خادم
- حسب المهمة تكون المحطة زبون أو خادم
- مثال: عند وصل زبون بطابعة ومشاركتها والتحكم فيها يصبح خادم لهذه الطباعة والزبون الذي يطلبها
- محطة عمل أخرى تتشارك المودم الانترنت وتصبح خادم للاتصالات.
- تكون صغيرة لا تتجاوز 25 محطة عمل فرعية.

معمارية النظير ـ للنظير





معمارية تصميم البرامج

تستخدم معمارية خادم -الزبون أيضاً لوصف نوع ما من البرامج تتعلق بمعمارية شبكة خادم – الزبون. في وصف محتوى تصميم البرنامج وتلعب معمارية خادم –الزبون دور وصف نموذج لتوزيع العمل والمعالجات. لبرنامج مفرد على مختلف أجهزة الحاسوب المتصلة والمرتبطة في شبكة من الأجهزة.

- **تطبيقات المضيف:** وهو برنامج وعمليات معالجة صممت للعمل على جهاز المضيف الرئيس(المركزي) ولا يكون مشاركة من احد.
- **تطبيقات القائمة بذاتها stand alone application**: وهي التي تنفذ على حواسيب مفردة لمعظم المستخدمين مثل برنامج الورد، وهي تعمل لوحدها.
- **تطبيقات الخادم – الزبون**: وهي برامج تتقاسم العمل بين الخادم والزبون.

معمارية الخادم الزبون

تستعمل في معمارية خادم
الزبون نداءات للإجراء البعيد (Remote Procedure Calls(RPCs أو لغة الاسترجاع
المنظمة (standard query language (SQL للاتصال بين الزبونِ والخادمِ.

أمثلة على معمارية خادم- الزبون

معمارية خادم- الزبون ذي طبقة- واحدة
معمارية خادم-الزبون ذي- الطبقتين
الزبائن ذات غالبية المعالجات (السمينة)
الخدم السمينة:
معمارية خادم - الزبون ذي الثلاث طبقات

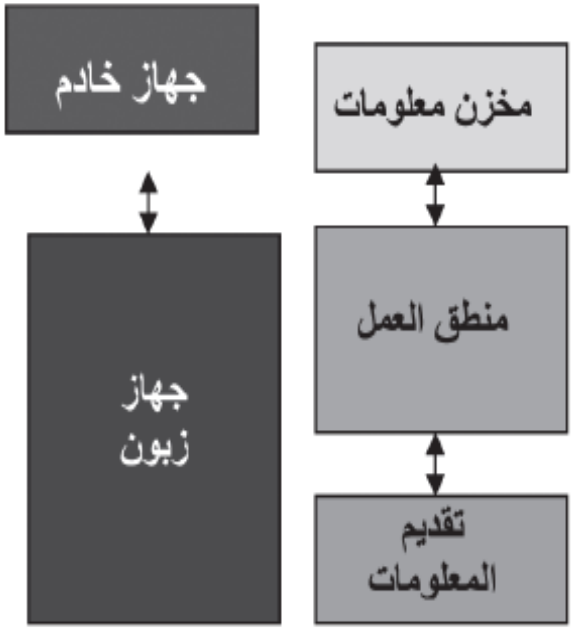
معمارية خادم الزبون ذي طبقة واحدة

- حاسوب كبير مضيف يقوم بكافة الأعمال
- محطة طرفية غير ذكية لإرسال الطلبات والحصول على تقارير

معمارية خادم الزبون ذي الطبقتين

- يتصل الزبون مباشرة بخادم قاعدة البيانات
- يقوم الخادم بتلبية طلبات الزبون
- يتشارك الزبون في بعض بجانب الخادم
- مثال على ذلك FoxPro وكذلك dBase
- لا تتحمل أكثر من 100 مستخدم بشكل عام

الزبائن السمينة FAT CLIENT

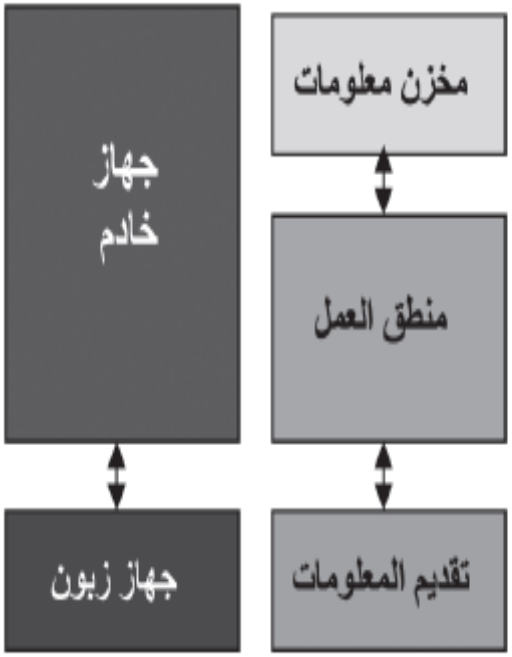


الشكل (4): الزبائن السمينة

- يقوم الزبون السمين بأغلب المعالجات ،
- يحصل على القليل من الخادم النحيل
- مواصفاته عالية وكلما زاد تعقيد التطبيق كان الزبون اسمن لأنه بحاجة لجهاز اقوي لتقديم الدعم

الخادم – السمين FAT SERVER

- بديل عن الخادم النحيل
- يقوم بكافة المعالجات عليه
- أكثر فعالية و الحمل اخف على الشبكة



معمارية خادم – الزبون ذي الثلاث طبقات

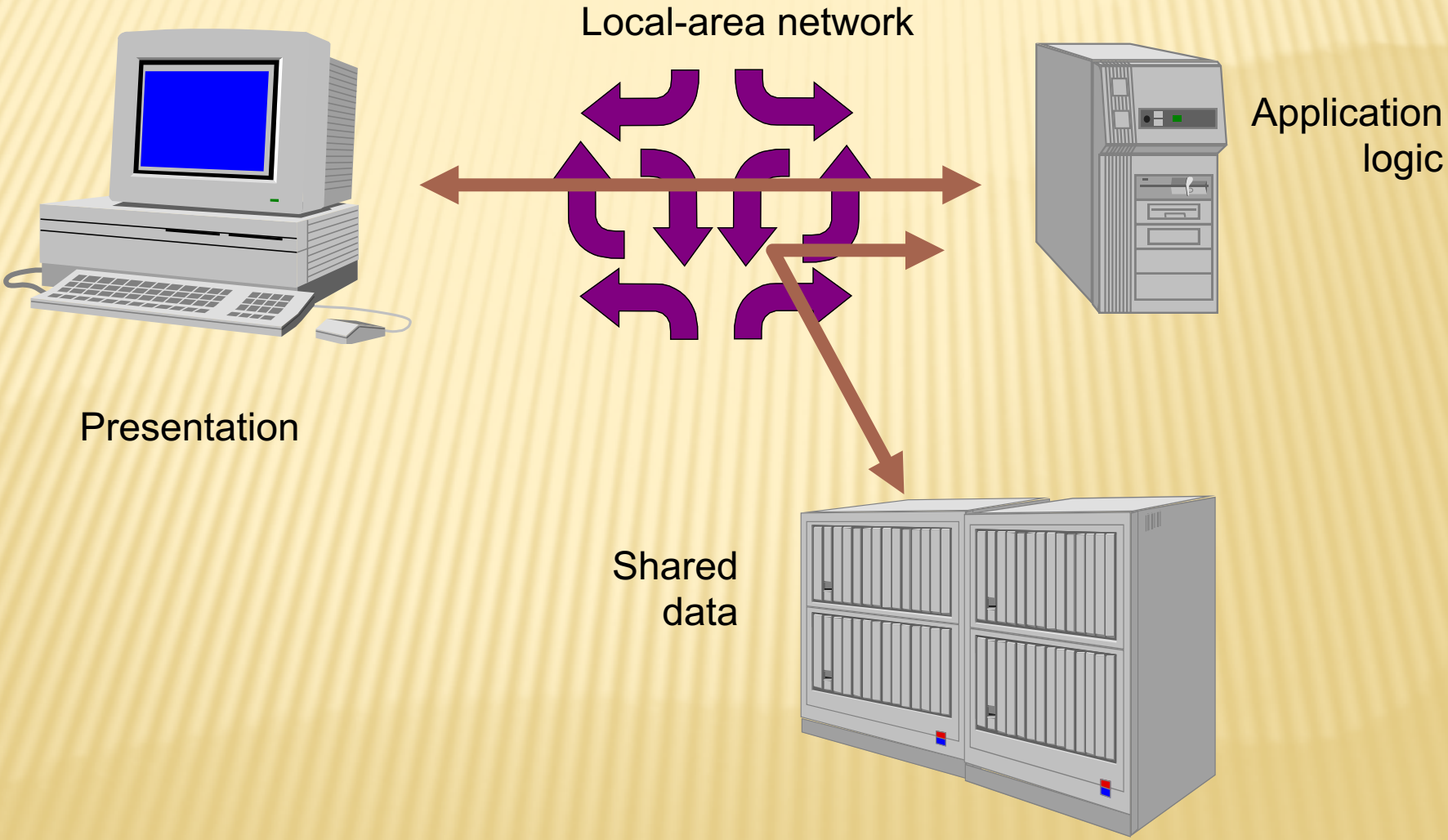
تقسم معمارية الثلاث طبقات إلى ما يلي:

1- الواجهة الأمامية. وهي المسؤولة عن تقديم منطق تقديم قابل للنقل.

2- الواجهة الخلفية. وهي التي تمكن من الإيصال إلى الخدمات المكرسة مثل خادم قاعدة البيانات.

3- الطبقة المتوسطة. التي تسمح للمستخدم بالمشاركة والتحكم بمنطق العمل وذلك بعزله عن التطبيق الحقيقي.

معمارية خادم – الزبون ذي الثلاث طبقات



مميزات معمارية خادم – الزبون ذي الثلاث طبقات

- التغيرات على واجهة المستخدم مستقلة عن بعضها البعض مما يسمح للتطبيق بالتطوير بسهولة ويسر
- الأعناق الزجاجية تقل لان التطبيق لا ينقل معلومات إضافية للزبون
- الزبون مفصول عن قاعدة البيانات وعمليات الشبكة لذلك المستخدم لا يعرف موقع وعدد الخوادم على النظام
- تجميع قواعد البيانات وبالتالي يشترك مستخدمو الخادم في التطبيق فقلل التكلفة والترخيص للبرامج

أنواع معمارية الطبقات الثلاث

- **معمارية الثلاث طبقات مع مراقب معالجة النشاطات:**
  - يعتمد على برامج تكتب بلغة الآلة
  - يقوم بالمراقبة ومعالجة النشاطات
  - يقوم بتعديل عدة أنظمة إدارة قواعد بيانات في نشاط واحد

- **معمارية الثلاث طبقات مع خادم الرسائل**
  - التراسل هو الطريقة المستخدمة في المراقبة
  - تركز على الرسائل الذكية

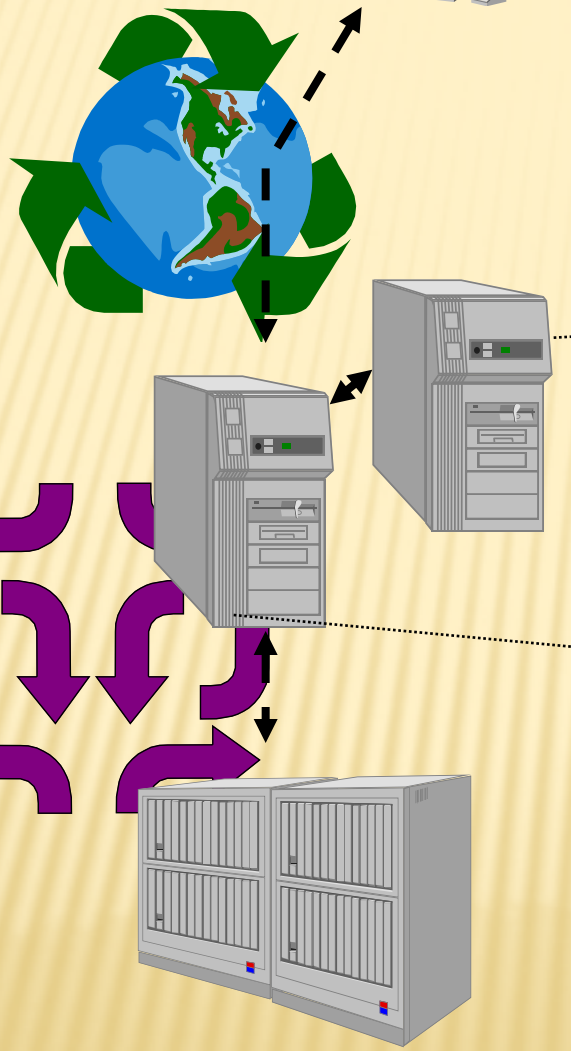
معمارية الثلاث طبقات مع خادم التطبيقات

- **الوسيط السمين**
  - يتفاعل الزبون من خلال بروتوكول RPC, HTTP
  - ويتفاعل الخادم من خلال SQL , ODBC
- **معمارية ن – طبقة:**
  - بحيث يتم تقسيم الوسيط التطبيقي لأكثر من ثلاث طبقات
  - تعتبر الأكثر فاعلية
  - الشريحة التالية توضح مثال على **ن طبقة**

Client

Host architecture

Web browser



Web server

Common gateway interchange

Application logic

Databases and DBMS

Application partition

نماذج خادم - الزبون

فإن برامج خادم الزبون تقوم بإنشاء ثلاث من الوظائف هي:

1- مخازن البيانات: تستخدم بشكل مثالي في حالة البيانات الكثيرة أو الكبيرة.

2- منطقية العمل: عمليات مثل طلب البيانات أو فرزها أو إعادة البيانات، وعملية معالجة البيانات إلى التقارير.

3- ممثل البيانات: ويكون عادة على شاشة المستخدمة

نماذج خادم - الزبون

تم تطويرها لسببين:

إدارة البيانات: نموذج قاعدة بيانات SQL.

في هذا النموذج يتم تحمل بيانات كبيرة على جهاز الخادم ويتم عليها عمليات مشاركة ما بين المستخدمين. والتركيز في هذا النموذج هو إدارة البيانات وإدارة معالجتها. ويمكن أن تكون محطات العمل واجهات أمامية لبرامج الزبون والخادم أو النماذج القائمة بذاتها. تقوم بإرسال SQL وهي لغة رسمية لاسترجاع البيانات. وترسل الطلبات إلى الخادم ويقوم بإرجاع نتائج هذه االطلبات إلى جهاز الزبون.

نماذج خادم - الزبون

إدارة التدفق للمعلومات:

هذا النموذج صمم لدعم العمل المتدفق المعتمد على بعضه البعض.

نظام الجماعة (Workgroup) لم يصمم لمعالجة البيانات بشكل أساسي ولكن لإدارة العمليات وذلك بالسماح بالبيانات للتدفق ما بين المستخدمين بطريقة تسمح بتقريب العمليات إلى الواقع الحقيقي للعمليات.

إن أبسط الأدوار هو نظام الجماعة وقد صمم ليسمح لمجموعة من المستخدمين المرتبطين على شبكة من الحواسيب. ولتنظيم النشاطات باستخدام جهاز حاسوب يحتوي على المصادر.

فئات الخادم

- **خادم الملفات File Server**
  - يدير تطبيق مجموعة عمل وملفات البيانات
  - شديد التوجه للإدخال والإخراج
  - يسحب كمية كبيرة من البيانات ويمررها على الشبكة
- **خادم البيانات Data Server**
  - يستعمل فقط للتخزين وإدارة البيانات
  - يقوم بعمليات مثل تقييم البيانات وإدارتها
  - يتطلب معالج سريع وكمية كبيرة من الذاكرة وقرص صلب كبير
- **خادم قاعدة البيانات Database Server**
  - مثل البريد الالكتروني وخادم الانترنت

الخصائص والمميزات في استعمال خادم - الزبون

الخصائصِ والميزاتِ التي تُميّزها عِنْ بيئةِ حوسبة الحاسوب الكبير التقليديةِ. ومن ميزات معمارية خادم- زبون:

1. شبكات مُشَبَّكة مكونة مِنْ الأجهزة الصغيرةِ والقويَّةِ (الخادمات والزبائن)
2. أنظمة مفتوحة (Open systems)
3. التجزيء في البرامج(modularity)
4. التعقيد والصعوبة (Complexity)

أسباب لتبني نموذج حوسبة الخادم الزبون

- تطبيقات قائمة بحد ذاتها.
- تطبيقات طُبّقتْ كأنظمة مثيلة.
- تطبيقات كَانتْ معقّدة.
- التقنية المساندة كَانتْ مستندة على نموذج السيطرةِ المركزية.

ونتيجة لهذه التطبيقات الجاهزة بدت وكأنها غيرمتينة بما فيه الكفاية لحاجاتِ اليومِ. وإن كُلّ هذا قد دَعمَ تقنية خادم – الزبون للنَمُو بهذه النسبةِ.

- **بسبب هذه المشكلات في التقنيات القديمة تم تبني تقنية الخادم الزبون**

انتهت الوحدة الثالثة

تمنياتي لكم بالتوفيق

الشبكات المحلية LAN

- الشبكة المحلية هي شبكة كمبيوتر تصمم لمنطقة جغرافية محدودة كبناء أو حرم جامعي .
- أيضا يمكن استخدام شبكة LAN كشبكة عزل أو فصل لربط الكمبيوترات في منظمة لغرض وحيد هو مشاركة المصادر
- معظم شبكات LAN اليوم تربط إلى شبكات واسعة النطاق WAN أو انترنت .
- هناك عدة تقنيات مثل الايثرنيت Token Ring, Token Bus, FDDI, and ATM LAN. .
- بعض هذه التقنيات بقي لفترة ولكن Ethernet بقي التقنية المهيمنة

تبولوجيا الشبكات المحلية LAN

يشير عزيزي الدارس، مصطلح «تبولوجيا الشبكات» Network Topol-ogy إلى الكيفية التي يتم بها توصيل الحواسيب والأسلاك والمكونات الأخرى لتكوين شبكة. المصطلح Topology يطلق عليه أيضاً Physical Layout أو Design تصميم أو تخطيط الشبكات.

يعتمد اختيار التصميم المناسب للشبكة المحلية على العوامل التالية:

1. نوع المعدات التي تحتاجها الشبكة.
2. إمكانيات هذه المعدات.
3. نمو الشبكة في المستقبل.
4. أدوات إدارة الشبكة.

الشبكات المحلية LAN

لهذا عند اختيار تصميم ما للشبكة يجب الأخذ بعين الاعتبار المكونات التالية:

1. نوع أسلاك التوصيل.
2. نوع بطاقة الشبكة.
3. موصلات خاصة للأسلاك Cable Connectors.

تقوم جميع شبكات النطاق المحلي LAN على ثلاثة تصاميم أساسية:

Bus أو الناقل ويسمى أيضا Backbone أو العمود الفقري.

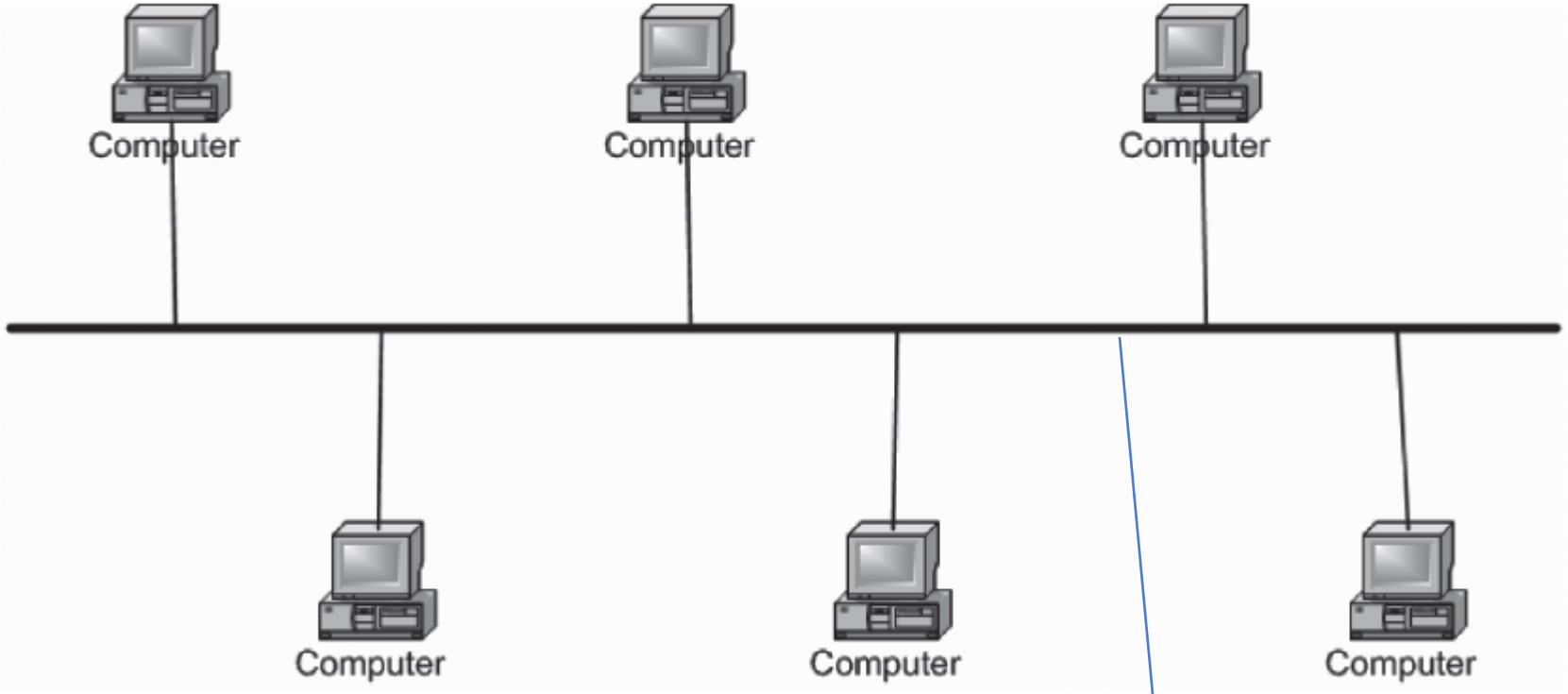
Star أو النجمة.

