طبقة ربط البيانات والشبكات المحلية

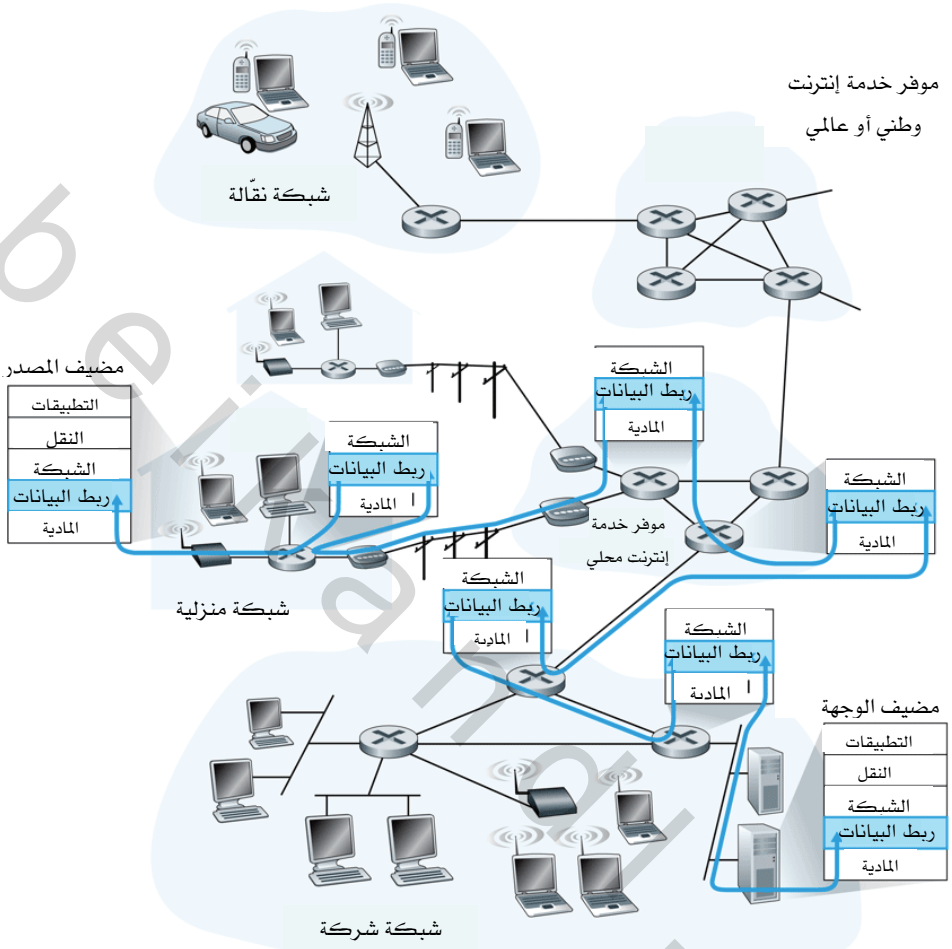
The Link Layer and Local Area Networks

محتويات الفصل:

- مقدمة عن طبقة ربط البيانات وخدماتها
- أساليب اكتشاف أخطاء البيانات وتصحيحها
- بروتوكولات الوصول المتعدد
- العنونة في طبقة ربط البيانات
- شبكة الإيثرنت
- محوّلات طبقة ربط البيانات
- بروتوكول نقطة إلى نقطة (PPP)
- الوصلة الافتراضية: الشبكة كطبقة ربط البيانات
- الخلاصة

في الفصل السابق عرفنا كيف تقوم طبقة الشبكة بتوفير خدمة اتصال بين مضيفين. كما هو موضح في الشكل 5-1 يتألف مسار الاتصال من سلسلة من الوصلات تبدأ من مضيف المصدر وتمر بسلسلة من الموجّهات حتى تنتهي إلى مضيف الوجهة. بينما نواصل المضي إلى أسفل عبر رصة البروتوكولات (أي من طبقة الشبكة إلى طبقة ربط البيانات)، من الطبيعي أن نتساءل كيف تُرسل الرزم عبر الوصلات المختلفة التي تكوّن مسار الاتصال من طرف إلى طرف؟. كيف يتم تغليف وحدات بيانات طبقة الشبكة في إطارات طبقة ربط البيانات تمهيداً لإرسالها على وصلة واحدة؟ هل بإمكان بروتوكولات طبقة ربط البيانات توفير نقل موثوق للبيانات من موجّه إلى موجّه؟ هل يمكن استخدام بروتوكولات مختلفة لطبقة ربط البيانات على طول مسار اتصالٍ ما؟ سنجيب على هذه الأسئلة وغيرها من الأسئلة المهمة في هذا الفصل.

في دراستنا لطبقة ربط البيانات سنجد أن هناك نوعين مختلفين بشكل جوهري من قنوات طبقة ربط البيانات. يضم النوع الأول قنوات الإذاعة (broadcast channels)، والتي توجد بكثرة في الشبكات المحلية (LANs)، والشبكات المحلية اللاسلكية، وشبكات الأقمار الصناعية، والشبكات الهجينة ذات الألياف الضوئية والكبلات المحورية (HFC). في هذا النوع من قنوات الإذاعة يوصّل العديد من المضيفات بنفس قناة الاتصال، ومن ثم يحتاج الأمر إلى ما يسمّى ببروتوكول الوصول للوسط لتنسيق عملية الإرسال على تلك القناة المشتركة ولتفادي الاصطدام بين الإطارات المُرسَلة. أما النوع الثاني من قنوات طبقة ربط البيانات فهو وصلة الاتصال من نقطة إلى نقطة، كما هو الحال بين موجّهين أو بين المودم والموجّه الخاص بموفر خدمة الإنترنت. واضح أن تنسيق الوصول إلى وصلة من نوع نقطة إلى نقطة تعتبر عملية سهلة، إلا أنه لا يزال هناك عدد من القضايا الهامة تتعلق بالتأطير، والنقل الموثوق للبيانات، واكتشاف الأخطاء، وضبط التدفق.



الشكل 5-1 طبقة ربط البيانات.

سنستكشف في هذا الفصل عدّة تقنيات مهمة لطبقة ربط البيانات. سنلقي نظرة متعمقة على شبكة الإيثرنت، والتي تعتبر إلى حد كبير التقنية الأكثر رواجاً وأهمية للشبكات المحلية، وسنتناول كذلك بروتوكول نقطة إلى نقطة (PPP)، وهو البروتوكول المفضل الذي تستخدمه المضيفات السكنية في الوصول للإنترنت عن طريق المودم.

رغم أن شبكة WiFi – والشبكات المحلية اللاسلكية على وجه العموم – تُعد بالتأكيد مواضيع ضمن طبقة ربط البيانات، إلا أننا لن نغطيها في هذا الفصل. ليس ذلك لعدم أهميتها، فثورة WiFi تغيّر بشكلٍ مثير الطريقة التي يدخل بها الناس على الإنترنت ويستعملونها، ولكننا سنغطي هذا الموضوع بعمق في الفصل السادس، والذي يركز على شبكات الحاسب اللاسلكية وقابلية الحركة.

5-1 مقدمة عن طبقة ربط البيانات وخدماتها

دعنا نبدأ ببعض المصطلحات المفيدة. ونرى أنه من الأسهل في هذا الفصل الإشارة إلى المضيفات والموجّهات ببساطة كعقد، حيث لن نكترث بشكلٍ خاص ـ كما سنبين بعد قليل ـ بما إذا كانت تلك العقدة مضيفاً أو موجّهاً. سنشير أيضاً إلى قنوات الاتصال التي تربط ما بين العقد المتجاورة على طول مسار الاتصال كوصلات. لكي يتم نقل وحدة بيانات من مضيف المصدر إلى مضيف الوجهة يجب أن تنتقل عبر كل الوصلات المختلفة كلٍّ على حدة على المسار من طرف إلى طرف. وعلى كل وصلة تقوم العقدة (التي عند أحد طرفي الوصلة) بتغليف وحدة البيانات في إطار طبقة ربط البيانات ثم ترسل الإطار عبر تلك الوصلة . تتلقّى عقدة الاستلام الإطار عند طرف الوصلة الآخر، ثم تقوم بدورها بانتزاع وحدة البيانات منه.

5-1-1 الخدمات التي توفرها طبقة ربط البيانات

يُستخدم بروتوكول طبقة ربط البيانات لنقل وحدات بيانات طبقة الشبكة على نفس الوصلة. يعرّف بروتوكول طبقة ربط البيانات صيغة الرزم التي يتم تبادلها بين العُقد الموجودة عند طرفي الوصلة، وكذلك الإجراءات التي تتخذها تلك العُقد عند إرسال واستلام الرزم. تذكّر أنه مرّ علينا في الفصل الأول أن رزم البيانات التي يتم تبادلها ضمن بروتوكول طبقة ربط البيانات يُطلق عليها إطارات، وأن كل إطار من إطارات طبقة ربط البيانات يغلّف في العادة وحدة بيانات لطبقة الشبكة. كما سنرى بعد قليل تتضمن الأعمال التي يقوم بها بروتوكول طبقة ربط البيانات عند إرسال واستلام الإطارات: اكتشاف أخطاء البيانات، وإعادة الإرسال، وضبط

التدفق، والوصول العشوائي. من أمثلة بروتوكولات طبقة ربط البيانات: بروتوكول الإيثرنت للشبكات المحلية، وبروتوكول 802.11 للشبكات المحلية اللاسلكية (والمعروفة أيضاً بـ WiFi)، وبروتوكول حلقة العلامة (token ring)، وبروتوكول نقطة إلى نقطة (PPP). وفي العديد من السياقات يمكن اعتبار بروتوكول نمط النقل غير المتزامن (ATM) بروتوكول طبقة وصلة أيضاً. سنغطي العديد من هذه البروتوكولات بالتفصيل في النصف الثاني من هذا الفصل.

في حين تضطلع طبقة الشبكة بمهمة نقل قطع بيانات طبقة النقل من طرف إلى طرف (أي من مضيف المصدر إلى مضيف الوجهة) عبر مسار الاتصال، تقتصر مهمة بروتوكول طبقة ربط البيانات على نقل وحدات بيانات طبقة الشبكة عبر كل وصلة على حدة من ذلك المسار (أي من عقدة إلى عقدة). من الخصائص المهمة لطبقة ربط البيانات أن وحدة البيانات يمكن أن تُنقل ببروتوكولات مختلفة لطبقة ربط البيانات على الوصلات المختلفة عبر المسار. فمثلاً قد تُنقل وحدة بيانات ببروتوكول الإيثرنت على الوصلة الأولى، وببروتوكول نقطة إلى نقطة (PPP) على الوصلة الأخيرة، وببروتوكول شبكة المناطق الواسعة (WAN) على الوصلات المتوسّطة. من المهم أيضاً ملاحظة أن البروتوكولات المختلفة لطبقة ربط البيانات قد توفر خدمات مختلفة. فعلى سبيل المثال توفر بعض تلك البروتوكولات توصيلاً موثوقاً للبيانات في حين لا توفر بروتوكولات أخرى ذلك، ولهذا يتعين أن تكون طبقة الشبكة قادرة على تحقيق مهمتها من طرفٍ إلى طرف في وجود مجموعة متباينة من خدمات طبقة ربط البيانات على الوصلات الفردية التي تكوّن مسار الاتصال الكلي.

لكي نفهم طبيعة طبقة ربط البيانات وعلاقتها بطبقة الشبكة، دعنا نتأمل المثال التالي من عالم السفريات. افترض أن وكيل سفريات يخطط لرحلة لأحد السياح من برينستون في نيو جيرسي إلى لوزان بسويسرا. افترض أنه قرر أنه من الملائم للسائح أن يركب سيارة من برينستون إلى مطار JFK بنيويورك، ثم طائرة من مطار JFK إلى مطار جنيف، وأخيراً قطاراً من مطار جنيف إلى محطة قطار لوزان. بعد قيام الوكيل بعمل الحجوزات الثلاثة، تكون مسؤولية شركة ليموزين

برينستون توصيل السائح من برينستون إلى JFK، ومسؤولية شركة الطيران توصيل السائح من JFK إلى جنيف، ومسؤولية مصلحة القطارات السويسرية توصيل السائح من جنيف إلى لوزان. تمثل كل مرحلة من الرحلة تلك انتقالاً "مباشراً" بين موقعين "متجاورين"، كما أن تلك المراحل تدار من قِبَل شركات مختلفة وتستخدم وسائل انتقال مختلفة تماماً (ليموزين، وطائرة، وقطار). ومع ذلك وبالرغم من أن أنماط النقل مختلفة، فإنها تقدم الخدمة الأساسية لنقل المسافرين من موقع إلى موقع آخر مجاور. في هذا المثال من عالم السفريات، يمثل السائح "وحدة بيانات"، بينما تمثل كل مرحلة من الرحلة "وصلة اتصال"، وكل نمط نقل يمثل "بروتوكول طبقة ربط البيانات"، في حين يقوم وكيل السفريات بدور "بروتوكول التوجيه".

