الباب التاسع
التقنيات المتطورة في الشبكات

الفصل السادس والعشرون: الشبكات الموسعة (WAN)

الفصل السابع والعشرون : الشبكات اللاسلكية

الفصل الثامن والعشرون : شبكات VPN

الفصل السادس والعشرون
الشبكات الموسعة (WAN)

*تعرفت في الفصول السابقة علي شبكة **LAN** ومكوناتها وطريقة عملها وكيفية إنشائها ، ولكن ماذا لو زاد عمل الشركة واتسع ليشمل بلداناً وأقطاراً متعددة. ستحتاج بالقطع إلي أكثر من شبكة **LAN** مرتبطة ببعضها بوسيلة ما. من هنا جاءت فكرة شبكة **WAN**. فهي شبكة مكونة من شبكتي **LAN** أو أكثر متصلين بواسطة خطوط هاتف رقمية ويتم توجيهها بين مقاطع.*

بانتهاء هذا الفصل ستتعرف علي :

- *ما هي شبكة **WAN** ومن يحتاج إليها.*
- *مكونات شبكة **WAN**.*
- *الموجهات.*
- *بروتوكولات الموجه.*
- *خطوط نقل البيانات.*
- *خطوط **DSL**.*
- *الانترنت وشبكة **WAN**.*

نشأت فكرة شبكة **WAN** أو شبكة الاتصال الواسعة من الحاجة إلى القدرة على نقل البيانات عبر مسافات طويلة بسرعة كبيرة لقد كانت الشبكات الأولى بطيئة ومحدودة المدى. لكن مع التطور الذى أصاب الحياة بصفة عامة وتكنولوجيا الاتصالات بصفة خاصة، ابتكرت شركات ربط الشركات طرق لربط الشبكات معاً تسمح للمستخدمين بالاتصال من مسافات طويلة إلى نفس البيانات ولكن ما هى شبكة **WAN**؟

ما هي شبكة WAN (Wide Area Network)

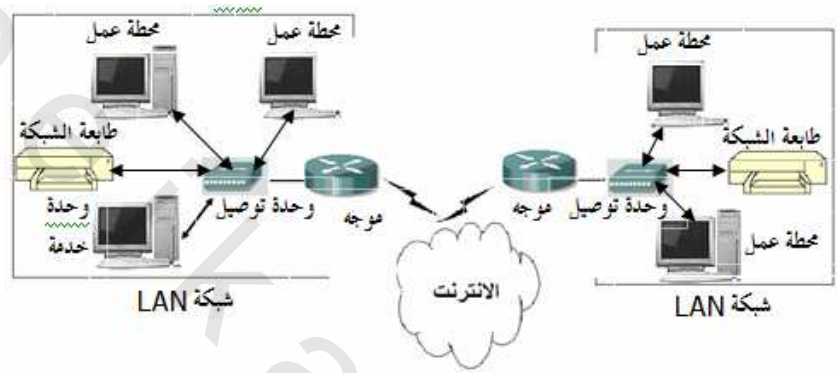
عبارة عن مجموعة شبكات محلية متعددة **(LANs)** توجد عادة فى مواقع مختلفة يتم وصلها ببعضها البعض.

إذن تسمية شبكة واسعة أو موسعة **(WAN)** جاءت من طبيعة عملها حيث تربط شبكتى كمبيوتر محلية أو أكثر موجودة فى مواقع جغرافية متفرقة معا. يتم ربط شبكات **WAN** باستخدام خطوط هاتف عالية السرعة. يتشارك مستخدمو الكمبيوتر على شبكة **LANs** متعددة فى الموارد. ولكن فى الحقيقة هذا التعريف تبسيط لحقيقة شبكة **WAN** وطبيعة عملها، يتضح ذلك من المثال التالى:

عندما تستخدم بطاقة الائتمان الخاصة بك **Credit Card** فى أحد المحلات لدفع قيمة مشترياتك أو لسداد فاتورة خدمة معينة. يتم الحصول على هذه الخدمة عن طريق شبكة **WAN**. لأن الذى يحدث بالضبط أن الجهاز الذى يستخدمه الصراف رغم أنه لايعد جهاز كمبيوتر بالمعنى المعروف وإنما هو جهاز ذو أغراض محدودة جدا. يقوم هذا الجهاز بالبحث فى قواعد بيانات الشركات المشتركة فى الخدمة عبر خطوط هاتف مؤجرة للتأكد من بطاقة الائتمان وصلاحيتها.

من هذا المثال نفهم أن شبكة **WAN** تعتبر طريقة لمد موارد الشبكة فيما وراء المنطقة المحلية. وفى عصر الإنترنت، توجد الكثير من الطرق لتنفيذ ذلك منها مثلا خطوط الهاتف الرقمية باهظة التكاليف ونوع من الشبكات يسمى **Virtual Private Network** (شبكات ظاهرية خاصة) تختصر هكذا **VPN**. (وهى طريقة لتوصيل الشبكات تستخدم الإنترنت لحمل الشبكات) .

يوضح شكل ١-٢٦ فكرة شبكة WAN في هذا الشكل تم ربط شبكتي LAN تتكون كل منهما من وحدة خدمة Server ووحدتين تابعتين وتستخدم وحدة توصيل Hub لربط الوحدات التابعة وتربط الموجهات (Routers) بين الشبكات لتكون في النهاية شبكة WAN.



شكل ٢٦-١ ربط شبكتي LAN

تستخدم شبكات WAN أنواع من الروابط للربط بين الشبكات المحلية LAN منها

- موجات الميكروويف Microwave.
- الأقمار الصناعية Satellites.
- أسلاك الألياف البصرية Fiber Optic
- الأسلاك المحورية Coaxial cables

من يحتاج إلى شبكة WAN

حيث أن شبكة WAN تمتد إلى مناطق جغرافية متفرقة وتستخدم تقنيات باهظة التكاليف كما أوضحنا قبل قليل، فإنها تعد بواسطة الشركات الكبرى أو المؤسسات التى ترغب فى تأسيس وجود شبكى مهم فى أنحاء القطر الواحد أو حتى فى أنحاء العالم.

ورغم أن هذه الشبكة باهظة التكاليف، إلا أن الفائدة التى تجنيها الشركات الكبرى من ورائها يمكن أن تتفوق على التكاليف عدة مرات.

تصور مثلا شركات الطيران التى تحتاج لإدارة بيانات الرحلات الجوية فى المطارات بدون شبكة WAN بالطبع لن تستطيع تقديم أى نوع من الخدمات لعملائها.

مكونات شبكة WAN

أجهزة المودم Modems

كلمة **Modem** اختصار لعبارة **Modulator / demodulator** ومعناها "تعديل – إلغاء التعديل). ويستخدم أساسا لتبادل البيانات بين أجهزة الكمبيوتر عبر خطوط الهاتف وهو جهاز يستخدم لتحويل إشارات الكمبيوتر الرقمية **(Digital)** إلى إشارات قياسية **(Analog)** ثم تنتقل تلك الإشارات القياسية من خلال خطوط التليفون عند الإرسال. وعند الاستقبال (فى الجهاز المستقبل) يقوم المودم بعملية عكسية أى يتم تحويل الإشارات القياسية إلى إشارات رقمية يفهمها الكمبيوتر.

تقاس سرعة المودم فى نقل البيانات بعدد البتات **(Bits)** فى الثانية وتختلف تلك السرعات باختلاف نوع المودم وسعره. وهى تتراوح بين ٢٤٠٠ إلى ٥٧٠٠ بايت فى الثانية (٥٦ كيلوبايت).

يوجد نوعين من أجهزة المودم : مودم داخلي : وهو عبارة عن بطاقة تركب داخل جهاز الكمبيوتر فى إحدى فتحات التوسعة **Expansion Slots** الموجودة على اللوحة الأم لجهاز الكمبيوتر، مودم خارجى: ويكون منفصلا عن جهاز الكمبيوتر ويتصل به بواسطة سلك توصيل يستخدم المودم نوعين من خطوط الهاتف.

خطوط الهاتف العادية Dial-up network Lines:

وفى هذا النوع يقوم المستخدم بإجراء اتصال تليفونى فى كل مرة يرغب فيها فى استخدام المودم

الخطوط المؤجرة Leased lines

وهى خطوط تعمل على مدار ٢٤ ساعة ولا تحتاج إلى إجراء اتصال تليفونى وهى أسرع وأجود من خطوط الهاتف العادية.

الجسور Bridges

الجسر **Bridge** عبارة عن جهاز يستخدم للربط بين الشبكات المحلية **LAN** وتوسيعها. ويمكنه التوصيل بين شبكات ذات تصميمات مختلفة مثل شبكات **Ethernet** مع شبكات

Token Ring كما يمكنه الربط بين شبكات تعمل باستخدام بروتوكولات مختلفة مثل IPX و TCP.

تعد الجسور أجهزة قديمة لم تعد مستخدمة كثيراً، ولكننا أوردناها هنا لأنك قد تصادفها في المواقع القديمة، لايعد استخدام الجسور لربط الشبكات طريقة فعالة لمعالجة اتصالات WAN. نظراً لأن الجسر يمرر تدفق اتصالات البث (وهي الرسائل التي يتم إرسالها إلي كل جهاز علي شبكة معينة) وهذا يهدر بعض تردد نطاق ارتباط WAN .

بصفة عامة يعد الجسر (Bridge) موجهاً تم توصيفه لتوصيل الشبكات عند طبقة Data Link "ربط البيانات" وهي الطبقة رقم ٢ من نموذج OSI بدلاً من طبقة Network "شبكة الاتصال" من النموذج. وهي الطبقة التي تعمل فيها الموجهات (Routers). عندما يربط جسر الشبكات، يتم توسيع الشبكة الحالية بحيث يري المستخدمون إصداراً أكبر من الشبكة المحلية، ويمكنهم الوصول إلي الموارد البعيدة بنفس الطرق المستخدمة في شبكة LAN. ولأن الجسور تعتبر بطيئة، فيتم استخدام الموجه (Router) لربط شبكات LAN في الوقت الحالي بدلاً من الجسور (Bridges). وبالتالي لم يعد استخدام الجسر مستخدماً. سوف نشرح بعد قليل الموجهات، وستعرف الفرق بينها وبين الجسور.

تتعرف الجسور على أجهزة الكمبيوتر على الشبكة بأن ترسل رسائل موجهة إلى كل الأجهزة، وعندما تقوم الأجهزة بالرد تتعرف الجسور على عناوين تلك الأجهزة ومواقعها. ثم تستخدم تلك المعلومات لإنشاء جدول توجيه Routing Table وهناك طريقة أخرى تستخدمها الجسور للتعرف على الأجهزة وهى الكشف عن حزم البيانات المارة بها، ويقوم الجسر بمقارنة عنوان الكمبيوتر المرسل للحزمة مع العناوين المخزنة فى جدول التوجيه (Routing Table). وفى حالة عدم عثور الجسر على العنوان يقوم بإضافته إلى الجدول. وهكذا يتم تحديث الجداول بصفة مستمرة.

مترجمات البروتوكولات Protocol Translators

عبارة عن أجهزة يمكنها الترجمة بين بروتوكولين من بروتوكولات الشبكة. تستخدم مترجمات البروتوكولات لترجمة بين بروتوكول IPX لشبكة NetWare وبروتوكول

TCP/IP حتى يمكن للشبكات التى تعتمد على **IPX** الاتصال بالإنترنت إذا كنت تستخدم شبكة **NetWare**، قد يكون بروتوكول الترجمة أفضل طريقة لتمكين وصول الإنترنت للمستخدمين.

على الرغم من ذلك ، يعد بروتوكول **IPX NetWare** الأساس وهو قابلا للتوجيه، وربما يكون الموجه **(Router)** اختياراً أفضل إذا كنت ترغب فى ربط شبكتى **LANs** لإنشاء شبكة **WAN**، تابع قراءة البند التالى للتعرف على الموجهات

الموجهات Routers

يمكن تعريف الموجه **(Router)** بأنه جهاز يقوم بمعالجة وتمرير حزم البيانات داخل الشبكة الواحدة أو بين شبكات **LAN** منفصلة ويتم إرسال البيانات من مصادرها إلى وجهاتها فى أسرع طريق ممكن.