Ring أو الحلقة.

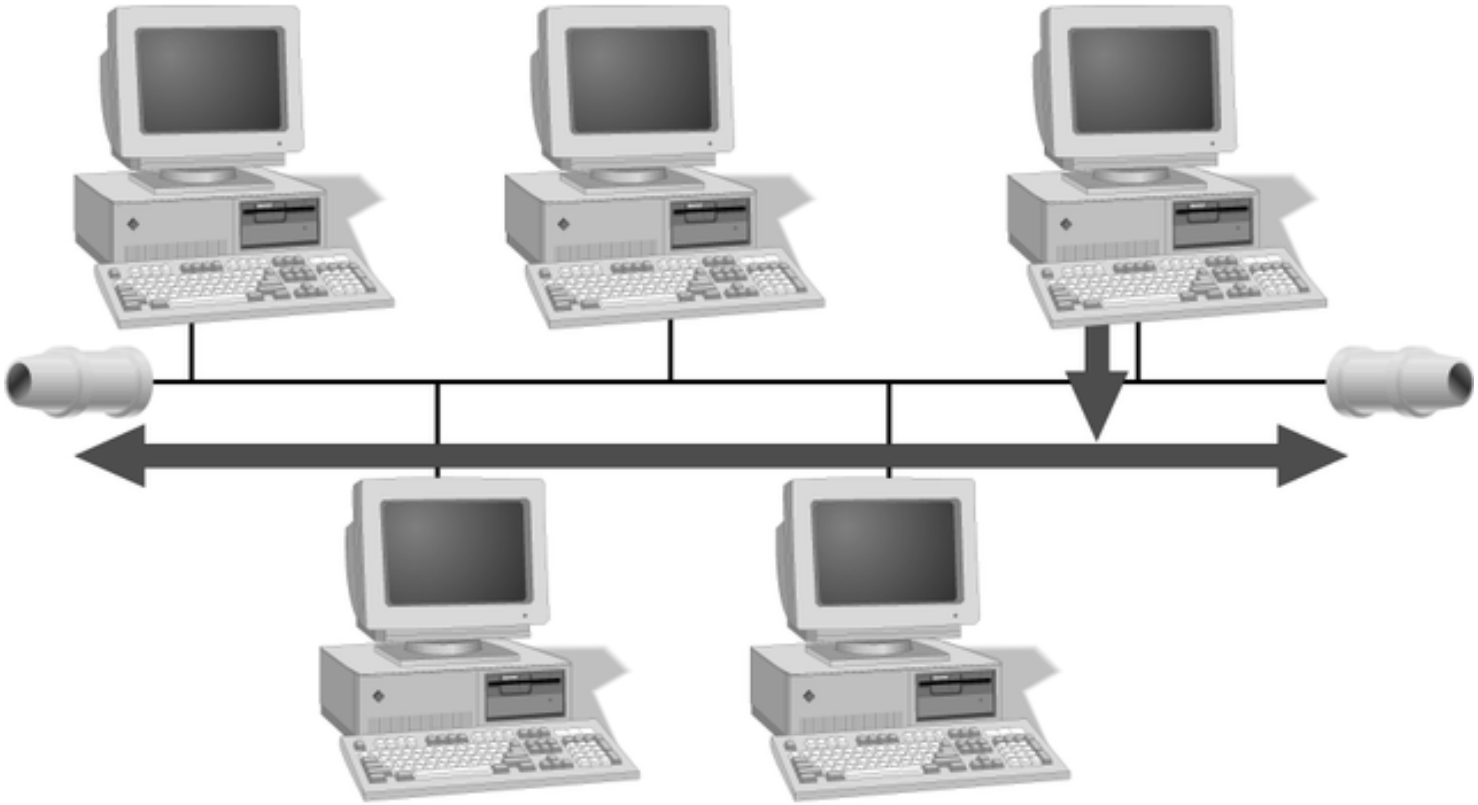
تبولوجيا الناقل BUS TOPOLOGY

- يعتبر الأبسط وربما الأكثر شيوعاً في الشبكات المحلية
- ترسل البيانات لكافة الأجهزة الموجودة على الخط في كلا الاتجاهين
- يتم قبول الإشارة من الجهاز الذي يتفق عنوانه مع عنوان المشفر
- ممكن أن يحدث تصادم في الإشارات Collision
- لذلك كل جهاز لابد من انتظار دوره في إرسال البيانات على الشبكة
- كلما زاد عدد الأجهزة على الشبكة زاد وقت الانتظار للإرسال وبالتالي زاد بطء الشبكة

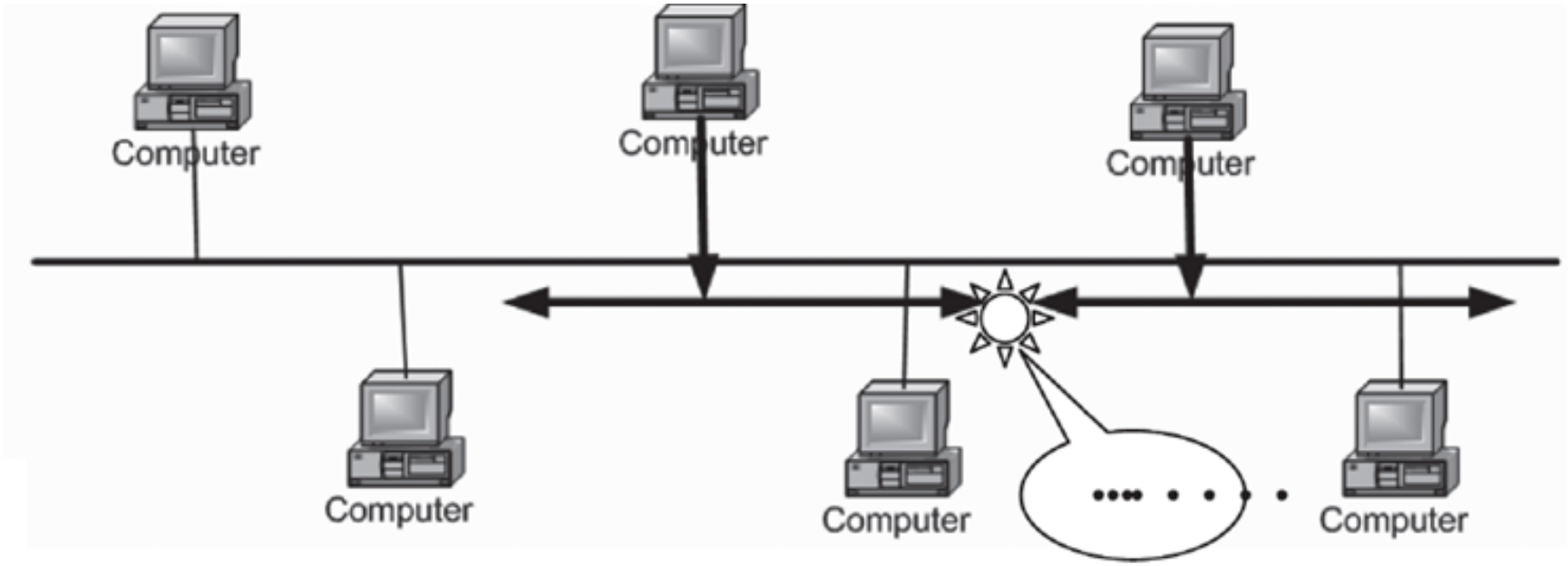
BUS TOPOLOGY تبولوجيا الناقل



BUS تبولوجيا الناقل TOPOLOGY



تبولوجيا الناقل BUS TOPOLOGY



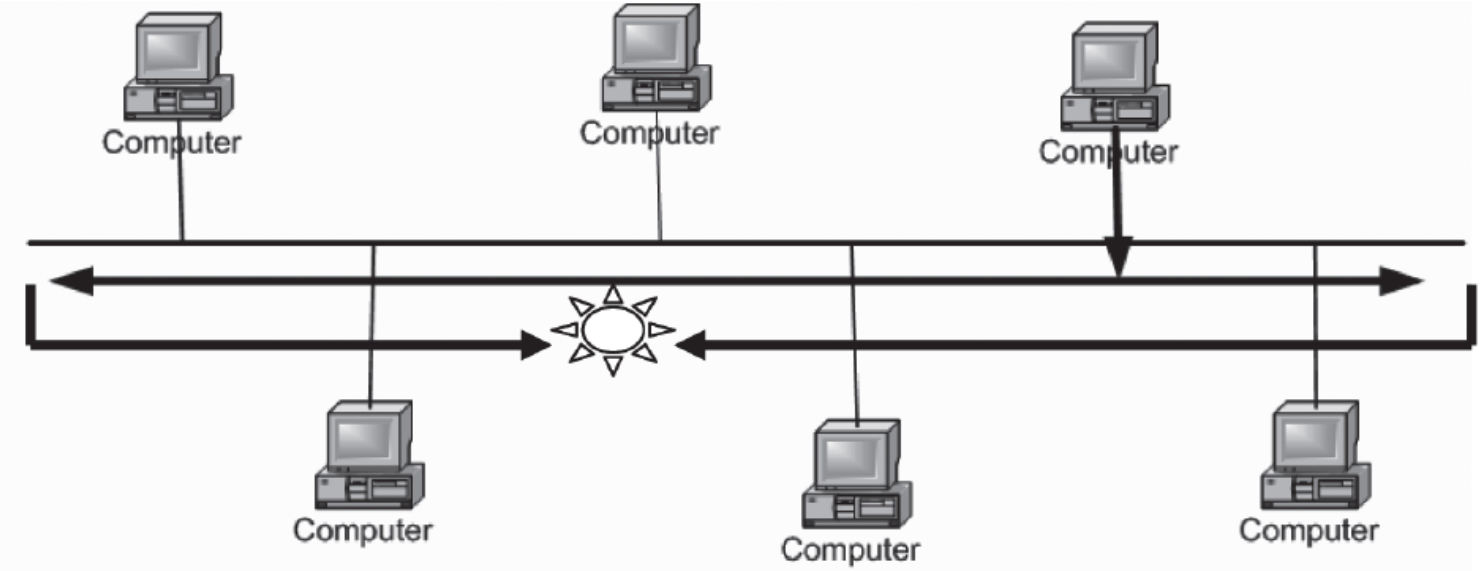
الشكل (3): تصادم الاشارات عند ارسال جهازين معا

العوامل التي تؤثر على أداء شبكة BUS هي:

1. الإمكانيات التي تقدمها مكونات الأجهزة المتصلة بالشبكة (Hardware Capabilities)
2. عدد الأجهزة المتصلة بالشبكة.
3. نوعية البرامج المشغلة على الشبكة.
4. المسافة بين الأجهزة المتصلة بالشبكة.
5. سرعة نقل البيانات على الشبكة مقاسة بالبت في الثانية.

ارتداد الإشارة عند نهايتي الناقل

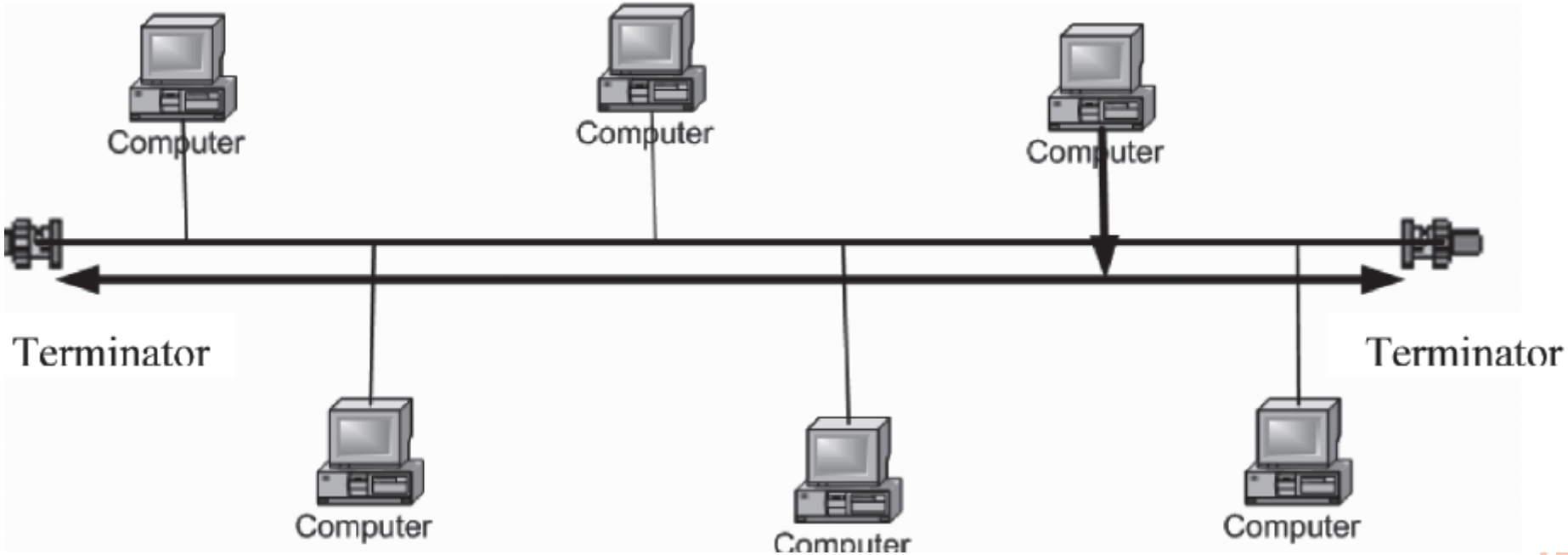
عندما ترسل إشارة البيانات على الشبكة فإنها تنتقل من بداية السلك إلى نهايته. وإذا لم يتم مقاطعة هذه الإشارة فإنها ستبقى ترتد جيئة وذهاباً على طول السلك، وستمنع الأجهزة الأخرى من إرسال إشاراتها على الشبكة. كما يبين الشكل



الشكل (4): ارتداد الإشارة عند نهايتي الناقل

المنهي TERMINATOR

لهذا يجب إيقاف هذه الإشارة بعد وصولها إلى عنوانها المطلوب الممثل بالجهاز الذي أرسلت إليه البيانات. ولإيقاف الإشارة ومنعها من الارتداد، يستخدم مكون من مكونات الشبكة يسمى منهي Terminator ويتم وضعه عند كل طرف من أطراف السلك ويوصل بكل حاسوب متصل بالشبكة. كما يوضح الشكل (5).



المنهي TERMINATOR

- يقوم بامتصاص أي إشارة حرة على السلك مما يجعله مفرغاً من أي إشارات
- وبالتالي يصبح مستعد لاستقبال أي إشارات جديدة
- وهذا يمكن الكمبيوتر التالي من إرسال بياناته على ناقل الشبكة

تتوقف الشبكة في BUS في الحالات التالية

1. في حال قطع السلك.
2. في حالة انفصال السلك في أحد أطرافه عن أي من الأجهزة الموصل إليها ويؤدي هذا إلى توقف جميع الأجهزة عن الاستفادة من موارد الشبكة.

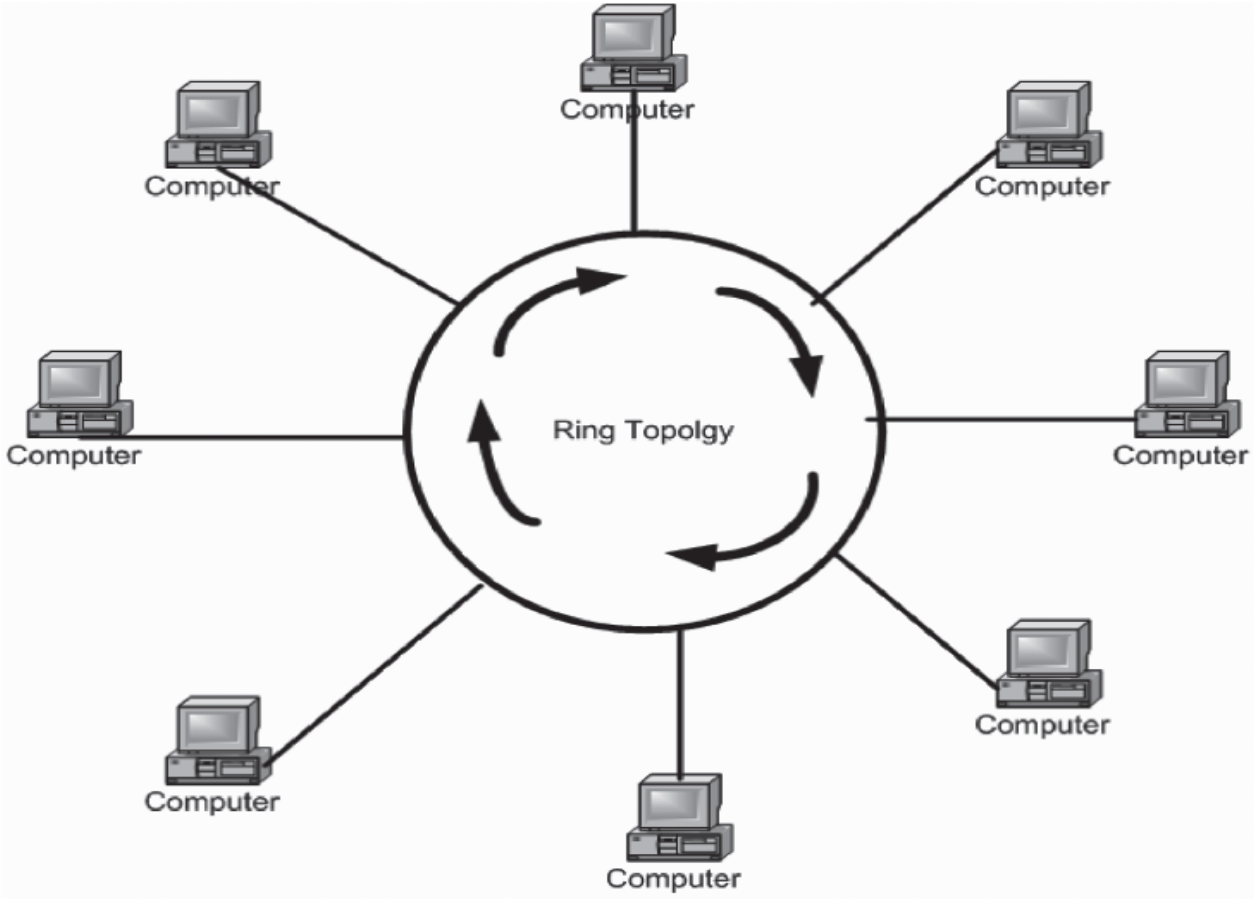
تبولوجيا الحلقة RING TOPOLOGY

تنتقل الإشارات على مدار الحلقة في اتجاه واحد وتمر من خلال كل جهاز على الشبكة. ويقوم كل جهاز على الشبكة بعمل دور مكرر الإشارة حيث إن كل جهاز تمر من خلاله الإشارة يقوم بإنعاشها وتقويتها ثم يعيد إرسالها على الشبكة إلى الجهاز التالي. ولكن لأن الإشارة تمر على كل جهاز في الشبكة فإن فشل أحد الأجهزة أو توقفه عن العمل سيؤدي إلى توقف الشبكة ككل عن العمل.

يطلق على التقنية المستخدمة في إرسال البيانات على شبكات الحلقة اسم Token Passing أو تمرير وحدة بيانات. حيث يتم تمرير وحدة البيانات المسمى Token

تبولوجيا الحلقة RING TOPOLOGY

في تصميم الشبكات من هذا النوع يتم ربط الأجهزة في الشبكة بحلقة أو دائرة من السلك بدون نهايات توقف كما يظهر الشكل (6).



الشكل (6): تبولوجيا الحلقة Ring Topology

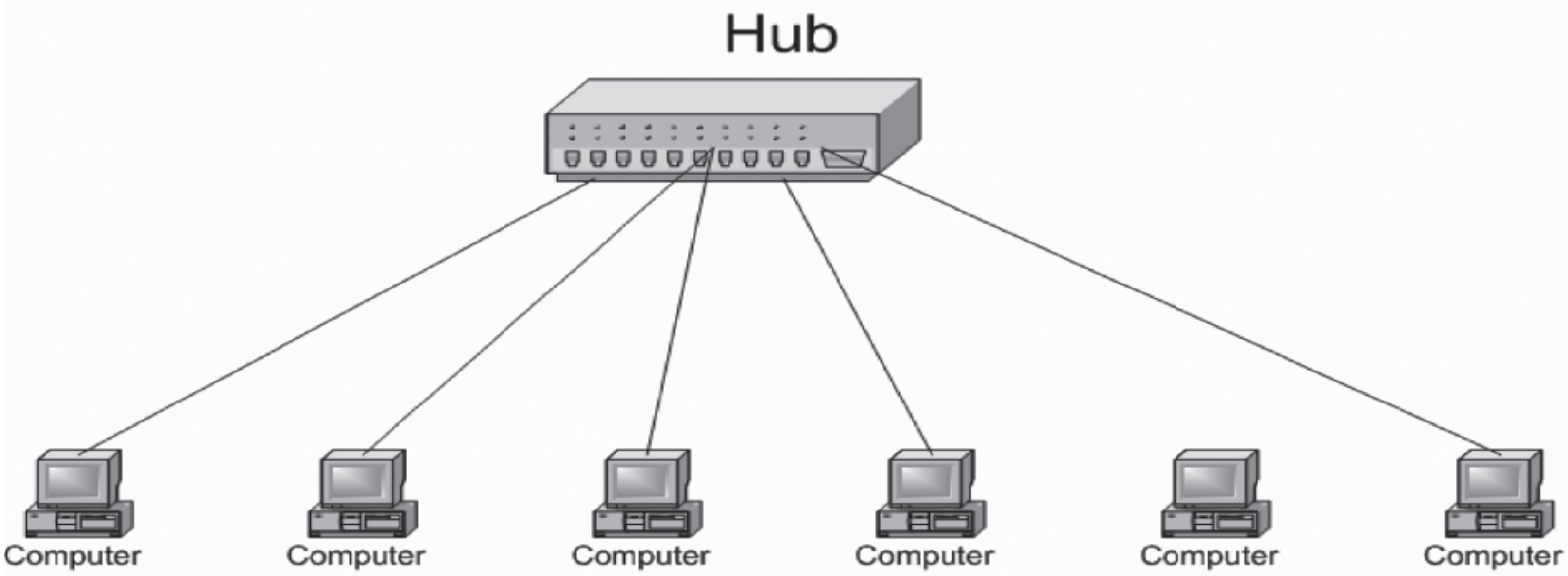
تبولوجيا الحلقة RING TOPOLOGY

- عندما يتسلم الجهاز إشارة حرة Free Token يصبح قادر على الإرسال ويضيف بياناته ويضيف عنوان الكتروني يحدد وجهة الرسالة ثم يرسل Token.
- تنتقل الرسالة حتى يصل العنوان الذي يفك التشفير
- يقوم المستقبل بنسخ البيانات ثم يرسل Token للجهاز الأصلي يخبره انه استلم الرسالة صحيحة وخالية من الأخطاء.
- وهكذا تمر الإشارة حتى تصل للجهاز المرسل مرة أخرى ومن ثم يقوم بإزالتها ويرسل بدل منها Free Token
- تعتبر من الوسائل السريعة لإرسال البيانات.
- حيث تنتقل الإشارة من جهاز لأخر بسرعة مقاربة لسرعة الضوء.
- بسبب هذه السرعة يكون أداء الشبكة ممتاز حتى في وجود عدد كبير من الأجهزة

مشكلاته: يجب إيقاف الشبكة عند تطوير عملها، وفي حال حدوث خلل في واحد يؤثر على الجميع.