رغم أن الخدمة الأساسية لطبقة ربط البيانات تنحصر في نقل وحدة البيانات من عقدة إلى عقدة مجاورة على وصلة اتصال واحدة، فإن تفاصيل الخدمة التي يتم توفيرها قد تتفاوت من بروتوكول لآخر في طبقة ربط البيانات. يمكن أن تتضمن الخدمات التي يوفرها بروتوكول طبقة ربط البيانات ما يلي:

- التأطير: تقوم كل بروتوكولات طبقة ربط البيانات تقريباً بتأطير كل وحدة بيانات من طبقة الشبكة ضمن إطار طبقة ربط البيانات قبل إرسالها على الوصلة. يتضمن الإطار حقل بيانات يتم فيه إدخال وحدة بيانات طبقة الشبكة، وعدداً من حقول الترويسة (header) في بدايته (ويمكن أن يتضمن الإطار حقولاً في نهايته أيضاً، غير أننا سنشير إلى كل هذه الحقول مجتمعةً على أنها "حقول الترويسة"). يحدد بروتوكول طبقة ربط البيانات هيكل الإطار، وسنرى عدة صيغ مختلفة للإطارات عند دراسة أمثلة محددة لبروتوكولات طبقة ربط البيانات في النصف الثاني من هذا الفصل.
- تنسيق الوصول للوصلة: يحدد بروتوكول التحكم في الوصول للوسط (medium access control (MAC)) القواعد التي تحكم عملية إرسال إطار على الوصلة. في حالة الوصلات من نقطة إلى نقطة حيث يوجد مُرسِل واحد على أحد طرفي الوصلة ومُستقبِل واحد على الطرف الآخر، يكون

بروتوكول MAC بسيطاً (أو غير موجود بالمرة) حيث يكون بوسع المُرسِل إرسال إطار في أي وقت تكون الوصلة فيه شاغرة (غير مستخدمة). أما الحالة الأكثر تشويقاً فهي عندما تشترك عدة عقد في وصلة إذاعة واحدة حيث نواجه مشكلة تُعرف بالوصول المتعدد للوصلة. في هذه الحالة يوفر بروتوكول MAC خدمة تنسيق عملية إرسال الإطارات من العديد من العقد، وسنغطي بروتوكولات MAC بالتفصيل في الجزء 5-3.

- التوصيل الموثوق للبيانات: عندما يوفر بروتوكول طبقة ربط البيانات خدمة توصيل موثوق، فإنه يضمن نقل كل وحدة بيانات لطبقة الشبكة عبر الوصلة بدون أخطاء. ولعلك تذكر أن بعض بروتوكولات طبقة النقل (كبروتوكول التحكم في الإرسال TCP) توفر هي الأخرى خدمة توصيل موثوق. كما في خدمة النقل الموثوق للبيانات بطبقة النقل، يتم توفير خدمة التوصيل الموثوق على مستوى طبقة ربط البيانات في أغلب الأحيان باستخدام إشعارات الاستلام وإعادة الإرسال (انظر الجزء 3-4). غالباً ما تستخدم خدمة طبقة ربط البيانات للتوصيل الموثوق على الوصلات التي تكون عرضة لمعدلات خطأ عالية في البيانات ـ كوصلات اللاسلكي ـ بهدف تصحيح الأخطاء التي تقع محلياً على الوصلة التى يحدث عليها الخطأ بدلاً من الالتجاء إلى إعادة إرسال البيانات من طرف إلى طرف عن طريق بروتوكولات طبقة النقل أو طبقة التطبيقات. ومع ذلك، فإن التوصيل الموثوق للبيانات على مستوى طبقة ربط البيانات قد يُعتبر عبئاً غير ضروري على الوصلات التي تمتاز بمعدلات خطأ منخفضة كالألياف الضوئية، والكبل المحوري، والعديد من وصلات أزواج الأسلاك النحاسية المجدولة. لهذا السبب فإن العديد من بروتوكولات طبقة ربط البيانات المستخدمة على الوصلات السلكية لا توفر خدمة توصيل موثوق بها.
- ضبط التدفق: تتوافر بالعقدتين على طرفي الوصلة سعة محدودة للتخزين المؤقت للإطارات، مما قد يؤدي إلى مشاكل محتملة. فقد تتلقى عقدة الاستقبال الإطارات بمعدل أسرع من المعدل الذي تستطيع معالجتها به، ولذا

قد يفيض المخزن المؤقت لدى المُستقبِل عند عدم توفر ضبط للتدفق مما يؤدي إلى فقد إطارات. كما هو الحال في طبقة النقل، يمكن أن يوفر بروتوكول طبقة ربط البيانات ضبطاً للتدفق لمنع عقدة الإرسال على أحد طرفي الوصلة من غمر عقدة الاستقبال على الطرف الآخر.

- اكتشاف الأخطاء: يمكن أن تقرر عقدة الاستقبال بشكلٍ خاطئ أن البت الذي استقبلته "0" بينما البت المُرسِل هو في الحقيقة "1"، والعكس بالعكس. تنشأ أخطاء البتات نتيجة اضمحلال الإشارة المُرسَلة واختلاطها بالضوضاء الكهرومغناطيسية. نظراً لأنه لا طائل من تمرير وحدة بيانات تتضمن خطأ في بتاتها، توفر العديد من بروتوكولات طبقة ربط البيانات آليات تمكّن المُستقبِل من اكتشاف وجود خطأ في بت واحد أو أكثر. لتحقيق ذلك تضيف عقدة الإرسال في الإطار مجموعة بتات خاصة باكتشاف الأخطاء، وفي المقابل تقوم عقدة الاستقبال بعملية فحص لاكتشاف وجود خطأ من عدمه. تعتبر آليات اكتشاف الأخطاء من الإمكانات المشهورة جداً في بروتوكولات طبقة ربط البيانات. ذكرنا في الفصلين الثالث والرابع أن كلاً من طبقتي النقل والشبكة توفر أيضاً إمكانيات محدودة لاكتشاف الأخطاء، كما في حالة المجموع التدقيقي (checksum) بالإنترنت. عادةً ما تكون وسائل اكتشاف الأخطاء في طبقة ربط البيانات أكثر تطوراً ويتم إنجازها في مكونات مادية (hardware) وليست برمجية (software).
- تصحيح الأخطاء: تشبه وسائل تصحيح الأخطاء وسائل اكتشاف الأخطاء، غير أن عقدة الاستقبال هنا لا تكتفي فقط باكتشاف ما إذا كانت هناك أخطاء في البتات قد طرأت على الإطار أثناء انتقاله ولكنها أيضاً تحدد بالضبط مواضع تلك الأخطاء في الإطار (ومن ثم يمكنها تصحيحها). بعض البروتوكولات (كبروتوكول نمط النقل غير المتزامن (ATM) توفر إمكانية لتصحيح الأخطاء في ترويسة الرزمة فقط وليس في الرزمة بكاملها. سنتناول اكتشاف وتصحيح الأخطاء في الجزء 5-2.

- اتصال مزدوج الإرسال في الاتجاهين (نصفي Half-duplex أو كامل Full-duplex): في حالة الإرسال المزدوج الكامل يمكن للعقدتين على طرفي الوصلة إرسال الرزم في نفس الوقت، وفي حالة الإرسال المزدوج النصفي لا تستطيع العقدة القيام بكلٍ من البث والاستقبال في نفس الوقت.

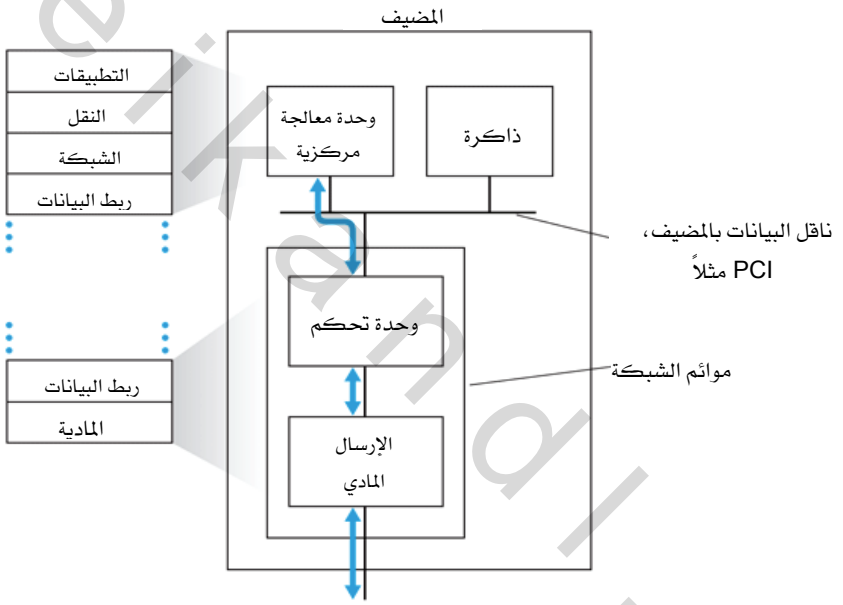
يتضح مما تقدم أعلاه أوجه الشبه القوية بين العديد من الخدمات التي توفرها طبقة ربط البيانات ونظيراتها من خدمات طبقة النقل. على سبيل المثال بوسع كلتا الطبقتين توفير توصيل موثوق للبيانات. ورغم تماثل الآليات المستخدمة في الطبقتين للحصول على ذلك التوصيل الموثوق (انظر الجزء 3-4)، فإن خدمتي التوصيل الموثوق في الحالتين ليستا واحدة. فبروتوكول النقل يوفر توصيلاً موثوقاً بين عمليتين على أساس من طرف إلى طرف، في حين يوفر بروتوكول طبقة ربط البيانات تلك الخدمة بين عقدتين متصلتين بوصلة واحدة. بنفس الطريقة يمكن أن توفر كلتا الطبقتين خدمات لضبط التدفق واكتشاف الأخطاء، ولكن ـ مرةً أخرى ـ يوفر بروتوكول النقل ضبط التدفق على أساس من طرف إلى طرف بينما يوفر بروتوكول طبقة ربط البيانات ذلك على أساس من عقدة إلى عقدة مجاورة فقط.

5-1-2 أين يُنفّذ بروتوكول طبقة ربط البيانات؟

قبل الخوض في دراستنا التفصيلية لطبقة ربط البيانات دعنا ننظر في مسألة المكان الذي يتم فيه إنجاز الوظائف والمهام المنوطة بتلك الطبقة. سنركّز هنا على نظام طرفي (حيث عرفنا في الفصل الرابع كيف تُضمّن وظائف طبقة ربط البيانات على الموجّه في بطاقة (كرت) الخط line card))، فهل يتم إنجاز طبقة ربط البيانات على مضيف بواسطة مكونات مادية أم برمجية؟ هل تنجز على كرت أو رقاقة مستقلة؟، وكيف تتواصل مع بقيّة المكونات المادية للمضيف والأجزاء المختلفة لنظام التشغيل؟

يبين الشكل 5-2 مخططاً لبنية معمارية نمطية لمضيف. يتم إنجاز الجزء الأكبر من طبقة ربط البيانات في بطاقة التوصيل بالشبكة، والتي تُعرف أحياناً ببطاقة واجهة الشبكة (Network Interface Card (NIC)). تقبع وحدة التحكم

التي تؤدي مهام طبقة ربط البيانات في قلب بطاقة التوصيل بالشبكة، وعادةً ما تأخذ شكل رقاقة واحدة مصممة خصيصاً للقيام بالعديد من وظائف طبقة ربط البيانات (التأطير، الوصول للوصلة، ضبط التدفق، اكتشاف الأخطاء، إلخ)، والتي تعرّفنا عليها في الجزء السابق. وعليه فإن الجزء الأكبر من وظائف وحدة التحكم الخاصة بطبقة ربط البيانات يتم تنفيذها داخل مكونات مادية.



الشكل 5-2 بطاقة مواءمة الشبكة: علاقتها بمكونات المضيف الأخرى وبوظائف رصة البروتوكولات.

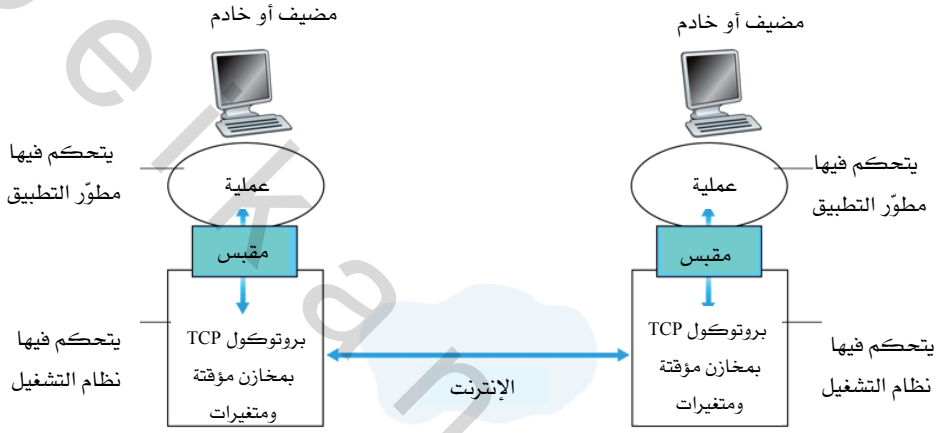
على سبيل المثال تحقق وحدة التحكم طراز 8254x من Intel [Intel 2006] بروتوكولات الإيثرنت التي سندرسها في الجزء 5-5، بينما تحقق وحدة التحكم طراز AR5006 من Atheros [Atheros 2006] بروتوكولات WiFi 802.11 التي سندرسها في الجزء 6-3. حتى أواخر التسعينيات كانت أكثر بطاقات المواءمة للشبكة مستقلةً مادياً (مثل بطاقة PCMCIA)، أو بطاقات تركّب في فتحة من فتحات التوسع القياسية في الحاسب الشخصي من نوع PCI مثلاً). أما الآن فيتم دمج

عددٍ متزايدٍ من بطاقات المواءمة للشبكة على اللوحة الأم (motherboard) للمضيف، ومن ثم الحصول على ترتيبة يطلق عليها LAN-on-motherboard (شبكة محلية على اللوحة الأم).

على جانب الإرسال: تأخذ وحدة التحكم رزمة البيانات التي أنشأتها الطبقات الأعلى من رصة البروتوكولات وخزّنتها في ذاكرة المضيف، وتغلفها في إطار طبقة ربط البيانات (بملء حقول الإطار المختلفة) ثم تقوم بعد ذلك ببث الإطار على الوصلة تبعاً للبروتوكول المستخدم للوصول للوصلة. على جانب الاستقبال: تستلم وحدة التحكم إطار طبقة ربط البيانات كاملاً، وتستخرج منه رزمة بيانات طبقة الشبكة. إذا كانت طبقة ربط البيانات تؤدي وظيفة اكتشاف الأخطاء، فإن وحدة التحكم على المُرسِل هي التي تضيف بتات اكتشاف الأخطاء في ترويسة الإطار، بينما تقوم وحدة التحكم على المُستقبِل بعملية الفحص لاكتشاف الأخطاء. أما إذا كانت طبقة ربط البيانات تتضمن ضبطاً للتدفق، فإن وحدتي التحكم على كلٍّ من المُرسِل والمُستقبِل تتبادلان رسائل تتضمن معلومات خاصة بضبط التدفق بحيث يقوم المُرسِل بإرسال الإطارات بمعدل يستطيع المُستقبِل التعامل معه.