يعمل الموجه عند طبقة **NetWare** (شبكة الاتصال) وهى الطبقة الثالثة فى نموذج **OSI** الذى مر بنا .

فى حالة الشبكة الواحدة، تتجه حزم البيانات من الجهاز المرسل إلى الجهاز الوجهة دون أية وسائط. أما إذا كان عنوان الوجهة لحزمة البيانات خارج الشبكة المحلية، سيتم إرسالها إلى الموجة (الذى يعرفه الجهاز المرسل بصفته المدخل الافتراضى) بدون معالجتها.

عندما يتلقى الموجه حزمة بيانات موجهة لمكان خارج الشبكة المحلية، سوف يقوم الموجه بإرسال حزمة البيانات إلى النقطة التالية.

وللتوضيح نقول . ترسل الموجهات حزم البيانات وفقا للموجهات المتوفرة بين الشبكات وتحاول تحديد أقصر مسار توجيه ممكن فى أى وقت محدد. كيف يتم ذلك؟ يوجد داخل الموجه (وهو جهاز كمبيوتر صغير لكنه قوى جدا) توجد مجموعة بيانات تسمى **Routing Tables** أو "جداول التوجيه". يتم تحديث هذه الجداول بواسطة بروتوكولات توجيه يطلق على أحدها **Routing Information Protocol (RIP)** أو "برتوكول توجيه المعلومات" وعلى الثانى **Open Shortest Path first (OSPF)** "فتح أقصر مسار أولا".

سنتعرض لشرح كلا من RIP وOSPF فى البند التالى

ويقوم أى من البروتوكولين بتمرير البيانات بصفة مستمرة بين الموجهات للتأكد أن كل الموجهات لديها أحدث البيانات فيما يتعلق بمسارات التوجه المتوفرة.

كيف يتم توجيه البيانات

تحتوى جداول التوجيه على جميع مسارات التوجيه الممكنة، ويستعين الموجه بجداول التوجيه لتحديد ما إذا كان لديه مسار توجيه إلى عنوان وجهة معين أو لا.

إذن كل ما يفعله الموجه هو إعادة إرسال حزم البيانات إلى وجهاتها. ويحاول الموجه فعل ذلك بأفضل طريقة كيف ذلك ؟ فى كل مرة يتم توجيه حزمة البيانات بين موجه وآخر يزيد رقم فى حزمة البيانات يطلق عليه عدد الوثبات أو العداد بمقدار واحد (١) إذا وصل عدد الوثبات إلى عدد من المرات محددة سلفا (مثلا يسمح لبروتوكول RIP بعدد ١٦ وثبة بين المصدر والوجهة) يتم تجاهل حزمة البيانات، باعتبار أن الموجه حاول ١٦ مرة ولم يفلح فى تسليمها إلى عنوان الوجهة.

بروتوكولات الموجه Router Protocol

تستخدم الموجهات مجموعة من البروتوكولات لتحديد الطريقة المناسبة لتوجيه حزم البيانات. تسمى هذه البروتوكولات "بروتوكولات المداخل" أو **Gateways Protocols**. وتعد هذه البروتوكولات أفراداً فى مجموعة بروتوكولات TCP/IP التى تستخدمها الموجهات لتحديد أفضل مسار توجيه لحزم البيانات.

شرحنا في الفصل الثامن عشر بالتفصيل بروتوكولات الموجه وهي تستخدم أساساً في الشبكات الواسعة لذلك. لا نري ضرورة لإعادة تكرار الشرح هنا، ننصح بالرجوع إلي الشرح السابق عن بروتوكولات التوجيه في الفصل الثامن عشر للتعرف علي البروتوكولات المستخدمة في التوجيه بالتفصيل.

خطوط نقل البيانات

عادة يتم ربط شبكات **WANs** باستخدام خطوط هاتف رقمية **Digital Phone Lines**. توفر خطوط الهاتف الرقمية سرعات عالية جدا لنقل البيانات عبر مسافات بعيدة، تقوم خطوط الهاتف الرقمية بتحويل الصوت العادى إلى بيانات رقمية **Digital Data**والبيانات الرقمية هى البيانات التى يفهمها الكمبيوتر والتى تتكون من الصفر والواحد والتى تعرف بالنظام الثنائى.

ولتوضيح الفرق بين خطوط الهاتف الرقمية وخطوط الهاتف القياسية نجد أن خطوط الهاتف القياسية **Analog Phone Lines** مثل تلك التى تستخدمها فى مكتبك للاتصال بعملائك ترسل الصوت على شكل موجات (مثل موجات الراديو).

لإرسال البيانات من التليفون القياسى (التليفون المتصل ببيتك أو مكتبك) يجب تحويلها من الصوت إلى بيانات رقمية. ويستخدم لهذا الغرض عادة جهاز المودم **Modem** وفيما يلى نوضح أشهر الخطوط الرقمية المستخدمة فى نقل البيانات.

خطوط T1 و T3 الرقمية

تعرف خطوط **T1** و **T3** بالخطوط الرئيسية. وهى خطوط رقمية تماما وتغطى هذه الخطوط نطاقا واسعا من احتياجات ربط الشبكات ويعتبر نظام الخطوط الرئيسية هو أول نظام خطوط هاتف رقمية. يوفر خط **T1** معدل إرسال يصل إلى **1.544** ميجابت فى الثانية، ويتم استخدامه غالبا لتوصيل شبكات **WANs** داخليا، بينما تبلغ سرعة خط **T3** **44.736** ميجابت فى الثانية، ويستخدم عادة بواسطة الشبكات الكبيرة ومزودى خدمة الإنترنت، لأن تكلفة هذا الخط عالية جداً ولا تقدر عليها الشركات الصغيرة.

قد لا توجد خطوط **T3** إلا إذا كنت تعمل لصالح مزود خدمة انترنت أو كان لديك اتصال بمركز بيانات رئيسى. حيث تصل سرعتها إلى حوالى ٤٥ ميجابت فى الثانية. بالنسبة لشبكات **WANs** الصغيرة والمتوسطة يكفى استخدام خط **T1**. بل قد تستخدمه جزئيا لعدم حاجتك إلى استخدامه كاملاً .

الخطوط المؤجرة Leased Lines

كثيرا ما يطلق على الخطوط الرئيسية **Leased Lines** (الخطوط المؤجرة). وتستخدم عادة بواسطة شركة أو مؤسسة واحدة.

تمر الخطوط المؤجرة بين نقطتين . ويمكن أن تكون هاتين النقطتين فرعين لشركتك أو قد تكون واحدة منهما شركتك والأخرى موقع لمزود خدمة انترنت يزودك بخدمات الإنترنت.

توفر شركات الاتصالات الكثير من الطرق لحساب رسوم خطوط الهاتف الرقمية. وتختلف تلك الرسوم من شركة لأخرى.

نقل البيانات عبر الخطوط الرقمية

يتم نقل البيانات عبر خطوط الهاتف الرقمية باستخدام طريقتين الأولى تسمى **frame relay** (نقل الأطر) والثانية **Clear channel signaling** وتختصر عادة **CCS** وتعنى "إشارة القناة الواضحة".

يتم استخدام نقل الأطر **Frame relay** فى الغالب للاتصال بالإنترنت بالإضافة إلى استخدامه لربط مواقع متعددة. من السهل استخدام نقل الأطر ولكنه أقل كفاءة من **CCS** "خط قناة واضح".

أحيانا يطلق على طريقة **Clear channel signaling** "إشارة القناة الواضحة" اسم **Common channel signaling** "إشارة القناة العامة" وهما بنفس المعنى، وهى طريقة لتعويض عدم كفاءة طريقة **Frame Relay** لنقل البيانات.

فى طريقة **CCS** يتم إرسال كل الإرشادات عن كيفية نقل البيانات عبر قناة منفصلة عن البيانات ولذلك ليست هناك حاجة لوضع البيانات فى أطر البيانات الخاصة بها. وبالتالى سوف تحصل على مخرجات أعلى.

فى المقابل فإن تكلفة طريقة **CCS** (طريقة القناة الواضحة) أعلى بكثير من طريقة نقل الأطر.

الخطوط المشتركة الرقمية DSL

الطريقة الأرخص والأوفر لنقل البيانات باستخدام خطوط الهاتف الرقمية هى **Digital Subscriber Line** وتختصر هكذا **DSL** وتعنى "خط المشترك الرقمى" توفر هذه الخطوط خدمة ممتازة للاتصال بالإنترنت. أصبحت خدمة **DSL** منخفضة يمكن أن يتحملها المشترك. كما أنها سهلة التزويد من قبل شركات الاتصالات. وقد انتشرت خدمة **DSL** وأصبح من الممكن الحصول عليها من قبل مزودى خدمة الإنترنت وليس شركات الاتصالات فقط.

من مزايا **DSL** أن تكلفتها أقل بكثير من تلك الخاصة بخدمة خط **T1** والثانية أنها تمر عبر نفس السلك النحاسى التى تستخدمه خطوط الهاتف العادية، والثالثة أنها توفر سرعة عالية جدا لنقل البيانات.

وعلي الرغم من فوائد **DSL** فإن لها بعض العيوب. ففي معظم الحالات تعد أقصي مسافة لدوائر **DSL** الكهربائية أقل من ستة أميال فإذا كانت المسافة بين مكتبك والمكتب الرئيسي للشركة أكثر من تسعة أميال لن تتمكن من استخدام الخدمة. يمثل ذلك مشكلة محتملة بالنسبة لإضافة **DSL** إلي شبكات **WANs** الموجودة في الأقاليم.

تتوفر **DSL** فى مجموعة مختلفة من التوصيفات أشهرها:

- **ADSL** : كلمة **ADSL** اختصار لعبارة **Asymmetric Digital Subscriber Line** ومعناها "خط مشترك رقمى غير متماثل" وتعد **ADSL** مفيدة جدا للوصول إلى الإنترنت لأن البيانات التى تأتى للشبكة تعد أهم من البيانات التى تخرج منها. في حين لا تعد مفيدة بالنسبة لشبكات **WAN** .

يستخدم الكثيرين ممن يستخدمون **DSL** فى المنازل هذا التوصيف من **DSL**. لأن المستخدمين في المنازل يُحمِّلون قدراً أكبر بكثير من الانترنت إلي أجهزتهم المنزلية مما يحملونه إلي أعلي (يرسلونه عبر الانترنت).

- **HDSL**: كلمة **HDSL** اختصار للعبارة **High-speed Digital Subscriber Line** أو "خطوط المشترك الرقمى عالية السرعة".

ويعتبر هذا الشكل من DSL أكثر فائدة لشبكات WANs ، حيث ترسل HDSL البيانات بسرعات تصل إلى معدلات خط T1(1.544 ميجابايت فى الثانية) وتصل إلى مسافات طويلة.

الانترنت وشبكة WAN

مع وضع التكاليف المرتفعة لخدمة الهاتف الرقمية في الاعتبار، يمكن أن يصبح إنشاء شبكة بها الكثير من المواقع البعيدة المرتبطة بخطوط رقمية أمراً باهظ التكلفة بسرعة كبيرة. يعد جزء من هذه التكلفة لا مفر منه؛ لتوصيل الشبكات معاً على أساس مستمر يمكن الاعتماد عليه، تعد خدمة الهاتف الرقمية ضرورية. على الرغم من ذلك، هناك تكاليف تزايدية إضافية لتطوير شبكة WAN خاصة، مثل: تكلفة رواتب مدير نظام واحد أو أكثر والنفقات الإضافية التي تأتي مع إدارة شبكة خاصة.

تتمثل إحدى الطرق لتقليل تكاليف إدارة WAN في تكليف جهة أخرى بإدارتها، أو توظيف شخص آخر للتعامل مع ربط شبكة LAN الداخلية من أجلك.

على الرغم من ذلك، مع زيادة حجم الإنترنت، دخل الكثير من كبار مزودي خدمة الإنترنت في مجال توفير خدمات WAN. وعرض هؤلاء خدمات الاتصال بصفتها الخدمة التي يتم بيعها. لقد اختار مزودو خدمة الإنترنت تحمل جزء كبير من تكلفة دمج خطوط الهاتف الرقمية وتكنولوجيا WAN، واختاروا بدلاً من ذلك تحقيق الربح من خدمة الشبكة التي يتم تزويدها.