تبولوجيا النجمة
STAR TOPOLOGY

تقوم الشبكات المحلية ذات التصميم من النوع النجمة أو Star بربط أجهزة الكمبيوتر بأسلاك موصلة بمكون أو جهاز مركزي يطلق عليه الموزع Hub وأحياناً يسمى النقطة المركزية Central Point أو Wiring Center كما يوضح. الشكل (7).



تبولوجيا النجمة
STAR TOPOLOGY

تنتقل الإشارات من الجهاز المصدر الذي يرغب في إرسال البيانات إلى النقطة المركزية أو Hub ومنه إلى باقي أجهزة الحاسوب على الشبكة. نظام التوصيل في Hub يعزل كل سلك من أسلاك الشبكة عن الآخر. وبالتالي إذا توقف جهاز الحاسوب ما أوانقطع السلك الذي يوصله بالموزع فلن يتأثر إلا الجهاز الذي توقف أو انقطع سلكه بينما باقي الأجهزة ستبقى تعمل من خلال الشبكة دون أي مشكلات. ولكن إن توقف الموزع (HUB) عن العمل فستتوقف الشبكة ككل عن العمل.

تبولوجيا النجمة
STAR TOPOLOGY

- **مميزاته:**
- يعتبر الأكثر استعمالا من بين التصاميم المختلفة
- بسبب سهولة تحريك الأجهزة من مكان لأخر وصيانتها دون
- توقف الشبكة.
- **عيوبه:-**
- يعتبر مكلف في حال زيادة حجم الشبكة بسبب حاجة لأسلاك كثيرة والموزع سعره غالي.

بطاقة الشبكة
NETWORK INTERFACE CARD

- تمكن أجهزة الحاسوب من الاتصال بالشبكة
- تركب في اللوحة الرئيسية أو تكون داخلية
- يتم وصل السلك الشبكة بالبطاقة ليصبح متصلا

تنظيم البيانات عبر الشبكة وإرسالها

- كل بطاقة شبكة لها عنوان فريد يسمي MAC address
- هذا العنوان تحدده لجنة IEEE
- هذه اللجنة تخصص مجموعة من العناوين لكل مصنع من مصنعي بطاقات الشبكة
- يتكون من 48 بت ويكون مخزن داخل ROM
- يحتوى على 24 بت على تعريف للمصنع و24 بت على الرقم المتسلسل للبطاقة
- تنشر البطاقة عنوانها على الشبكة مما يسمح للأجهزة بالتخاطب معها
- تحتوى على جزء مادي وجزء برمجي
- مسؤولة عن تحويل البيانات من الجريان بشكل متواز إلى شكل متسلسل على السلك الشبكة وبالعكس في الطرف الاخر.

تقوم بطاقة الشبكة بتنظيم عملية بث البيانات على الشبكة كما يلي

1) نقل البيانات من الحاسوب إلى البطاقة تمهيدا لبثها إلى الوسط الناقل
2) تخزين البيانات مؤقتا على البطاقة تمهيد لبثها
3) إجراء تفاهم على شروط نقل البيانات بين البطاقة المرسلة والمستقلة
4) ترجمة الإشارات الكهربائية من سلك الشبكة إلى ثنائيات يفهمها المعالج وعندما ترسل تترجم الإشارات الرقمية إلي نبضات كهربائية تستطيع حملها قناة الاتصال
5) التحكم بتدفق البيانات على بشكل متسلسل

لكي يتم اتصال ناجح بين البطاقات لابد من توفير:

1) الحجم الأقصى لمجموعات البيانات التي سيتم إرسالها
2) الفترة الزمنية التي تفصل بين إرسال حزم البيانات
3) مقدار البيانات التي تستطيع كل بطاقة استقبالها

وبعد أن يتم الاتصال تقوم البطاقة الشبكة:

- مراقبة وسط الإرسال
- طلب حزم البيانات والتعرف عليها والتأكد من عنوان البطاقة المستلمة
- اكتشاف الأخطاء وحلها

العوامل المؤثرة على سرعة بطاقة الشبكة

- الأسلوب المستخدم في نقل البيانات
- المشغلات البرمجية المستخدمة driver
- سعة ناقل البيانات في الحاسوب بين أجزاء الشبكة
- قوة المعالج الموجود على البطاقة
- مقدار ذاكرة التخزين المؤقت على البطاقة

أساليب تبادل البيانات بين الحاسوب والبطاقة

1. برمجة المدخل والمخرج I/O programmed
2. ذاكرة البطاقة المشتركة Shared Adapter Memory
3. الوصول المباشر للذاكرة DMA
4. التحكم بالناقل Bus Mastering

عنق الزجاجة BOTTLENECK

- إذا كانت سرعة الناقل bus أكبر من سرعة معالجة البطاقة للبيانات فتصبح البطاقة مسببة لمشكلة عنق الزجاجة ولحل هذه المشكلة تستخدم البطاقة:
  - ذاكرة احتياطية مركبة عليها لتحزين البيانات مؤقتا قبل إرسالها ولكما زاد حجم هذه الذاكرة زادت سرعة نقل البطاقة للبيانات إلى الوسط الناقل
  - معالج خاص مركب على البطاقة وكلما زاد قوة المعالج تطور أداء البطاقة أكثر

بطاقة الشبكة لاسلكية

- نوع خاص من الشبكات المحلية اللاسلكية
- تستخدم البطاقة لعمل شبكة محلية لاسلكية
- نفس عمل البطاقات السلكية والاختلاف يكون في:

1) وسط الإرسال المستخدم للبث
2) المكون المسؤول عن عملية البث ويسمي المجمع اللاسلكي ويشمل:

1. موجات الراديو
2. موجات الميكروويف
3. موجات الأشعة تحت الحمراء

مشغل بطاقة الشبكة
NETWORK DRIVER CARD

- لكل بطاقة لها المشغل الخاص بها يصدر من الشركة المصنعة لها
- تقوم بعملية الاتصال بين الجزء المادي والجزء البرمجي للحاسوب
- ويجب أن تكون المشغلات متوافقة مع:
  1. مواصفات مشغل الشبكة البيني NDIS
  2. وصل البيانات المفتوح البيني ODI
- هذه النوعين يكفي لان تتم الصناعة حسب المواصفات وتكون فاعلة لجميع الأجهزة

التقنيات الرئيسية في الشبكات المحلية

أنواع التقنيات في الشبكات المحلية

1. الايثرنت Ethernet
2. شبكة توكن رينغ المحلية Token Ring LAN
3. شبكة البيانات الموزعة بالألياف الضوئية FDDI

شبكات الاتصال اللاسلكية المحلية

شبكات الاتصال اللاسلكية المحلية WIRELESS

- خيار فعال لتبادل البيانات والموارد عبر الشبكات
- تعمل بشكل مشابه للشبكات السلكية
- الاختلاف في الوسط الناقل
- كل جهاز يحتوى على بطاقة لاسلكية
- تشكل خيار فعال والسبب:

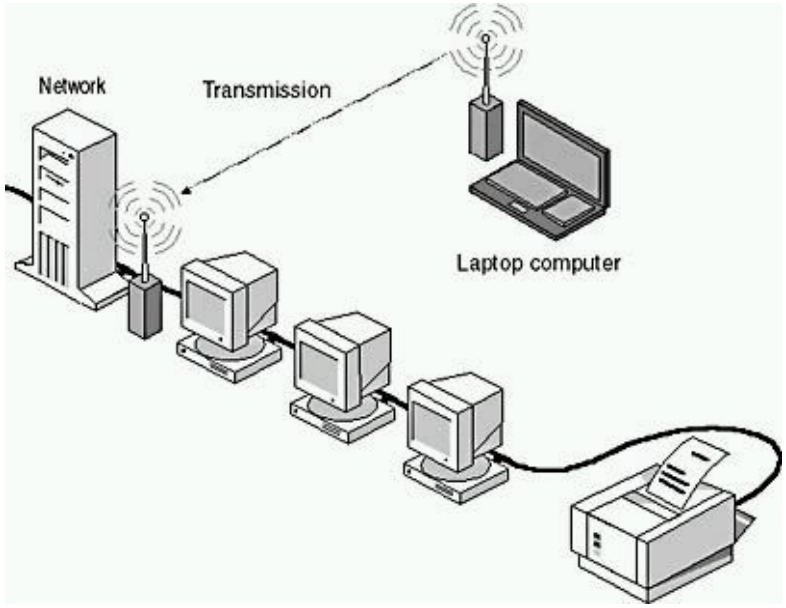
1. التطورات المتلاحقة في التقنيات والمنتجات اللاسلكية
2. الانخفاض المتواصل في الأسعار
3. الطلب المتزايد على الشبكات
4. سهل التركيب في الأماكن الأثرية

خصائص الشبكات اللاسلكية ومزاياها

1. توفر اتصالات مؤقتة لشبكات سلكية في حل فشل هذه الاسلاك
2. المساعدة في عمل نسخة احتياطية للبيانات على شبكة سلكية لجهاز متصل لاسلكيا
3. توفير درجة من الحرية في التنقل لبعض المستخدمين في شبكة السلكية
4. توفير اتصالات في الأماكن المزدحمة
5. بناء شبكات في الأماكن المعزولة التي يصعب توصيلها بأسلاك

الموجات الضوئية

- تستخدم الضوء لنقل البيانات وهي نوعان
  - شبكات الاشعة تحت الحمراء
  - شبكات الليزر وهي توفر سرعات عالية جدا وتكلفة مرتفعة
- شبكات الاشعة تحت الحمراء تستخدم التقنيات التالية:
  - نقطة إلى نقطة point to point
  - ارسال منتشر إو إذاعي Broadcast
  - إرسال عاكس Reflective



تقنية السن الأزرق BLUETOOTH

1. تربط عدد من الأجهزة الالكترونية بعضها ببعض عن طريق موجات الراديو بدلا من الكابلات
2. اسخداماتها:
   1. ربط وتوصيل الأجهزة لاسلكيا
   2. ربط وتوصل الأجهزة المختلفة مع بعض
   3. توصيل بقية الأجهزة المنزلية مع الحاسوب أو الجوال

شبكات الاتصال الهجينة

1. مشتركة بأكثر من نوع بحيث جزء
2. منها سلكي والجزء الاخر لاسلكي

الوحدة الخامسة
معمارية الشبكات المحلية الموسعة

مقدمة في معمارية الشبكات المحلية الموسعة

- توسيع الشبكة المحلية للحصول على شبكة محلية موسعة بسبب
- تزايد الحاجة لإرسال بيانات عبر مسافات بعيدة وكذلك
- زيادة عدد الأجهزة في الشبكة مع الاحتفاظ بفاعليتها

- **الشبكات المحلية الموسعة** تتكون من مجموعة من الشبكات المحلية مرتبطة مع بعضها البعض باستخدام الألياف الضوئية، موجات الميكروويف ، أو اتصالات عبر أقمار صناعية أو أنظمة الأسلاك المحورية.

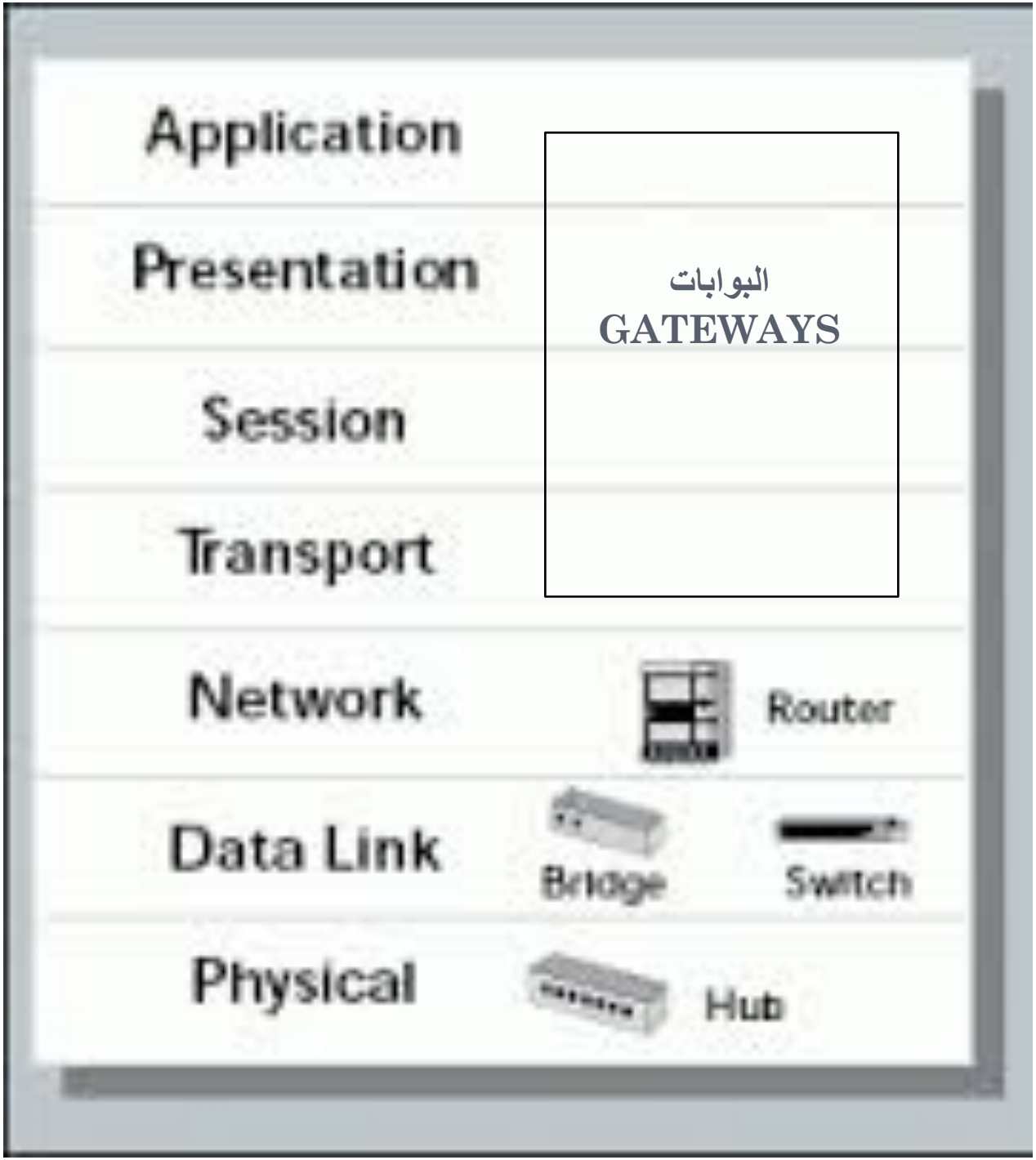
يمكن زيادة حجم الشبكة دون التأثير على كفاءتها

1) التوسيع المادي للشبكة لاستيعاب حواسيب إضافية
2) تقسيم الشبكات المحلية الموجودة إلى عدة أقسام لكل قسم شبكة محلية صغيرة
3) ربط شبكتين محليتين منفصلتين معا
4) ربط شبكة محلية مستقلة بمجموعة من الشبكات المحلية المرتبطة معا لتكوين شبكة أكبر.

عملية التوسيع الشبكة

- عملية توسيع الشبكة تتطلب واحد أو كل المكونات التالية:

1. مكررات الإشارة Repeater
2. الجسور Bridges
3. المقسمات LAN Switches
4. الموجهات Routers
5. البوابات Gateways

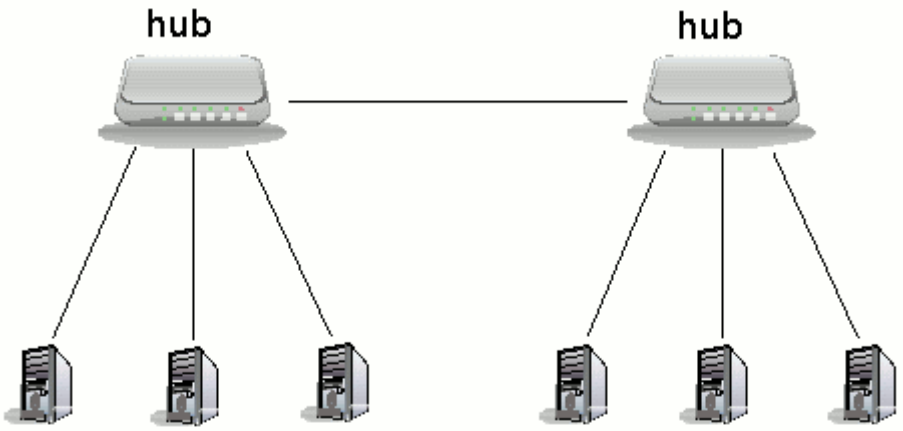

Application
Presentation
Session
Transport
Network
Data Link
Physical
البوابات
GATEWAYS
Router
Bridge
Switch
Hub

مكررات الإشارة REPEATERS

- تستخدم لمعالجة مشكلات توهين (ضعف أو تلاشي) الإشارة عند انتقالها إلي مسافات طويلة
- تقوم هذه المكررات باستقبال هذه الإشارة ثم تعيد توليدها وتقويتها ثم ترسلها مرة أخرى
- مما يسمح لهذه الإشارة بالوصول لمسافات طويلة دون ضعف أو تلاشي
- تعتبر وسيلة لتوسيع الشبكات المحلية
- لابد استخدام نفس البروتوكولات بين الشبكتين الموصولتين بالمكرر بحيث لا يربط شبكتين مختلفتين مثل ايثرنت وتوكن رنغ
- لا تستطيع ترجمة أو فلتره الإشارات

مكررات الإشارة REPEATERS

- وسيلة غير مكلفة لتوسيع الشبكات
- تعاني من بعض المشكلات :
  - لا فلتر البيانات
  - ولا تمنع البيانات المعطوبة من المرور
  - تنقل الخلل من الأقسام إلى الأخرى



مميزات المكررات

1. تستعمل لوصل شبكتين محليتين تكون المسافة بينهما قد تجاوزت الحد الأعلى بحيث تصبح شبكة واحدة بالربط
2. تستقبل الإشارات الواردة وتعيد توليدها وتقويتها ثم ترسلها إلى الجزء الآخر
3. لا يقوم المكرر بقراءة إطارات البيانات
4. كل مكرر يسمح بمضاعفة طول الشبكة
5. يضيف المكرر بعض التأخير وكلما زاد طول الشبكة زاد التأخير
6. يمكن استخدام شبكة واحدة من المكررات لتغضية بناية كاملة

عيوب المكررات

1) لا يقوم المكرر بتصفية الضجيج ويمرره كما هو
2) ينظر إلي الشبكة بأكملها كشبكة محلية خطية bus وهذا يمكن أن يسبب احتمالية التصادم في حال شبكة عدد الأجهزة كبير
3) لا يمكن ربط شبكات مختلفة التقنية معاً

الموزعات HUBS

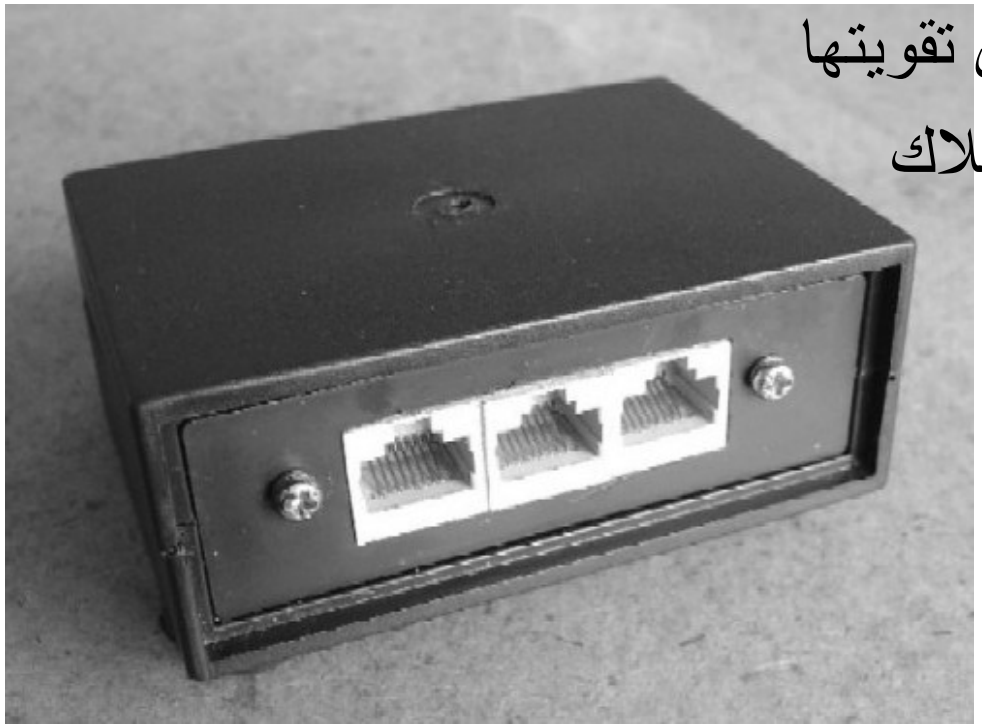
- هي عبارة عن أجهزة تستخدم عادة مع الشبكات من نوع نجمة
- ويمكن أن يطلق عليها مكرر الإشارة متعدد المنافذ
- يكون لدي الموزع 8-12 منفذا وأحيانا أكثر
- يكون الاتصال بين الأجهزة عن طريق الموزع ويعزل الأسلاك عن بعضها البعض
- إذا انفصل جهاز عن الشبكة لا يؤثر ذلك على الشبكة
- إذا توقف الموزع عن الشبكة يحدث خلل وتتوقف الشبكة

أنواع أساسية للموزعات

1. موزع خامل Passive Hub. يقوم فقط بتمرير الإشارات
2. موزع نشط Active Hub. تُعيد توليد الإشارات
3. موزع هجين Hybrid Hub. توسيع الشبكة بتركيب أكثر من موزع واحد

موزع خامل PASSIVE HUB

- وهو ابسط الموزعات وقلة في التكلفة
- يقوم فقط بتمرير الإشارة دون تقويتها
- مثال عليه لوحات توزيع الأسلاك
- وهي تعمل نقاط توصيل
- ولا تقوم بتقوية الإشارة
- ولا تحتاج لطاقة كهربائية.