يبين الشكل 5-2 بطاقة مواءمة للشبكة موصلة بناقل البيانات على مضيف (مثلاً ناقل البيانات (data bus) من نوع PCI أو PCI-X) حيث تبدو للمكونات الأخرى للحاسب المضيف كأي أداة أخرى على الناقل لإدخال وإخراج البيانات. كما يبين الشكل 5-2 أيضاً أنه رغم أن معظم وظائف بروتوكول طبقة ربط البيانات يتم إنجازها على مكونات مادية على بطاقة المواءمة إلا أن جزءاً من ذلك البروتوكول يجري تنفيذه من خلال برمجيات يتم تشغيلها على وحدة المعالجة المركزية للمضيف. تقوم الأجزاء البرمجية من طبقة ربط البيانات عادةً بتنفيذ الوظائف بالمستوى الأعلى من الطبقة كاستلام وحدة البيانات من طبقة الشبكة، وتجميع معلومات العنونة الخاصة بطبقة ربط البيانات، وتفعيل وحدة التحكم. على جانب المُستقبِل: تستجيب برمجيات طبقة ربط البيانات لإشارات المقاطعة (interrupts) التي تولدها وحدة التحكم (مثلاً عند استلام إطار أو أكثر) حيث تقوم بالتعامل مع حالات حدوث الخطأ، وتقوم بتمرير وحدة البيانات التي يتم

استلامها إلى طبقة الشبكة. وهكذا فإن طبقة ربط البيانات تمثل تشكيلة من المكونات المادية والبرمجية؛ إنها بمثابة المكان في رصة البروتوكول الذي تلتقي فيه المكونات المادية بالبرمجيات. يتضمن المرجع [Intel 2006] نظرةً عامّةً سهلة القراءة (مع وصف تفصيلي) لوحدة التحكم Intel طراز 8254 x من وجهة نظر برمجية.



الشكل 5-3 الاتصال بين بطاقات المواءمة: تغلّف رزمة بيانات طبقة الشبكة ضمن إطار طبقة ربط البيانات قبل إرسالها على الطبقة المادية.

يبين الشكل 5-3 بطاقات المواءمة للمُرسِل والمُستقبِل. لمّا كانت الوظائف الرئيسة لبروتوكول طبقة ربط البيانات تقوم بها وحدة التحكم، فإن بطاقات المواءمة تعتبر وحدات شبه ذاتية وظيفتها نقل إطار من بطاقة إلى أخرى. قام عدد من الباحثين بدراسة إمكانية نقل المزيد من الوظائف الأخرى (فيما وراء معالجة طبقة ربط البيانات) إلى بطاقات المواءمة للشبكة. فمثلاً بوسع وحدة التحكم طراز 8254x حساب المجموع التدقيقي (checksum) لقطع بيانات TCP/UDP ولترويسة وحدة بيانات IP – أي استخدام المكونات المادية (وحدة التحكم بطبقة ربط البيانات) لأداء وظائف تتبع طبقتي الشبكة والنقل. رغم أن هذا قد يبدو انتهاكاً صارخاً لمبدأ طبقية رصة البروتوكولات إلا أنه يحقق فائدة، فالمكونات المادية

يمكنها حساب المجموع التدقيقي أسرع بكثير من البرامج. يتضمن المرجع [Mogul 2003] مناقشة شائقة لفوائد ومضار القيام بعمليات المعالجة الخاصة ببروتوكول التحكم في الإرسال (TCP) على بطاقات المواءمة.

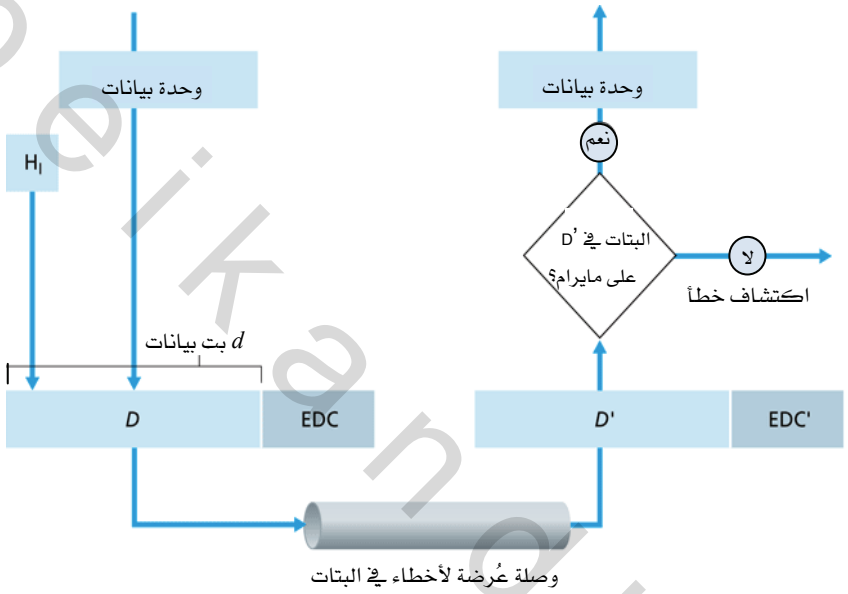
أما [Kim 2005] فينظر في إمكانية أداء وظائف طبقات أعلى حتى من ذلك على بطاقات المواءمة (مثل HTTP caching أي تخزين نسخة من ملفات HTTP المستخدمة بكثرة في الذاكرة المخبأة).

2-5 أساليب اكتشاف أخطاء البيانات وتصحيحها

في الفصل السابق ذكرنا أن اكتشاف وتصحيح أخطاء البيانات على مستوى البتات هما خدمتان توفرهما غالباً طبقة ربط البيانات، وذلك لاكتشاف وإصلاح أخطاء البتات التي يتكون منها إطار طبقة ربط البيانات أثناء انتقاله من عقدة إلى عقدة أخرى مجاورة تتصل بها عبر وسط مادي. رأينا في الفصل الثالث أن خدمات اكتشاف الأخطاء وتصحيحها يتم توفيرها في أغلب الأحيان في طبقة النقل أيضاً. في هذا الجزء سندرس بعض الأساليب البسيطة المستخدمة لاكتشاف – وفي بعض الأحيان تصحيح – مثل تلك الأخطاء. هناك العديد من الكتب الدراسية المخصصة لمعالجة نظرية وتطبيق هذا الموضوع بالكامل (على سبيل المثال [Schwartz 1980] أو [Bertsekas 1991]). ستكون معالجتنا للموضوع هنا مختصرة بالضرورة حيث نهدف لتطوير مفهوم بدهي للإمكانات التي توفرها أساليب اكتشاف وتصحيح الأخطاء، وتوضيح كيف تفي بعض الأساليب البسيطة بهذا الغرض وتُستخدم فعلياً في طبقة ربط البيانات.

يوضح الشكل 5-4 الإطار العام لدراستنا للموضوع. في عقدة الإرسال يُلحَق بالبيانات D المعدّة للإرسال والمطلوب حمايتها من تأثير الأخطاء مجموعة بتات خاصة باكتشاف وتصحيح الأخطاء (EDC). لا تقتصر البيانات المطلوب حمايتها عادةً على وحدة البيانات التي دفعت بها طبقة الشبكة لنقلها عبر الوصلة، ولكنها تتضمن أيضاً معلومات العنونة والأرقام التسلسلية والحقول الأخرى في ترويسة إطار بيانات طبقة ربط البيانات. يتم إرسال كلٍّ من D وEDC إلى عقدة الاستقبال ضمن

إطار طبقة ربط البيانات. في عقدة الاستقبال يتم استلام D' و'EDC. لاحظ أن كلاً من D' و'EDC قد يختلفان عن البيانات الأصلية D وEDC نتيجةً للأخطاء التي تنتج من تغيير بعض البتات (من 1 إلى 0 أو العكس) أثناء انتقال الإطار عبر الوصلة.



الشكل 5-4 سيناريو اكتشاف وتصحيح الأخطاء.

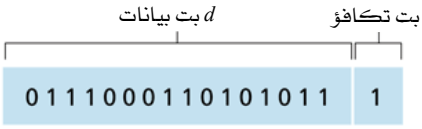
يكمن التحدي الذي يواجهه المُستقبِل في تحديد ما إذا كانت البيانات المستلَمة D' هي نفسها البيانات الأصلية المُرسَلة D، علماً بأنه لم يتلقّ سوى D' و'EDC. من المهم ملاحظة التعبير الدقيق لقرار المُستقبِل في الشكل 5-4 (نسأل عما إذا كنا قد اكتشفنا وجود خطأ، وليس عما إذا كان هناك خطأ قد حدث فعلاً!). فأساليب اكتشاف الأخطاء وتصحيحها تمكّن المُستقبِل أحياناً – ولكن ليس دائماً! – من اكتشاف حدوث أخطاء في البتات. حتى باستعمال بتات لاكتشاف الأخطاء فقد تبقى هناك أخطاء في البتات لا يتسنى اكتشافها (بمعنى أن المُستقبِل مع ذلك قد لايدرك أن البيانات المستلَمة فيها بتات خاطئة). ولذا فقد يُسلّم المُستقبِل وحدة بيانات غير صحيحة إلى طبقة الشبكة، أو يفوته أن محتويات

أحد حقول ترويسة إطار البيانات فيها خطأ. ومن ثم فإن هدفنا هنا هو اختيار نظام لاكتشاف الأخطاء يقلل إلى درجة مقبولة من احتمال مرور الأخطاء دون ملاحظتها. عموماً تتطلب أساليب اكتشاف الأخطاء وتصحيحها الأكثر تطوراً (أي التي تضمن احتمالاً ضئيلاً لبقاء أخطاء في البتات بدون اكتشاف) أعباءً إضافية أكثر تتمثل في إمكانيات الحساب اللازمة وعدد البتات الإضافية التي ترسل خصيصاً لغرض اكتشاف الأخطاء وتصحيحها.

دعنا الآن نفحص ثلاثة أساليب لاكتشاف الأخطاء في البيانات المُرسَلة: أسلوب فحص التكافؤ (parity check) لتوضيح المبادئ الأساسية وراء اكتشاف الأخطاء وتصحيحها، وأسلوب الفحص بالجمع (checksum) والمستخدم عادةً في طبقة النقل، وأسلوب فحص الفائض الدوري ((Cyclic Redundancy Check (CRC) والمستخدَم عادةً في طبقة ربط البيانات المحققة في بطاقات مواءمة الشبكة.

5-2-1 فحص التكافؤ (Parity Check)

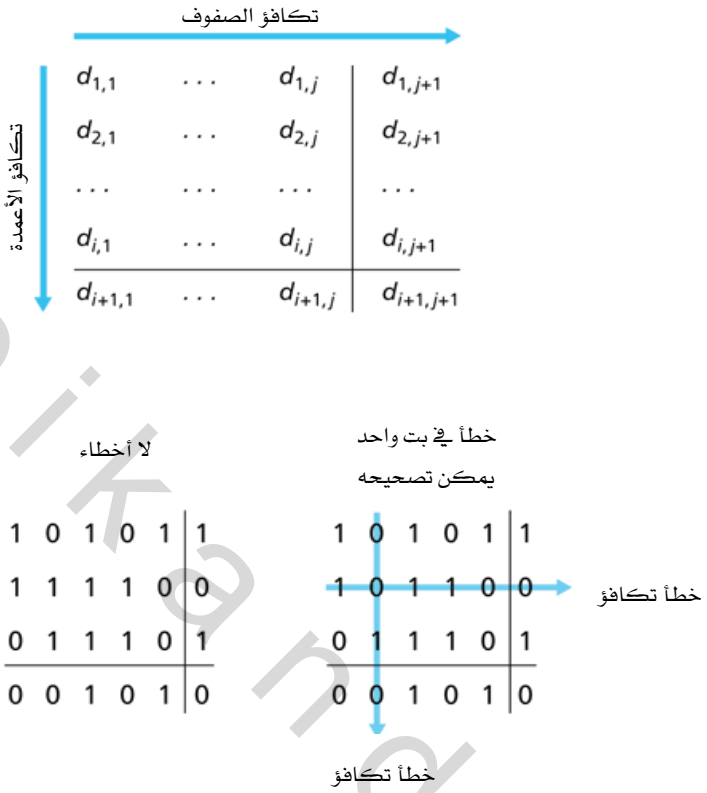
لعل أبسط أشكال اكتشاف الأخطاء هو استخدام بت واحد للتكافؤ. افترض أن وحدة البيانات المطلوب إرسالها في الشكل 5-5 هي D، والتي تتألف من بتات عددها d. في نظامٍ يستخدم فحص التكافؤ الزوجي يضيف المُرسِل بتاً واحداً ويختار قيمتها ببساطة بحيث يكون عدد البتات التي قيمتها 1 ضمن العدد الكلي للبتات $d + 1$ (أي بتات البيانات الأصلية علاوة على البت الإضافي للتكافؤ) عدداً زوجياً. أما في أنظمة فحص التكافؤ الفردي فيتم اختيار قيمة بت التكافؤ بحيث يكون العدد الكلي للبتات التي قيمتها 1 فردياً. يوضح الشكل 5-5 نظام فحص التكافؤ الزوجي حيث يتم تخزين بت التكافؤ الوحيد في حقل مستقل.



الشكل 5-5 تكافؤ زوجي ببت واحد.