على أيه حال، لنموذج مزود خدمة الإنترنت جانب إيجابي آخر: يعد مزودي خدمة الإنترنت مجرد شبكات توجيه تعتمد على أجهزة الكمبيوتر. نظراً لأن مزود خدمة الإنترنت لديه شبكة تعتمد على أجهزة الكمبيوتر، فمن المؤكد أنه سوف يعد شبكات WANs مؤمنة نسبياً، ويمكن الاعتماد عليها من أجل العملاء.كيف يفعلون ذلك؟ يتوفر لمزودي خدمة الإنترنت خبرات ربط الشبكات بالفعل، والأهم من ذلك، أنهم لديهم البنيات الأساسية لربط الشبكات. يتم تصميم البنية الأساسية لربط الشبكات الخاصة بمزود خدمة الإنترنت بغرض تحديد قدر البيانات التي تتجه من النقطة (أ) إلى النقطة (ب)

وتعود مرة أخرى. إذا أعد مزود خدمة الإنترنت الموجهات لتوجيه حزم بيانات تأتي من شبكات معينة إلى شبكات أخرى معينة فقط وتستخدم الإنترنت بصفتها وسيلة نقل بين مواقع خدمة مزود خدمة الإنترنت، يعني ذلك أنه أعد نوعاً من شبكة **WAN** يطلق عليه **Virtual Privet Network (VPN)** (شبكة ظاهرية خاصة). لكل الأغراض العلمية، تنفذ **VPN** نفس المهام التي تؤديها شبكة **WAN** مخصصة تعتمد على خط هاتف رقمي من نقطة إلي نقطة، ولكن بصفة عامة، تتكلف هذه الشبكة أقل وتتطلب صيانة أقل من المستخدم النهائي. مادام مزود خدمة الإنترنت يؤدي مهمته، يجب تضمين تكاليف صيانة ارتباطات الشبكة الداخلية ضمن الرسوم الشهرية لمزود خدمة الإنترنت. هناك بعض المحاذير المهمة بشأن **VPN**. أولاً: تستخدم الإنترنت لتوجيه بعض بياناتها أو كلها. من الواضح أن الإنترنت كما توجد حالياً لا تعد مكاناً مؤمناً بصورة تامة. هناك طرق لالتقاط الكثير من تدفق اتصالات الشبكة، إذا عرف شخص ما كيفيه ذلك. إذا التقط هذا الشخص تدفق اتصالات يحتوي على معلومات بطاقة ائتمان غير مشفرة أو مذكرات سرية، يمكن أن تقع في مشكلة كبيرة. إذا قررت أن استخدام **VPN** يبدو فكرةً جيدةً، تعلم أولاً كيفية تأمين أجهزة الكمبيوتر (كما مر بنا في الباب الثامن) ونفذ الأمر بصورة صحيحة. تعد شبكات **VPNs** حلاً جيداً للمعركة القديمة بين التكلفة والميزات، ولكن فقط إذا تم إنشاؤها بصورة صحيحة. إذا فعلت ذلك بطريقة صحيحة، يمكنك زيادة قوة الإنترنت لتلبية احتياجاتك .

ملخص الفصل

شرحت في هذا الفصل فكرة شبكة **WAN** والفرق بينها وبين شبكة **LAN** ومن يحتاج إليها. شرحنا بعد ذلك الأجهزة المستخدمة مع شبكات **LAN**، مع التركيز علي الموجهات **Routers**. شرحنا أيضاً الخطوط الرقمية المستخدمة في نقل البيانات مثل خطوط **T1** و **T3** الرقمية لأن شبكات **WAN** هي التي تحتاج لهذه الخطوط السريعة لتباعد المسافات التي تغطيها. أخيراً قدمنا فكرة عن شبكات **VPN** باعتبارها بديلاً رخيصاً لشبكة **WAN**. ووسيلة لزيادة قوة الانترنت لتلبية احتياجاتك.

تدريبات

١. متي يقال عن شبكة ما أنها شبكة WAN ؟

٢. ما نوع خطوط الهاتف التي يمكن أن تستخدمها شبكة WAN ؟

٣. ضع علامة (✓) أمام العبارة الصحيحة وعلامة (✗) أمام العبارة الخطأ.

أ. من مزايا شبكة WAN أنها قليلة التكاليف.

ب. شبكة WAN عبارة عن مجموعة شبكات LAN مرتبطة ببعضها.

ج. الموجهات جزء أساسي في شبكات WAN. ولا يمكن الاستغناء عنها في هذا النوع من الشبكات.

الفصل السابع والعشرون
الشبكات اللاسلكية

*يناقش هذا الفصل استعمال شبكات **LAN** اللاسلكية والتي تسمي **WLAN** (**Wireless LAN**) والتي يزدهر استعمالها في كل مكان تقريباً. في المطاعم والمقاهي والمطارات والفنادق وحتي منازل الأشخاص.*

بالانتهاء من هذا الفصل ستتعرف علي :

- *ما هى الشبكات اللاسلكية*
- *معيار **802.11***
- *كيف تنشئ شبكة تجمع بين مكونات سلكية ولاسلكية*
- *وصل الشبكات اللاسلكية*
- *كيفية استخدام شبكة لاسلكية*
- *المخاطر الأمنية التى تتعرض لها الشبكات اللاسلكية*
- *كيف نحمي الشبكة اللاسلكية*

تقنية الشبكة اللاسلكية

تعتمد شبكة **LAN** والشبكات الموسعة **WAN** على الأسلاك وتعتبر الأسلاك فى الشبكات السلكية طريقة فعالة لنقل البيانات.

مرت الكابلات (الأسلاك) بتطورات متعددة شأنها شأن بقية مكونات الشبكة – أصبحت خلالها أصغر وأسهل استخداما

كانت الأسلاك سميكة وثقيلة الوزن وكان يصعب طيها. ثم ظهر كابل **Coax** الذى أصبح أخف وزنا وأسهل استخداما. ثم ظهر كابل **UTP (Unshielded Twisted Pair)** ليصبح هو الكابل القياسى. ولذلك فمعظم الشبكات تستخدمه فى هذه الأيام

ولكن نظرا للمشاكل التى تواجه الأسلاك كوسط إرسال حيث أن جميع الكابلات تتطلب إحداث ثقوب فى الحوائط وسحبها من خلالها وعبر الأسقف لإنشاء شبكة تغطى شركتك أو مصنعك نتيجة لهذه المشاكل نشأت فكرة استخدام الشبكات اللاسلكية.

لقد أدي نمو أجهزة الكمبيوتر في الثمانينيات إلي إنشاء شبكات **LAN**، أو إنشاء شبكة الانترنت في التسعينات، مما وفر إجراء اتصالات بغض النظر عن المكان الجغرافي. برهنت الشبكات **WLAN** علي أنها منطقة النمو التقنية بدءاً من القرن الحادي والعشرين .

تعتبر الشبكات المحلية اللاسلكية **WLAN (Wireless LAN)** حاليا من الخيارات الفعالة فى مجال الشبكات. ويرجع ذلك إلي التطور الكبير فى التقنيات اللاسلكية وانخفاض أسعار منتجاتها.

تظهر أهمية تقنية الشبكات اللاسلكية عندما ترغب فى ربط أجهزة الكمبيوتر محمولة بالشبكة، حيث يمكنك حيث يمكنك حمل الجهاز واستخدامه من أى مكان.

الشبكة اللاسلكية

الشبكة اللاسلكية عبارة عن شبكة تعتمد على موجات الراديو لتبادل المعلومات بدلا من الكابلات التقليدية. تشبه الشبكة اللاسلكية شبكة الهاتف المحمول (الجوال) من حيث أن المستخدم يمكنه التنقل بحرية من مكان لآخر ويظل متصلا بالشبكة من خلال جهاز

الكمبيوتر المحمول الخاص به دون أن يتصل بكابل الشبكة.

تقدم الشبكات **WLAN** ملحقاً سريعاً وفعالاً لشبكة **LAN** سلكية. بمجرد تثبيت نقاط وصول إلي الشبكة اللاسلكية تصبح أجهزة الكمبيوتر المكتبية والمحمولة المجهزة ببطاقات **LAN** لاسلكية قادرة علي الاتصال بالشبكة السلكية بسرعات عريضة النطاق (أو أكبر) بمسافة تصل إلي ٢٧٥ متراً عن نقطة الوصول اللاسلكي. هذا يعني أن أجهزة الكمبيوتر لم تعد مربوطة بالبنية التحتية للأسلاك. حرية تامة.... أليس كذلك ؟؟؟

من مزايا الشبكة اللاسلكية رغم المصاعب التى ترد عليها والتى سيرد ذكرها فى نهاية هذا الفصل ما يلى:

- عملية بالنسبة للأشخاص كثيرى التنقل.
- مناسبة للأماكن التى يصعب استخدام الأسلاك فيها.
- توفير الاتصالات فى الأماكن المزدحمة.

يحتوى كل جهاز كمبيوتر فى الشبكة اللاسلكية على جهاز مرسل مستقبل **Transceiver** لاسلكى يقوم باستقبال الإشارات وإرسالها إلي أجهزة الكمبيوتر المحيطة.

من الأجهزة التى تستخدم الشبكة اللاسلكية أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر الشخصية والتليفونات الجوالة. يطلق على الشبكات اللاسلكية عبارة **Wireless Local Area Network** وتختصر هكذا **WLAN** كما يستخدم مصطلح **Wi-Fi** عادة للإشارة إلي الشبكات اللاسلكية رغم أنه من الناحية الفنية يشير إلي نوع واحد فقط من هذه الشبكات هو تلك التى تعتمد على معيار **802.11b** (سنشرح المعيار **802.11b** بعد قليل)

تستخدم الشبكات اللاسلكية ما يعرف بـــ **Service Set identifier** وتختصر هكذا **SSID**. ومعناها "معرِّف محدد الخدمة لتعريف الشبكة اللاسلكية. وتعرف الشبكات اللاسلكية باسم **SSID**. وعادة تستخدم جميع أجهزة الكمبيوتر المتصلة بنفس الشبكة اللاسلكية نفس **SSID**.

تستخدم الشبكات اللاسلكية جهاز يسمى **Wireless Access Point (WAP)** لوصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية الموجودة بالفعل.

معيار 802.11

أكثرية الشبكات **WLAN** قيد الاستخدام تستعمل معياراً قياسياً للإرسال اللاسلكي معروف كـ **802.11B**. يعمل المعيار القياسي **IEEE 802.11B** عند تواتر الراديو **2.4** جيجاهرتز – وهو تواتر غير منظم من قبل الحكومات. يقدم المعيار القياسي **802.11b** سرعات اتصال تصل إلي **11** ميجابت في الثانية ، وهذه سرعة كافية لمعالجة مرفقات البريد الإلكتروني الكبيرة ولتشغيل البرامج المرهقة لعرض نطاق البث كمؤتمرات الفيديو. بينما أصبح المعيار القياسي **802.11b** يهيمن الآن على سوق الشبكة **LAN** اللاسلكية، يتم تطوير تنويعات أخرى عن المعيار القياسي **802.11**، أو تمت الموافقة عليها من قبل، لمعالجة السرعات المتزايدة. **802.11g** هو أحداث إصدار عن المعيار، وهو يقدم سرعات لاسلكية تصل إلي **56** ميجابت في الثانية.

إن مختلف المعايير القياسية اللاسلكية تستهدف مجالات مختلفة في الصناعة كما هو مبين في الجدولين ٢٧–١ و ٢٧–٢ .