موزع الفاعل ACTIVE HUB

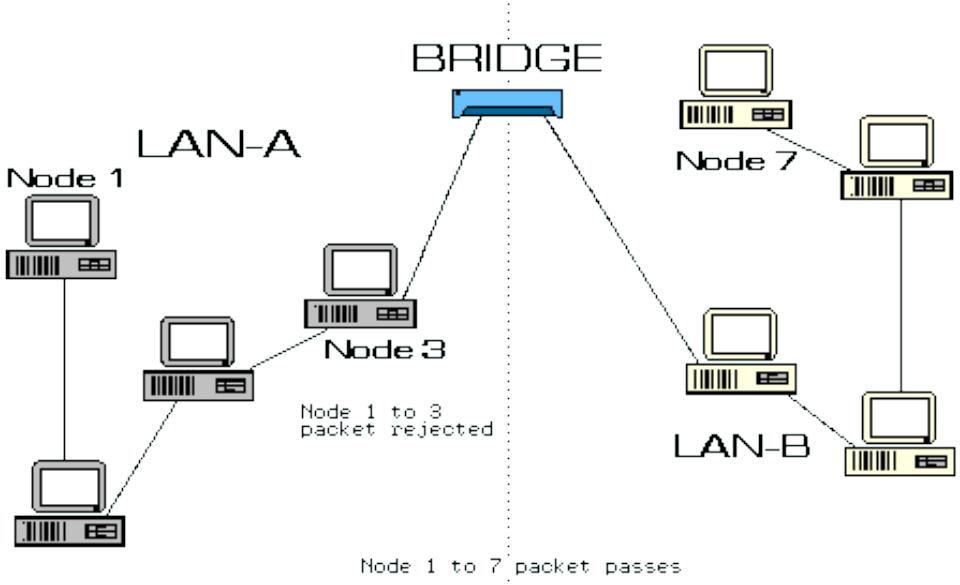
- يحتوى أجزاء إلكترونية تعيد توليد الإشارة في الشبكة
- وبالتالي تزيد المسافة بين الأجهزة في الاتصال
- يوجد منه نوع محسن يسمي الذكي
- الأكثر شيوعا وتشبه عمل المكرر Repeater
- يكون من 8 – 12 منفذ توصل به الأجهزة
- يسمي مكرر الإشارة متعدد المنافذ
- تحتاج إلى طاقة كهربائية لتشغيله

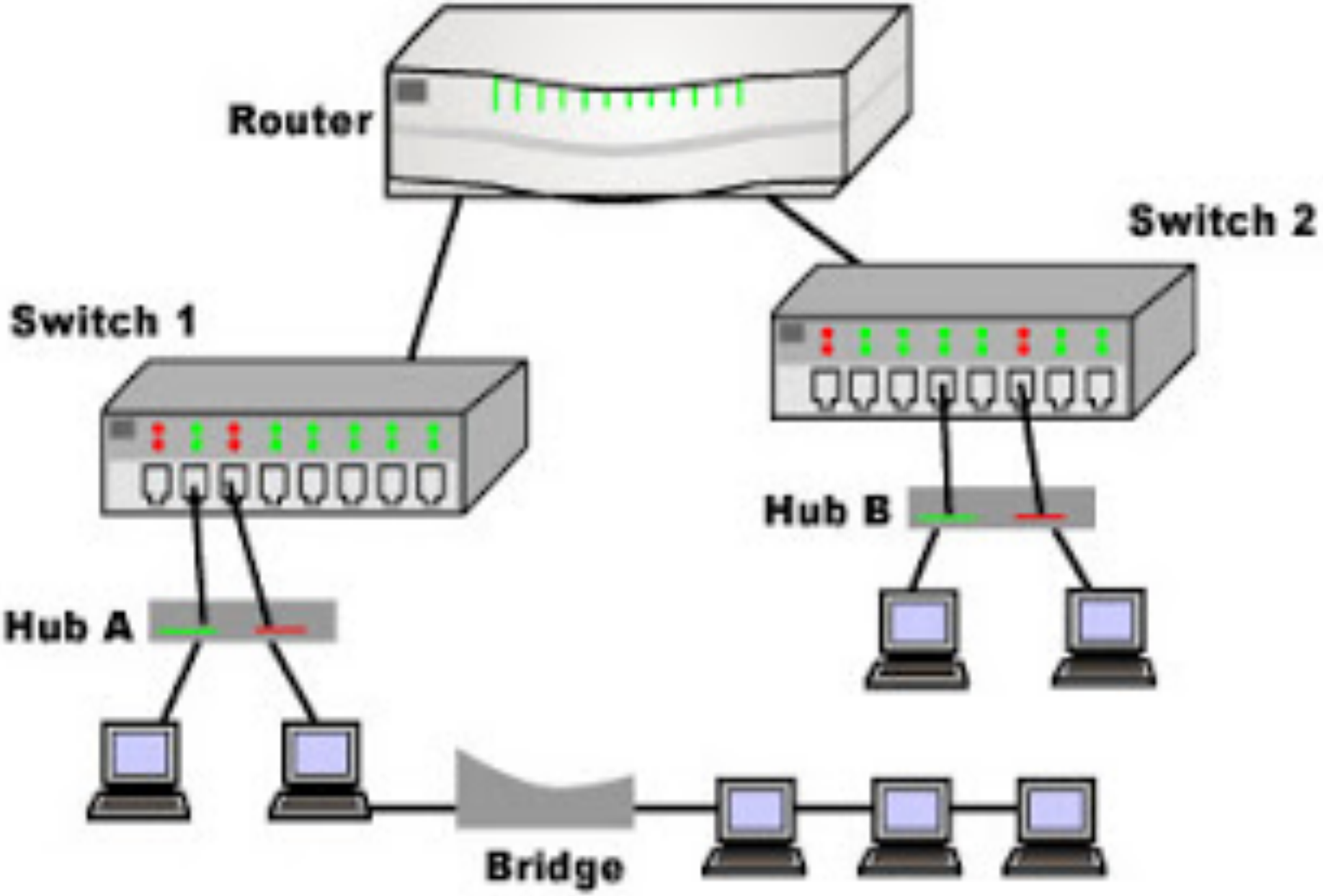
مميزات الموزعات HUBS

1. تسمح بتوسيع الشبكة وتغير مكوناتها بكل سهولة ودون توقف الشبكة
2. تستطع استخدام منافذ متنوعة تتوافق مع أنواع مختلفة من الأسلاك
3. تساعد على المراقبة المركزية لنشاط الشبكة وحركة المرور
4. تستطيع عزل المشكلات بعزل الجهاز المسبب المشكلة
5. لديه معالج يقوم بعد الجزم البيانات التي تمر عبره
6. تستطيع اكتشاف المشكلات في الحزم البيانات المرسلة وتوجيه تحذير
7. بعض منها يحدد المدة الزمنية المسموح بها الاتصال على الشبكة

الجسور BRIDGES

- عبارة عن جهاز يمكن استخدامه للربط بين عناصر الشبكة المحلية ويمكن تلخيص عمله في نقطتين:
  1) توسيع الشبكة المحلية
  2) تقسيم الشبكة المحلية إلى أكثر من قسم وتوزيع حركة المرور بين هذه الأقسام




Router
Switch 2
Switch 1
Hub B
Hub A
Bridge

مميزات الجسور

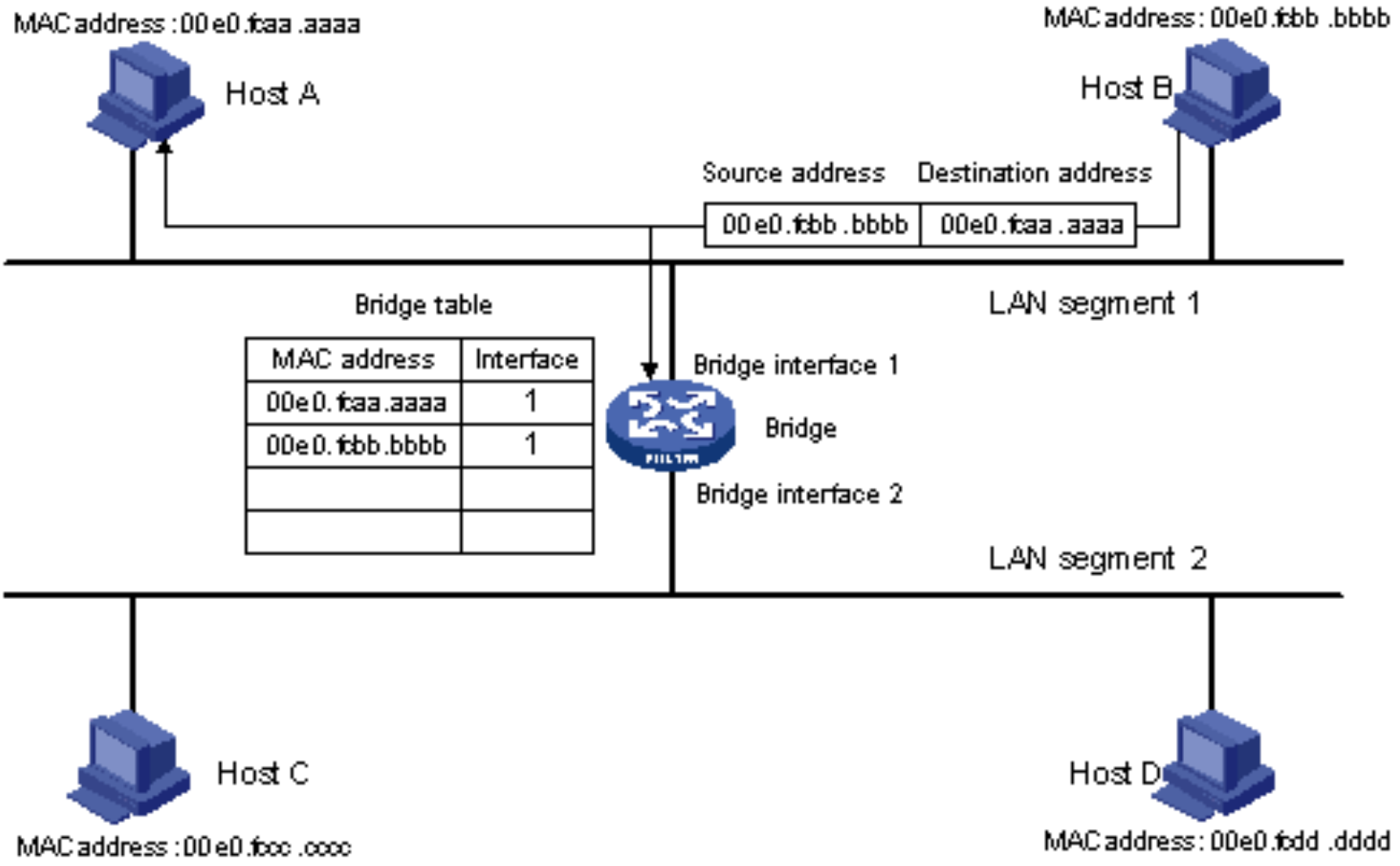
1) الربط بين أسلاك الشبكات المتشابه والمختلفة
2) إعادة توليد البيانات
3) تجاوز معيار 802.3 فيما يخص الحد الأعلى لعدد الأجهزة المسموح لها بالاتصال بالشبكة المحلية
4) إعادة توليد البيانات ولكن على مستوى الحزمة
5) توفير أداء أفضل للشبكة
6) ترشيح filtering مرور البيانات لتخفيض التزاحم
7) تجهيز جدول عناوين مادية للأجهزة المتصلة بالشبكة

أنواع الجسور وتقسيماتها

- **هناك نوعان من الجسور :**
  - داخلية : تركب داخل جهاز المزود
  - خارجية: تكون في جهاز مستقل ذاتيا
- **تقوم بعمليتين :**
  - توجيه اطر البيانات عند وصولها من خط المرسل إلى خط المستقبل
  - بناء جدول التقسيم.
- وتقسم الجسور حسب عملها :
  - **جسور محلية** : تقوم بالربط بين الأسلاك المحورية الثخينة للأقسام المختلفة للشبكة وتكون متصلة بشكل مباشر
  - **جسور بعيدة المدى**: تربط بين الأسلاك الثخينة والأسلاك بعيدة المدى مثل الأسلاك الهاتف المؤجرة.

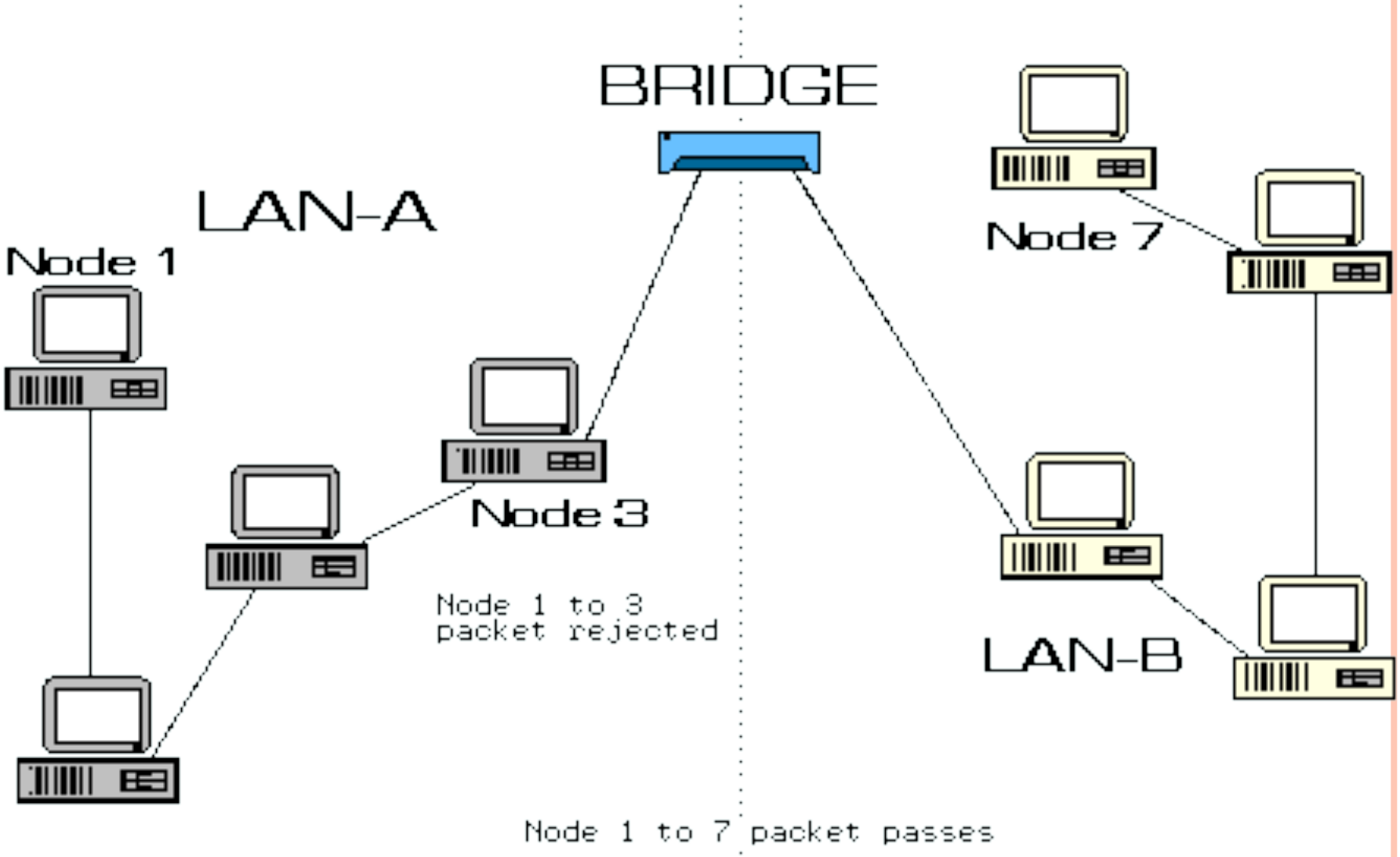
مبدأ عمل الجسور

- تعمل الجسور على مبدأ أن لكل جهاز على الشبكة عنوان فريد MAC يتم توجيه الحزم لهذا العنوان
- تمتلك بعض السمات الذكية عن طريق جمع المعلومات عن الأجهزة على الشبكة ويطلق عليها الجسور المتعلمة
- تتعرف الجسور على الأجهزة بإرسال رسائل موجه إلي كل الأجهزة على الشبكة وترد الأجهزة فتصل على العناوين MAC وموقعها Interface لإنشاء **جدول التوصيل** بين الأجهزة


MAC address :00e0.fcaa .aaaa
Host A
MAC address: 00e0.fcbb .bbbb
Host B
Source address
Destination address
00e0.fcbb .bbbb
00e0.fcaa .aaaa
LAN segment 1
Bridge table
MAC address
Interface
00e0.fcaa.aaaa
1
00e0.fcbb.bbbb
1
Bridge interface 1
Bridge
Bridge interface 2
LAN segment 2
Host C
MAC address :00e0.fccc .cccc
Host D
MAC address: 00e0.fcdd .dddd

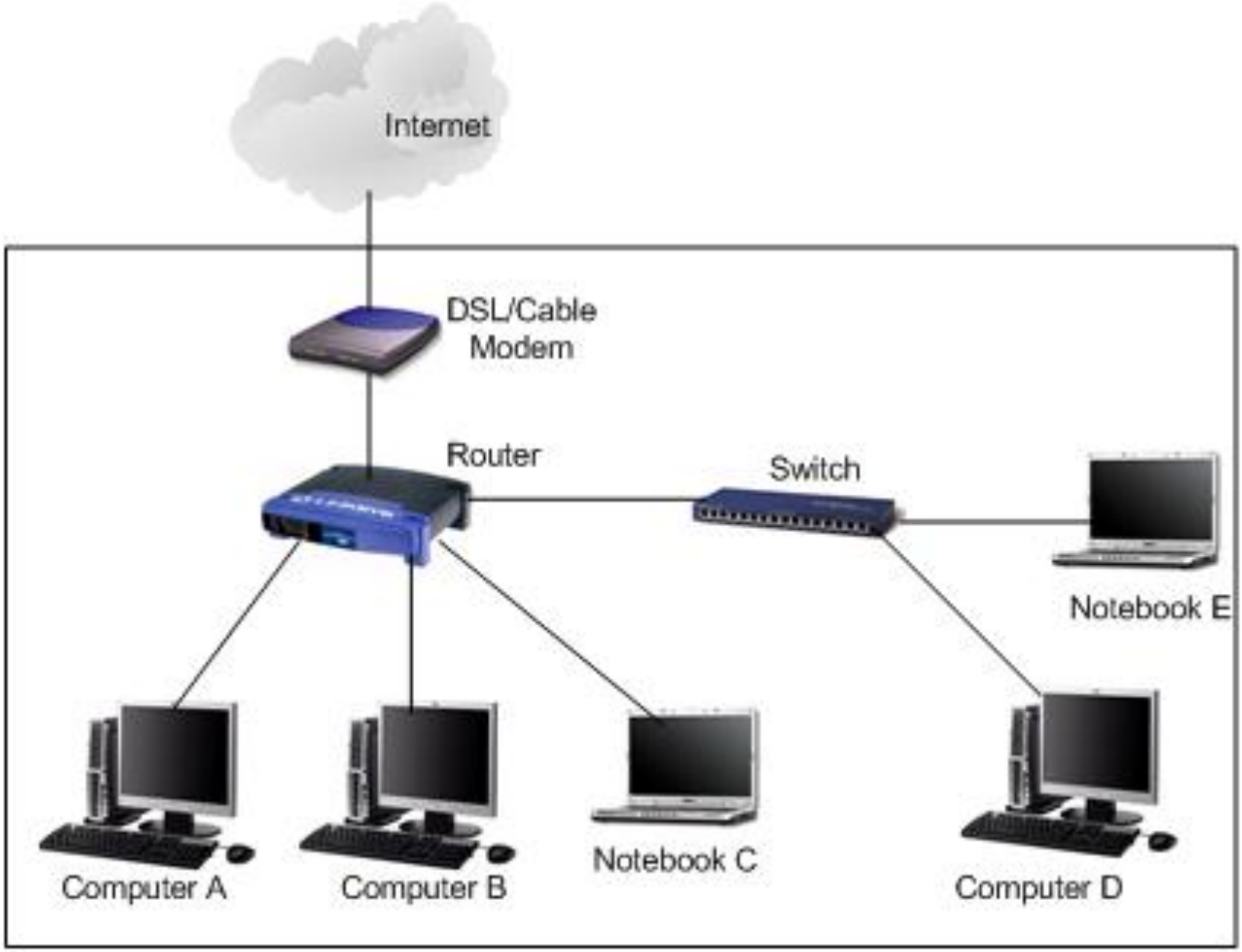
طرق تعامل الجسور مع الحزم التي يستقبلها

- **أولاً: المرسل والمستقبل ينتميان إلى نفس الشبكة الفرعية subnet:**
  - في هذه الحالة يكون عنوان المستقبل وعنوان المرسل ضمن الشبكة الفرعية في جدول التوصيل وبالتالي لا يقوم بتمرير الإشارة ولا داعي لاستخدام الجسر لذلك
- **ثانياً: المرسل والمستقبل ينتميان إلى نفس شبكتين فرعيتن مختلفين ضمن نفس الشبكة:**
  - يقوم الجسر بتمرير الحزمة إلي الشبكة الفرعية بناء على جدول التوصيل للجسر التي تحتوى على العنوان المطلوب للمستقبل.
- **ثالثاً: عنوان المستقبل غير موجود في جدول التوصيل:**
  - يقوم الجسر بتمرير الحزمة إلي كل الأقسام ما عدا القسم الذي ينتمي إليه جهاز المرسل