باستخدام بت واحد للتكافؤ تكون عملية الفحص في المُستقبِل بسيطةً كذلك، حيث يحتاج المُستقبِل فقط لأن يعد البتات التي قيمتها 1 في الرسالة الكلية التي تم استلامها بطول ($d + 1$) بت. فإذا وُجد في نظام لفحص التكافؤ الزوجي أن عدد تلك البتات فردي، فإن المُستقبِل يدرك أن خطأ ما قد طرأ في بت واحد على الأقل (وبتحديد أكثر يدرك أن عدداً فردياً من أخطاء البتات قد حدث). لكن ماذا لو حدث عدد زوجي من أخطاء البتات؟ عليك أن تقنع نفسك بأن ذلك سيؤدي إلى خطأ غير مكتشف. إذا كان احتمال حدوث خطأ في البت ضئيلاً وبافتراض أن أخطاء البتات تحدث بشكلٍ مستقل من بت إلى آخر، فإن احتمال حدوث أخطاء في عدة بتات في نفس الإطار يكون ضئيلاً جداً، وفي هذه الحالة قد يكفي بت تكافؤ واحد. ومع ذلك فقد أظهرت القياسات العملية أن أخطاء البتات لا تحدث فقط بشكلٍ مستقل، بل غالباً ما تحدث سويةً على شكل تجمّعات (دفقات) (bursts). عند حدوث أخطاء البتات على شكل تجمعات، يزداد احتمال الأخطاء غير المكتشفة في إطار بيانات محمي ببت تكافؤ واحدٍ ليقارب 50٪ [Spragins 1991]. واضح أننا بحاجة إلى أسلوب أكثر فعالية لاكتشاف الأخطاء. لحسن الحظ هذا الأسلوب موجود، بل ومستخدم عملياً! لكن قبل الانتقال لأساليب اكتشاف الأخطاء المستخدمة في الواقع، دعنا نتناول تعميماً بسيطاً لنظام بت التكافؤ الواحد والذي سيوضح لنا بعض الأمور فيما يتعلق بأساليب تصحيح الأخطاء.

يوضح الشكل 5-6 تعميماً في بعدين لنظام بت التكافؤ الواحد. في هذه الحالة تُقسّم البتات d التي تشكّل قطعة البيانات D المطلوب إرسالها إلى i صف وj عمود، ويتم حساب قيمة بت التكافؤ لكل صف ولكل عمود على حدة بالإضافة إلى حساب بت التكافؤ للقطعة D ككل. تشكّل بتات التكافؤ والتي عددها $i + j + 1$ بتات اكتشاف الأخطاء لإطار طبقة ربط البيانات.



الشكل 5-6 تكافؤ زوجي في بُعدين.

لنفترض الآن أن خطأً وقع في بت واحد من بتات البيانات الأصلية والتي عددها d. في هذا النظام ثنائي الأبعاد لفحص التكافؤ سينتج عن ذلك خطأ في تكافؤ كلٍّ من العمود والصف اللذين يحتويان على البت الذي انعكست حالته بسبب الخطأ. وبالتالي يكون بوسع المُستقبِل ليس فقط اكتشاف حدوث خطأ في بت واحد، ولكن أيضاً تحديد موقع ذلك البت بمعلومية موقعي العمود والصف اللذين أظهرا خطأ تكافؤ، ومن ثم تصحيح ذلك الخطأ! يبين الشكل 5-6 مثالاً فيه خطأ في البت الذي موقعه (2، 2) والذي قيمته الأصلية 1، وهو خطأ يمكن اكتشافه، بل وأيضاً تصحيحه عند المُستقبِل. رغم أن مناقشتنا السابقة تركزت على خطأ في بتات البيانات الأصلية التي عددها d، فإنه يمكن أيضاً اكتشاف وتصحيح خطأ

واحد في بتات التكافؤ الإضافية. بوسع نظام فحص التكافؤ ثنائي الأبعاد أيضاً أن يكتشف أي خطأين في إطار البيانات، ولكنه لا يصححها إلا إذا كانا في صفّين مختلفين وعمودين مختلفين. سيتم استكشاف الخواص الأخرى لنظام فحص التكافؤ ثنائي الأبعاد من خلال التمارين الموجودة في نهاية هذا الفصل.

يُطلق على اكتشاف وتصحيح الأخطاء بواسطة المُستقبل "التصحيح الأمامي للخطأ" (FEC)، ويُستخدم عموماً في تخزين وتشغيل الملفات السمعية كما في حالة الأقراص السمعية المدمجة. ويمكن في مجال الشبكات استخدام أساليب FEC منفردة أو بالاشتراك مع أساليب إعادة الإرسال التلقائي (ARQ) في طبقة ربط البيانات التي تشبه الأساليب التي درسناها في الفصل الثالث. تكمن أهمية أساليب FEC في كونها تقلل من كمية البيانات التي يحتاج المُرسِل لإعادة إرسالها نتيجة حدوث خطأ فيها، كما أنها تسمح بالتصحيح الفوري للأخطاء لدى المُستقبِل وبالتالي تجنب الانتظار لمدة رحلة الذهاب والإياب لتلقّي المُرسِل إشعار استلام سلبي من المُستقبِل، ووصول الإطار المعاد إرساله إليه. لهذه الميزة أهميتها الكبيرة بشكلٍ خاص في التطبيقات الفورية للشبكة [Rubenstein 1998]، ووصلات البيانات ذات تأخيرات الانتقال الطويلة (كوصلات الأقمار الصناعية). من الأبحاث التي تناولت استخدام أساليب FEC في بروتوكولات التحكم في الخطأ: [Biersack 1992; Nonnenmacher 1998؛ Byers 1998؛ Shacham 1990].

2-2-5 أساليب الفحص بالجمع (Checksum)

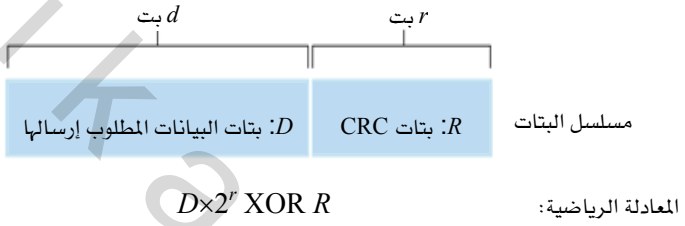
في أساليب الفحص بالجمع تُعتبر رسالة البيانات المكونة من d بت – كما في الشكل 5-5 – بمثابة سلسلة من الأعداد الصحيحة يتألف كلٌّ منها من k بتاً. يتضمن أحد الأساليب البسيطة للفحص جمع تلك الأعداد الصحيحة وإرسال حاصل الجمع الناتج كبتات اكتشاف الأخطاء. وتستخدم هذه الطريقة في الإنترنت حيث تُعدّ بايتات البيانات أعداداً صحيحة يتألف كلٌّ منها من 16 بتاً ويتم جمعها، ثم يُحسب مكمل الواحد (1's complement) لحاصل الجمع ويوضع في ترويسة قطعة البيانات (سنطلق على تلك البتات "المجموع التدقيقي"). كما بيّنا في الجزء 3-3 يقوم

المُستقبِل بإجراء نفس العملية على البيانات التي تم استلامها (بما في ذلك المجموع التدقيقي للبيانات المُرسِلة) لمعرفة ما إذا كانت البتات الناتجة كلها لها القيمة 0. فإذا كان أيٌّ من البتات الناتجة قيمته 1، فإن هذا يدل على وجود خطأ. يناقش طلب التعليقات RFC 1071 خوارزمية الفحص بالجمع في الإنترنت وتطبيقاتها بالتفصيل. يتم حساب المجموع التدقيقي في بروتوكولات TCP وUDP في الإنترنت باستخدام كل الحقول (بما في ذلك حقول البيانات والترويسة). أما في بروتوكول IP فيُحسَب المجموع التدقيقي من بتات ترويسة IP فقط (نظراً لأن كلاً من قطعتي TCP وUDP لهما المجموع التدقيقي الخاص بهما). في البروتوكولات الأخرى (على سبيل المثال بروتوكول XTP [Strayer 1992]) يتم حساب مجموع تدقيقي على الترويسة ومجموع تدقيقي آخر على القطعة بأكملها.

تمثّل أساليب الفحص بالجمع عبئاً إضافياً ضئيلاً نسبياً على قطع البيانات المُرسِلة. فعلى سبيل المثال يستخدم المجموع التدقيقي في بروتوكولي TCP وUDP 16 بتاً فقط. غير أنها توفر حماية ضعيفة نسبياً ضد الأخطاء مقارنةً بأسلوب فحص الفائض الدوري (CRC)، والذي سنتناوله لاحقاً والمستخدم غالباً في طبقة ربط البيانات. السؤال الذي يطرح نفسه الآن: لماذا يُستخدم الفحص بالجمع في طبقة النقل بينما يُستخدم أسلوب فحص الفائض الدوري في طبقة ربط البيانات؟ تذكّر أن طبقة النقل تنفّذ عادةً على شكل برامج تمثل جزءاً من نظام التشغيل على المضيف، لذا فمن المهم استخدام طريقة بسيطة وسريعة كالفحص بالجمع. في المقابل ينفّذ اكتشاف الأخطاء في طبقة ربط البيانات في مكونات مادية مخصّصة لذلك في بطاقات مواءمة الشبكة، والتي يمكنها أن تؤدّي العمليات الأكثر تعقيداً ضمن أسلوب فحص الفائض الدوري بسرعة. يعرض [Feldmeier 1995] أساليب برمجية سريعة لتنفيذ العديد من طرق اكتشاف الأخطاء منها الفحص بالجمع الموزون وفحص الفائض الدوري وغيرها.

3-2-5 فحص الفائض الدوري (CRC)

يعتمد أحد أساليب اكتشاف الأخطاء المستخدم بكثرة في شبكات الحاسب اليوم على شفرات فحص الفائض الدوري (CRC)، والتي تُعرف أيضاً بشفرات الدوال متعددة الحدود (polynomials) نظراً لأنه يمكن اعتبار سلسلة البتات المُرسِلة كدالة متعددة الحدود تكون معاملات الحدود فيها هي قيم البتات في السلسلة (0 أو 1) والعمليات على سلسلة البتات كعمليات رياضية على تلك الدوال.



الشكل 5-7 شفرات فحص الفائض الدوري (CRC).

تتلخص طريقة عمل شفرات CRC كالتالي: افترض أن عقدة الإرسال تريد بث قطعة بيانات D طولها d بت إلى عقدة الاستقبال. ينبغي أن يتفق المُرسِل والمُستقبِل بادئٍ ذي بدء على مسلسل بتات مكون من $r+1$ بت ويُعرف بالمولّد(generator)، ونرمز له بالرمز G. سنشترط أن تكون البت في أكبر خانة (أي الخانة في أقصى اليسار) في المولّد G هي 1 دائماً. يوضح الشكل 5-7 الفكرة الرئيسة لعمل أسلوب شفرات CRC. لكل قطعة بيانات D مطلوب إرسالها، يختار المُرسِل قطعة إضافية R طولها r بت، ويلحقها على يمين القطعة D بحيث تقبل القطعة الناتجة بطول $d + r$ بت (باعتبارها عدداً ثنائياً) القسمة بالضبط (أي بدون باقٍ) على المولّد G باستعمال حساب الباقي الثنائي (modulo-2 arithmetic). وبهذا تكون عملية التدقيق بحثاً عن الأخطاء بسيطة، حيث يَقسِم المُستقبِل القطعة التي استلمها بطول $d + r$ بت على المولّد G. فإذا وجد أن باقي القسمة ليس صفراً، يعرف

المُستقبِل إن خطأً ما قد طرأ على البيانات أثناء انتقالها من المُرسِل؛ وإلا فإنه يفترض أن البيانات التي وصلته صحيحة.

تتم كل عمليات شفرات CRC باستخدام حساب modulo-2 بدون حَمل (carry) من خانة إلى الخانة التي تليها في عمليات الجمع، أو استلاف (borrow) إلى خانة من الخانة التي تليها في عمليات الطرح. هذا يعني أن الجمع والطرح هنا عمليتان متكافئتان، وكلاهما يكافئ العملية المنطقية "أو - الحصرية"(XOR) عند إجرائها على كل زوج من البتات على حدة. فعلى سبيل المثال:

$$1011 \text{ XOR } 0101 = 1110$$
$$1001 \text{ XOR } 1101 = 0100$$

وبالمثل نحصل أيضاً على:

$$1011 - 0101 = 1110$$
$$1001 - 1101 = 0100$$

يتم الضرب والقسمة كما في الحساب الثنائي (base-2 arithmetic)، فيما عدا أن أي عمليات جمع أو طرح مطلوبة تُجرى بدون حمل أو استلاف كما ذكرنا أعلاه. كما في الحساب الثنائي العادي يؤدي ضرب عدد في 2^k إلى إزاحة مسلسل بتات العدد إلى اليسار k خانة. وهكذا فبمعلومية D وR فإن العملية:

$$D \times 2^r \text{ XOR } R$$

تنتج مسلسل بتات بطول $d + r$ والمبين في الشكل 5-7. سنستخدم هذا التمثيل الجبري لمسلسل البتات بطول $d + r$ في الشكل 5-7 في مناقشتنا التالية.