الجدول ٢٧–١ المميزات القياسية لـ **802.11a/ WLAN**

المعيار القياسي	**WLAN , IEEE 802.11a**
الطول الموجي للتواتر	**5** جيجاهرتز
عرض نطاق بث البيانات	**54** ميجابت بالثانية،**48** ميجابت بالثانية، **36** ميجابت بالثانية، **24** ميجابت بالثانية، **12** ميجابت بالثانية،**6** ميجابت بالثانية
نطاق التشغيل الأمثل	**45** متر في البيت، **90** متر في الهواء الطلق
الأفضل لهدف معين أو نوع أجهزة	الكمبيوترات المحمولة المتجولة في المنزل أو الشركة؛ الكمبيوترات المكتبية عند تمديد الأسلاك غير مريحة

الجدول ٢٧-٢ المميزات القياسية لـ Wi-Fi / 802.11g

المعيار القياسي	Wi-Fi , IEEE 802.11g
الطول الموجي للتواتر	2.4 جيجا هيرتز
عرض نطاق بث البيانات	54 ميجابت بالثانية، 48 ميجابت بالثانية، 36 ميجابت بالثانية، 24 ميجابت بالثانية، 12 ميجابت بالثانية، 6 ميجابت بالثانية
نطاق التشغيل الأمثل	300 متر في الظروف المثالية؛ توقع مسافة أشبه ب 45 متر في البيت و 90 متر في الهواء الطلق في الظروف العادية
الأفضل لهدف معين أو نوع أجهزة	الكمبيوترات المحمولة المتجولة في المنزل أو الشركة؛ الكمبيوترات المكتبية عند تمديد الأسلاك غير مريحة

لم يحقق 802.11a أى نجاح أبداً، لكن المعيار 802.11g المقر مؤخراً يتضمن بعض الخيارات المثيرة للاهتمام ليشمل المزيد من السرعة والأمان مثلما يبين الجدول ٢٧-٢.

لاحظ أنه عندما يُمنح عملاء 802.11b وصولاً إلي نقطة وصول لاسلكي 802.11g، لا مفر من ضبط (تخفيض) الأمان للسماح لعملاء 802.11b، بالدخول ؛ بفضل WEP ومشاكلها، تنخفض الشبكة بأكملها إلي أدنى مقام كسر شائع.

ما هو Wi-Fi ؟

يستعمل المصطلح Wi-Fi (اختصار Wireless Fidelity ، "الدقة اللاسلكية") في أغلب الأحيان في مناقشات الشبكات 802.11.Wi-Fi أو هي بالتأكيد الكلمة التسويقية الشعبية المستعملة هذه الأيام عند التكلم عن اللاسلكي. لقد بدأ المصطلح Wi-Fi بسرعة يصبح الطريقة الشائعة لوصف الشبكات 802.11 اللاسلكية.

يشير Wi-Fi أيضاً إلي شهادة من Wi-Fi Alliance، وهي اتحاد دولي لا يبغي الربح، يتألف من باعة المنتجات 802.11. إن منتجات 802.11 التى تنال الشهادة

Wi-Fi قد تم اختبارها ووجدت أنها قابلة للعمل بشكل متبادل مع المنتجات الأخرى المصادق عليها. هذا يعني أنه يمكنك استعمال منتجك الذي يحمل الشهادة Wi-Fi مع الشبكات 802.11 التي تحمل الشهادة Wi-Fi، سواء كانت كمبيوترات أبل أو شبكات مؤسسة على Windows. رغم أن منتجات 802.11 التي لا تحمل الشهادة Wi-Fi قد تعمل جيداً مع الأجهزة التي تحمل تلك الشهادة، إلا أن الشعار Wi-Fi Certified هو ضمانتك لقابلية العمل المتبادل. يمكنك أن تتعلم أكثر عن Wi-Fi Alliance على الانترنت في http:// www. Weca.net/ .

فوائد الشبكات اللاسلكية

- **سعر جذاب – نشر شبكة LAN لاسلكية يمكن أن يكون أرخص من شبكة LAN سلكية لأنك لن تحتاج إلي الأسلاك؛ فقط اتصل بنقطة وصول، ويمكنها أن تزود خدمة لعدة كمبيوترات.**
- **حركة – تعزز إنتاجية المستخدم مع إراحته بتمكينه من الاتصال بالشبكة لاسلكياً من أى نقطة ضمن نطاق نقطة وصول.**
- **نشر سريع ومرن – مدد شبكة سلكية بسرعة مع سهولة إرفاق نقطة وصول باتصال شبكي مرتفع السرعة.**
- **البرامج – كملحق للشبكة السلكية، تعمل الشبكات WLAN مع كل البرامج الموجودة. البروتوكول القياسي TCP/IP، مدعوم في كل أشكال اللاسلكي.**
- **الأداء – تقدم الشبكات WLAN اتصالاً مرتفع السرعة بينما يساوي الإيثرنت، بدأ يصبح أسرع منه بشكل متسارع .**

لقد بدأ الأفراد والشركات على حد سواء يدركون فوائد الشبكات WLAN ، ويتوقع في القريب العاجل ، أن تعتمد أكثرية الشركات على التقنية اللاسلكية لتلبية احتياجاتها المهنية والتشبيكية .

اللاسلكي يساوي تردد الراديو

المفهوم التقني الأول الذي تحتاج إلي فهمه عند مناقشة ما الذي يشكل تهديداً لشبكة لاسلكية هو أن الشبكات 802.11 تستعمل ترددات الراديو لإرسال البيانات جيئة وذهاباً بين نقاط النهاية، تماماً كالهواتف اللاسلكية أو أجهزة الراديو التي لديك في المنزل. الفرق الرئيسي هو التردد الذي تُرسل به الإشارات .

يمكن أن تسافر موجات الراديو مسافات طويلة، بناءً على التردد الجارى استخدامه. يمكن لبعض الترددات أن تسير 90-120 متراً، ويتطلب تحقيق ذلك طاقة قليلة. معظم الهواتف اللاسلكية وبطاقات الشبكة اللاسلكية الأقدم تستعمل التردد 900 ميجاهرتز كموجة حاملة، ويمكن لهذه أن تسافر أبعد بقليل مما يدرك معظم الأشخاص. ليس أمراً مستغرباً أن يعطى الهاتف اللاسلكي 900 ميجاهرتز المستخدم مجال استعمال يصل إلي شارع أو شارعين على الأقل قبل أن تفقد السماعة اتصالها بالوحدة القاعدة. شارع أو شارعين يعني 120-150 متر تقريباً.

إذا كانت سماعة هاتفك قادرة على البث بما أقصاه 150 متر هذا يعني أن اتصالك اللاسلكي قادر على مسافات مشابهة. إذا كانت لديك نقطة وصول لاسلكي (Wireless Access Point أو WAP) مثبتة في مكتبك أو منزلك، كن متأكداً أن الأشخاص الذين يسيرون في الخارج يقعون ضمن نطاقها التشغيلي. يصح نفس الشيء إذا كانت لديك نقطة WAP مثبتة في شبكة مكتبك الصغير أو مكتبك المنزلي. إذا تم تثبيت نقطة WAP اعتيادية في غرفة جلوسك وكنت تقيم في مبنى فيه عدة شقق، من الممكن جداً أن تكون تزود خدمة الانترنت لمعظم الشقق حتى دون أن تدرك ذلك.

تغطية الشبكات اللاسلكية

كل نقطة وصول لاسلكي لها نطاق محدود يمكن ضمنه المحافظة على اتصال لاسلكي بين كمبيوتر العميل ونقطة الوصول. تختلف المسافة الفعلية بناءً على البيئة؛ يذكر الصانعون عادة النطاقات داخل المنزل وفي الهواء الطلق لإعطائك فكرة معقولة عن الأداء الموثوق به.

انتبه أيضاً إلي أنه عند العمل عند حافة حدود النطاق، قد ينخفض الأداء بسبب تدهور نوعية الإشارة اللاسلكية.

الشبكات اللاسلكية تعمل على مدى محدود نسبيا، حيث يصل أقصى مدى تمتد إليه الشبكات العاملة بمعيار 802.11b داخل مكان مغلق إلي ٤٥-٩٠ متر وربما يصل مدي الشبكات اللاسلكية في الهواء الطلق إلي مسافة ٣٠٠ متر، لكن مرة أخري هذا يعتمد علي المكان والبيئة. ولكن هذه المسافة نظرية إلي حد ما ويرد عليها بعض القيود التى تقلصها إلي مسافة أقل من ٤٥-٩٠ متر والمثال على ذلك إذا كانت شبكة لاسلكية تحتوى على ثلاثة أجهزة محمولة الأول يعمل عليه عمر والثانى مخصص لشخص اسمه حمزة والثالث لشخص اسمه ميسرة افرض أن جهاز عمر يبعد عن جهاز حمزة بمسافة قدرها ٦٠ متر ويبعد جهاز حمزة عن جهاز ميسرة بمسافة قدرها ٦٠ متر أيضا فى الجهة المقابلة (انظر شكل ٢٧-١) فى هذه الحالة يمكن لجهاز حمزة الاتصال بنجاح بكل من عمر ، وميسرة، حيث تبعد المسافة بينه وبين كل منهما بمسافة قدرها ٦٠ متر. ولكن لا يمكن لكل من عمر و ميسرة الاتصال ببعضهما حيث تزيد المسافة بينهما عن ٩٠ متر وبالتالي يقعان خارج المدى المحدد للشبكة

شكل ٢٧-١ تغطية الشبكات اللاسلكية.

هناك قيد آخر على المدى الذى تصل إليه الشبكات اللاسلكية حيث يقل هذا المدى عمليا. يقل المدى الفعلى المخصص لبطاقة الشبكة اللاسلكية عن المدى المحدد نظريا بفعل بعض المعوقات التى تقع فى مدى الشبكة مثل الحوائط أو الأحوال الجوية السيئة أو تداخل الإشارات اللاسلكية مع إشارات التليفونات المحمولة ، والقيد الثالث الذى يعوق اتصال الشبكات اللاسلكية فى حدود الـــ ٩٠متراً. إذا كان الجهاز المعدنى الذى يقوم بإرسال واستقبال الإشارات الكهرومغناطيسية Antenna غير مضبوط جيدا.

من الجدير بالذكر أيضا أن سرعة الشبكات اللاسلكية تنخفض كلما زادت المسافة التى تغطيها مثلا . تعمل أجهزة الشبكة التى تعمل بمعيار **802.11b** بسرعة نظرية تصل إلي ١١ ميجابت فى الثانية **(11Mbps)**. ولكن الواقع يقول أن هذه السرعة تعمل فقط إذا كانت المسافة إلي حوالى ٤٥ متر فقط. أما إذا امتدت المسافة بين جهازين داخل الشبكة إلي ٩٠ متر فإن سرعتها تنخفض إلي ١ ميجابت فى الثانية **(1 Mbps)** إذا حاولت الاتصال من مسافة تتجاوز المدى المحدد للشبكة اللاسلكية وربما ينقطع الاتصال.

بطاقات الشبكة اللاسلكية

كما هو الحال فى الشبكات المحلية **LAN** والشبكات الموسعة **WAN** تحتاج الشبكات اللاسلكية إلي بطاقات شبكة. ولكنه يختلف عن ذلك المستخدم فى شبكات **LAN** حيث :

يلزم استخدام كارت شبكة لاسلكية **Network Interface Card (NIC)** لكل جهاز كمبيوتر متصل بشبكة لاسلكية حتى يتم الاتصال.

يوجد فى بطاقة الشبكة اللاسلكية جهاز معدنى لإرسال واستقبال الإشارات الكهرومغناطيسية بدلا من موصل الكابل فى خلف **NIC**. ورغم أن تكلفة بطاقة الشبكات اللاسلكية مرتفعة إلا أنها توفر ثمن الكابلات وتثبيتها.

توجد أنواع مختلفة من بطاقات الشبكة اللاسلكية، يمكنك اختيار ما يناسبك منها حسب متطلبات النظام نوع جهاز الكمبيوتر المستخدم.

وصل الشبكات اللاسلكية

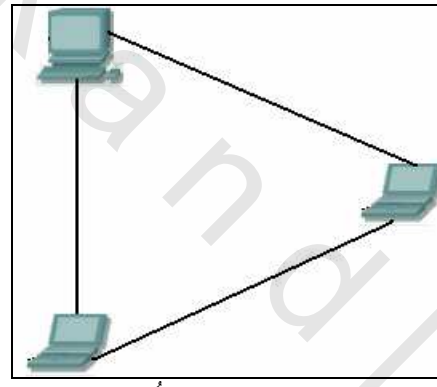
يتم الاتصال بين الأجهزة فى شبكات **LAN** باستخدام جهاز توصيل **HUB** أو مبدل **Switch**.