BRIDGE
LAN-A
Node 1
Node 3
Node 7
LAN-B
Node 1 to 3
packet rejected
Node 1 to 7 packet passes

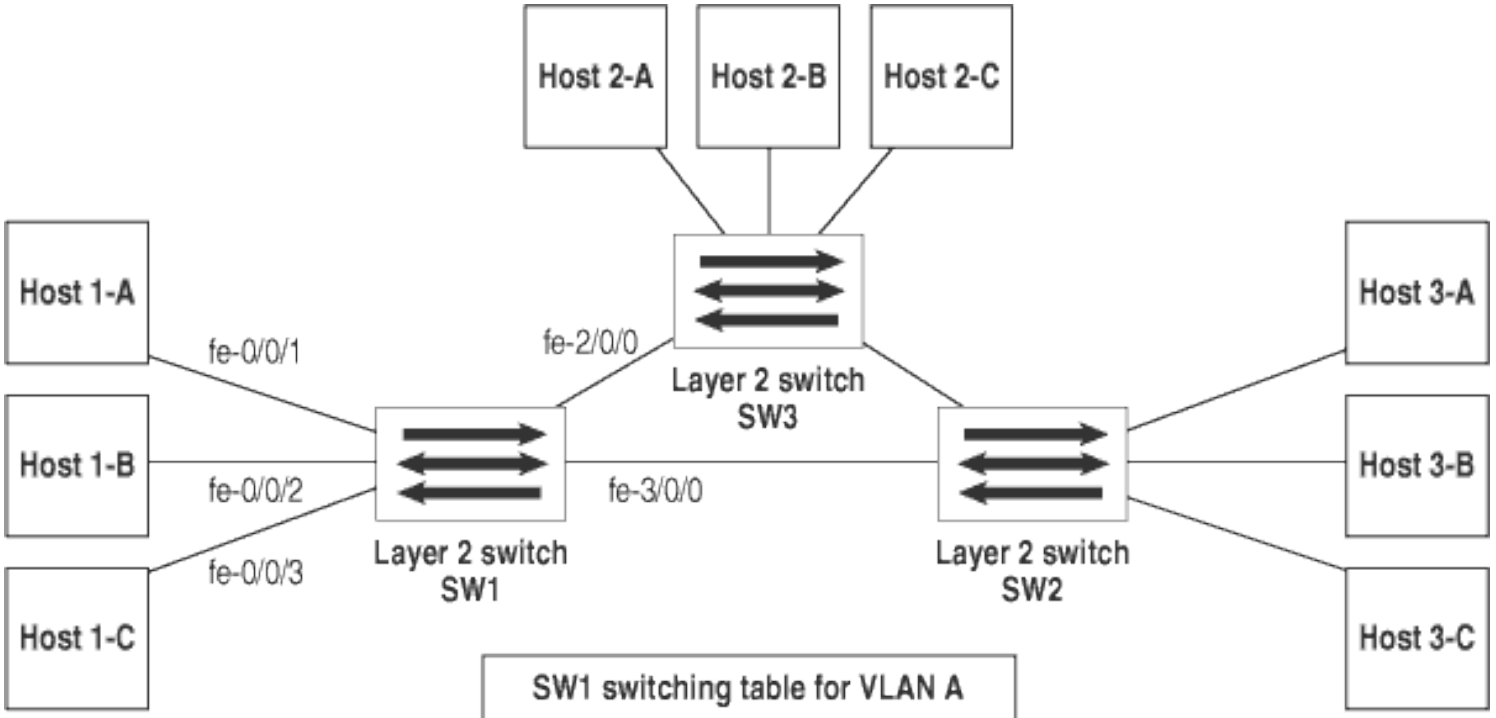
مقسمات الشبكات المحلية LAN SWITCH

- المقسمات أجهزة تستخدم لتوسيع الشبكة المحلية
- أكثر المعدات شيوعاً
- تم جمع الموزعات hub والجسور Bridges بالمقسمات LAN Switch
- المقسم أفضل في تجزئ الشبكة حيث يقسم الشبكة إلى عدد أكثر من الجسور في التقسيم
- الجسر يحتوي على ثلاث منافذ على الاكثر لربط شبكتين أو ثلاثة أما المقسمات فتحتوى على مئات المنافذ
- المقسم أسرع في انجاز المهام.


Internet
DSL/Cable
Modem
Router
Switch
Notebook E
Computer A
Computer B
Notebook C
Computer D

مميزات المقسمات

- قدرتها على تخصيص سرعة إرسال لكل مخرج
  - حيث يخصص لكل منفذ سرعة ولا يتشارك السرعة مع المخارج الأخرى
- قابليتها على الإرسال والاستقبال معا Full Duplex بعكس المكررات التي تستخدم التناوب في ذلك Half Duplex
- تستعمل المقسمات نفس الجدول التي تستخدمها الجسور
- تتعامل مع الشبكات الافتراضية VLAN التي تقسم الشبكة
- تتميز بسهولة الإعداد والإدارة
- تعمل مع كافة أنواع الخطوط التوصيل السلكي واللاسلكي والمجدول والمحوري والضوئي.



SW1 switching table for VLAN A	
Port	MAC Address
fe-0/0/1	1a1a.1a1a.1a1a
fe-2/0/0	2a2a.2a2a.2a2a
fe-3/0/0	3a3a.3a3a.3a3a

SW1 switching table for VLAN B	
Port	MAC Address
fe-0/0/2	1b1b.1b1b.1b1b
fe-2/0/0	2b2b.2b2b.2b2b
fe-3/0/0	3b3b.3b3b.3b3b

SW1 switching table for VLAN C	
Port	MAC Address
fe-0/0/3	1c1c.1c1c.1c1c
fe-2/0/0	2c2c.2c2c.2c2c
fe-3/0/0	3c3c.3c3c.3c3c

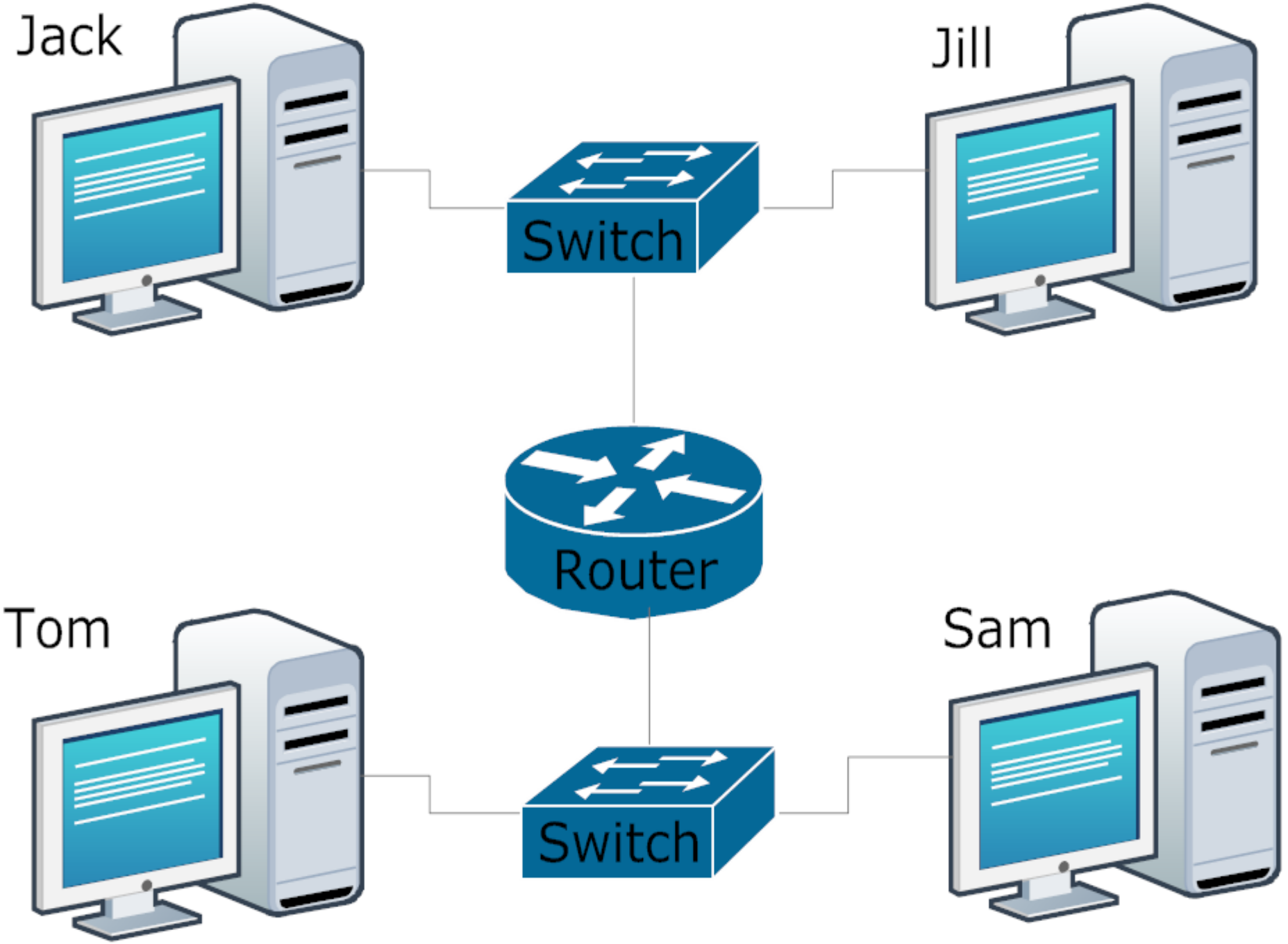
g017130

الموجهات ROUTERS

- جهاز من أجهزة طبقة الشبكة ويستخدم لتوسيع الشبكة المحلية
- يستخدم في شبكات ذات تصاميم بروتوكولات مختلفة
- يقوم ربط شبكتين أو أكثر وتستمر كل شبكة بالعمل منفصل
- يقوم الموجه بربط تلك الشبكات لعمل internetwork
- من الأمثلة على ذلك ربط شبكات الايثرنت وشبكات FDDI
- ويستطيع المستخدم في شبكة الوصول لمصادر شبكة أخرى
- ومن أكثر الأمثلة على ذلك شبكة الانترنت والانترانت

الموجهات ROUTERS

- **تقوم بأعمال مشابه للجسور ومنها:**
  - تصفية حركة المرور بين أقسام الشبكة المختلفة
  - ربط أقسام الشبكة معاً
- **وتقوم بعكس عمل الجسور حيث أنها:**
  - لا تمرر الرسائل الموجه لجميع المستخدمين بعكس الجسور
  - توفر تحكم اكبر بحركة المرور بين الشبكات
  - بعكس الجسور التي تقسم الشبكة الواحدة إلى شبكات فرعية يقوم الموجه بربط الشبكات المحلية مع بعضها البعض


Jack
Jill
Switch
Router
Tom
Sam
Switch

مهام الموجهات

- تقرأ العناوين المنطقية IP Address التي تحملها حزم البيانات
- توجه الحزم عبر عدة شبكات وتقوم بتبادل معلومات محددة للبرتوكولات بين الشبكات
- تقوم بمشاركة معلومات التوجيه مع الموجهات الأخرى
- تستخدم المعلومات لاختيار المنفذ والمسار المناسب لتوجيه الحزم
- تقوم بمراقبة المسارات على الشبكة وتحديد الأقل ازدحام
- تستخدم الموجهات جدول التوجيه لتحديد عنوان وجهة الحزم التي يستقبلها

يحتوى جدول التوجيه على المعلومات التالية

- جميع عناوين الشبكة
- كيفية الاتصال بالشبكات الأخرى
- المسارات المتوفرة بين موجهات الشبكة
- تكلفة إرسال البيانات عبر هذه المسارات

تحكم الموجه بالحزم

- منع البيانات المعطوبة من المرور عبر الشبكة
- تقليل ازدحام حركة المرور بين الشبكات
- استخدام أكثر كفاءة للوصلات بين الشبكات بالمقارنة مع الجسور
- تقسيم شبكة كبيرة إلى أقسام أصغر حجماً
- تمنع مرور الرسائل الموجه إلي كل المستخدمين وبالتالي تخفف المشاكل الواقعة في الأجهزة الأخرى

جداول التوجيه

- تختلف جداول التوجيه في الموجهات عن جداول الجسور والمقسمات.
- الجسر يحفظ المسار المادي لكل جهاز من خلال عناوين مادية التي يخزنها على جدول التوصيل
- أما الموجهات فتتعامل مع العناوين المنطقية للشبكات والموجهات التي تتصل بها

العلاقة بين الجسور والموجهات

- **هناك صفات مشتركة بين الجسور والموجهات**
  - توجيه الحزم بين الشبكات
  - إرسال بيانات عبر وصلات الشبكات الواسعة
- **هناك نقاط اختلاف بين الجسور والموجهات:**
  - الجسر لا يرى سوي عنوان المرسل وعنوان المستقبل وإذا لم يعرف المستقبل يمرر الحزمة لكافة الأقسام ويسبب إبطاء الشبكة في حالة عدد الأقسام يكون كبير
  - لا تعرف الموجهات أن يقع كل جهاز على الشبكة بالتحديد وبدل من ذلك تعرف عناوين الشبكات المختلفة المكونة للشبكة الواسعة وعناوين الموجهات الأخرى ولا تستخدم Broadcasting
  - لا تتعرف الجسور إلا على مسار وحيد بين الشبكات أما الموجهات فتتعرف على جميع المسارات المتوفرة وتختبر الأفضل بينها
  - تمرير البيانات في الموجهات أبطأ من الجسور

الجسر الموجه BROUTER

- جهاز يجمع بين مميزات الجسور والموجهات
- يستطيع عمل كموجه مع بروتوكول وكجسر مع باقي البروتوكولات عندما لا تكون هناك حاجة لاستخدام الموجه.
- يقوم بالمهام التالية:
  - توجيه بروتوكولات مختارة وقابلة للتوجيه
  - يعمل كجسر للسماح بمرور البروتوكولات غير المتوافقة مع الموجهات
  - يحقق تكلفة أقل وكفاءة أكبر من استخدام جسر وموجه معاً

البوابات GATEWAYS

- جهاز يربط بين نظامين يستخدمان:
  1. بروتوكولات مختلفة
  2. تصميما متبايناً لحزم البيانات
  3. لغات مختلفة
  4. تصاميم مختلفة
- تستطيع البوابات بالقيام بتحويل كامل من بروتوكول إلى بروتوكول أخر وبشكل عام تستعمل البوابات لطرق الربط:
  - ربط LAN-to-Host
  - ربط LAN- to – LAN
  - الاتصال عن بعد
  - ربط الأنظمة مع mainframe

الخلاصة

- تعتبر مكررات الإشارة وسلة غير مكلفة لتوسيع الشبكات المحلية
- تعاني المكررات من عدم القدرة على تصفية البيانات التي تمر من خلالها
- الجسور والمبدلات تتفوق على مكررات الإشارة وتسمح للربط بين شبكات تستخدم تصاميم وبروتوكولات مختلفة
- كما أنها تقسم الشبكة الملية إلي شبكات فرعية
- تقوم الموجهات بتوجيه البيانات بين عدة شبكات وهي نوعان ساكنة وديناميكية وهي لا تتعرف إلا على عنوان الشبكة وليس عنوان الجهاز

الوحدة السادسة

بروتوكولات TCP/IP

بروتوكول TCP/IP

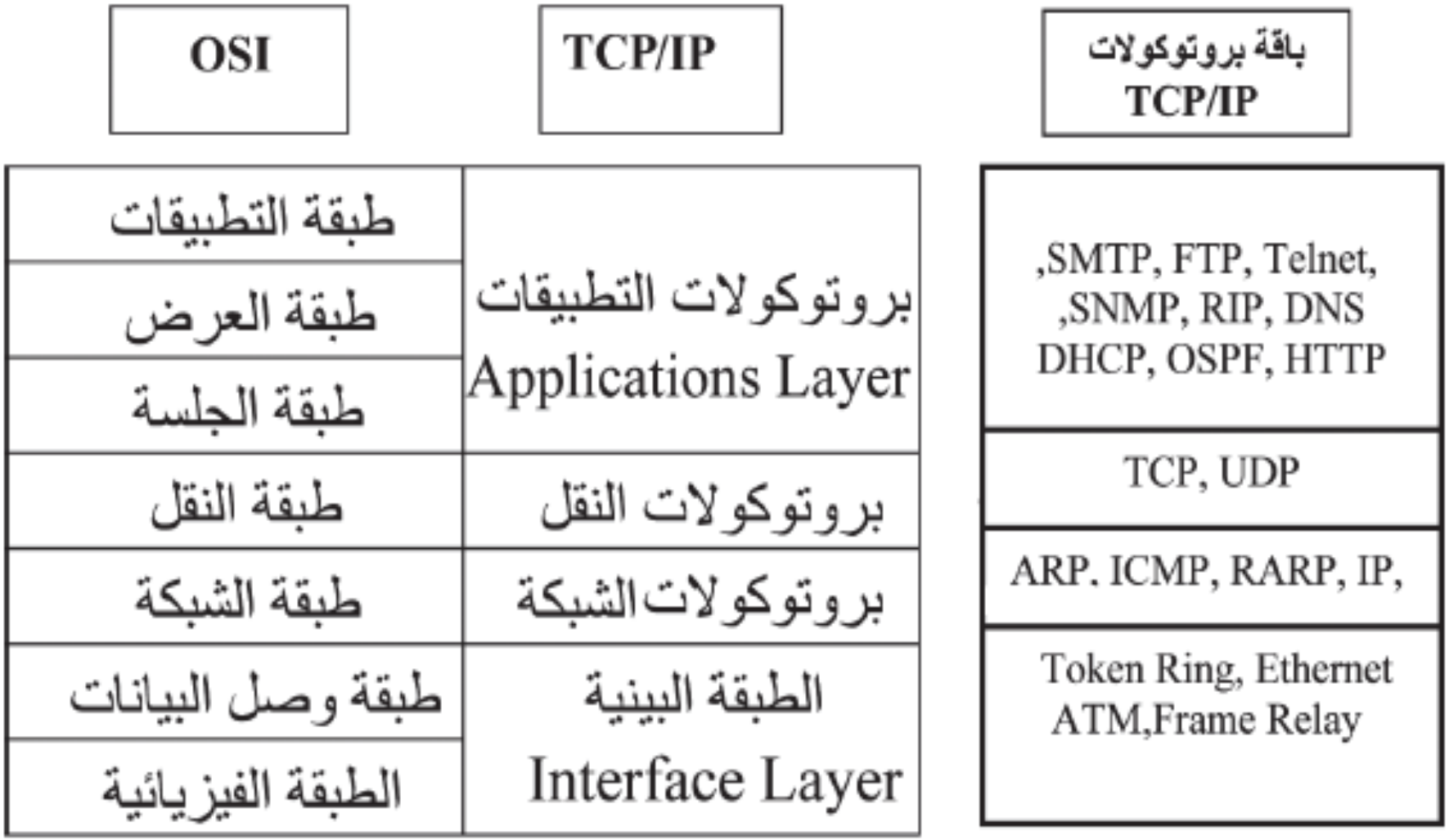
- هو نظام قياسي تعتمد عليه جميع أنواع الحواسيب للاتصال والتعرف على بعضها بمختلف أنواعها وأنظمتها
- الهدف من إنشائه توصيل أنواع مختلفة من الشبكات وأجهزة الكمبيوتر مع بعضها البعض بواسطة عدد كبير من المنافذ port التي يتمكن هذا البروتوكول من فتحها
- **مكونات بروتوكول TCP/IP:**
- TCP, IP, ICMP, UDP, SMTP, FTP, SNMP, Telnet

مميزات بروتوكول TCP/IP

1. يؤمن الاتصال بين عدة أنظمة تشغيل وبنى عتادية مختلفة، فهو متوفر في كافة أنظمة التشغيل.
2. يدعم تقنيات التوجيه.
3. البروتوكول الوحيد المستخدم على شبكة الإنترنت.
4. مرن بشكل كبير ويمكن التحكم بأدائه
5. يدعم بروتوكول SNMP

عيوب بروتوكول TCP/IP

- ليس بسرعة NetBEUIعلى الشبكات الصغيرة
- يحتاج إلى معرفة كبيرة بهذا البروتوكول للتعامل معه وخاصة مفهوم العنونة ومفهوم قناع الشبكة الجزئية Subnet mask



الشكل (1): العلاقة بين بروتوكول TCP/IP وبروتوكول OSI

بروتوكولات طبقة التطبيقات

ويمكن تسميتها طبقة البرامج والعمليات حيث إن البروتوكولات الموجودة في هذه الطبقة تستعمل في عمليات توصيل العقدة إلى العقدة (Node- to- Node) وتتحكم في مواصفات الواجهة الأمامية للمستخدم (User Interface). وسنورد هنا بعضاً من بروتوكولات هذه الطبقة:

بروتوكول نقل الملفات FTP

- **هو البروتوكول الخاص بنقل الملفات بين الأجهزة.**
- وهو ليس بروتوكولا فقط بل هو أيضا برنامج لتعديل الملفات.
- ففي أغلب الأوقات يُستعمل بروتوكول نقل الملفات مع الشبكة الهاتفية.
- بروتوكول نقل الملفات يعطيك الكثير من الحرية في تغيير ترتيب الملفات وتغيير اسم الملفات .
- ويوجد بروتوكول بسيط لنقل الملفات TFTP ويعمل هذا البروتوكول كبروتوكول نقل الملفات
- TFTP مميزاته محدودة حيث إن وظيفته الوحيدة هي نقل الملفات فقط.