لنلتفت الآن للسؤال الجوهري: كيف يحسب المُرسِل العدد R؟ تذكّر أننا نريد إيجاد R بحيث يكون هناك عدد n يحقق العلاقة:

$$D \times 2^r \text{ XOR } R = n \times G$$

أي أننا نريد اختيار R بحيث إن G تقسم ($D\times 2^r$ XOR R) بدون باقٍ. إذا قمنا بعملية XOR لـ R على الطرفين (أي أضفنا R بحساب modulo-2 بدون حمل من خانة إلى خانة) فإننا نحصل على:

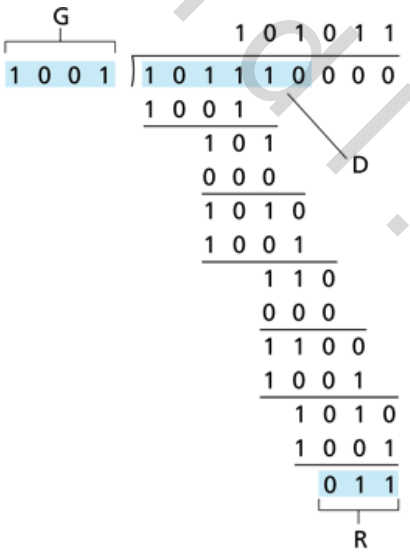
$$D\times 2^r = n\times G \text{ XOR } R$$

تخبرنا هذه المعادلة بأننا إذا قسمنا $D\times 2^r$ على G فإن الباقي يكون R بالضبط. بمعنى آخر يمكننا حساب R كالتالي:

$$R = \text{remainder}\left(\frac{D\times 2^r}{G}\right)$$

يوضح الشكل 5-8 هذه العملية الحسابية للحالة التي فيها: $D = 101110$، $d = 6$، $G = 1001$ وبالتالي $r = 3$. عندئذٍ تكون البتات التسعة التي يتم إرسالها هي 101110 011. عليك التأكد من أن:

$$D\times 2^r = 101011\times G \text{ XOR } R$$



الشكل 5-8 مثال لحساب شفرة فحص الفائض الدوري (CRC).

تم وضع مواصفات معيارية دولية لمولدات G بمقاسات: 8، 12، 16، 32 بتاً. تُستخدم شفرة CRC بمقاس 8 بتات لحماية ترويسة تضم 5 بايتات في وحدات بيانات شبكات ATM (أو ما سنطلق عليه "خلايا"). يُستخدم CRC-32 المعياري بمقاس 32 بت والمنفّذ في عددٍ من بروتوكولات IEEE لطبقة ربط البيانات المولّد:

$$G_{\text{CRC-32}} = 10000010011000001000111010110111$$

بوسع كلٍّ من شفرات CRC المعيارية اكتشاف تجمع أخطاء (burst) طوله أقل من $r + 1$ بت (أي سيتم اكتشاف كل الأخطاء في r بت متتالية أو أقل). علاوة على ذلك ـ عند تحقق الفرضيات المناسبة ـ سيتم اكتشاف تجمع أخطاء بطول أكبر من $r + 1$ بت بإحتمال $1 - 0.5^r$. وأيضاً يمكن لكل شفرات CRC المعيارية اكتشاف أي عدد فردي من أخطاء البتات. راجع [Williams 1993] لمناقشةٍ لتنفيذ العمليات المتعلقة بشفرات CRC. إن نظرية شفرات CRC والشفرات الأخرى الأكثر فعالية في اكتشاف أخطاء البيانات وتصحيحها تقع خارج نطاق هذا الكتاب، ويمكنك الاطلاع على [Schwartz 1980] والذى يتضمن مقدمة ممتازة عن هذا الموضوع.

3-5 بروتوكولات الوصول المتعدد

في مقدمة هذا الفصل ذكرنا أن هناك نوعين من وصلات الشبكة: الوصلات من نقطة إلى نقطة (point-to-point links) ووصلات الإذاعة (broadcast links). تشمل الوصلة من نقطة إلى نقطة مُرسِلاً واحداً على أحد طرفي الوصلة ومُستقبِلاً واحداً على طرفها الآخر. تم تصميم العديد من البروتوكولات للعمل على الوصلات من نقطة إلى نقطة، ومنها بروتوكول "نقطة إلى نقطة" (PPP) وبروتوكول "التحكم عالي المستوى في وصلة البيانات" (High-Level Data Link Control (HDLC)) واللذان سنغطيهما لاحقاً في هذا الفصل. أما النوع الثاني من الوصلات فيتضمن عدة عقد للإرسال والاستقبال موصّلة بقناة إذاعة وحيدة ومشتركة بينهم (سنستخدم مصطلح "إذاعة" هنا لأنه عندما تبث إحدى العقد إطار بيانات تتم إذاعته على قناة الوصلة وتتلقى كل عقدة من العقد الأخرى نسخة منه).

من أمثلة تقنيات وصلات ربط البيانات بالإذاعة شبكات البيانات المحلية (LANs) من نوع إيثرنت (Ethernet) ومن النوع اللاسلكي (wireless). في هذا الجزء سنأخذ خطوة إلى الوراء مبتعدين قليلاً عن البروتوكولات المحددة لطبقة ربط البيانات لندرس أولاً مشكلة ذات أهمية جوهرية لعمل طبقة الربط، وهي كيفية تنسيق وصول عدة عقد للإرسال والاستقبال لقناة إذاعة وحيدة مشتركة – أي مشكلة الوصول المتعدد. غالباً ما تستخدم قنوات الإذاعة في شبكات البيانات المحلية – وهي شبكات تقع جغرافياً في مبنى واحد (أو داخل شركة أو حرم جامعي) – ولذا سنتناول كيفية استخدام قنوات الوصول المتعدد في شبكات البيانات المحلية في نهاية هذا الجزء.

كلنا على دراية بفكرة الإذاعة – فالتلفزيون يستخدمها منذ نشأته. لكن الاتصال في التلفزيون التقليدي أحادي الاتجاه، حيث تقوم عقدة ثابتة واحدة بالبث للعديد من العقد التي تستقبل ذلك البث؛ بينما يمكن لكل عقدة على قناة إذاعة ضمن شبكة حاسب الإرسال والاستقبال. لعل المثال الأكثر ملاءمةً لحالة قناة الإذاعة هو تجمع الناس في حفل بقاعة كبيرة يتحدثون ويستمعون لبعضهم البعض (حيث يوفر الهواء الوسط المادي للإذاعة). مثال آخر جيد ومألوف لدى العديد من القرّاء هو قاعة الدرس حيث يستخدم المعلّم والطلاب نفس وسط الإذاعة الوحيد بنفس الطريقة. من المشاكل الجوهرية في كلا المثالين تقرير من الذي يتكلم (أي يبث على القناة) ومتى. لقد طوّر البشر مجموعة متقنة من البروتوكولات للاشتراك في استخدم قناة إذاعة، مثل:

"أعط كل شخص فرصةً للحديث."

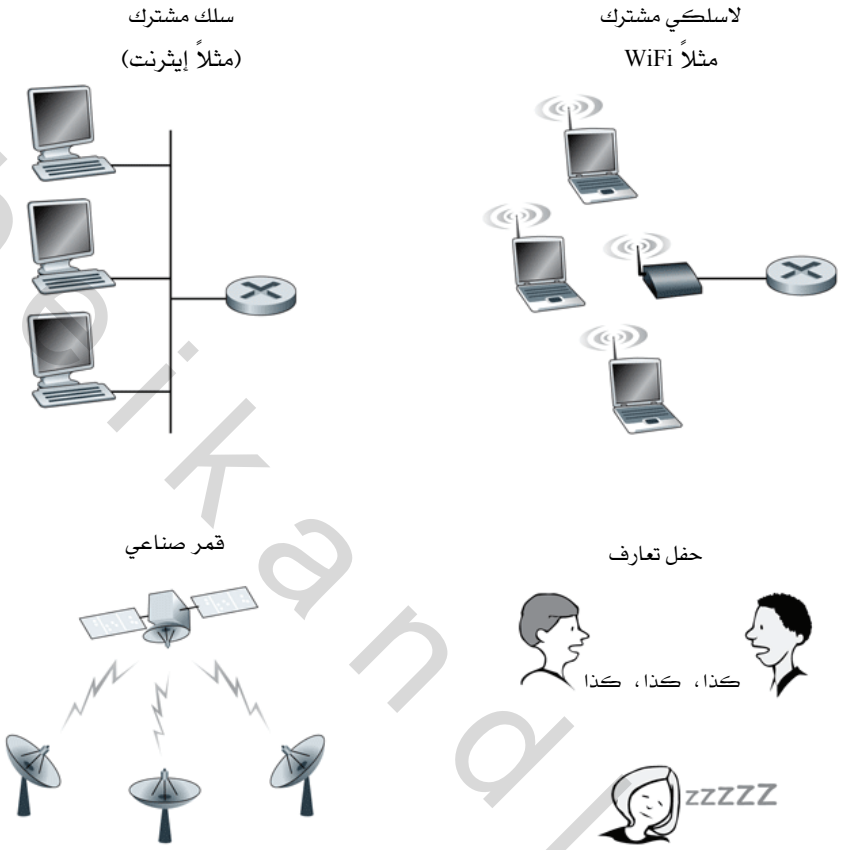
"لا تتحدث إلا إذا تحدث شخص إليك."

"لا تحتكر المحادثة."

"ارفع يدك إذا كان لديك سؤال."

"لا تقاطع شخصاً يتحدث."

"لا تنعس بينما شخص يتحدّث."



الشكل 5-9 أمثلة متنوعة لقنوات الوصول المتعدد.

بالمثل فإن لشبكات الحاسب ما يعرف ببروتوكولات الوصول المتعدد والتي تستخدمها العُقد في تنظيم إرسالها على قناة الإذاعة المشتركة. كما يبين الشكل 5-9 نحتاج لبروتوكولات الوصول المتعدد في العديد من الشبكات بما في ذلك شبكات البيانات المحلية – السلكية منها واللاسلكية – وشبكات الأقمار الصناعية. رغم أنه من الناحية الفنية توصّل كل عقدة بقناة الإذاعة من خلال بطاقة مواءمة، إلا أننا للتبسيط سنعتبر في هذا الجزء أن العقدة هي نفسها أداة الإرسال والاستقبال. بوسع المئات بل الآلاف من العقد الاتصال مباشرةً عبر قناة إذاعة.

نظراً لأنه بوسع كل العقد إرسال إطارات بيانات، يمكن أن تقوم أكثر من عقدتين بإرسال إطارات في نفس الوقت. عندما يحدث ذلك تتلقى كل العقد على قناة الإذاعة المشتركة عدة إطارات في نفس الوقت مما يؤدي إلى تصادم الإطارات المُرسَلة عند كل العقد المُستقبِلة، وفي حالة حدوث ذلك لا تستطيع أيٌّ من العقد المُستقبِلة فهم أيٍ من الإطارات التي أُرسِلت. ويرجع ذلك إلى تداخل إشارات الإطارات المصطدمة بشكلٍ معقد، ومن ثم تعتبر كل الإطارات المشتركة في الاصطدام مفقودة، وبالتالي لا تتحقق أي فائدة من قناة الإذاعة أثناء فترة الاصطدام. واضح أنه إذا كان هناك العديد من العقد التي تريد إرسال الإطارات بكثرة، فإن نسبةً كبيرةً من عمليات الإرسال ستؤدي إلى اصطدامات، وسيضيع جزء كبير من الحيز الترددي (سعة الإرسال) لقناة الإذاعة سُدىً.

لكي نضمن قيام قناة الإذاعة المشتركة بعمل مفيد عند تفعيل عقد متعددة من الضروري تنسيق عمليات الإرسال بين تلك العقد بطريقة ما. إن هذا التنسيق هو مسؤولية بروتوكول الوصول المتعدد. خلال الأعوام الثلاثين الماضية كُتبت آلاف الأبحاث والمئات من أطروحات الدكتوراه حول هذا الموضوع، ويتضمن [Rom 1990] مسحاً شاملاً لهذا الجهد. وعلاوة على ذلك فالبحث في مجال بروتوكولات الوصول المتعدد مازال نشطاً بسبب ظهور أنواع جديدة من الوصلات باستمرار، وبخاصة الوصلات اللاسلكية الجديدة.

على مرّ السنين استُخدمت العشرات من بروتوكولات الوصول المتعدد ضمن الأنواع المختلفة من تقنيات طبقة ربط البيانات. ومع ذلك يمكننا تصنيف أي بروتوكول للوصول المتعدد تقريباً ضمن واحد من الأصناف الثلاثة التالية: بروتوكولات تقسيم القناة، وبروتوكولات الوصول العشوائي للقناة، وبروتوكولات التناوب على القناة. سنغطّي هذه الأصناف الثلاثة من بروتوكولات الوصول المتعدد في الأجزاء الثلاثة التالية.

دعنا نختم هذا الاستعراض العام بالملاحظة التالية: في الحالة المثالية عند استخدام قناة إذاعة مشتركة لها سعة إرسال R بت/ثانية يجدر ببروتوكول الوصول المتعدد تحقيق الخصائص المرغوبة التالية:

1. عندما تكون عقدة واحدة فقط لديها بيانات للإرسال، يتم توفير طاقة إنتاجية قدرها R بت/ثانية لتلك العقدة.
2. عندما تكون هناك M عقدة لديها بيانات للإرسال يتم توفير طاقة إنتاجية قدرها R/M بت/ثانية لكلٍّ منها، ولا يلزم بالضرورة تحقيق معدّل إرسال آني قدره R/M بصفة دائمة، ولكن يكفي توفير معدّل إرسال متوسط قدره R/M لكل عقدة على مدى فترة زمنية يتم تحديدها بشكلٍ مناسب.
3. أن يكون البروتوكول غير مركزي؛ بمعنى ألاّ يعتمد في تنفيذه على وجود عقد رئيسة (سيادية) قد تتعرض للتعطل ومن ثم تؤدي إلى تعطل النظام بالكامل.
4. أن يكون البروتوكول بسيطاً بحيث يمكن تنفيذه بكلفة قليلة.