فى الشبكات اللاسلكية لايلزمك أى من هذين الجهازين، يكفى أن تشترى بطاقة شبكة لاسلكية لكل جهاز كمبيوتر مع وضع الأجهزة كلها فى مدى ٣٠٠ قدم من بعضها البعض.

أما إذا كان عندك شبكة سلكية وتريد إضافة أجهزة أخرى إلي الشبكة لاسلكيا، فيلزمك شراء موصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية، يستخدم لهذا الغرض جهاز

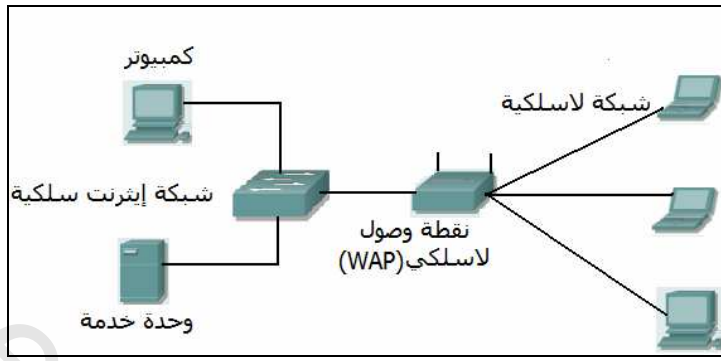
يسمى **Wireless Access Point** أو **WAP**. من هذا نفهم أن هناك طريقتان ممكنتان من الشبكات اللاسلكية. ويختلفان حسب الطريقة التي تتصل بها الأجهزة اللاسلكية ببعضها البعض علي النحو التالي:

الطريقة الأولي : وهي التشبيك المنشأ لغرض خاص ويعرف أيضاً بالتشبيك اللاسلكي نظير لنظير. كما هو مبين في شكل ٢٧-٢. وفي هذا الشكل توجد ثلاثة كمبيوترات لاسلكية تحتاج لإرسال بيانات إلي بعضها البعض. تسمي هذه الطريقة "مجموعة الخدمة الأساسية المستقلة" (**IBSS**). يستطيع كل كمبيوتر أن يتصل بكل الكمبيوترات اللاسلكية الأخرى مباشرة. ويمكنها أن تشارك ملفات وطابعات بهذه الطريقة ولكنها لا تستطيع الوصول إلي موارد شبكة **LAN** في حالة وجودها.



شكل ٢٧-٢ التشبيك اللاسلكي المُنشأ لغرض خاص

الطريقة الثانية : تتطلب هذه الطريقة من التوصيل نقطة وصول لاسلكي **Wireless Access Point** أو **WAP**. نقطة الوصول مطلوبة ليس فقط للسماح للكمبيوترات اللاسلكية بالاتصال ببعضها البعض، بل أيضاً للاتصال بشبكة سلكية كما هو مبين في شكل ٢٧-٣. معظم شبكات **WLAN** تعمل بهذه الطريقة. وتسمي هذه الطريقة "البنية التحتية" لأنها تتطلب وصولاً إلي شبكة **LAN** السلكية لاستعمال خدمات كالطابعات وخادمات الملفات.



شكل ٢٧–٣ التشبيك اللاسلكي ذو البنية التحية

يشتمل الشكل على شبكة سلكية تحتوى على جهازى كمبيوتر مرتبطين بواسطة سويتش ولأننا نرغب فى إضافة جهازى كمبيوتر محمول وجهاز آخر مكتبي **Desktop** إلي الشبكة اللاسلكية. قمنا بتوصيل جهاز السويتش بجهاز **WAP** الذى يتمكن بدوره من وصل الأجهزة اللاسلكية.

Wireless Access Point عبارة عن جهاز على شكل صندوق به جهاز معدن (أو جهازين) لإرسال واستقبال الإشارات الكهرومغناطيسية ومنفذ **RJ-45**. يتم ربط **WAP** بكابل الشبكة وإدخال الطرف الآخر من الكابل فى جهاز سويتش أو **hub** . وبذلك تتصل الشبكة اللاسلكية بأخرى سلكية.

التشبيك اللاسلكي

يشير المصطلح تشبيك لاسلكى (**Wireless Network**) إلي تقنية الراديو التي تّمكن كمبيوترين أو أكثر من الاتصال باستعمال بروتوكولات الشبكة القياسية ك **IP**، لكن من دون كبلات. تتطلب أجهزة التشبيك اللاسلكي استعمال تقنية تتعاطى مع ترددات الراديو وإرسال البيانات. المعيار القياسي الأكثر استعمالاً هو **802.11**، هذا هو المعيار القياسي الذي يعرف كل نواحي التشبيك اللاسلكي ذي تردد الراديو .

يحدد **802.11b** أن أجهزة الراديو تتكلم على النطاق **2.4** جيجاهرتز غير المرخص بسرعة إرسال تبلغ **11** ميجابت بالثانية في إحدى الأقنية الـ **15** الخاصة. تبحث بطاقات الشبكة اللاسلكية بين تلك الأقنية تلقائياً لإيجاد الشبكات **WLAN**، لذا لا حاجة لضبط

تكوين محطات العملاء عند أقنية معينة. عندما تجد بطاقة الشبكة القناة الصحيحة، تبدأ التكلم مع نقطة الوصول. طالما كانت كل إعدادات الأمان لدى العميل ونقطة الوصول متطابقة، يمكن أن تبدأ الاتصالات عبر نقطة الوصول، ويستطيع المستخدم أن يشارك كجزء من الشبكة.

802.11g هو معيار لاسلكي جديد مرتفع السرعة يتيح للمستخدمين إرسال البيانات بسرعات تصل إلي 54 ميجابت بالثانية – تقريباً خمس مرات أسرع من التقنية 802.11b لأن 802.11g يعمل في نطاق الترددات 2.4 جيجاهرتز فإنه متوافق كلياً مع 802.11b ومتوفر ليستعمل في جميع أنحاء العالم. حالياً، تدعم شركة أبل المعيار 802.11g في كل أجهزتها، وستلحقها سيسكو قريباً .

الشبكات اللاسلكية الكبرى

يمكن استخدام اثنين أو أكثر من Wireless Access Point (WAP) لإنشاء شبكة لاسلكية كبرى تسمح لمستخدميها بالتجوال من مكان لآخر مع استمرار إمكانية اتصالهم بالشبكة. والفكرة أن المستخدم عندما ينتقل خارج المدى المخصص لـــ WAP تلتقطه WAP أخرى وتحل محل WAP الأولى بدون أن تنقطع خدمة الاتصال المتاحة للمستخدم.

لإعداد اثنين أو أكثر من WAP ولكى تتحقق خاصية التجوال يجب تحديد مواقع WAPs بدقة بحيث تقع كل المسافة التى ترغب فى مد خدمة التجوال إليها فى المدى المحدد لواحد على الأقل من WAP . لابد أن تتأكد أن جميع أجهزة الكمبيوتر و WAPs تستخدم نفس SSID ونفس قناة الاتصال.

اتصال أكثر من شبكة

افرض أن شركتك تستخدم شبكتين منفصلتين فى مكانين مختلفين بنفس المبنى. وأنه يصعب الربط بينهما بكابلات. الحل الأمثل فى هذه الحالة هو استخدام اثنين من Wireless Access Point لإنشاء ما يسمى بقنطرة لاسلكية (جهاز وصل لاسلكى) بين الشبكتين. وصَّل أحد WAPs بالشبكة الأولى والآخر بالشبكة الثانية. ثم قم بتوصيل كلا من WAPs لاستخدام نفس SSID ونفس قناة الاتصال.

التهديدات اللاسلكية

تأتي التهديدات اللاسلكية بكل الأشكال والأحجام، من شخص يرتبط بنقطة وصولك اللاسلكي من دون ترخيص، إلي التقاط رزم من الهواء وفك تشفيرها من خلال شمام رزم "Packet Sniffer" . لا يملك الكثير من المستخدمين اللاسلكيين أي فكرة عن أنواع الأخطار التي تواجههم بمجرد ربطهم نقطة وصول لاسلكي بشبكتهم السلكية. نوضح فيما يلي التهديدات الأكثر شيوعاً عند إضافة مكون لاسلكي إلي شبكتك.

الطبيعة الجوية لإرسالات الشبكة WLAN تعرض شبكتك للمقتحمين والهجمات التي يمكن أن تأتي من أى اتجاه. تسافر حركة مرور الشبكة WLAN على موجات الراديو التي لا تستطيع جدران المباني أن تكبحها كلياً. رغم أن الموظفين قد يتمتعون بالعمل على كمبيوتراتهم المحمولة من مكان طبيعي خارج المبنى، إلا أنه بإمكان المقتحمين والقراصنة الوصول إلي الشبكة من موقف السيارات أو من الشارع باستعمال هوائي علبة البرينجلز.

كيف يتم اختراق الشبكة اللاسلكية

لا يلزم فى حالة الشبكات اللاسلكية أن ينجح المخرب في الوصول إلي جهاز الكمبيوتر فى شركتك حتى يخترق الشبكة ، حيث يمكن التسلل إلي الشبكات من خلال وسيلة تعرف بـــــ"التوجيه اللاسلكي ".وفكرة التوجيه اللاسلكي تتلخص فى استخدام جهاز كمبيوتر محمول لاسلكي للبحث عن شبكات لاسلكية غير مؤمنة والاتصال بها .

يجهز الهاكرز أجهزتهم بهوائيات لاسلكية خارجية لتسهيل مهمة الحصول علي النقاط الفعالة اللاسلكية ويلجأون في الغالب الي استخدام جهاز يدوي يسمي Global Positioning System او GPS وتعني (نظام تحديد مواضع عامة) لمساعدتهم في تعيين الحدود الفعلية للنقط الفعالة .

بمجرد إيجاد نقطة فعالة لاسلكية غير مؤمنة ، يستطيع الهاكرز الوصول مجاناً إلي الانترنت . بل أنهم يقومون أكثر من ذلك بإرسال معلومات عن النقاط الفعالة الي غيرهم من المخربين الذي يستخدمون التوجيه اللاسلكي من خلال بعض المواقع علي الويب .

بل إن الأمر يصل بالبعض منهم إلي التجوال بسيارتهم في المدينة ومعهم أجهزتهم المحمولة بحثاً

عن أي اتصال مفتوح بشبكة لاسلكية .

يستخدم الهاكرز مصطلح **War driving** للإشارة إلي أدوات اختراق الشبكات اللاسلكية . إذا بحثت عن كلمة **War Driving** باستخدام احد محركات البحث، ستجد الكثير من المواقع تحتوي علي عدد كبير من الأدوات للتسلل علي الاتصالات اللاسلكية . ولكن ليس بالضرورة أن يقتحم المخربون أو "الهاكرز" الشبكات اللاسلكية بواسطة التوجيه اللاسلكي. إن الأمر أصبح أسهل من ذلك بكثير لأن الاتصال اللاسلكي عبارة عن بث علي موجات الراديو، ولذلك فبإمكان الأشخاص الذي يتنصتون علي الإرسالات اللاسلكية أن يلتقطوا الرسائل غير المشفرة بسهولة. وهذا خلافاً لشبكات **LAN** السلكية. في الحقيقة أن مستخدم شبكة **WLAN** ليس محصوراً بالمنطقة الجغرافية للشركة، أو بنقطة وصول واحدة. يمكن أن يمتد نطاق شبكة **WLAN** إلي خارج الحدود الجغرافية للمكتب أو المبني، مما يسمح للمستخدمين غير المرخص لهم بالوصول من مكان عام أو من غرفة مكتب مجاور. المخرب الذي يستهدف نقطة **WAP** غير محمية، يحتاج فقط أن يتواجد إلي جوار الهدف، ولم يعد اليوم إلزامياً أن يمتلك مهارات متخصصة أو التوجيه اللاسلكي لكي يقتحم الشبكة. كثيراً ما تجد في الشبكات اللاسلكية لأحد أمرين:

- شركة مجاورة لديها شبكة لاسلكية مفتوحة.
- مستخدم مجاور قد انضم إلي شبكة لاسلكية شغالة.