نظام ملف الشبكة
NETWORK FILE SYSTEM(NFS)

- هذا النظام يسمح لأنظمة الملفات المختلفة أن تعمل مع بعضها فمثلاً إذا وجد شبكة خادم/زبون
- ونظام الخادم ويندوز NT وأنظمة الزبون هي Unix
- في هذه الحالة يسمح نظام ملف الشبكة لجزء في ذاكرة الخادم بتخزين ملفات Unix وبذلك تستطيع أجهزة الزبون استعمال هذه الملفات
- رغم الاختلاف في (طول اسم الملف، أمن، وطريقة تسمية الملف) إلا انه يمكن الوصول لهذه الملفات بدون الحاجة لتغيرات على الملف.

بروتوكول صندوق البريد
POST OFFICE PROT(POP3)

- هو مقياس لتخزين البريد الإلكتروني في ملف بريد إلى أن يمكنك الوصول إليه وتحميله إلى الحاسوب الشخصي.
- إنه يتيح للمستخدمين تلقي بريد من صندوق وارداتهم باستعمال مستويات مختلفة من الأمان.

بروتوكول نقل البريد البسيط
SIMPLE MAIN TRANSFER PROTOCOL) SMTP

- يُستعمل هذا البروتوكول للسيطرة على إرسال البريد الإلكتروني عبر شبكات الحاسوب.
- وهو لا يزود دعماً لإرسال بيانات أخرى غير النص العادي.

خدمة نطاق الاسم
DOMAIN NAME SERVICE (DNS)

- نظراً لصعوبة حفظ أرقام عنوان IP التي بواسطتها نستطيع الوصول لأي جهاز على الشبكة
- فقد تم استحداث خدمة نطاق الاسم بحيث يتم إيجاد واجهة أمامية للرقم IP
- فلا يحتاج الفرد إلى حفظه،
- ولكنه يستطيع معرفة نطاق اسم الجهاز ومن خلال ذلك يستطيع الوصول إليه.

بروتوكول إرسال النصوص التشعبية HYPER TEXT TRANSFER PROTOCOL (HTTP)

- هو مقياس يدعم تبادل المعلومات في الشبكات.
- وهو يدعم عدة أنواع مختلفة من الملفات، بما في ذلك النصوص والرسوم والأصوات والفيديو.
- إنه يعرف العملية التي يستخدمها مستعرضو صفحات الوب لطلب معلومات لإرسالها إلى ملفات الوب.

بروتوكول تحكم التوصيل TCP

- هو بروتوكول محدد خط الاتصال Connection Oriented
- يقوم بأخذ مجموعة كبيرة من البيانات من برنامج معين ومن ثم تقسيمها إلى أقسام صغيرة يتم ترقيمها وترتيبها
- عندما يتم إرسال هذه الأجزاء المرقمة، فإن TCP في الجهاز المرسل ينتظر رسالة تأكيد وصول من الTCP في الجهاز المُستقبل
- فإذا لم تصل رسالة تأكيد وصول إلىTCP جهاز المرسل فان TCP يقوم بإعادة إرسال الأجزاء التي لم يأتِ تأكيد بوصولها.
- يتميز هذا البروتوكول بالموثوقية في تراسل البيانات.
- وتتلخص الخدمات الرئيسة له بما يلي:

خدمات TCP

1. إنشاء، حفظ، وإنهاء الاتصال بين العمليات.
2. موثوقية تراسل المعلومات، من خلال عملية إشعار المرسل.
3. تسلسل الحزم.
4. آلية ضبط الأخطاء.
5. القدرة على السماح بارتباطات متعددة ذات عمليات مختلفة داخل مرسل أو مستقبل ما من خلال استعمال المنافذ.
6. تراسل البيانات باتجاهين Full- Duplex

منفذ المصدر SOURCE PORT

- رقم منفذ الجهاز الذي يقوم بالإرسال يستعمل لتمرير المعلومات إلى الطبقات العليا.
- تُستعمل أرقام المنافذ لتعقب أثر المحادثات المختلفة التي تعبر الشبكة في الوقت نفسه.
- لقد وافق مطورو البرامج على استعمال أرقام المنافذ المعروفة جيداً والمعرَّفة في الوثيقة RFC 1700
- مثلاً، أي محادثة مربوطة لبرنامج FTP تستعمل رقم المنفذ القياسي 21
- المحادثات التي لا تستلزم برنامجاً مع رقم منفذ معروف جيداً تُعطى أرقام منافذ منتقاة عشوائياً من ضمن نطاق مع من الأرقام. وتُستعمل أرقام المنافذ تلك كالعناوين، المصدر، والوجهة في قسم TCP

أرقام المنافذ لها النطاقات التالية المعطاة لها:

- الأرقام تحت 255 هي للبرامج العمومية.
- الأرقام 1023-255 مخصصة للشركات للبرامج الصالحة للعرض في السوق.
- الأرقام فوق 1023 تعين ديناميكياً.
- تستعمل الأنظمة أرقام المنافذ لانتقاء البرنامج الملائم. أرقام منافذ المصدر البادئة، وهي عادة بعض الأرقام أكبر من 1023، يعيّنها المضيف المصدر ديناميكياً.

بروتوكول المستخدم غير الموجه
USER DATAGRAM PROTOCOL (UDP)

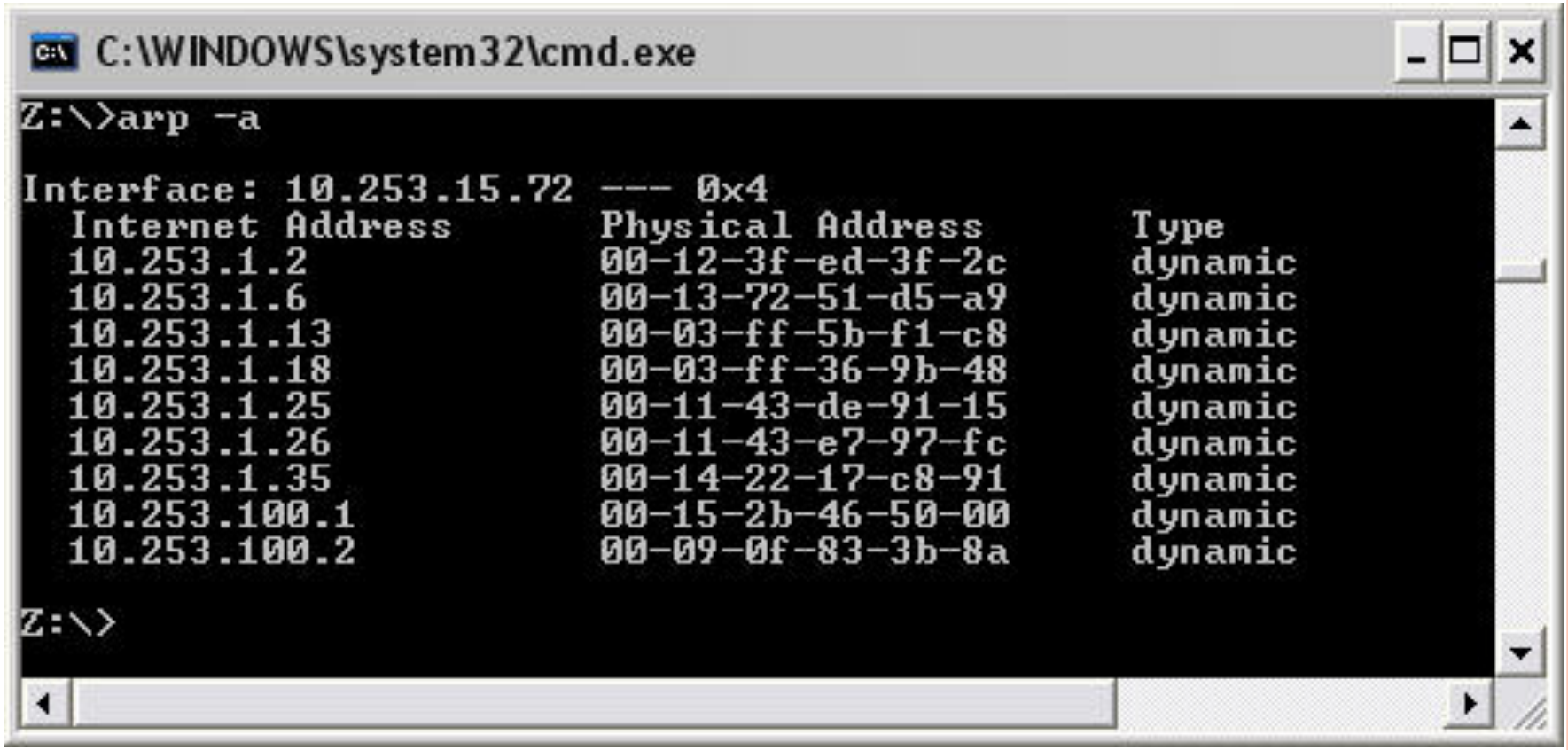
- بروتوكول غير محدد لخط الاتصالConnectionless وغير موثوق به.
- مسؤول عن إرسال الرسائل، لا يتم في هذه الطبقة تزويد برنامج للتحقق من تسليم الأقسام.
- لا يزود إشعارات لتأكيد وصول الحزم مما يقلل من حركة المرور على الشبكة، وهذا يؤدي إلى زيادة في سرعة التراسل.
- لا يستعمل أطراً أو إشعارات
- إنه مصمم للبرامج التي لا تحتاج إلى وضع تسلسلات أقسام سوية.
- يستخدم في البروتوكولات : TFTP، SNMP, NFS, DNS:

مميزات وخواص UDP

1. خط الاتصال غير محدد. Connection less
2. عدم الموثوقية في نقل البيانات.
3. عدم إشعار المرسل باستلام البيانات.
4. لا يقوم بتسلسل الحزم القادمة.
5. ربما قد يخسر حزماً أو يضاعفها دون إشعار بوجود خطأ
6. أسرع من TCP وأقل تكلفة في المراقبة Less Overhead

بروتوكول إقرار العنوان
ADDRESS RESOLUTION PROTOCOL (ARP)

يُستعمل ARP لترجمة أو لمطابقة عنوان IP معروف إلى عنوان طبقة فرعية MAC من أجل السماح بحصول اتصال على وسائط متعددة الوصول كالإيثرنت. أي أن هذا البروتوكول يقوم بإيجاد العنوان المادي (MAC Address) لمستضيف من خلال عنوان الـ IP التابع له. فعندما يكون لدى الـIP بعض الرزم للإرسال، فإن على الـIP أن يخبر بروتوكولات دخول الشبكة بعنوان MAC التابع للجهاز المستقبل على الشبكة المحلية. ولكن إن لم يجد الـIP عنوان MAC الخاص بالجهاز المستقبل، فإنه يستعمل ARP لمعرفة هذا العنوان.


C:\WINDOWS\system32\cmd.exe
Z:\>arp -a
Interface: 10.253.15.72 --- 0x4
Internet Address Physical Address Type
10.253.1.2 00-12-3f-ed-3f-2c dynamic
10.253.1.6 00-13-72-51-d5-a9 dynamic
10.253.1.13 00-03-ff-5b-f1-c8 dynamic
10.253.1.18 00-03-ff-36-9b-48 dynamic
10.253.1.25 00-11-43-de-91-15 dynamic
10.253.1.26 00-11-43-e7-97-fc dynamic
10.253.1.35 00-14-22-17-c8-91 dynamic
10.253.100.1 00-15-2b-46-50-00 dynamic
10.253.100.2 00-09-0f-83-3b-8a dynamic
Z:\>

بروتوكول إقرار العنوان المعاكس
REVERSE ADDRESS RESOLUTION PROTOCOL (RARP)

يستخدم لإيجاد عنوانIP عندما يكون العنوان المادي MAC معروفاً. فمثلاً عندما يكون جهاز الـ IP جهازاً بدون ديسك، فإنه لا توجد أية طريقة لمعرفة عنوان الـ IP الخاص به ولكنه يعرف عنوان MAC الخاص به. فعلى ذلك، فإن هذا الجهاز يستخدم بروتوكول إقرار العنوان المعاكس لإرسال رزمة يستفسر من خلالها عن عنوان الـIP التابع له من خلال معرفة عنوان MAC التابع له. ومن ثم يقوم جهاز معين يسمى بخادم RARP بالإجابة على السؤال.

بروتوكول الإنترنت
INTERNET PROTOCOL IP

الهدف الرئيس لـ بروتوكول IP هو ربط الشبكات الفرعية بشبكة الإنترنت للتمكن من تراسل البيانات. وبشكل عام يقوم هذا البروتوكول بأربع مهام رئيسة هي:

1. إعداد وحدة البيانات الأساسية للإرسال Basic Unit for Data Transfer.
2. التوجيه Routing.
3. تجزئة البيانات Fragmentation of Datagram.
4. العنونة Addressing.

إليك، عزيزي الدارس، شرحاً مفصلاً عن كل من المهام الأربع التي يقوم بها بروتوكول الإنترنت IP.

أولاً: إعداد وحدة البيانات الأساسية للإرسال

- يعتمد على تكنولوجيا التراسل غير المحدد لخط الإرسال Connectionless لتوصيل البيانات إلى الطبقات العليا.
- يقوم البروتوكول بإرسال حزم البيانات للمستقبل دون وحدة البيانات من طبقة IP انتظار الإجابة بوصول تلك الحزم.
- عندما يتسلم بروتوكول IP وحدة البيانات من طبقة النقل Transport Layer يقوم بإضافة معلومات تحكم IP Header خاصة به.
- يطلق على وحدة البيانات لهذا البروتوكول Datagram أو حزمة Packet

ثانياً: التوجيه ROUTING

التوجيه هو الوظيفة الأساسية لـ IP . تسلم حزمة البيانات إلى بروتوكول IP بواسطة بطاقة الشبكة حيث تحتوي كل حزمة على عنوان IP للمرسل والمستقبل فيقوم البروتوكول بفحص عنوان المستقبل لكل حزمة ويقارن هذا العنوان بالعنوان الموجود في جدول التوجيه لديه وبناء على تلك المقارنة يقرر القيام بإحدى العمليات التالية:

1. تمرير الحزمة إلى الطبقة العليا (طبقة النقل Transport layer) للمضيف Host
2. تمرير الحزمة إلى شبكة أخرى.
3. إهمال الحزمة.

ثالثاً: تجزئة البيانات أو تجميعها
FRAGMENTATION OR REASSEMBLY OF DATAGRAM

- بالإضافة إلى عملية التوجيه يوفر بروتوكول الإنترنت التبليغ عن الاخطاء وكذلك يقوم بعمليتي التجزئة والتجميع للبيانات في حالة اختلاف حجم وحدات البيانات الواردة.
- ففي حالة استقبال الموجه حزمة بيانات كبيرة الحجم لتمريرها عبر الشبكة.
- يقوم بروتوكول الإنترنت بتجزئتها إلى حزم أصغر حجماً قابلة للإرسال.
- وعندما تصل هذه الحزم إلى المستقبل يقوم بروتوكول الإنترنت بإعادة تجميعها للحجم الأصلي.
- وكذلك تستخدم عمليتي التجزئة والتجميع عندما يكون التراسل بين شبكات مختلطة التوبولوجيا مثل إيثرنت وتوكن رنج

رابعاً: العنونة ADDRESSING

تستخدم العنونة لإعطاء كل حاسوب على الشبكه رقماً خاصاً به ويسمى عنوان إنترنت IP Address وهو عنوان متفرد ليس له شبيه في النطاق الشبكي.

يعتمد تحديد عناوين IP على طبيعة ربط الشبكات وهي إحدى الطريقتين التاليتين:

إذا كان المضيف متصلاً بالإنترنت فإن الجزء المخصص لعنوان الشبكة من عنوان IP يحدد بواسطة إدارة عامة مركزية تعرف باسم " مركز معلومات الشبكات" Network Information Center. في هذه الحالة فإنه يمكن الوصول إلى الجهاز المضيف مباشرة من قبل مستخدمي الإنترنت.

إذا لم تكن الشبكة متصلة بالإنترنت فإن عناوين IP تحدد محلياً من قبل مدير الشبكة المحلية.

عناوين بروتوكول الإنترنت
IP ADDRESSES

عناوين بروتوكول الإنترنت
IP ADDRESSES

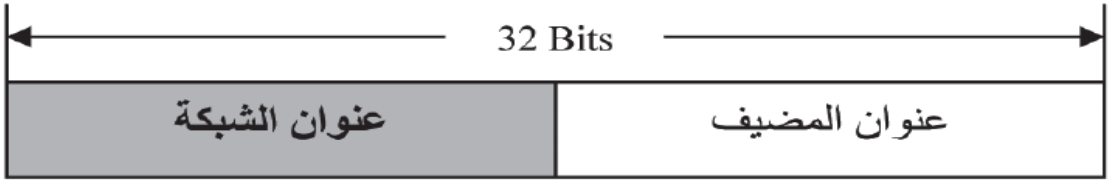
يتألف عنوان IP من 32 بتاً مقسمة إلى أربع مجموعات وكل مجموعة تحتوي على 8 بتات ولسهولة التعامل معها تمثل هذه البتات بأرقام عشرية يفصل بين كل مجموعة وأخرى نقطة (.) مثل 131.107.2.200 وبما أن كل مجموعة مكونة من 8 بتات فإن قيم كل مجموعة تقع بين الأرقام من صفر إلى 255. يوضح الشكل (5) التمثيل الثنائي للرقم 131.107.2.200.

10000011 • 01101011 • 00000010 • 11001000
131 • 107 • 2 • 200

الشكل (5): التمثيل الثنائي للرقم 131.107.2.200

عناوين بروتوكول الإنترنت
IP ADDRESSES

ونظراً لكون الشبكات الموسعة والمتداخلة (Interconnected) تتكون من مجموعات من الشبكات المحلية المتصلة معاً فقد تم تقسيم رقم IP إلى قسمين كما يوضح الشكل (6): يمثل القسم الأول عنوان الشبكة (Network Address) كما يمثل القسم الثاني عنوان المضيف (Host Address).



الشكل (6): قسما عنوان IP

عناوين بروتوكول الإنترنت
IP ADDRESSES

يميز عنوان شبكة الأجهزة الواقعة على نفس المقطع من شبكه الـ (Seg-ment) فجميع الأجهزة الواقعة على نفس المقطع من الشبكة لا بد أن يكون لها نفس العنوان ويجب أن يكون هذا العنوان فريداً على مستوى العالم إذا كانت هذه الشبكة متصلة مع شبكة الإنترنت. أما عنوان المضيف فهو عنوان لأحد الأجهزة المنتمية لنفس المقطع من الشبكة والذي يمكن أن يكون: حاسوب (PC)، موجه (Router)، خادم (Server) أو أي جهاز ثاني يستخدم بروتوكول TCP/IP وضمن نفس المقطع من الشبكة. يجب أن يكون العنوان هنا فريداً من نوعه لكل جهاز داخل نفس المقطع.

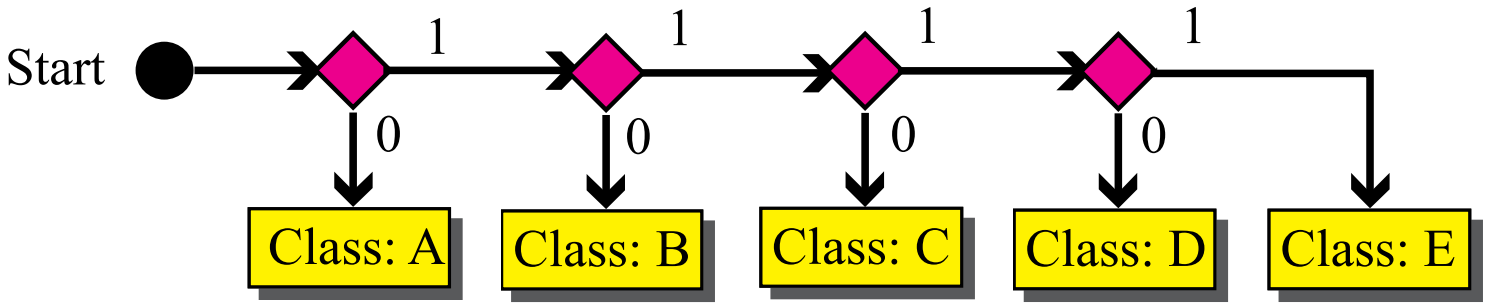
-: (IP ADDRESS) ملاحظات

❶- لا يمكن أن يبدأ بالأرقام التالية (0 – 127 – 255) .

❷- يتم تحديد الفئة بناءاً على الخانة الأولى .

❸- لا يمكن أن يكون جميع الخانات IP أصفاراً (0.0.0.0) أو (255.255.255.255) حيث أن هذه الأرقام محجوزة من النظام .

❹- رقم الشبكة لابد أن يتكرر على جميع الأجهزة في الشبكة الواحدة ورقم الجهاز يجب أن يختلف في جميع الأجهزة في الشبكة الواحدة .



هناك بعض العناوين التي لا يستطيع مدير الشبكة منحها للأجهزة أبدا رغم أنها قد تنتمي الى مدى مسموح به كما يلي:

- 1- العنوان 0.0.0.0 و يستخدم من قبل موجهات routers التابعة لشركة Cisco للإشارة الى الوجهة الافتراضية default route عند توجيه حزم البيانات.