1-3-5 بروتوكولات تقسيم القناة

تذكّر من مناقشتنا السابقة في الجزء 1-3 أنه يمكن استخدام تقنية الإرسال المتعدد بتقسيم الزمن (Time-Division Multiplexing (TDM)) أو بتقسيم التردد (Frequency-Division Multiplexing (FDM)) لإشراك كل العقد في الحيز الترددي لقناة إذاعة مشتركة. كمثال افترض أن القناة تدعم N عقدة وأن معدل الإرسال المسموح به على القناة هو R بت/ثانية. تقوم تقنية TDM بتقسيم الوقت إلى إطارات زمنية (time frames) ثم تقسّم كل إطار بدوره إلى N شريحة زمنية، وتُخصّص شريحةً زمنيةً لكل واحدة من العقد التي عددها N. ينبغي عدم الخلط بين إطار TDM الزمني ووحدة تبادل البيانات في طبقة ربط البيانات والتي يطلق عليها أيضاً اسم إطار. لكي نقلل من احتمال حدوث هذا الخلط سنطلق في هذا الجزء على وحدة تبادل البيانات في طبقة ربط البيانات اسم رزمة (packet). عندما يكون لدى عقدة رزمة تريد إرسالها فإنها تقوم بإرسال تلك الرزمة أثناء الشريحة الزمنية

المخصصة لها في إطار TDM الدوّار. عادةً ما يتم اختيار مدة الشريحة الزمنية بحيث يمكن إرسال رزمة واحدة أثناء كل شريحة. يبين الشكل 5-10 مثالاً مبسطاً لتقنية TDM بأربع عقد. وبتطبيق ذلك على مثال الحفل المذكور آنفاً، يسمح هذا البروتوكول لكلٍّ من مرتادي الحفل بالحديث لمدة محددة من الوقت ويتوقف بعدها ليتيح الفرصة لشخص آخر للحديث لنفس الفترة، وهكذا. عند الانتهاء من إتاحة الفرصة لكل شخص ليقول ما لديه تُعاد الكَرّة من جديد.

الشكل 5-10 مثال لتقنيات TDM وFDM بأربع عقد.

تعتبر تقنية TDM مرغوبة من حيث إنها تمنع الاصطدام وتعتبر عادلة جداً، فهي تخصص لكل عقدة معدّل إرسال قدره R/N بت/ثانية خلال وقت كل إطار. ومع ذلك فهي تعاني من عيبين رئيسين، أولهما أن معدل الإرسال المتوسط المتاح لعقدة لن يتجاوز R/N بت/ثانية حتى ولو كانت هي العقدة الوحيدة التي لديها رزم

للإرسال. أما العيب الثاني فهو أنه يتعين على كل عقدة دائماً انتظار دورها في طابور الإرسال ـ مرةً أخرى حتى ولو كانت هي العقدة الوحيدة التي لديها رزم للإرسال. تخيّل أن أحد الحضور في الحفل هو الشخص الوحيد الذي لديه ما يقوله، وتخيّل الحالة الأندر التي يكون فيها كل الحضور يريدون سماع ما يقوله ذلك الشخص. من الواضح أن تقنية TDM ستكون اختياراً سيئاً كبروتوكول وصول متعدد لذلك الحفل.

بينما تقسّم تقنية TDM وقت استغلال قناة الإذاعة المشتركة بين العقد على الوصلة، تقوم تقنية FDM بتقسيم الحيز الترددي للقناة (بسعة إرسال R بت/ثانية) إلى نطاقات تردد مختلفة (لكلٍّ منها سعة إرسال قدرها R/N بت/ثانية) وتخصّص كل نطاق لاستخدام عقدة من العقد التي عددها N. وبهذا يكوّن FDM عدد N من القنوات الأصغر لكلٍّ منها سعة إرسال قدرها R/N بت/ثانية من القناة الأكبر ذات سعة الإرسال R بت/ثانية. تشترك تقنية FDM مع تقنية TDM في المزايا التي ذكرناها أعلاه، فهي تتفادى حدوث الاصطدام وتقسّم الحيز الترددي بإنصاف بين العقد. وبالمثل فإنها تشترك معها أيضاً في العيب الرئيس، ألا وهو أن سعة الإرسال المتاحة للعقدة ستكون محدودة بـ R/N بت/ثانية حتى ولو كانت هي العقدة الوحيدة التي يتوافر لديها رزم تودّ إرسالها.

يُعد بروتوكول الوصول المتعدد بتقسيم الشفرات (CDMA) بروتوكولاً ثالثاً لتقسيم القناة. بينما تخصّص تقنية TDM وتقنية FDM شرائح زمنية ونطاقات تردد على التوالي للعقد، يخصّص بروتوكول CDMA شفرةً مختلفةً لكل عقدة، حيث تستخدم كل عقدة شفرتها الفريدة لتشفير بتات البيانات التي ترسلها. إذا تم اختيار الشفرات بعناية تتوافر لشبكات CDMA الخاصية الرائعة التي تسمح للعقد المختلفة بالإرسال في نفس الوقت، ومع ذلك يستطيع كل مُستقبِل استلام بتات البيانات المشفّرة والمُرسِلة إليه بشكلٍ صحيح (بافتراض أن المُستقبِل يعرف شفرة المُرسِل) على الرغم من التداخل بسبب الإرسال من العقد الأخرى. لقد استُخدمت تقنية CDMA في الأنظمة العسكرية لبعض الوقت (بسبب خاصية مقاومة التشويش التي تتمتع بها) ولها الآن استخدامات مدنية على نطاق واسع، خصوصاً في شبكات

الهاتف الخلوي. نظراً لأن استعمال تقنية CDMA وثيق الصلة جداً بقنوات اللاسلكي، فسنؤجل مناقشتنا للتفاصيل الفنية لتقنية CDMA إلى الفصل السادس. أما الآن فيكفي أن نعرف أن الشفرات في CDMA – كما هو الحال مع شرائح الوقت في TDM ونطاقات التردد في FDM – يمكن تخصيصها لمستخدمي القناة المشتركة للوصول المتعدد.

5-3-2 بروتوكولات الوصول العشوائي

المجموعة الثانية من البروتوكولات العامة للوصول المتعدد هي بروتوكولات الوصول العشوائي. في بروتوكول للوصول العشوائي تقوم العقدة بالإرسال دائماً بمعدّل الإرسال الأقصى للقناة، أي R بت/ثانية. عند حدوث اصطدام تقوم كل عقدة اشتركت في الاصطدام بإعادة إرسال إطارها (أو بمعنى آخر رزمتها) مراراً وتكراراً إلى أن يتمكن الإطار من المرور بدون اصطدام. غير أنه عندما تواجه عقدة اصطداماً فإنها لا تعيد إرسال الإطار بعد ذلك مباشرةً بالضرورة، ولكنها بدلاً من ذلك تنتظر لمدة تأخير عشوائية قبل إعادة إرسال الإطار. تختار كل عقدة اشتركت في اصطدام تأخيرات عشوائية مستقلة. ولأن التأخيرات العشوائية يتم اختيارها بشكلٍ مستقل فمن المحتمل أن إحدى العقد ستختار تأخيراً يقل عن تأخيرات عقد الاصطدام الأخرى بما فيه الكفاية بحيث تستطيع أن تدفع بإطارها إلى القناة بدون اصطدام.

هناك العشرات بل المئات من بروتوكولات الوصول العشوائي الموجودة على الساحة [Bertsekas 1991؛ Rom 1990]. في هذا الجزء سنتناول عدداً من بروتوكولات الوصول العشوائي الأكثر استعمالاً: بروتوكولات ألوها (ALOHA) [Abramson 1970; Abramson 1985] وبروتوكولات الوصول المتعدد بالإنصات للناقل ((Carrier Sense Multiple Access (CSMA) [Kleinrock 1975b]. سنغطّي لاحقاً ـ في الجزء 5-5 ـ تفاصيل الإيثرنت [Metcalfe 1976] وهي بروتوكول مشهور ومستخدم بكثرة من نوع CSMA.

بروتوكول ألوها الشرائحي

دعنا نبدأ دراستنا لبروتوكولات الوصول العشوائي بواحد من أبسط تلك البروتوكولات، ألا وهو بروتوكول ألوها الشرائحي (Slotted ALOHA). في وصفنا لهذا البروتوكول سنفترض الآتي:

- كل الإطارات تتكون من L بت بالضبط.
- يُقسّم الوقت إلى شرائح مدة كلٍّ منها L/R ثانية (أي أن الشريحة الزمنية تكفي لإرسال إطار واحد فقط).
- تبدأ العقد ببث إطاراتها في بدايات الشرائح فقط.
- هناك تزامن بين العقد بحيث تعرف كل عقدة وقت بدأ الشرائح الزمنية.
- إذا اصطدم إطاران أو أكثر فإن كل العقد تكتشف حدوث الاصطدام قبل أن تنتهي الشريحة الزمنية التي حدث فيها.

افترض أن p تمثل احتمالاً، أي أن قيمتها تتراوح ما بين 0 و1. إن تنفيذ بروتوكول ألوها الشرائحي في كل عقدة هو عملية بسيطة تتلخص في الخطوات التالية:

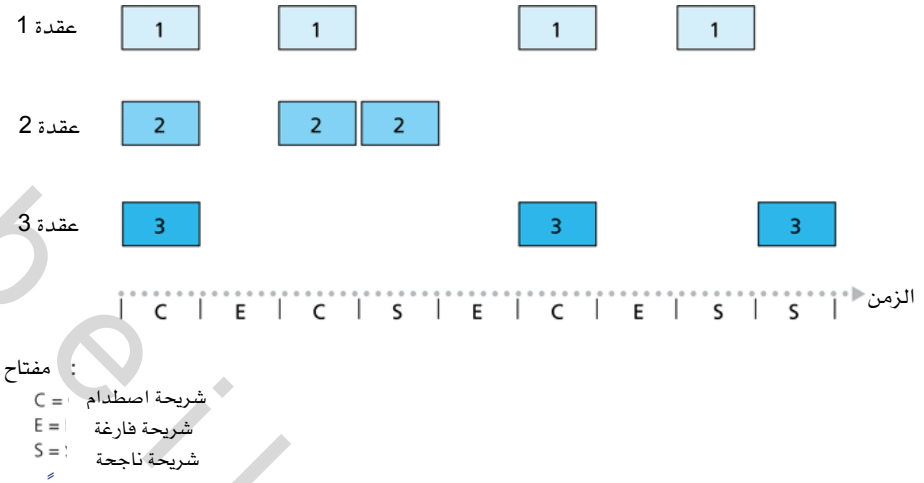
- عندما يكون لدى العقدة إطار جديد تريد إرساله فإنها تنتظر حتى بداية الشريحة التالية، وترسل الإطار بكامله أثناء تلك الشريحة.
- إذا لم يحدث اصطدام تكون العقدة قد أرسلت إطارها بنجاح، ومن ثم لا تحتاج لإعادة إرسال الإطار (بل يمكن أن تجهز العقدة إطاراً جديداً لإرساله إن وُجد).
- أما في حالة وجود اصطدام، فتكتشف العقدة الاصطدام قبل نهاية الشريحة الزمنية، وتعيد محاولة إرسال إطارها في كل شريحة تالية باحتمال p إلى أن يتم إرسال الإطار بدون اصطدام.

نعني بـ "إعادة الإرسال باحتمال p" أنّ العقدة عملياً ترمي قطعة عملة معدنية منحازة؛ حيث يناظر الحدث "صورة" "إعادة إرسال" (ويتكرر باحتمال p)، ويناظر الحدث "كتابة" "انتظر حتى تنتهي هذه الشريحة ثم ارمِ قطعة العملة مرة ثانية في الشريحة التالية" (ويتكرر باحتمال $(p - 1)$). تقوم كل العقد التي اشتركت في الاصطدام برمي قطع العملة لديها بشكلٍ مستقل.

يتضح أن لبروتوكول ألوها الشرائحي العديد من المزايا، فبخلاف بروتوكولات تقسيم القناة يسمح البروتوكول للعقدة بالإرسال بشكلٍ مستمر بمعدل الإرسال الكامل R بت/ثانية عندما تكون تلك العقدة هي العقدة الوحيدة النشطة على القناة (توصف العقدة بأنها نشطة إذا كان لديها إطارات للإرسال). كما أن بروتوكول ألوها الشرائحي بروتوكول بسيط للغاية، ويمتاز أيضاً بأنه غير مركزي بشكلٍ كبير حيث إن كل عقدة تكتشف الاصطدام وتقرر متى تعيد الإرسال بشكلٍ مستقل. ومع ذلك فإن البروتوكول يتطلب تزامن الشرائح لدى العقد. سنناقش بعد قليل نوعية غير شرائحية من ذلك البروتوكول، وكذلك بروتوكولات CSMA، والتي لا يتطلب أيٌّ منها تحقيق أي تزامن، مما يجعلها غير مركزية تماماً.

يعمل بروتوكول ألوها الشرائحي بشكلٍ جيد عندما تكون هناك عقدة نشطة واحدة، لكن ما مدى كفاءته في وجود عدة عقد نشطة؟ هناك عاملان قد يؤثران سلباً على الكفاءة:

- أولاً: كما هو موضح في الشكل 5-11، عند وجود عدة عقد نشطة ستعاني نسبة معينة من الشرائح الزمنية من حدوث اصطدامات أثناءها، ومن ثم ستُهدر تلك الشرائح.
- ثانياً: هناك نسبة أخرى من الشرائح الزمنية ستبقى غير مستغلّة (فارغة) إثر حدوث اصطدام نتيجةً لامتناع كل العقد النشطة عن الإرسال لاتباعها سياسة الاحتمالات. الشرائح الوحيدة التي لن تضيع هباءً ستكون تلك التي تقوم فيها عقدة واحدة فقط بالإرسال (وعندئذ يطلق عليها شريحة ناجحة). سنعرّف كفاءة أي بروتوكول شرائحي للوصول المتعدد بأنها نسبة الشرائح الناجحة على المدى البعيد عند وجود عدد كبير من العقد النشطة لدى كل منها عدد كبير من الإطارات التي تريد إرسالها. لاحظ أنه في غياب أي شكل من أشكال التحكم في الوصول، وقيام كل عقدة بإعادة الإرسال فوراً عقب كل اصطدام، ستكون الكفاءة صفراً. واضح أن كفاءة بروتوكول ألوها الشرائحي تزيد شيئاً ما عن الصفر، ولكن بكَم؟



الشكل 5-11 تصطدم العقد 1 و2 و3 في الشريحة الأولى. تنجح العقدة 2 أخيراً في الشريحة الرابعة، والعقدة 1 في الشريحة الثامنة، والعقدة 3 في الشريحة التاسعة.