الاختراق بالتقاط الرزم

أفضل وسيلة لفحص البيانات التي تخرج عبر اتصال ايثرنت (سلكي أو لاسلكي) هي استخدام برنامج **Packet Sniffer** أو "شمام الرزم". وهو برنامج يتيح التقاط كل الرزم الخارجة عبر اتصال ايثرنت واحد أو عدة اتصالات لفحصها لاحقاً. تلك البرامج الشمامة تمسك الرزمة وتحللها، وتكشف حمولة البيانات المتواجدة فيها. توجد بعض برامج شمام الرزم مجانية مثل برنامج **Ethereal** ولأن الشبكة اللاسلكية لا ترسل أي شئ مشفر، ترسل البيانات كنص عادي. المهاجم الذي يملك شمام الرزم يستطيع الآن أن يسرق هوية المستخدم ويسجل دخوله إلي خادم البريد بصفته المستخدم المرخص له.

أظن أنك الآن وبعد أن قرأت عن التقاط الرزم، قد أحسست بالرعب عند معرفتك أن هناك شمامات متوفرة بسهولة للشبكات اللاسلكية وبعضها مجاني. تخيل مدي الخطورة إذا كنت تسجل دخولك إلي الميدان وتفحص حسابك المصرفي وما هو حجم الخسارة التي ستلحقك إذا أختطف أي من المخربين هذه المعلومات.

كيف نحمي الشبكة اللاسلكية

فيما يلي بعض الإرشادات التي قد تعينك علي حماية الشبكة اللاسلكية.

- تستخدم الشبكات اللاسلكية جهاز يسمي **Wireless Access Point** وتختصر هكذا **WAP** لوصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية الموجودة بالفعل . لذلك يجب عليك تنشيط سمة **Wired Equivalent Privacy** وتختصر **WEP** لجميع الأجهزة اللاسلكية في شبكتك . تعمل سمة **WEP** علي تأمين البيانات المنقولة في الشبكات اللاسلكية . ورغم أن هذه السمة لا توفر حماية تامة للبيانات إلا أنها تمنع محاولات التسلل المعتاد إلي الشبكة .
- تستخدم الشبكات اللاسلكية ما يعرف بـــ **Service Set Identifier** وتختصر هكذا **SSID** ومعناها (معرف محدد الخدمة) لتعريف الشبكة اللاسلكية . بعبارة أخري يستخدم كاسم للشبكة اللاسلكية . يتم الاتصال بنقاط الوصول للشبكة اللاسلكية عن طريق **SSID** بواسطة أجهزة كمبيوتر محمولة .

  يوصف كل مورد نقطة وصول نقاط الوصول الخاصة به باستخدام **SSID** افتراضي ويعرف الهاكرز ما هية معرفات **SSID** الافتراضية لمعظم نقاط الوصول للشبكة . لحماية شبكتك قم بتغيير القيم الافتراضية لـــ **SSID** .

  ولكننا ننصحك ألا تعول كثيراً علي تغيير **SSID** لأن التغيير لن يحمي الشبكة كثيرا.
- احذر من تثبيت أجهزة **Wireless Access Point** بخلاف تلك التي قمت بنفسك بتثبيتها على الشبكة. نظرا لانخفاض أسعار **WAP** وسهولة تثبيتها فقد يقوم أحد المستخدمين بتثبيت أحدها على الشبكة بدون إذن من مديرها. قد تعرض هذه الأجهزة الشبكة بالكامل للخطر .

- قم بتغيير جميع كلمات المرور الافتراضية، خاصية كلمات مرور **WAP** وحقوق دخول مدير الشبكة، وذلك لجميع وحدات الخدمة
- ترجع معظم حالات فشل الخطط التأمينية لأجهزة الكمبيوتر إلي استخدام كلمات مرور غير قوية.

ملخص الفصل

ألقينا نظرة علي الشبكات اللاسلكية باعتبارها حالياً من الخيارات الفعالة في مجال الشبكات لأنها تتطور بشكل هائل وتنخفض أسعار منتجاتها أيضا. شرحنا في هذا الفصل مزايا الشبكات اللاسلكية وفكرة عملها. شرحنا معيار **802.11** باعتباره المعيار القياسي للإرسال اللاسلكي في الشبكات اللاسلكية ، وتعرضنا لمجال تغطيتها.

شرحنا بعد ذلك بطاقة الشبكة اللاسلكية وكيفية وصل الشبكات اللاسلكية العادية أو الشبكات اللاسلكية الكبرى ، أخيراً شرحنا التهديدات التي تواجه الشبكات اللاسلكية وختمنا ببعض الإرشادات التي تعينك علي حماية الشبكة اللاسلكية .

تدريبات

١. ما هي العوامل التي تؤثر في المدي الفعلي المخصص لبطاقة الشبكة اللاسلكية عن المدي المحدد نظرياً؟

٢. صح أم خطأ

أ. لا تؤثر البيئة أو المكان علي مدي تغطية الشبكات اللاسلكية.

ب. المصطلح **Wi-Fi** مرادف لمصطلح الشبكات اللاسلكية.

ج. المدي الذي تغطيه الشبكات اللاسلكية ثابت في كل الأحوال والظروف.

د. لتوصيل أجهزة كمبيوتر إلي شبكة موجودة لاسلكياً، يلزمك شراء جهاز يسمي **WAP** .

٣. أذكر ثلاثة أسباب تدعوك لاقتناء شبكة لاسلكية .

٤. ما هو الاختلاف والتشابه بين المصطلح **802.11** والمصطلح **Wi – Fi** ؟

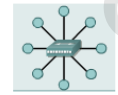
٥. أذكر أحد برامج شمام الرزم المجانية ؟

٦. صح أم خطأ

أ. الشبكات اللاسلكية محصنة أمام نفس أنواع هجمات الحرمان من الخدمة كالشبكة السلكية.

ب. الشبكات اللاسلكية سريعة التأثر بالهجمات التي تتدخل بإشارات الراديو كالتشويش.

ج. تغيير إعدادات SSID الافتراضية من حين لآخر يقلل من مخاطر التهديدات اللاسلكية .



الفصل الثامن والعشرون
الشبكات VPN

*إن أكثر موضوع تداولاً في أمان البيانات هذه الأيام ، الشبكات الخصوصية الوهمية (الشبكات **VPN**) وهي تقنية واعدة ومهمة جداً للشركات التي تسعي إلي تخفيض التكلفة وزيادة المرونة وقابلية التحجيم وضمان أمان اتصالاتها. بانتهاء هذا الفصل ستتعرف علي :*

- *استعمال الشبكات **VPN** وكيف تعمل.*
- *أنواع الشبكات **VPN**.*
- *فوائد الشبكات **VPN**.*
- *التشفير الذي يزوده **IPSec**.*
- *كيف تضمن **VPN** المحافظة علي أمان شبكتك.*
- *البروتوكولات المستخدمة خلال شبكة **VPN IPSec**.*

مقدمة

مع نمو حجم الاتصال وازدياد معدل التنقل الشخصي ، تزداد أيضاً الحاجة للشبكات من أجل التكيف وتزويد خدمات. لا يفهم المستخدمون الهموم الأمنية للخدمات البعيدة التي يتطلبونها للإنتاجية، المستخدمون الذين يسافرون إلي بلدان أخري، في المطارات ، مواقع العملاء...الخ . يلزمهم الاتصال بموارد الشركة لكي ينجزوا أعمالهم. مع المستويات المتزايدة لنوعية الاتصال من T1 واللاسلكي في المطارات ، إلي العملاء ذوي الاتصالات المرتفعة السرعة، يواجه المسئولون عن صيانة الشبكات السؤال التالي. كيف يجب عليهم تزويد المستخدمين بخدمات تكنولوجيا المعلومات المطلوبة، بغض النظر عن مكانهم، بأسلوب آمن ومعقول؟

والحل الرائد لهذه الطلبات هو "بروتوكول أمان بروتوكول الانترنت" (Internet Protocol Security Protocol) أو IPSec الملقّب بـــ "الشبكات الخصوصية الوهمية" (أو الشبكات VPN).

لكن ما الذي تفعله الشبكة VPN بالضبط، وكيف يمكنها أن تؤثر علي أعمال شركتك ؟ إن شعبية تقنية الشبكة VPN مرتبطة مباشرة بإمكانيتها علي إعطاء عائدات كبيرة علي الاستثمار للشركات التي تدفع التكاليف الباهظة في أغلب الأحيان للاتصالات الخصوصية عبر الخطوط المؤجرة ، عند نشر شبكات VPN لاستبدال تلك الاتصالات المكلفة يصبح التوفير في التكاليف كبيراً.

التقنيات التي تستبدلها الشبكات VPN في معظم الأحيان هي :

- تحل الشبكات VPN بين المواقع (Site – to – Site) محل الشبكات الواسعة (الشبكة WAN) المكلفة عن طريق استبدال خدمات الخط الخصوصية بالشبكات VPN التي تستعمل الانترنت بدلاً منها.
- تزيل أو تقلل الشبكات VPN للوصول عن بعد بشكل كبير تكاليف المكالمات الهاتفية البعيدة المسافة للاتصال بمندوبي المبيعات البعيدين أو المكاتب الصغيرة .

إذا كانت مؤسستك تستثمر مبالغ كبيرة بشكل متكرر إما علي الشبكة WAN أو علي

تكاليف المكالمات الهاتفية البعيدة المسافة ، فإن شبكة VPN يمكن أن تكون أسلوباً بديلاً ذي فائدة كبيرة بكلفة أقل ومرونة أكثر.

نظرة عامة على الشبكة VPN

الشبكة الخصوصية الوهمية (الشبكة VPN) هي اتصال شبكي مشفر يستعمل نفقاً آمناً بين نقاط نهاية عبر الانترنت أو شبكة أخري، كشبكة WAN. في الشبكة VPN تحل الاتصالات المحلية بمزود خدمة الانترنت (ISP) محل الاتصالات الهاتفية بالمستخدمين البعيدين أو اتصالات الخط المؤجر بالمواقع البعيدة.

السيطرة المتزايدة لاتصالات الانترنت العريضة النطاق بالمكاتب البعيدة الصغيرة بالمنازل تجعل استعمال الوصول الأرخص إلي الانترنت جذاباً. بعد الاستثمار الأوَّلي في الشبكات VPN ، تصبح تكلفة إضافة مزيد من المواقع أو المستخدمين صغيرة جداً.

تتيح الشبكات VPN لكل مستخدم بعيد لشبكتك بأن يتصل بأسلوب آمن وموثوق به باستعمال الانترنت كوسط للاتصال بشبكتك LAN الخصوصية. يمكن أن تنمو الشبكة VPN لتتسع مزيداً من المستخدمين وأماكن مختلفة بسهولة أكبر من الخط المؤجر. في الواقع، قابلية التحجيم هي ميزة رئيسية للشبكات VPN بالمقارنة مع الخطوط المؤجرة النموذجية. في حالة الخطوط المؤجرة تزداد التكلفة كلما زادت المسافة أما في الشبكة VPN فلا تهم الأماكن الجغرافية لكل مكتب .

تتيح الشبكة VPN تمديد شبكة انترانت خصوصية بأمان من خلال تشفير IPSec عبر الانترنت أو خدمة شبكة أخري، مما يسهل التجارة الالكترونية الآمنة واتصالات الاكسترانت مع الموظفين المتنقلين، والشركاء المهنيين والموردين والعملاء.