2- العنوان 255.255.255.255 و يستخدم لبث أو إرسال البيانات الى جميع الأجهزة nodes على الشبكة الحالية.

3- لا يمكن أن يكون الجزء من عنوان IP الخاص بالجهاز كله 255 أو 0 أي أنك لا تستطيع منح جهاز ما العنوان التالي على سبيل المثال : 128.2.255.255 أو 128.2.0.0 و مثال آخر: 192.168.1.255 أو 192.168.1.0، حيث يشير كل من 128.2.0.0 و 192.168.1.0 الى عنوان الشبكة بينما يشير كل من 192.168.1.255و 128.2.255.255 الى العنوان المستخدم في البث لجميع أجهزة الشبكة.

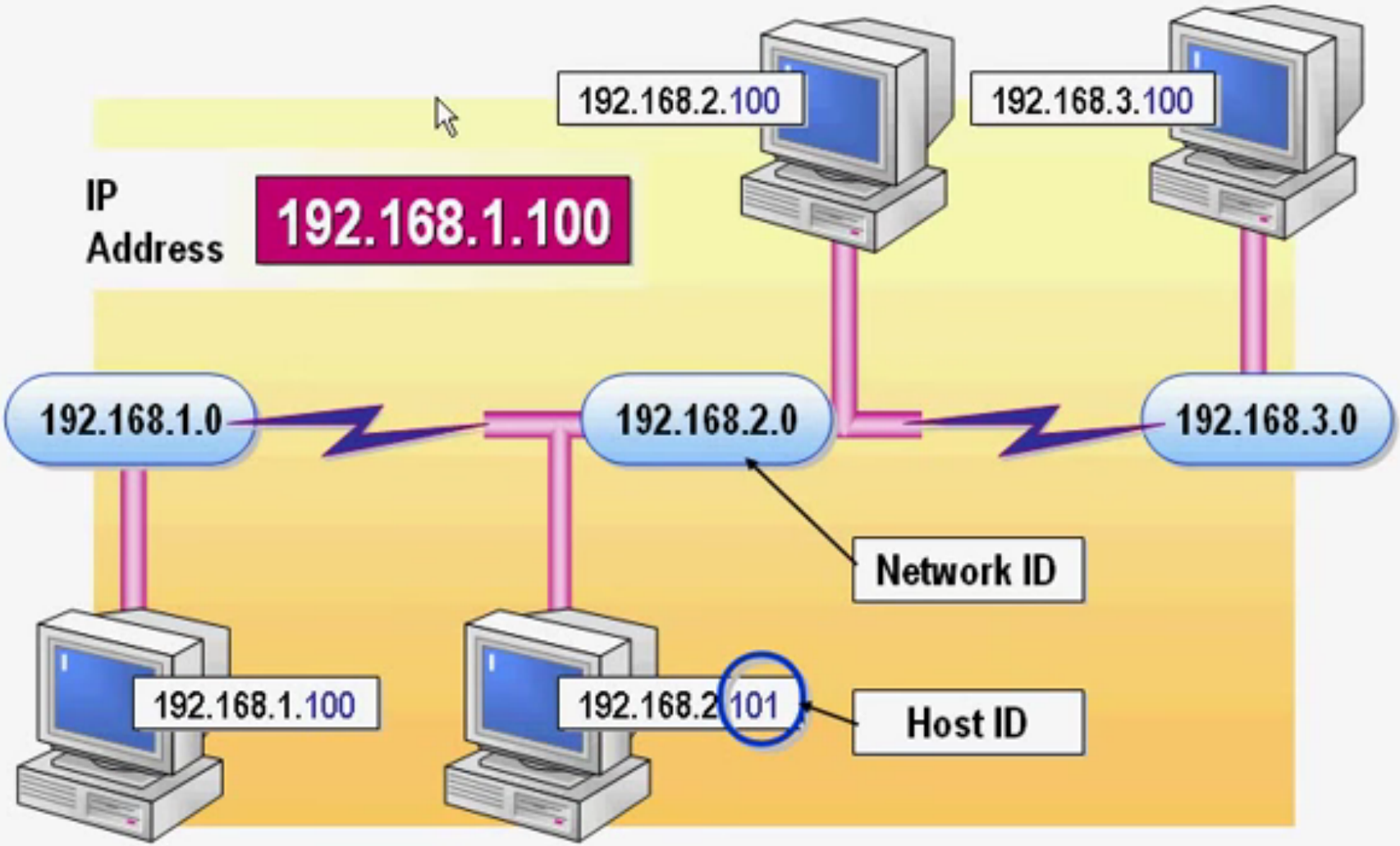
4- لا يمكن أن يكون الجزء من عنوان IP الخاص بالشبكة كله 0 أو 255 أي أنك لا تستطيع منح جهاز ما العنوان التالي: 0.1.5.3 .

5- العنوان 127.0.0.1 لا يمكن منحه لأي جهاز و هو يستخدم تلقائيا من قبل الجهاز لغرض اختبار اتصاله بأن يقول بإرسال حزمة من البيانات الى نفسه.

-: (IP ADDRESS) ملاحظات -

- عنوان الشبكة Network address و هو يستخدم لإرسال البيانات الى شبكة محددة عن بعد و من الأمثلة عليه : 10.0.0.0 ، 172.16.0.0 و 192.168.10.0.
- عنوان النشر Broadcast address و هو العنوان الذي يستخدم من قبل الأجهزة و التطبيقات لإرسال المعلومات الى جميع الأجهزة على الشبكة
  - و من الأمثلة عليه : 172.16.255.255 و الذي يعني أرسل المعلومات الى جميع الأجهزة و الشبكات الفرعية في الشبكة ذات العنوان 172.16.0.0 ،
  - و مثال آخر : 10.255.255.255 و الذي يقوم بإرسال البيانات الى جميع الأجهزة و الشبكات الفرعية في الشبكة 10.0.0.0.
- عليك أن تعرف أن جميع الأجهزة المتصلة بنفس الشبكة يشتركون في أن عناوين IP لكل منهم تحتوي على عنوان نفس الشبكة مثلا لنفترض وجود جهازين في الشبكة أحدهما له العنوان 192.168.1.2 و الآخر لديه العنوان 192.168.1.3 نلاحظ أنهما يشتركان في نفس عنوان الشبكة و هو 192.168.1 ، و لكن يكون لكل منهما عنوانه الخاص و يطلق عليه node address أو host address وهو في مثالنا للجهاز الأول 2 و للجهاز الثاني 3.

IP Addresses



أمثلة على عنوان IP

- حول العنوان IP من النظام الثنائي للنظام العشري

- a. 10000001 00001011 00001011 11101111
- b. 11000001 10000011 00011011 11111111
- c. 11100111 11011011 10001011 01101111
- d. 11111001 10011011 11111011 00001111

الحل

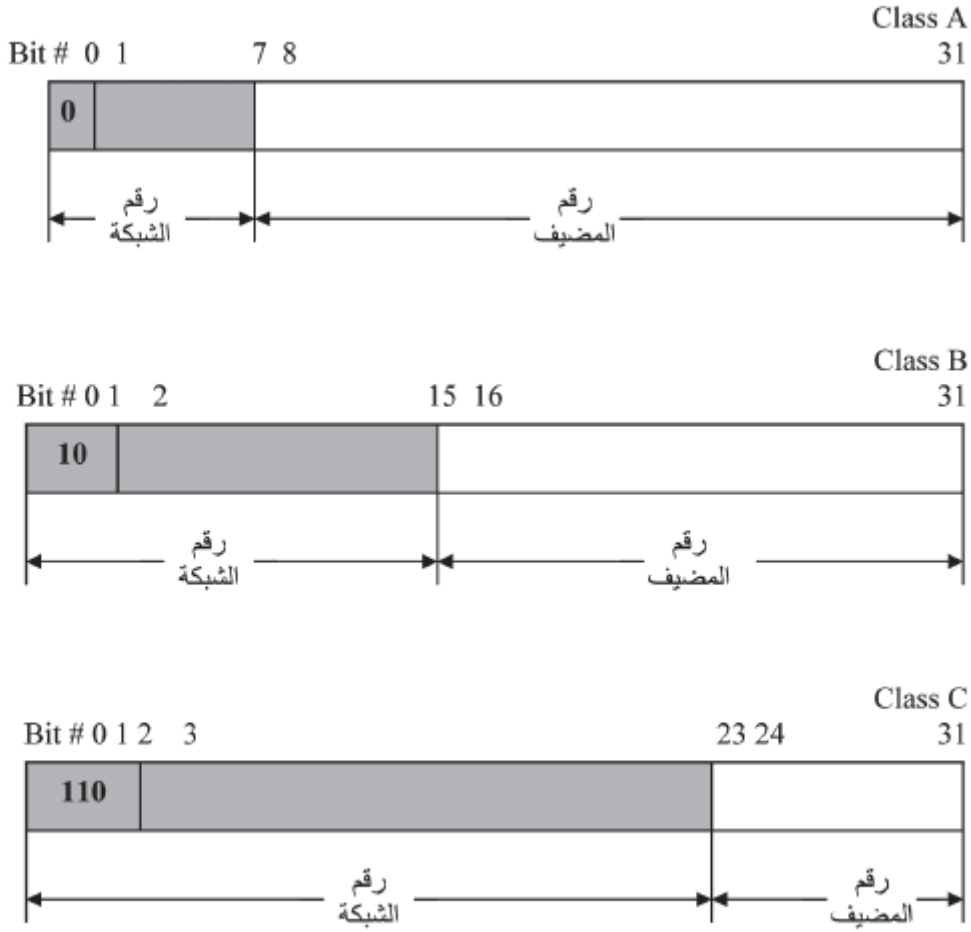
- a. 129.11.11.239
- b. 193.131.27.255
- c. 231.219.139.111
- d. 249.155.251.15

ما هي الاخطاء في العناوين IP التالية:

- a. 111.56.045.78
- b. 221.34.7.8.20
- c. 75.45.301.14
- d. 11100010.23.14.67

- *الحل*
- ممنوع استخدام الصفر في عنوان الجهاز.(045)
- تم استخدام أكثر من اربع بايت في العنوان وهذا غير مسموح
- تم استخدام رقم 301 وهو أعلى من 255 وهذا غير مسموح
- تم استعمال نظام ثنائي في المكان العشري وهذا غير مسموح

فئات أرقام IP



الشكل (7): أصناف عناوين IP

فئات أرقام IP

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Address Class	First Octet Range	Number of Possible Networks	Number of Hosts per Network
Class A	0 to 127	128 (2 are reserved)	16,777,214
Class B	128 to 191	16,348	65,534
Class C	192 to 223	2,097,152	254

CLASS الفئة	RANGE المدى	HOSTورقم الجهاز NETWORKرقم الشبكة	SUBNET MASK قناع الشبكة
A	1 → 126	NETWORK.HOST.HOST.HOST	255.0.0.0
B	128 → 191	NETWORK. NETWORK.HOST.HOST	255.255.0.0
C	192 → 223	NETWORK. NETWORK.HOST.HOST	255.255.255.0
D	224 → 239	لم تستخدم حتى الآن ووضعت للإستخدام المستقبلي وذكرت هنا للعلم فقط .	
E	240 → 254		

مثال

لأي صنف ينتمي كل من العناوين التالية:

a. 227.12.14.87

b. 193.14.56.22

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first byte is 227 (between 224 and 239); the class is D.

b. The first byte is 193 (between 192 and 223); the class is C.

c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.

هناك بعض الملاحظات التي يجب أن نأخذها بعين الاعتبار وهي:

1. عدد الشبكات الفرعية = $2^{\text{(عدد بتات حقول الشبكة - عدد مجموعات حقول الشبكة)}}$

   عدد المضيفين = $2^{\text{(عدد بتات حقول المضيف)}} - 2$

2. الصنف A يأخذ من الرقم 1 إلى 126 حيث تم استثناء الرقم 127 وهذا الرقم 127.0.0.0 محجوز لما يسمى LOOPBACK على بطاقة الشبكة وذلك لفحص أية بطاقة عن طريق عمل PING. كما تم استثناء الرقم 0.0.0.0 كونه محجوزاً لما يسمى Default Route.

3. نلاحظ في البند الأول أنه تم طرح عنوانين من عدد المضيفين وذلك لأنه إذا كان عنوان المضيف (0) فإنه هو عنوان الشبكة الفرعية, وعندما يكون 255 فإنه يستخدم كعنوان للبث Broadcasting.

4. هناك ثلاثة عناوين محجوزة للشبكات الخاصة وهي: 10.0.0.0/8 والثانية 172.16.0.0/12 والثالثة 192.168.0.0/16 هذه العناوين يمكن أن تستخدم لإنشاء شبكة محلية.

5. لا يمكن استخدام نفس رقم ال IP مرتين في نفس الشبكة لأن ذلك يؤدي إلى تعارض وعدم عمل الجهاز بشكل سليم.

العناوين المتاحة CLASS A

- أما العناوين المتاحة لجزء الجهاز node من عنوان IP في Class A فهي تتكون من 3 بايتات أو 24 بت
- مما يعني أننا نستطيع الحصول على 2 ^ 24 عنوان مختلف
- أي أننا نستطيع في شبكة واحدة من النوع Class A أن نشبك عدد 16,777,216 جهاز و نعطي كل جهاز عنوان مختلف
- ولكننا ذكرنا أنه لا يمكن لعنوان الجهاز أن يكون كله 0 أو 255 مما يعني أن العدد الحقيقي الأجهزة التي من الممكن شبكها هو 2^24 – 2 = 16.777,214.

سؤال

- لنفترض أن لدينا شبكة تابعة للمدى Class A و عنوانها 10 ، ما هي العناوين التي يمكن استخدامها للأجهزة؟
- للإجابة على هذا السؤال نكتب عنوان الشبكة network address و عنوان البث broadcast address كما يلي:

- 10.0.0.0 (Network address).
- 10.255.255.255 (Broadcast address).
- و تكون عناوين IP التي يمكن منحها للأجهزة هي كل العناوين بدءا من 10.0.0.1 و انتهاء ب 10.255.255.254.

العناوين المتاحة CLASS B

في المدى Class B يتم تعيين البايت الأول و الثاني لعنوان الشبكة بينما يتوفر البايتان الباقيان لعناوين الأجهزة على الشكل التالي:

Network.Network.node.node ، على سبيل المثال فإن في عنوان IP التالي: 172.16.30.56 يعتبر 172.16 هو عنوان الشبكة بينما يعتبر 30.56 هو عنوان الجهاز.

العدد الأقصى لعناوين الشبكات التي يمكن الحصول عليه في المدى B هو 2^14=16,384 ، لأننا ذكرنا أنه يخصص بايتان لعنوان الشبكة أي 16 بت و لكننا ذكرنا أن المصممين نصوا على حجز البت الأول لتكون قيمته 1 و حجز البت الثاني لتكون قيمته 0 مما يترك لنا 14 بت لاستخدامها بدءا من 128.0 و انتهاء ب 191.255.

أما العناوين المتاحة لجزء الجهاز node من عنوان IP في Class B فهي تتكون من بايتان أو 16 بت و بالتالي فإن العدد الأقصى للعناوين التي يمكن استخدامها للأجهزة هو 2^16 – 2 = 65,534 حيث استثنينا عنوانين (الكل 0 و الكل 255).

سؤال

- نفترض أن لدينا شبكة تابعة للمدى Class B و عنوانها 172.16 ، ما هي العناوين التي يمكن استخدامها للأجهزة؟
- للإجابة على هذا السؤال نكتب عنوان الشبكة network address و عنوان البث broadcast address كما يلي:

172.16.0.0 (Network address).
172.16.255.255 (Broadcast address).

- و تكون عناوين IPالتي يمكن منحها للأجهزة هي كل العناوين بدءا من 172.16.0.1 و انتهاء ب 172.16.255.254.

العناوين المتاحة CLASS C

في المدى Class C يتم تعيين البايتات الثلاثة الأولى لعنوان الشبكة بينما يتوفر البايت الأخير لعناوين الأجهزة على الشكل التالي:

Network.Network.Network.node ، على سبيل المثال فإن في عنوان IP التالي: 192.168.100.102 ، يعتبر 192.168.100 هو عنوان الشبكة ، بينما يعتبر 102 هو عنوان الجهاز.

العدد الأقصى لعناوين الشبكات التي يمكن الحصول عليه في المدى C هو 2,097,152=21^2 ، لأننا ذكرنا أنه يخصص 3 بايتات لعنوان الشبكة أي 24 بت و لكننا ذكرنا أن المصممين نصوا على حجز البتات الثلاثة الأولى لتكون 110 مما يترك لنا 21 بت لاستخدامها بدءا من 192.0.0 و انتهاء ب 223.255.255.

أما العناوين المتاحة لجزء الجهاز node من عنوان IP في Class C فهي تتكون من بايت واحد أو 8 بت و بالتالي فإن العدد الأقصى للعناوين التي يمكن استخدامها للأجهزة هو 2^8 – 2 = 254 حيث استثنينا عنوانين (الكل 0 و الكل 255).

سؤال

- لنفترض أن لدينا شبكة تابعة للمدى Class C و عنوانها 192.168.100 ، ما هي العناوين التي يمكن استخدامها للأجهزة؟

للإجابة على هذا السؤال نكتب عنوان الشبكة network address و عنوان البث broadcast address كما يلي:

192.168.100.0(Network address).
192.168.100.255 (Broadcast address).

و تكون عناوين IP التي يمكن منحها للأجهزة هي كل العناوين بدءا من 192.168.100.1 و انتهاء ب 192.168.100.254.

تقسيم الشبكات SUBNITTING

- سنتعلم سويا كيفية تقسيم شبكة كبيرة الى شبكات أصغر ، و لكن قبل ذلك لنتعرف على الفوائد التي سنجنيها من عملية التقسيم:

1- التقليل من حركة المرور و الازدحام على الشبكة ، حيث كلما قل عدد الأجهزة على الشبكة قل الازدحام فيها و يمكن تحقيق ذلك بتقسيم الشبكة الكبيرة الى شبكة أصغر تحتوي على عدد أقل من الأجهزة.

2- تحسين أداء الشبكة.

3- تسهيل إدارة الشبكة و حل مشاكلها.

- فكرة التقسيم تتلخص في حجز بعض البتات من جزء عنوان الجهاز في عنوان IPلتخصيصها كعنوان للشبكة الفرعية مما يعني تقليل عدد العناوين المتاحة للاستخدام من قبل الأجهزة.
- بشكل عام يجب على مدير الشبكة قبل التفكير في تقسيمها أن يحدد بعض الأمور كما يلي:

1- عدد الشبكات الفرعية التي يريد الحصول عليها.

2- عدد الأجهزة التي يريد من كل شبكة فرعية أن تحتويها.

SUBNET MASKS أقنعة الشبكة الفرعية

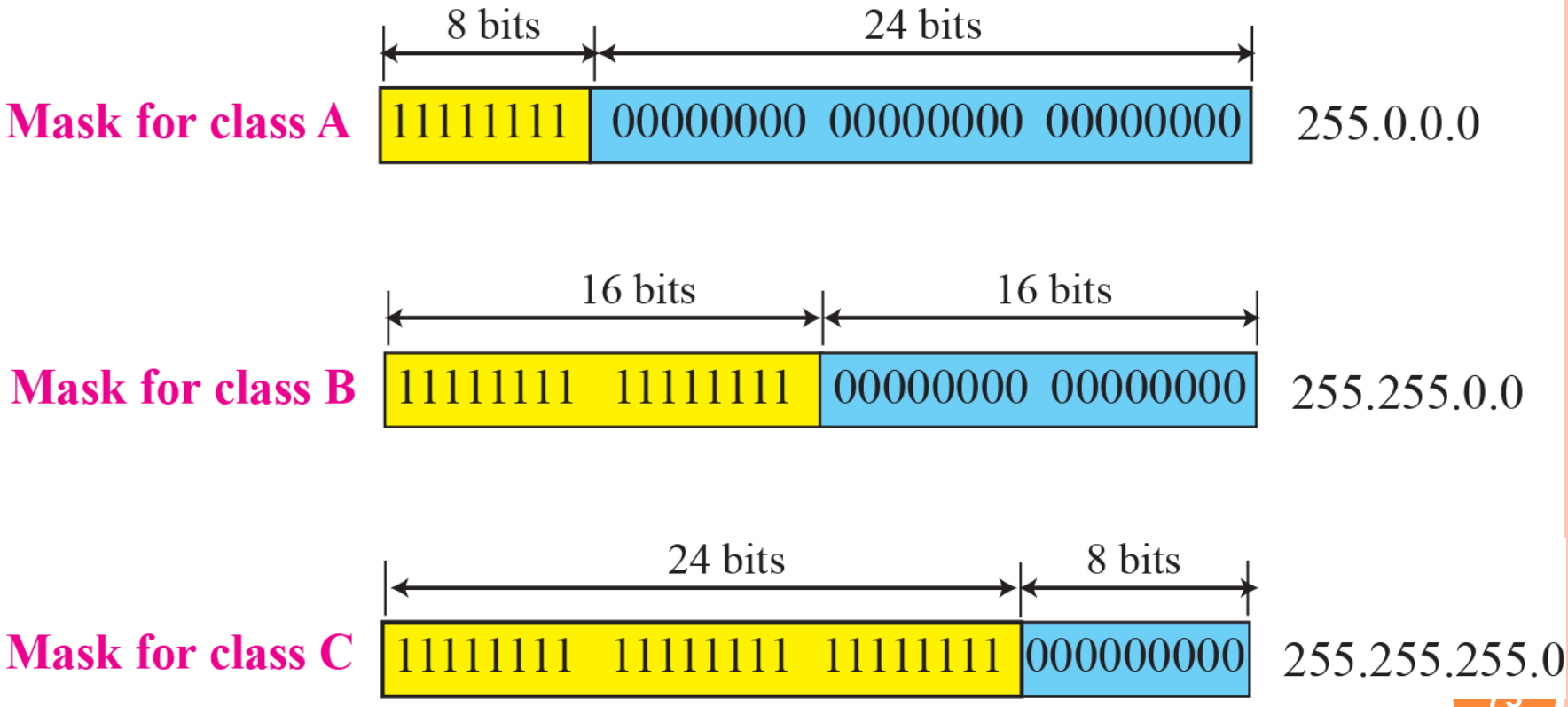
- قناع الشبكة الفرعية هو قيمة من 32 بت تسمح لمتلقي عناوين IPأن يحدد الشبكة الفرعية التي ينتمي إليها الجهاز المرسل وفقا لعنوانه.
يتكون القناع من القيم 1 و 0 حيث تشير قيم 1 في القناع الى الجزء الذي يمثل عنوان الشبكة الأم أو عنوان الشبكة الفرعية.