نمضي الآن في اشتقاق تعبير رياضي للكفاءة القصوى لبروتوكول ألوها الشرائحي. لتبسيط هذا الاشتقاق دعنا نعدّل البروتوكول قليلاً بأن نفترض أن كل عقدة تحاول إرسال إطارٍ في كل شريحة زمنية باحتمال p (بمعنى أننا نفترض أن كل عقدة لديها دائماً إطار للإرسال، وأن العقدة ترسل الإطارات باحتمال p دائماً سواءً الإطار الجديد أو الذي عانى من اصطدام). افترض أن لدينا N عقدة، عندئذ يكون احتمال أن شريحة بعينها هي شريحة ناجحة هو احتمال قيام إحدى العقد بالإرسال بينما تمتنع بقية العقد الـ $(N - 1)$ عن الإرسال. احتمال قيام عقدة بالإرسال هو p، واحتمال عدم قيام كل العقد الباقية بالإرسال هو $(1 - p)^{N-1}$ وعليه يكون احتمال نجاح عقدة بعينها هو $p(1 - p)^{N-1}$. ونظراً لأننا لدينا N عقدة، فإن احتمال نجاح أي عقدة في الإرسال هو $Np(1 - p)^{N-1}$.

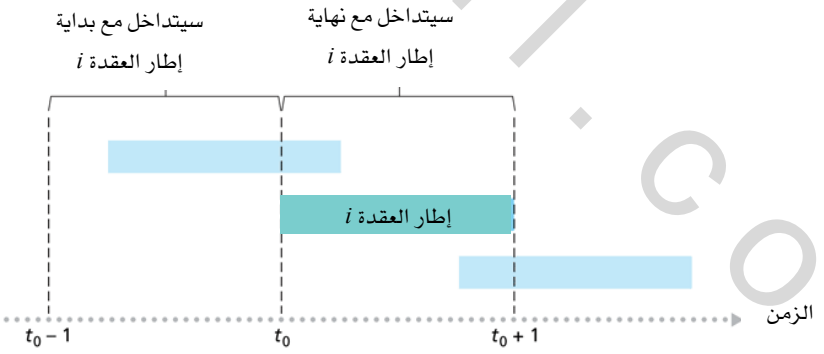
وبالتالي فعند وجود عقد نشطة تكون كفاءة بروتوكول ألوها الشرائحي $Np(1- p)^{N-1}$. للحصول على الكفاءة القصوى لـ N عقدة نشطة، علينا إيجاد القيمة p^* التي تحقق أقصى قيمة لذلك التعبير (راجع تمارين هذا الفصل للاطلاع على استعراض عام لهذا الاشتقاق). وللحصول على الكفاءة القصوى لعدد كبير من

العقد النشطة، نأخذ نهاية $Np^*(1-p^*)^{N-1}$ بينما تقترب N من ما لانهاية (مرةً أخرى راجع التمارين في نهاية الفصل). بعد القيام بهذه الحسابات سنجد أن الكفاءة القصوى للنظام تساوي تقريبا $1/e = 0.37$. أي أنه في وجود عدد كبير من العقد لديها العديد من الإطارات لإرسالها، فإنه (في أحسن الأحوال) تُستخدم 37 بالمائة من الشرائح الزمنية فقط للقيام بعمل مفيد. وعليه فإن نسبة الإرسال الفعّالة للقناة ليست R بت/ثانية ولكن فقط $0.37\ R$ بت/ثانية. يبين تحليل مماثل أن 37 بالمائة من الشرائح تذهب فارغة و26 بالمائة منها تعاني من اصطدامات. تخيّل خيبة أمل مشرف الشبكة الذي اشترى نظام ألوها الشرائحي للعمل على قناة بسعة إرسال 100 ميجابت/ثانية متوقعاً أن يكون بوسعه استعمال الشبكة لإرسال البيانات بين عدد كبير من المستخدمين بمعدل إرسال كلي قدره مثلاً 80 ميجابت/ثانية! رغم أن القناة قادرة على إرسال الإطار بمعدل الإرسال الكامل للقناة (100 ميجابت/ثانية)، فإنه على المدى البعيد ستكون الطاقة الإنتاجية الناجحة لتلك القناة أقل من 37 ميجابت/ثانية.

بروتوكول ألوها

يتطلّب بروتوكول ألوها الشرائحي من كل العقد أن تُزامِن إرسالها بحيث يبدأ مع بداية الشريحة الزمنية. غير أن بروتوكول ألوها الأصلي [Abramson 1970] كان في الواقع بروتوكولاً غير شرائحي وغير مركزي تماماً. ففي ذلك البروتوكول عندما يصل إطار لأول مرة (بتمرير قطعة بيانات في عقدة الإرسال من طبقة الشبكة إلى طبقة ربط البيانات) تُرسِل العقدة الإطارَ كله فوراً عبر قناة الإذاعة المشتركة. وإذا واجه إطارٌ مُرسَلٌ اصطداماً مع واحد أو أكثر من الإطارات المُرسَلة، فإن العقدة تعيد إرسال ذلك الإطار فوراً (بمجرد الانتهاء من إرسال الإطار المصطدم)، وذلك بالاحتمال p. وإلا فإن العقدة تنتظر (تبقى عاطلة) لفترة إرسال إطار، وبعدها ترسل الإطار بالإحتمال p أو تنتظر لفترة إرسال إطار آخر باحتمال $(1-p)$.

لتعيين الكفاءة القصوى لبروتوكول ألوها الأصلي سنركّز على عقدة بعينها. سنفترض نفس فرضيات التحليل السابق لبروتوكول ألوها الشرائحي، ونفترض أن وقت إرسال الإطار يمثل وحدة الزمن. في أي وقت يكون احتمال قيام العقدة بإرسال إطار هو p. افترض أن العقدة i تبدأ في إرسال هذا الإطار في الوقت t_0. كما هو مبيّن في الشكل 5-12 لكي يتم إرسال هذا الإطار بنجاح ينبغي ألا تبدأ أي عقدة أخرى إرسالها خلال الفترة $[t_0\text{-}1, t_0]$، لأن مثل هذا الإرسال يتداخل مع بداية إرسال إطار العقدة i. احتمال أن كل العقد الأخرى لا تبدأ إرسالها خلال تلك الفترة هو $(1\text{-}p)^{N\text{-}1}$. بالمثل لا ينبغي أن تقوم عقدة أخرى بالإرسال بينما العقدة i ترسل، حيث إن ذلك يتداخل مع الجزء الأخير من إرسال إطار العقدة i. احتمال أن كل العقد الأخرى لا تبدأ الإرسال في تلك الفترة هو أيضاً $(1\text{-}p)^{N\text{-}1}$. وعليه فإن احتمال أن تتمكن عقدة بعينها من القيام بإرسال ناجح هو $p(1\text{-}p)^{2(N\text{-}1)}$. بأخذ النهايات كما في حالة بروتوكول ألوها الشريحي، نجد أن الكفاءة القصوى لبروتوكول ألوها الأصلي هي $(1/2e)$ فقط (أي بالضبط نصف القيمة لبروتوكول ألوها الشرائحي). هذا إذن هو الثمن الذي ندفعه مقابل استخدام بروتوكول ألوها غير المركزي تماماً.



الشكل 5-12 تداخل عمليات الإرسال في بروتوكول ألوها.

تاريخ حالة (Case History)

نورم أبرامسون وشبكة ألوهانت:

نورم أبرامسون هو مهندس يحمل شهادة الدكتوراه، وقد كان لديه هواية التزلج على الماء واهتمام بتحويل رزم البيانات. قاده هذا الاهتمام إلى جامعة هاواي في عام 1969، ونظراً لأن هاواي تضم مجموعة من الجزر الجبلية فقد كان تركيب وتشغيل الشبكات الأرضية أمراً صعباً. عندما لم يكن أبرامسون يتزلج على الماء، كان يفكر كيف يصمّم شبكة تقوم بتحويل رزم البيانات على موجات الراديو. تضمنت الشبكة التي صمّمها مضيفاً مركزياً واحداً وعدّة عقد ثانوية مبعثرة على جزر هاواي، وكانت تستخدم قناتين لكلٍ منهما نطاق ترددي مختلف. استُخدمت قناة الوصلة الهابطة (downlink) لإذاعة الرزم من المضيف المركزي إلى المضيفات الثانوية، بينما استخدمت قناة الوصلة الصاعدة (uplink) لإرسال الرزم من المضيفات الثانوية إلى المضيف المركزي. علاوةً على إرسال رزم المعلومات كان المضيف المركزي يرسل أيضاً على قناة الوصلة الهابطة إشعار استلام لكل رزمة يتم استلامها بنجاح من المضيفات الثانوية.

ونظراً لأن المضيفات الثانوية ترسل الرزم بشكلٍ غير مركزي كانت الاصطدامات تحدث حتماً على قناة الوصلة الصاعدة. قادت تلك الملاحظة أبرامسون لابتكار بروتوكول ألوها الأصلي كما وصفناه من قبل في هذا الفصل. في عام 1970 وبتمويل مستمر من الوكالة الأمريكية لمشاريع البحوث المتقدمة (ARPA)، قام أبرامسون بتوصيل شبكة ألوهانت (ALOHAnet) إلى شبكة أربانت (ARPAnet). تكمن أهمية عمل أبرامسون ليس فقط في كونه أول شبكة راديو من نوعها لتحويل الرزم، ولكن أيضاً لأنه كان مصدر إلهام لبوب ميتكالف (Bob Metcalfe). فبعد سنوات قليلة عدّل ميتكالف بروتوكول ألوها ليبتكر بروتوكول الوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام CSMA/CD وشبكة الإيثرنت المحلية.

الوصول المتعدد بالإنصات للناقل (CSMA)

في بروتوكول ألوها – بكلا نوعيه الشرائحي والأصلي – تتخذ كل عقدة قرارها بالإرسال أو عدمه بشكلٍ مستقل عن نشاط العقد الأخرى المشتركة معها في نفس قناة الإذاعة، وبالتحديد لا تكترث العقدة إذا صادفت عقدةً أخرى تقوم بالإرسال في الوقت ذاته التي تشرع هي فيه ببدء الإرسال، كما أنها لا توقف إرسالها إذا ما بدأت عقدة أخرى بالتداخل مع ما ترسله. في مثال الحفل الذي ذكرناه آنفاً تشبه بروتوكولات ألوها تماماً مرتاد الحفل الفظ الذي يواصل

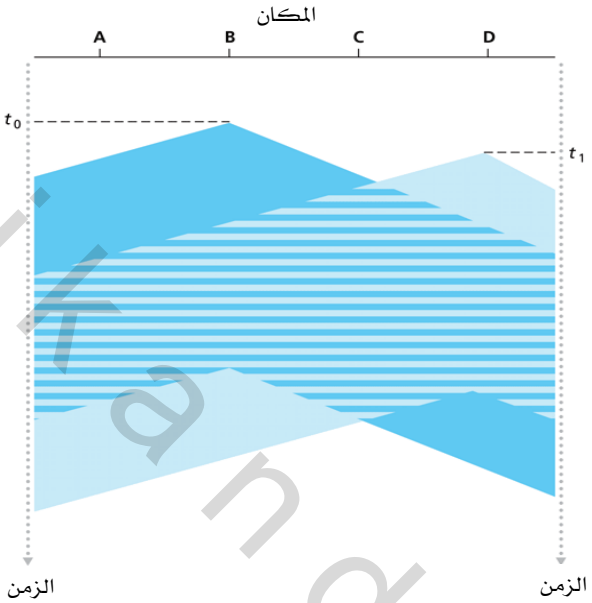
دردشتة سواء كان الآخرون يتكلمون أم لا. إننا كبشر لدينا بروتوكولات تجعلنا نتصرّف ليس فقط بلطف ولكن أيضاً بحيث نقلل الوقت الذي "تصطدم" فيه محادثاتنا مع الآخرين، ومن ثم زيادة كمية البيانات التي نتبادلها من خلال تلك المحادثات. وبشكلٍ محدّد هناك قاعدتان ذهبيتان للمحادثة البشرية الدمثة:

1. استمع قبل الكلام، فإذا كان هناك شخص آخر يتكلم فانتظر حتى ينتهي. في عالم الشبكات يُعرف هذا الأسلوب بالإنصات للناقل، حيث تنصت العقدة إلى القناة قبل الشروع في الإرسال. إذا حدث وكانت هناك عقدة أخرى تبث إطاراً حالياً على القناة فإن العقدة التي تُنصت تنتظر (تتراجع) لفترة عشوائية من الوقت وبعد ذلك تنصت للقناة مرةً أخرى. إذا وجدت العقدة أن القناة خالية فإنها تبدأ إرسال إطارها، وإلا فإنها تنتظر لفترة عشوائية أخرى وتكرّر العملية.
2. إذا بدأ شخص آخر الكلام في نفس الوقت توقّف أنت عن الكلام. يُعرف هذا في عالم الشبكات باكتشاف الاصطدام، حيث تنصت العقدة المُرسِلة للقناة أثناء قيامها بالإرسال وإذا اكتشفت أن عقدة أخرى ترسل إطاراً يتداخل مع إطارها الذي ترسله، فإنها تتوقّف عن الإرسال وتستخدم بعض قواعد البروتوكول لتحديد متى يمكنها إعادة محاولة الإرسال مرةً أخرى.

تم تضمين هاتين القاعدتين في عائلة بروتوكولات الوصول المتعدد بأسلوب الإنصات للناقل والوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام (CSMA/CD) [Kleinrock 1975b; Metcalfe 1976; Lam 1980; Rom 1990]. تم اقتراح العديد من أنواع بروتوكولات CSMA وCSMA/CD، ويمكنك الرجوع لتلك المراجع للاطلاع على تفاصيل تلك البروتوكولات. سندرس نظام CSMA/CD المستخدم في شبكات الإيثرنت بالتفصيل في الجزء 5-5. أما هنا فسنلقي الضوء على بعض الخصائص الهامة والأساسية لبروتوكولات CSMA و CSMA/CD.