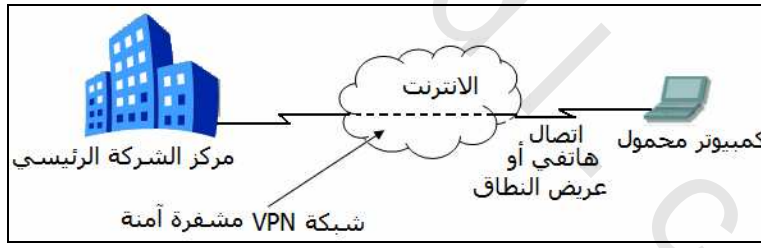
أنواع شبكات VPN

هناك ثلاثة أنواع رئيسية من الشبكات VPN

- الشبكات VPN للوصول عن بعد (Remote Access VPNs) :

تتيح للمستخدمين الهاتفيين الفرديين الاتصال بأمان بموقع مركزي عبر الانترنت أو

خدمة شبكة عمومية أخري. هذا النوع من الشبكات يتيح للموظفين الذين يحتاجون إلي الاتصال بشبكة الشركة من الخارج الاتصال بشبكة LAN . وهؤلاء تستعمل أنظمتهم برنامجاً خاصاً للشبكة VPN يسمح بإنشاء وصلة آمنة بينهم وبين شبكة الشركة. عادة، الشركة التي تريد إعداد شبكة VPN كبيرة للوصول عن بعد ستزود أحد أشكال حساب الانترنت الهاتفي للمستخدمين الذين يستعملون مزوداً. عندها، يستطيع المتصلون عن بعد أن يتصلوا برقم مجاني للوصول إلي الانترنت ويستعملوا برنامج شبكتهم VPN للوصول إلي شبكة الشركة. المثال الجيد عن شركة تحتاج إلي شبكة VPN للوصول عن بعد، شركة كبيرة فيها مئات مندوبي المبيعات في الأسواق. تسمي الشبكات VPN للوصول عن بعد أحياناً بـــ "الشبكات VPN البرمجية" أو "الشبكات الهاتفية الخصوصية الوهمية (VPDN)" أو "الشبكات VPN الهاتفية". يدفع المستخدمون "تكلفة ثابتة" منخفضة لمزود محلي باستعمال مكالمة محلية ولذا لا يتكبدون تكاليف المكالمات الدولية البعيدة المسافة ولا يضطرون إلي فتح مكالمة مباشرة دولية المسافة بمكتبهم في الشركة. يستطيع المستخدم عندها أن يستعمل اتصال المزود المحلي لإنشاء نفق VPN عبر الانترنت. يوضح الشكل ٢٨-١ هذا النوع من الشبكات.

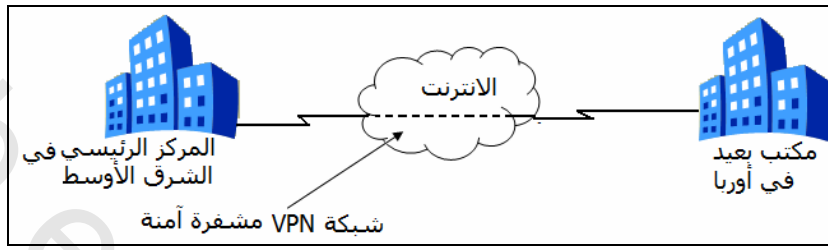


شكل ٢٨-١ شبكة VPN للاتصال عن بعد

- الشبكات VPN بين المواقع (Site – to Site)

تستعمل لتمديد شبكة LAN موجودة لشركة إلي أبنية ومواقع أخري من خلال استعمال معدات مكرسَّة، لكي يتمكن الموظفون البعيدون في تلك الأماكن من أن يستخدموا نفس خدمات الشبكة. تعتبر هذه الأنواع من الشبكات VPN متصلة بنشاط طوال الوقت. تسمي الشبكات VPN بين المواقع أحياناً بالانترنت، أو

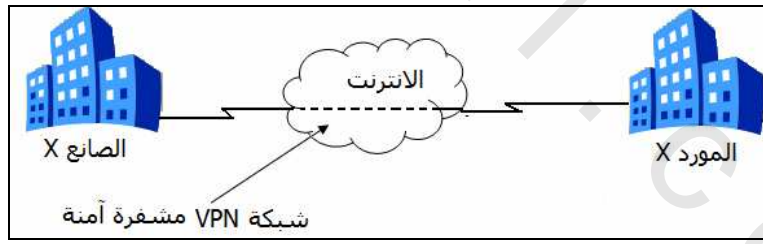
الشبكات VPN بين شبكات LAN . يوضح شكل ٢٨-٢ شبكات VPN بين المواقع.



شكل ٢٨-٢ شبكة VPN بين المواقع

- شبكات VPN الاكسترانت (Extranet VPNs)

تتيح إنشاء اتصالات آمنة مع الشركاء المهنيين والموردين والزبائن بهدف إجراء تجارة إلكترونية. شبكات VPN الاكسترانت هي الملحق لشبكات VPN الانترنت مع إضافة جدران النار لحماية الشبكة الداخلية. المثال الجيد هو شركات تعمل بشكل كثيف مع الموردين والشركاء لتحقيق أهداف مشتركة كعلاقات العرض والطلب مثلاً، عندما تحتاج شركة إلي موارد ويلبي المورد طلباتها. بالعمل عبر شبكة اكسترانت ، تستطيع تلك الشركتين أن تتشارك المعلومات بسرعة أكبر. يوضح شكل ٢٨-٣ شبكة VPN الاكسترانت.



شكل ٢٨-٣ شبكة VPN الاكسترانت

تهدف كل هذه الشبكات VPN إلي زيادة الثقة وتحسين الأداء وأمان لبيئات الشبكة WAN التقليدية باستعمال اتصالات مزودة أو خدمة أخري ذات تكلفة أقل ومرونة أكثر.

في الأشكال الثلاثة السابقة كل الشبكات VPN تستخدم الانترنت. يمكن استعمال تقنية الشبكة VPN أيضاً ضمن شبكتك لتزويد طبقة إضافية من الأمان للتحكم بالوصول إلي

المعلومات أو الأنظمة أو الموارد الحساسة. مثلاً، يمكن استعمال تقنية الشبكة VPN للحد من الوصول إلي الأنظمة المالية عند بعض المستخدمين أو لضمان إرسال المعلومات الحساسة أو السرية بطريقة آمنة . في هذا السيناريو ، بإمكان الشبكات VPN أن تشفر نقل البيانات إلي الأنظمة الحساسة وتحميها أكثر فأكثر.

فوائد وأهداف الشبكة VPN

يمكن إجمال فوائد تطبيق شبكة VPN في شبكتك فيما يلي :

- *تخفيض تكاليف الاتصالات*: قبل ظهور الشبكة VPN، كان الموظفون في الأماكن البعيدة يضطرون إلي إجراء مكالمات هاتفية بعيدة المسافة (دولية) للوصول إلي شبكة شركتهم. يمكن تخفيض تكاليف الاتصالات عن بعد نتيجة استبدال الاتصالات الهاتفية البعيدة المسافة باتصالات محلية بالانترنت التي يمكن من خلالها أن يستعمل المستخدمون شبكة VPN. بناء علي عدد الموظفين أو المندوبين في الأسواق، يمكن أن يشكل هذا لوحده وفراً كبيراً في التكلفة . بالنسبة للعديد من الشركات الصغيرة ذات الميزانية المحدودة، يمكن أن يشكل مزودو الشبكة VPN حلاً عملياً .
- *زيادة الإنتاجية* : زيادة إنتاجية المستخدمين بتمكينهم من الوصول إلي موارد الشبكة بأمان بعض النظر عن مكانهم الجغرافي.
- *تخفيض التكاليف التشغيلية* : المقترنة باتصالات الشبكة WAN المكرسة باستبدالها باتصالات مباشرة بالانترنت كالاتصال العريض النطاق الخاص بالشركات، الذي من خلاله ستتصل المواقع البعيدة عبر شبكة VPN بين المواقع.
- *تبسيط طوبولوجيا شبكتك* : بإضافة شبكات VPN استراتيجياً في كل أرجاء شبكتك.
- *زيادة الإيرادات*: باستعمال شبكات VPN، ستكسب عائدات أسرع علي الاستثمار من حل الشبكة WAN التقليدية .
- *تحقيق مرونة أكبر :* بسبب نشر الاستخدام المتنقل للكمبيوتر، والاتصال عن بُعد،

وتشبيك مكاتب الفروع، تجارة إلكترونية أسهل واتصالات اكسترانت مع الشركاء المهنيين ، وصول خارجي للموردين والعملاء إلي الانترنت، ووصول داخلي إلي الانترانت والاكسترانت يمكن تزويدها باستعمال اتصال آمن واحد.

- *إتاحة الفرصة للعمل في المنزل*: تخفيض تكاليف المكتب بجعل المستخدمين يعملون من منزلهم. للمستخدمين المنزليين عادة إنتاجية أعلي وضغوط أقل .

استراتيجيات تطبيق الشبكة VPN

بسبب عدم وجود معيار قياسي مقبول بشكل واسع لتطبيق الشبكة VPN، فقد طورت عدة شركات حلولاً جاهزة للعمل من تلقاء نفسها. نوضح فيما يلي بعض المكونات التي تتوفر من سيسكو، وكيف يمكن استعمال الأجهزة ذات الوظيفة الواحدة كجدران النار لتحقيق دور الشبكة VPN :

- *جدران النار* : إذا لم يكن لديك جدار نار قبل قراءة الفصل الخامس والعشرون "جدران النار" الأرجح أنه لديك واحد الآن. جدران النار حاسمة لأمان شبكتك. اليوم، كل جدران نار سيسكو تدعم دمج الشبكات VPN .
- *الموجهات القادرة علي VPN* : يمكن ترقية موجهات سيسكو لإعطائها القدرة علي استعمال الشبكات VPN .
- *مركّز الشبكة VPN* : (VPN Concentrator) جهاز دوره الوحيد في الشبكة هو السماح لشبكات VPN بالاتصال به، وبالتالي السماح للمستخدمين بالوصول إلي بقية موارد الشبكة ، يتم بناء مركزات VPN من سيسكو خصيصاً لإنشاء شبكات VPN لمستخدمي الوصول البعيد، التي تزود أداء مرتفعاً، وقابلية تحجيم، وتتضمن مكونات تدعي وحدات لمعالجة التشفير القابل للتحجيم (SEP)، التي تمكن مهندسي الشبكة من زيادة السعة والإنتاجية بسهولة.
- *برنامج العميل* : سهل نشره وتشغيله، ينشئ برنامج عميل VPN من سيسكو (أو Cisco VPN Client) أنفاقاً آمنة طرفاً لطرف إلي أجهزة الشبكة VPN المذكورة

هنا. هذا البرنامج المتوافق مع IPSec ذي التصميم الرفيع يمكن ضبط تكوينه مسبقاً لعمليات النشر الضخمة، وتتطلب تسجيلات الدخول الأولية تدخلاً قليلاً من المستخدم.

بناء علي نوع الشبكة VPN (للوصول عن بعد أو بين المواقع)، يجب أن تستعمل أجهزة معينة لكي تبني شبكتك VPN. لكن يجب أن تفكر بالأمور التالية أيضاً:

- *سهولة الإدارة* : سهولة إدارة الشبكة VPN تهتم بالجهد المطلوب للمحافظة بنجاح علي وصلة الشبكة المنشأة.
- *قابلية التحجيم* : مع نمو أعمال الشركة، وهذا ما يحصل غالباً، تنمو متطلباتها لتكنولوجيا المعلومات ايضاً. لتكبير البنية التحتية لشبكة VPN بسرعة وبشكل فعال من حيث التكلفة ، من المهم اختيار حل فيه قابلية تحجيم. فآخر شئ يريده مدير تكنولوجيا المعلومات هو البدء من الصفر واستبدال البنية التحتية لشبكة VPN بسبب وجود اختناق في احتمال نموها.

نظرة عامة علي شبكات IPSec الخصوصية الوهمية

لقد أصبح IPSec المعيار القياسي لإنشاء الشبكات VPN في عالم التشبيك. لقد طبقه كثير من الشركات ولأن فريق عمل هندسة الانترنت (IETF) قد عَّرف IPSec في مستند RFC فإن IPSec يعتبر أفضل خيار لبناء الشبكات VPN. يقدم IPSec وسيلة قياسية لإنشاء خدمات التحقق من الصحة والتشفير بين النظراء. لتبسيط هذه المناقشة، نظراء IPSec هم أجهزة تشكل كل طرف لنفق الشبكة VPN. يعمل IPSec في طبقة الشبكة للنموذج OSI المرجعي، فيحمي رزم IP ويتحقق من صحتها بين أجهزة IPSec المشاركة (النظراء) كموجهات أو جدران نار سيسكو. يزود IPSec خدمات أمان الشبكة التالية :

- سرية البيانات : يستطيع مرسل IPSec أن يشفر الرزم قبل إرسالها عبر شبكة. إذا لم يكن القرصان قادراً علي قراءة البيانات، لن تكون مفيدة له.
- سلامة البيانات : تتحقق نقطة نهاية IPSec المستلمة من صحة الرزم التي يرسلها

مرسل IPSec لضمان أنه لم يتم العبث بالبيانات خلال الإرسال.