لا تحتاج كل الشبكات الى تقسيم مما يعني أنها تستخدم قناع الشبكة الفرعية الافتراضي و الذي يعني أنه لا يوجد شبكات فرعية في هذه الشبكة.

فيما يلي جدول بأقنعة الشبكات الفرعية الافتراضية لكل مدى و الذي يستخدم في حال الرغبة في عدم تقسيم الشبكة:

Class	Format	Default Subnet Mask
A	*network.node.node.node*	255.0.0.0
B	*network.network.node.node*	255.255.0.0
C	*network.network.network.node*	255.255.255.0

SUBNET CLASS قناع الشبكات الفرعية



الوحدة السابعة
أمن الشبكات وآليات التشفير

مفهوم التشفير

- **التشفير** : (**Encryption**) هي عملية تحويل النص أو البيانات إلى شكل غير مفهوم بغرض إخفاء هذه البيانات أو هو عملية تحويل من نص صريح (Plain Text) إلى نص مشفر غير صريح(Cipher text)

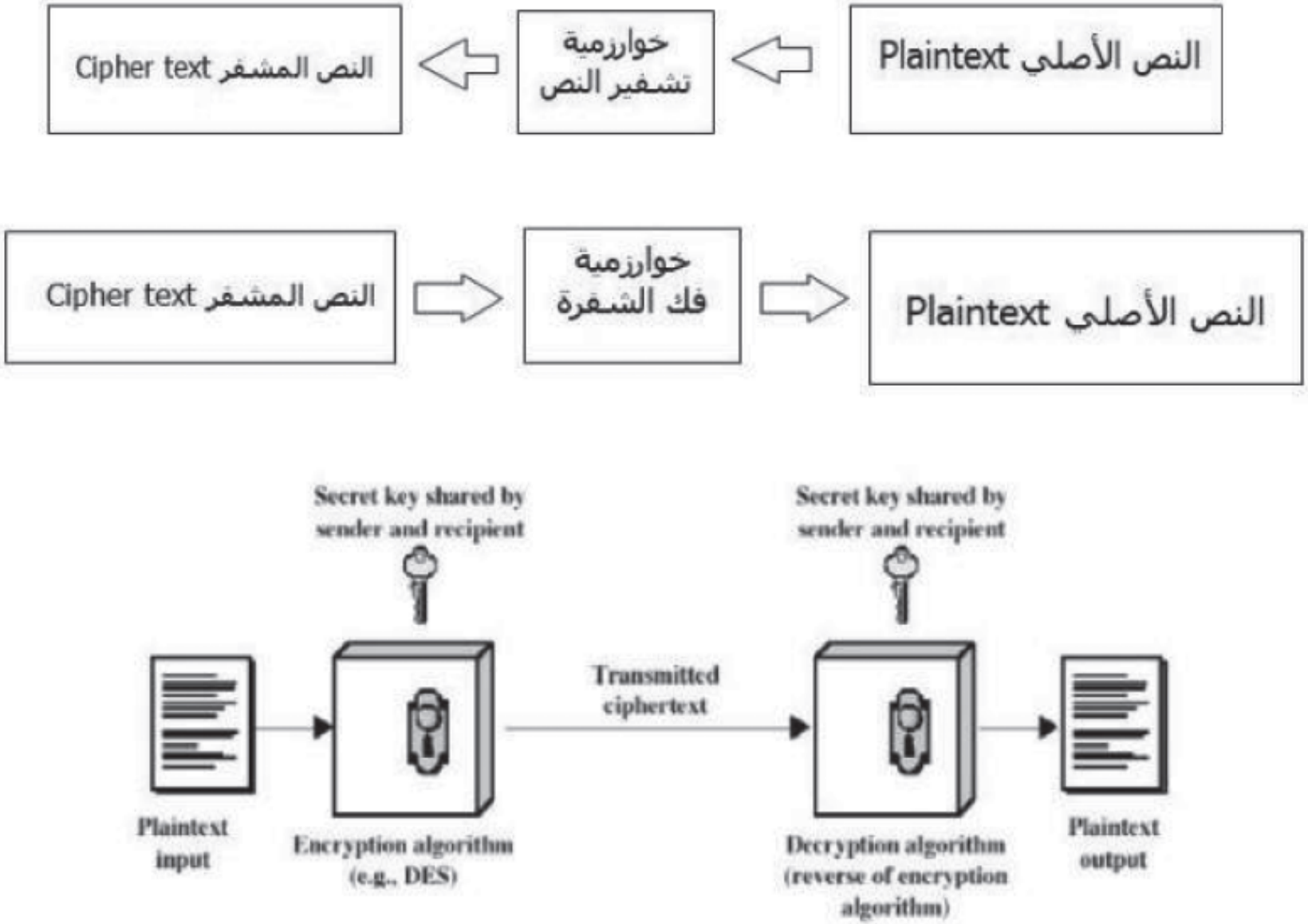
- مصطلح التشفير (Cryptography)هو عملية يتم فيها إخفاء المعلومات عن طريق مفتاح سري وخوارزمية.

حيث ان الشخص الذي يعلم المفتاح ويعلم خوارزمية التشفير يمكنه فك الشفرة (أي استعادة المعلومات الأصلية) ، يمكن ايضاً ان يقوم شخص لا يعرف خوارزمية التشفير ومفتاح التشفير بفك الشفرة ولكن تسمى العملية هنا عملية **غير مخولة**

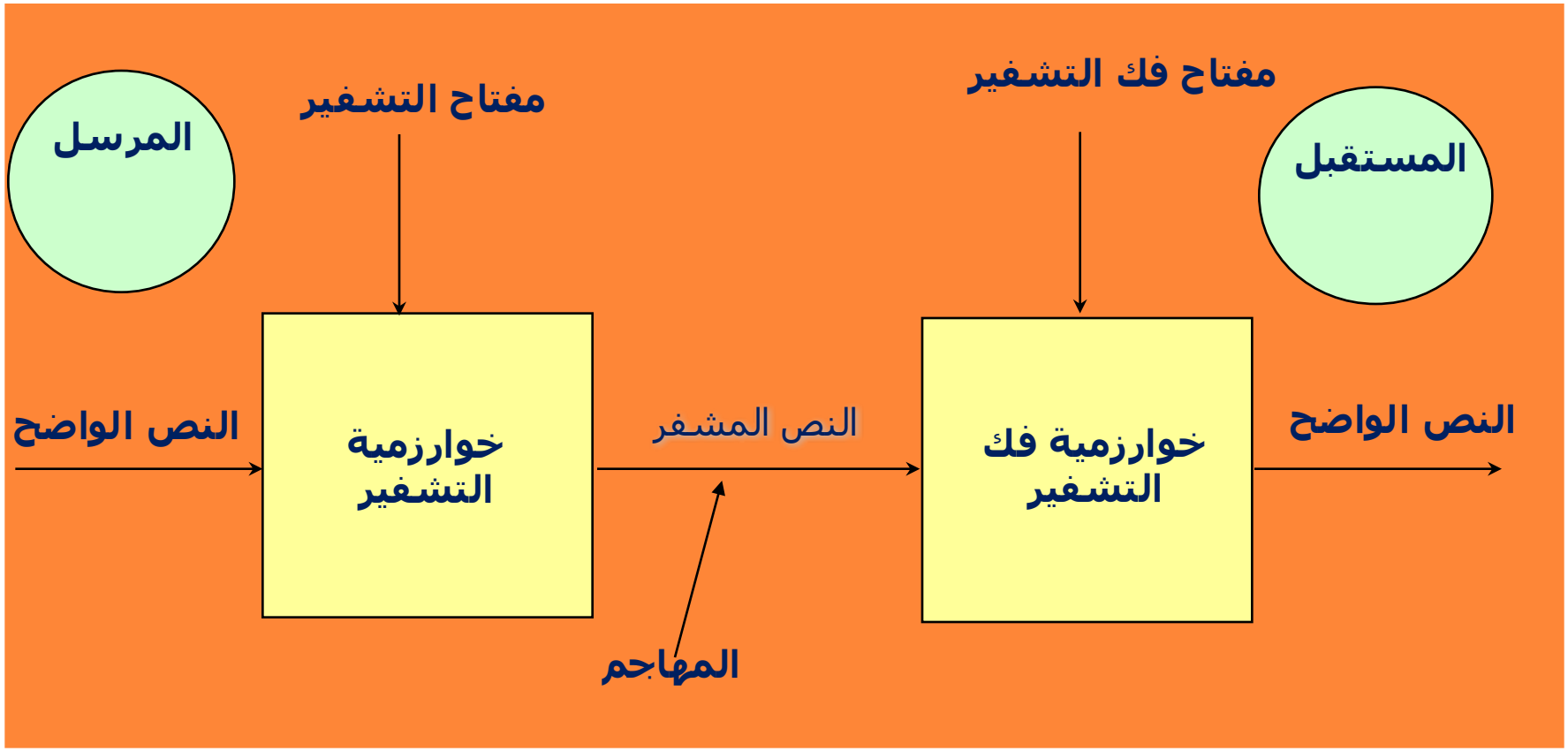
مصطلحات أساسية للتشفير

- **Plain text** النص الأصلي قبل عملية التشفير
- **Cipher text** النص المشفر بعد عملية التشفير
- **Encryption** تحويل النص العادي إلى نص مشفر
- **Decryption** فك التشفير اي تحويل النص المشفر إلى نص عادي

- **المفتاح (Key):** وهو عبارة عن كلمة السر المستخدمة في خوارزمية التشفير أو فك التشفير ويعتبر من أهم الأشياء التي يجب إخفائها حيث أنه يعتبر من الأشياء السرية التي لا يعرفها إلا المخول لهم فك الشفرة.
- **الخوارزمية (Algorithm):** الخوارزمية هي عبارة عن الخطوات اللازمة لحل مسألة ما, و قد تكتب هذه الخوارزمية باللغة العربية أو الإنجليزية أو قد يعبر عنها برسم أشكال هندسية معينة.



الشكل (4): التشفير وفك التشفير


المرسل
مفتاح التشفير
مفتاح فك التشفير
المستقبل
النص الواضح
خوارزمية التشفير
النص المشفر
خوارزمية فك التشفير
النص الواضح
المهاجم

مثال على مفهوم التشفير

وكمثال بسيط لتوضيح ذلك، عزيزي الدارس، نأخذ على سبيل المثال كلمة Arab فإن الخطوات المتبعة أو الخوارزمية المستخدمة لتشفير تلك الكلمة:

نجعل كل حرف يساوي الحرف الذي يليه بالترتيب الهجائي أي أن:

A = B

R = S

A = B

B = C

وفي هذا المثال النص الأصلي Plaintext هو Arab والنص المشفر هو BSBC وبذلك قد أخفينا النص الأصلي وعندما يصل النص إلى الطرف الثاني فإنه يقوم بعكس التشفير أي أننا: نجعل كل حرف يساوي الحرف السابق له، وبذلك نكون قد حصلنا على النص الأصلي.

أهداف التشفير

- **يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:**
  - **السرية أو الخصوصية (Confidentiality):** هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.
  - **تكامل البيانات (Integrity):** وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.
  - **إثبات الهوية (Authentication):** وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).
  - **عدم الجحود (Non-repudiation):** وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما، أو اثبات عمل قام به فعلاً فلا يستطيع انكاره أو التملص منه، فالتشفير يوفر الاثبات من خلال استخدامه في التوقيع الرقمي Digital Signature، والتوقيع الرقمي هو التوقيع الذي يستخدم تقنيات التشفير والذي يمتملك المفتاح العام والمفتاح الخاص والشهادة الرقمية.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.

فكرة عمل التشفير

- تقوم فكرة عمل التشفير على عدة طرق من أهمها:
  - طرق استبدال الأحرف.
  - المواراة أو الإخفاء.
  - الطرق الرياضية التي تعتمد على الخوارزميات.
  - الطرق الإحصائية التي تعتمد على تردد الأحرف في اللغة.

عناصر التشفير الرئيسية

1. الخوارزميـــــة
2. مفتاح التشفيـــر
3. البيانات الأصليـة
4. نـــص الشفـرة

ملاحظة

معرفة أي ثلاثة عناصر من العناصر المذكورة سوف يؤدي إلى استنتاج العنصر الرابع.

أنواع التشفير

التشفير باتجاه واحد

هو التشفير الذي لا يمكن الرجوع فيه من النص المشفر الى النص الأصلي مثل التشفير باستخدام خوارزمية MD5, SHA

التشفير باتجاهين

التشفير المتماثل

باستخدام مفتاح واحد هو المفتاح العام Public key

مثل: طريقة Monoalphabetic، طريقة Playfair، طريقة Vigenere, DES، IDEA

التشفير غير المتماثل

باستخدام زوج من المفاتيح هما المفتاح العام Public key, والمفتاح الخاص Private key مثل RSA، Diffie-Hellman، DSS

في هذا النوع من التشفير نتمكن من استرجاع النص الأصلي من خلال فك شيفرة النص المشفر

ثالثاً: التشفير باتجاه واحد

التشفير باتجاه واحد

- وفي هذا النوع من التشفير (التشفير باتجاه واحد) عادة يتم استخدام دالة الاختزال أو الـ **(Hash Function)** وهي عبارة عن عملية تحويل الرسالة أو البيانات إلى قيمة عددية .(numeric hash value)
  ودالة الهاش تعتبر إما أحادية الاتجاه أو مزدوجة.
- فإذا كانت الدالة أحادية الاتجاه فلا تسمح للرسالة بأن تعود إلى قيمتها الأصلية'،
- أما في حالة الدالة المزدوجة فيسمح للرسالة بأن يعاد بناءها من الهاش
- **وفي الأغلب** أكثر دالات الهاش أحادية الاتجاه أي **يستحيل فهم النص المشفر أو العودة منه للنص الأصلي**

ومن أنواع دالة الاختزال:

1. Secure Hash Algorithm (**SHA**)

وسلسلة تلخيص الرسالة (Message Digest) والمختصرة بـ (MD)

1. والسلسلة تتضمن MD2 و MD4 و أخيراً MD5

التشفير باتجاه واحد

- عملية يتم بموجبها تشفير المعلومات باستخدام خوارزمية التشفير ولكن لا يوجد خوارزمية فك تشفير الرسالة.
- لماذا نستخدم هذه الطريقة إن كنا غير قادرين على استعادة النص الأصلي؟

الجواب هو أن هناك بعض المعلومات لا يلزم معرفة المعلومات الاصلية منها ولكنها تستخدم التشفير لاستحداث بصة إلكترونية أو توقيع رقمي.

والمثال النموذجي هو كلمة السر وبطاقة الصراف الالى.

خوارزمية التشفير
MASSAGE DIGEST (MD5)

- هي دالة تشفير يدخل لها نص بأي طول ويتم تجزئته إلى نصوص قصيرة بحجم 512 bit وتنتج نص مشفر بطول 128 bit يمثل بـ 32 رقم ست عشري (Hexadecimal) , ناتج عملية التلخيص صعب الرجوع منه للنص الأصلي .
- ***مثال*** :

النص الأصلي : Message Digest 5

نتيجة الـ (MD5) له : b88402ac7072606ec70f190ba5dd011

- هذه الطريقة عادة ما تستخدم في إثبات صحة الملفات من التعديل و هويات المستخدمين والتواقيع الرقمية والتي سنرى تفصيلها لاحقاً

خوارزمية التشفير (MD5):

- **يمر النص فيها بست خطوات تشمل، يمكن اختصارها بالخطوات الاربعة التالية:**

1. تجزئة النص لأجزاء بحجم 512 bit
2. تكون الكلمات الإنشائية كل جزء بحجم 512 bit يتم تجزئته إلى 16 كلمه "Word" كل كلمه بحجم 32 bit.
3. من ثم مرورها في أربع دورات وتميز كل دوره بمعادله منطقيه خاصة بها
4. لتنتج نص غير مفهوم بطول 128 bit

خواص خوارزمية التشفير (MD5) :

1. طول نتيجة الخوارزمية ومنها دائما ما نستدل على نوع الخوارزمية المستخدمة , على سبيل المثال إذا عرفنا ان ناتج العملية **هو 128 bit** فبالتأكيد أننا أستخدمنا الـ (MD5) .

2. خوارزمية التشفير (MD5) **لا تعطي نتيجتين متماثلتين** لملفين مختلفين , حينما نجد دالتين للـ (MD5) متماثلتين فبالتأكيد أنهما نتيجة لملفين أو رسالتين متطابقتين تماماً.

3. إذا قمنا بعمل خوارزمية التشفير (MD5) لملف أو رسالة معينه أكثر من مره في أوقات مختلفة دون التعديل عليها فإن نفس نتيجة الخوارزمية سوف تتكرر في كل مره .

خوارزمية التشفير (MD5) ذات طريق واحد, أي انه من نص عادي تعطي نص مشفر لكن لا نستطيع أن نصل من النص المشفر إلى نص عادي.

خواص خوارزمية التشفير (MD5) :

- **إثبات صحة الملفات (File Integrity):**

حينما يكون لدينا ملف للمشاركة قراءة دون تعديل ونريد ان نتأكد دوماً أنه لم يتعرض لأي تحرير من قبل اشخاص غير مصرح بهم

- فكل ما علينا هو حساب دالة الـ (MD5) قبل عرض الملف للمشاركة وحفظ النتيجة في قاعدة بيانات ومن ثم يتم حساب الـ (MD5) بشكل دوري ومقارنة نتيجة الحساب بالقيمة المحفوظة سابقاً ,

- بمجرد اختلاف القيمتين عن بعضهم يعني ان الملف تعرض للتعديل عن محتواه الأصلي حتى وإن كان التغيير حرف واحد فقط! .

تطبيقات MD5

المرسل
المستقبل
شبكة المعلومات
استخدام الكارت الذكي ورقم التعريف الشخصي
التوقيع على اية بيانات او مستندات وإرسالها انيا مع ختم البيانات بتوقيت التوقيع
• التأكد من صحة التوقيع
• التأكد من صحة محتويات المستند
• التأكد من توقيت التوقيع
• التأكد من هوية القائم بالتوقيع
• أماكنية حفظ البيانات الموقعة والتوقيع

تطبيقات MD5

- **كلمة المرور(Password):**

حينما تضع كلمة مرور على جهاز الحاسب الخاص بك لتزيد الأمان والخصوصية عليه فإن ما يحدث فعلاً هو تخزين القيمه الناتجة من حساب الـ (MD5) لكلمة المرور خاصتك في ملفات النظام

- وفي المرة القادمة من محاولتك للدخول لحسابك فإن النظام يقوم بحساب الـ (MD5) لكلمة المرور المدخلة وبمقارنتها بالقيمة المحفوظة في ملفات النظام
- اذا تطابقت القيمتان سوف يسمح لك بالدخول والتعامل مع ملفاتك وفي حين اخطأت في ادخال كلمة المرور بالتالي ستختلف نتيجة الـ (MD5) عن المحفوظة سابقاً وستترك لك 3 محاولات لإدخال كلمة المرور مره اخرى وإلا سيتم اغلاق المحاولات لفترة من الوقت .

كسر خوارزمية MD5

- من الصعب جدا كسر خوارزمية التشفير (MD5) ولكن أكثر الطرق شيوعاً واستخداما في كسر الـ (Md5)
  - الـBrute Force وتستخدم خصوصا في فك تشفير كلمات المرور، والتي تعتمد على جمع عدد من الكلمات المتوقعه وتشفيرها بالـ (MD5) ومقارنة النتيجة بـ (MD5) الأصلي والمخزن كنص مشفر
  - جمع عدد كبير من النصوص بالإضافة للـ (Md5) الخاصة بها في ملف يدعى " Rainbow Table" ويتم العودة لهذا الملف والمقارنة كلما دعت الحاجه .
  - ان بعض المواقع على الشبكة العنكبوتية تقوم بحساب (MD5) لنص معين او العكس.

أوجه القصور في التشفير

تنقسم أوجه القصور في عملية التشفير إلى ثلاثة أنواع:

- **الأخطاء البشرية.**
- **أوجه الخلل في الشفرة ذاتها.**
- **عمليات الهجوم غير المنطقية.**

طرق اختراق التشفير على مستوى الشبكة

- يحاول المهاجمون اختراق الاتصالات المشفرة باستخدام عدة طرق منها:
  - **عن طريق القوة Brute-Force Attack:**
    - وهي أن يقوم المهاجم بتجريب كل احتمالات المفاتيح الممكن استخدامها بشكل متتال.
    - وتعتبر هذه الطريق حلا أخيرا لمعرفة المفتاح بسبب الوقت الطويل الذي تحتاج إليه هذه العملية.
    - ولكن مع مرور الوقت أصبح هذا النوع من طرق الاختراق أسهل بسبب الزيادة السريعة بسرعة وقوة وتطور أجهزة الحاسوب في الوقت الحالي.

طرق اختراق التشفير على مستوى الشبكة

الاختراق على طريقة القاموس Dictionary Attack :

- تجريب المفاتيح حسب قائمة بالكلمات التي يمكن استخدامها في تشفير الرسائل.
- و هذه التقنية تعتمد على استخدام الأشخاص لكلمات عادية في تكوين المفتاح.

الشمام Sniffer:

- هذه الطريقة تعتمد على تشغيل برنامج صغير داخل نظام
- يقوم بمراقبة الحركات في أنظمة الشبكات.
- هذه البرامج تقوم بالحصول على كلمة السر للمستخدم عندما يقوم هذا الشخص بإدخال كلمة سره عند تشغيل النظام.
- كما يمكن استخدام هذه الطريقة للتوصل لمعرفة مفاتيح التشفير.