- التحقق من أصل البيانات : يستطيع متلقي IPSec أن يتحقق من صحة مصدر رزم IPSec المرسلة. تعتمد هذه الخدمة علي خدمة سلامة البيانات.
- محاربة التكرار : يستطيع متلقي IPSec أن يكتشف ويرفض الرزم المتكررة.
- يحمي IPSec البيانات الحساسة التي تسافر عبر الشبكات غير المحمية، ويتم تزويد خدمات أمان IPSec في طبقة الشبكة (Network Layer). لذا لست مضطراً إلي ضبط تكوين محطات العمل أو الكمبيوترات أو البرامج الفردية. بإمكان هذه الفائدة أن تحقق توفيراً كبيراً في التكلفة .
- يزود IPSec ميزات أمان محسنة، كخوارزميات تشفير أفضل وتحقق شامل أكثر .
- بإمكان شبكات الشركات المتصلة بالانترنت أن تمكن وصول VPN آمن ومرن بواسطة IPSec.
- مع تقنية IPSec يستطيع العملاء الآن بناء شبكات VPN عبر الانترنت مع أمان حماية التشفير ضد اختراق السلك أو التصنت أو الهجمات الأخرى التي تتطفل علاي الاتصالات الخصوصية.

فقط الأنظمة المتوافقة مع IPSec يمكنها أن تستفيد من هذا البروتوكول. أيضاً، يجب أن تستعمل كل الأجهزة مفتاحاً مشتركاً، ويجب أن تملك جدران نار كل شبكة أساليب أمان ذات إعداد متشابه.

يزود IPSec خدمات التحقق من الصحة والتشفير لحماية البيانات من الإطلاع عليها أو تعديلها لغير المرخص لهم من أفراد شبكتك أو أثناء إرسالها عبر شبكة غير محمية، كالانترنت العمومية. يستطيع IPSec أن يشفر البيانات بين أجهزة مختلفة مثل :

- موجه إلي موجه.
- جدار نار إلي موجه.
- جدار نار إلي جدار نار.
- مستخدم إلي موجه.

- مستخدم إلي جدار نار.
- مستخدم إلي مركز الشبكة VPN.
- مستخدم إلي وحدة خدمة (Server)

التحقق من الصحة وسلامة البيانات

يمكن التحقق من صحة المستخدمين من خلال التحقق من هوية نقطتي نهاية الشبكة VPN والمستخدمين الذي يرسلون بياناتهم عبر الشبكة VPN. نقطة النهاية يمكن أن تكون عميل VPN أو مركّز VPN أو جدار نار أو موجهاً. التحقق من الصحة هي عملية IPSec التي تحدث بعد تشفير البيانات وقبل فك تشفيرها لدي الطرف المتلقي. إنها وظيفة ضرورية ضمن IPSec لضمان أن الجهة المرسلة والمتلقية هما حقاً صاحبتي الحق في البيانات.

سلامة البيانات هي وظيفة أخري ضمن IPSec، السلامة (Integrity) تعني أنه لم يتم العبث بالرزمة التي يستلمها الطرف المتلقي خلال إرسالها. يتم هذا من خلال استعمال خوارزمية معينة تسمي "بعثرة أحادية الاتجاه" .

تمرير البيانات عبر أنفاق Tunneling

الأنفاق هي ما تعتمد عليه الشبكات VPN لإنشاء شبكة خصوصية عبر الانترنت. مبدئياً، إنها عملية أخذ رزمة كاملة من البيانات وتغليفها ضمن رزمة أخري قبل إرسالها عبر شبكة. يجب أن تفهم الشبكة بروتوكول الرزمة الخارجية لدخول الشبكة والخروج منها.

شق الأنفاق المنقسم Split Tunneling

لا تتيح شبكات VPN التقليدية للمستخدمين الوصول إلي موارد الشبكة في قسمهم المحلي في نفس الوقت الذي يكونون فيه متصلين بشبكة VPN الخاصة بشركتهم. هذا الوضع يمثل مشكلة في بعض الحالات. مثلاً إذا أراد شخص الوصول إلي نظام من خلال شبكة VPN وفي نفس الوقت الطباعة علي الشبكة المحلية. لتصحيح هذه المشكلة المحتملة، ثم تقديم ميزة Split Tunneling أو شق الأنفاق.

يعمل شق الأنفاق بشكل جيد مع الشبكات VPN لأنه يمكنك استعمال بروتوكولات

ليست مدعومة علي الانترنت داخل رزمة IP، وسيظل بالإمكان إرسالها بأمان. في بداية إرسال نفقي VPN، يتم لف (أو تغليف) رزمة بيانات من الشبكة LAN المصدر بمعلومات رأس جديدة تتيح للشبكات الوسيطة أن تتعرف عليها وتسلمها. بعد أن يتم هذا ويكتمل الإرسال، يتم نزع "رأس" بروتوكولات شق الأنفاق، وتُرسل الرزمة الأصلية إلي الشبكة LAN الوجهة لتسليمها.

رغم أن شق الأنفاق يتيح نقل البيانات عبر شبكات الطرف الثالث، إلا أنه لوحده لا يضمن الخصوصية. لحماية إرسال نفقي من أي اعتراض أو تلاعب، يتم تشفير كل البيانات المنقولة عبر الشبكة VPN. بالإضافة إلي ذلك، تتضمن الشبكات VPN عادة ميزات إضافية، كجدران النار .

في الشبكات VPN بين المواقع، بروتوكول التغليف هو IPSec عادة أو تغليف التوجيه السائب (Generic Routing Encapsulation أو GRE). يتضمن GRE معلومات عن نوع الرزمة التي يتم تغليفها وعن الاتصال بين العميل ووحدة الخدمة. يعتمد الفرق علي مستوي الأمان المطلوب للاتصال، IPSec هو الأكثر أماناً و GRE له وظيفة أكبر. يستطيع IPSec أن يضع رزم IP في نفق ويشفرها، بينما يستطيع GRE أن يضع رزم IP ورزم غير IP في النفق. عندما تحتاج إلي إرسال رزم غير IP (كـ IPX) عبر النفق، يجب استعمال IPSec و GRE معاً.

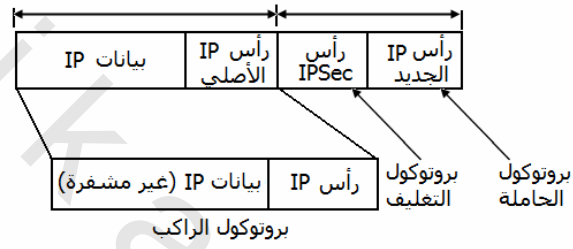
صيغ التشفير

لـ IPSec صيغتي تشفير : النفق (Tunnel) والإرسال (Transport). تختلف كل صيغة في طريقة تطبيقها وفي كمية العبء المضاف إلي رزمة البيانات الأصلية التي سيتم تشفيرها في شبكة VPN . سنلخّص صيغ العمل المختلفة هذه بإيجاز في أن النفق يشفر رأس الرزمة والحمولة لكل رزمة، بينما الإرسال يشفر الحمولة فقط.

صيغة النفق Tunneling

هذه هي الطريقة العادية التي يتم بها تطبيق IPSec بين جداري نار PIX (أو عّبارات أمان أخري) متصلين عبر شبكة غير موثوق بها، كالانترنت العمومية. كل المناقشات التي

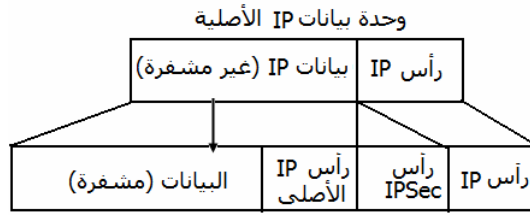
تستخدم IPSec ستكون علي صيغة النفق. صيغة النفق تغلف وتحمي رزمة IP كاملة. لأنها تغلف أو تخفي الرزم لكي يتم تمريرها بنجاح فإن موجهات التشفير نفسها تملك العناوين IP المستعملة في تلك الرؤوس الجديدة. يمكن استخدام صيغة النفق مع بروتوكول ESP أو بروتوكول AH أو مع كليهما (ستتعرف علي هذين البروتوكولين بعد قليل). يؤدي استعمال صيغة النفق إلي توسيع إضافي للرزمة بحوالي 20 بايت في رأس IP، يجب إضافة رأس IP جديد للرزمة مع رأس IP الجديد، كما هو مبين في الشكل ٢٨-٤.



شكل ٢٨-٤ صيغة النفق

صيغة الإرسال Transport

في صيغة الإرسال يتم تشفير الحمولة فقط وليس رزمة البيانات بأكملها. في صيغة النفق، يشفر IPSec الرزمة بأكملها ويكتب رأس IP جديداً في الرزمة، مما يحجب معلومات المصدر والوجهة الأصلية. صيغة النفق الأكثر أمناً بشكل متأصل من صيغة الإرسال (بسبب حقيقة أنه يتم تشفير الرزمة الأصلية بأكملها، وليس فقط الحمولة مثلما يحصل في صيغة الإرسال)، كما هو مبين في الشكل ٢٨-٥.



شكل ٢٨-٥ صيغة الإرسال

بروتوكولات IPSec

يستعمل **IPSec** ثلاثة بروتوكولات متممة تشكل عند استعمالها سوية هيكلاً متماسكاً وآمناً يرتكز علي معايير قياسية وملائماً مثالياً للشبكات **VPN**. البروتوكولات الثلاثة المشروحة في معايير **IPSec** القياسية هي :

- **Encapsulated Security Protocol** (أو **ESP**، بروتوكول الأمان المغلف) : يزود سرية وحماية البيانات مع تحقق اختياري للصحة وخدمات اكتشاف التكرار. يغلف **ESP** بيانات المستخدم كلياً. يمكن استعمال **ESP** إما لوحده أو إلي جانب **AH** .
- **Authentication Header** (أو **AH**، رأس التحقق من الصحة) : يزود تحققاً من الصحة وخدمات محاربة التكرار (اختياري). يزود **AH** خدمات لأجزاء محدودة من رأس **IP** والرأس الممدد، مضمَّن في البيانات المطلوب حمايتها (وحدة بيانات **IP** كاملة، مثلاً). يمكن استعمال **AH** إما لوحده أو مع **Encryption Service Payload** (أو **ESP**، حمولة خدمة التشفير) لقد حل **ESP** محل هذا البروتوكول إلي حد كبير ويعتبر استعماله مستنكراً.
- **Internet Security Association Key Management Protocol** (أو **ISAKMP**) "بروتوكول إدارة مفتاح اقتران أمان الانترنت" : يصف مرحلة التفاوض علي اتصال **IPSec** لإنشاء الشبكة **VPN**، يعرف البروتوكول **Oakley** طريقة إنشاء تبادل مفتاح تم التحقق من صحته.

ملخص الفصل

ناقش هذا الفصل استعمال الشبكات **VPN** ، كيف تعمل ، وما هي الفوائد التي تقدمها للشبكات في كل مكان التشفير الذي يزوده **IPSec**، وكيف تستطيع تلك التقنيات أن تضمن المحافظة علي أمان شبكتك وفي الوقت نفسه زيادة الخدمات المتوفرة لعملائك.

تدريبات

١. ما هي الأنواع الثلاثة لشبكات VPN؟

٢. أذكر ثلاثة مزايا لشبكة VPN؟

٣. ما هو الدور الذي يلعبه التحقق من الصحة في حماية تدفق البيانات؟

٤. في الشبكات VPN ما هي صيغتي التشفير ؟

٥. صح أم خطأ.

أ. الهدف من شبكة VPN هو الاتصال بالانترنت

ب. تسمح شبكات VPN بالاتصال عن بعد بالشبكة الرئيسية بأسلوب آمن وموثوق به .

ج. تتسم شبكة VPN بقابليتها للنمو بسهولة أكثر من الخطوط المؤجرة .

٦. متي يحصل شق الأنفاق المنقسم Split Tunneling ؟