لعل السؤال الذي سيتبادر إلى ذهنك للوهلة الأولى عن بروتوكول CSMA هو: لماذا تحدث الاصطدامات أساساً إذا كانت كل العقد تنصت للناقل؟ فكل عقدة ستمتنع عن الإرسال عندما تشعر بأن عقدة أخرى ترسل. لعل أفضل طريقة لتوضيح الإجابة عن هذا التساؤل هي استخدام مخططات المكان والزمن [Molle 1987].

يبين الشكل 5-13 مخطط المكان والزمن لأربع عقد (A, B, C, D) موصلة على ناقل إذاعة خطي (linear broadcast bus). يبين المحور الأفقي موقع كل عقدة على الناقل بينما يمثل المحور العمودي الزمن.

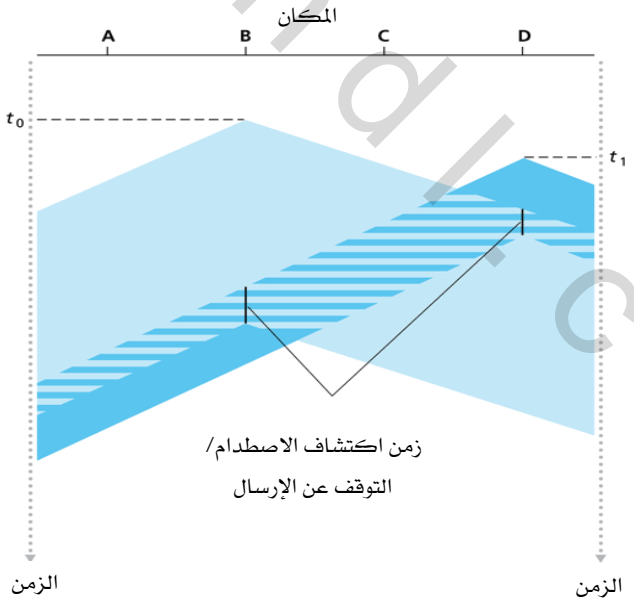


الشكل 5-13 مخطط المكان والزمن لعقدتي بروتوكول CSMA مع اصطدام للإرسال.

عند النقطة t_0 من الزمن تحس العقدة B أن القناة خالية، حيث لا توجد عقد أخرى تقوم بالإرسال حالياً. وعليه تبدأ العقدة B بالإرسال، فتنتقل البتات التي ترسلها في كلا الإتجاهين على طول وسط الإذاعة المشترك. إن انتقال بتات العقدة B إلى أسفل مع زيادة الوقت في الشكل 5-13 يبين أن تلك البتات تحتاج لفترة محددة من الوقت (ليست صفراً) لانتقال البتات على طول وسط الإذاعة المشترك (رغم انتقالها بسرعة كبيرة تقارب سرعة الضوء) . عند اللحظة t_1 – حيث ($t_1 > t_0$) – يتوافر لدى العقدة D إطارٌ للإرسال. رغم أن العقدة B تقوم فعلاً بالإرسال في اللحظة t_1، إلا أن البتات التي ترسلها B لم تصل بعد إلى D، ومن ثم تحس D أن القناة خالية عند t_1. تبعاً لبروتوكول CSMA تبدأ D بإرسال إطارها. بعد مرور فترة قصيرة من الوقت، يأخذ إرسال B في التداخل مع إرسال D. يتبين من الشكل 5-13 أن

تأخير الانتقال من طرف إلى طرف عبر قناة الإذاعة المشتركة يلعب دوراً حاسماً في تحديد أداء هذا النظام. فكلما كان هذا التأخير أطول ازداد احتمال عدم تمكن عقدة تنصت للناقل من الإحساس بإرسال بدأته عقدة أخرى على الشبكة.

في الشكل 5-13 لا تقوم العقد باكتشاف الاصطدام، فكل من العقدتين B وD تواصل إرسال إطاراتها كاملةً رغم حدوث اصطدام. عندما يتوافر لعقدة إمكانية اكتشاف الاصطدام، سوف توقف إرسالها بمجرد اكتشافها وقوع الاصطدام. يبين الشكل 5-14 نفس السيناريو الموضح في الشكل 5-13 فيما عدا أن العقدتين توقفان إرسالهما بعد فترة وجيزة من اكتشاف الاصطدام. واضح أن إضافة إمكانية اكتشاف الاصطدام لبروتوكول الوصول المتعدد بالإنصات للناقل سيحسّن أداء البروتوكول، وذلك بمنع إرسال الإطار عديم الفائدة بالكامل (أي الإطار الذي فسد بسبب التداخل مع إطارٍ مُرسَلٍ من عقدة أخرى). بروتوكول الإيثرنت الذي سندرسه في الجزء 5-5 هو بروتوكول من هذا النوع (أي الوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام).



الشكل 5-14 بروتوكول الوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام.

3-3-5 بروتوكولات التناوب على القناة

تذكّر أنه من الخواص المرغوبة في بروتوكول الوصول المتعدد: (1) عند وجود عقدة واحدة نشطة، تتوافر لتلك العقدة طاقة إنتاجية R بت/ثانية، و(2) عند وجود M عقدة نشطة، تتوافر لكل عقدة نشطة طاقة إنتاجية مقدارها R/M بت/ثانية تقريباً. يلاحظ أن بروتوكولات ألوها وCSMA تتحقق فيها الخاصية الأولى، لكن لا تتحقق فيها الخاصية الثانية. لقد حفّز هذا الأمر الباحثين لتطوير طائفة أخرى من البروتوكولات يطلق عليها بروتوكولات التناوب على القناة. كما هو الحال مع بروتوكولات الوصول العشوائي، هناك العشرات من بروتوكولات التناوب على القناة، ولكل واحدٍ منها العديد من النوعيات المختلفة. سنتناول هنا اثنين من أهم تلك البروتوكولات. يتطلّب الأول، وهو بروتوكول الاستفتاء (polling)، تعيين إحدى العقد كعقدة رئيسة (master node). تقوم العقدة الرئيسة باستطلاع وضع كلٍّ من العقد الأخرى بشكلٍ دوري لمعرفة ما إذا كان لديها ما تريد إرساله. وبالتحديد ترسل العقدة الرئيسة أولاً رسالة إلى العقدة 1 مفادها أنها (أي العقدة 1) يمكنها إرسال عدة إطارات كحدٍ أقصى يتم تعيينه في الرسالة. بعد انتهاء العقدة 1 من إرسال إطاراتها، تخبر العقدة الرئيسة عقدة 2 أنه بوسعها (أي العقدة 2) إرسال العدد الأقصى من الإطارات. يمكن للعقدة الرئيسة تحديد ما إذا كانت عقدة مُرسِلة قد انتهت من إرسال إطاراتها بملاحظة غياب الإشارة على القناة. تستمر العملية بهذه الطريقة، حيث تستطلع العقدة الرئيسة كل عقدة من العقد بطريقة دورية.

يتخلص بروتوكول الاستفتاء من الاصطدامات ومن ترك الشرائح الزمنية فارغة ـ وهي عيوب تعاني منها بروتوكولات الوصول العشوائي ـ وبالتالي يمكنه تحقيق كفاءة أعلى بكثير. غير أنه يعاني أيضاً من عدة عيوب. العيب الأول: هو أنه يتضمن تأخيراً جديداً هو تأخير الاستطلاع (أي الوقت اللازم لإخبار عقدة أنها يمكنها أن ترسِل). فمثلاً إذا كانت هناك عقدة واحدة نشطة، فإنها سترسل البيانات بمعدل إرسال أقل من R بت/ثانية، حيث إنه على العقدة الرئيسة استطلاع

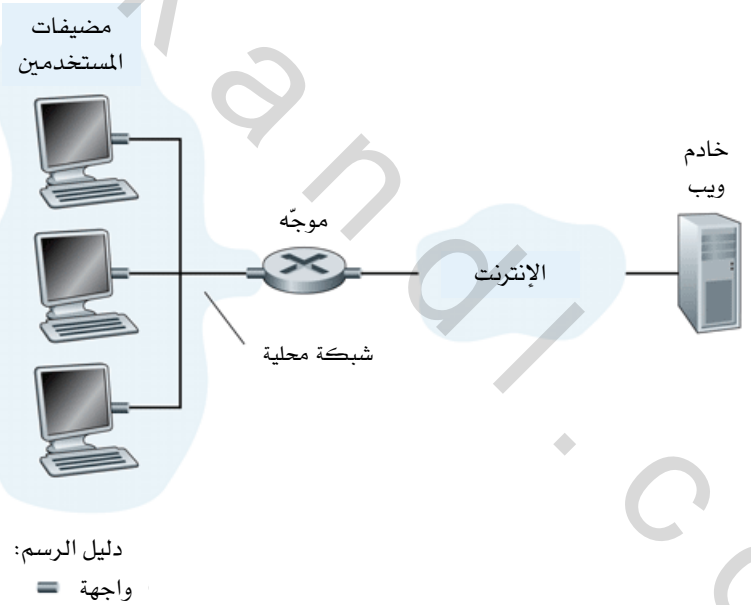
وضع العقد الخاملة تباعاً كلما انتهت العقدة النشطة من إرسال العدد الأقصى المحدد لها من الإطارات. أما العيب الثاني: وهو الأشد خطورة، فيكمن في العقدة الرئيسة؛ لأنه في حال تعطلها لا يمكن تشغيل القناة.

البروتوكول الثاني للتناوب على القناة هو بروتوكول تمرير العلامة ("التوكن") (token-passing). في هذا البروتوكول لا توجد عقدة رئيسة، وإنما يتم تبادل إطار خاص صغير يُعرف بالعلامة بين العقد بترتيب ثابت. فمثلاً قد ترسل العقدة 1 العلامة دائماً إلى العقدة 2، والعقدة 2 قد ترسلها دائماً إلى العقدة 3، والعقدة N قد ترسلها دائماً إلى العقدة 1. عندما تسلّم العلامة لعقدةٍ ما فإن العقدة تحتفظ بها فقط إذا كان لديها بعض الإطارات تريد إرسالها، وإلا فإنها ترسل العلامة مباشرة إلى العقدة التالية. إذا كان لدى عقدة إطارات للإرسال عندما تستلم العلامة، فإنها ترسل العدد الأقصى المسموح به من الإطارات ثم تمرر العلامة إلى العقدة التالية. يعتبر أسلوب تمرير العلامة غير مركزيٍ وذا كفاءة عاليةً، ولكن له مشاكله أيضاً. على سبيل المثال، قد يؤدي تعطل عقدة واحدة إلى تعطل القناة بأكملها. كما أنه إذا أهملت عقدة ما بشكلٍ عرَضي تمرير العلامة فسيحتاج الأمر إلى إجراءٍ للتعافي من هذا الخطأ واستئناف عملية تمرير العلامة. تم تطوير عدة بروتوكولات لتمرير العلامة على مدار سنين عديدة، وكل واحد منها كان عليه التصدي لتلك المشاكل وغيرها من القضايا المتعلقة. سنذكر اثنين من تلك البروتوكولات في الجزء التالي: بروتوكول FDDI وبروتوكول IEEE 802.5.

4-3-5 شبكات البيانات المحلية (LANs)

تُستخدَم بروتوكولات الوصول المتعدد مع العديد من الأنواع المختلفة لقنوات الإذاعة المشتركة، حيث تستخدم مع القنوات اللاسلكية وقنوات الأقمار الصناعية والتى تقوم فيها العقد بالإرسال على نفس النطاق الترددي، وتُستخدم حالياً للوصول للإنترنت عن طريق قناة الوصلة الصاعدة للكبل (انظر الجزء 1-2)، كما تُستخدم بكثرة على شبكات البيانات المحلية (LANs).

تذكّر أن شبكة البيانات المحلية LAN هي شبكة حاسب مركّزة في منطقة جغرافية كبناية أو حرم جامعي. عندما يدخل مستخدم على الإنترنت من جامعة أو مقر شركة، يكون الوصول غالباً عن طريق شبكة بيانات محلية. وبالتحديد يتم الوصول من المضيف إلى الشبكة المحلية إلى الموجّه إلى الإنترنت كما هو مبين في الشكل 5-15. جدير بالذكر أن معدل الإرسال R لمعظم شبكات البيانات المحلية عالٍ جداً. حتى في أوائل الثمانينيات كانت الشبكات المحلية التى تعمل بسرعات 10 ميجابت/ثانية منتشرة. واليوم تتوافر الشبكات المحلية بمعدلات إرسال قدرها 100 ميجابت/ثانية و1 جيجابت/ثانية و10 جيجابت/ثانية.



الشكل 5-15 وصول المضيفات إلى خادم الويب على الإنترنت عن طريق شبكة بيانات محلية. تتألف قناة الإذاعة المشتركة بين المضيفات والموجّه من وصلة واحدة.

في الثمانينيات وأوائل التسعينيات ظهر صنفان من تقنيات شبكات البيانات المحلية وانتشرا في أماكن العمل. شمل الصنف الأول شبكات الإيثرنت المحلية المعروفة بشبكات IEEE 802.3 [IEEE 802.3 2007]، وهي مصمّمة على أساس الوصول العشوائي. أما الصنف الثاني من شبكات البيانات المحلية فقد تضمّن تقنيات تمرير العلامة (token-passing)، ومن بينها حلقة العلامة (token ring) (والمعروفة كذلك بـ IEEE 802.5 [IEEE 802.5 2007]، وواجهة البيانات الموزعة عبر الألياف الضوئية (FDDI) [Jain 1994]. نظراً لأننا سنتناول تقنيات الإيثرنت بشيء من التفصيل في الجزء 5-5، فسوف نركّز مناقشتنا هنا على شبكات البيانات المحلية بتمرير العلامة. وستكون مناقشتنا لتقنيات تمرير العلامة قصيرة عن قصد؛ لأن المنافسة المستمرة من قِبَل الإيثرنت قد جعلت تلك التقنيات شبه منقرضة الآن تقريباً. ومع ذلك، ولكي نقدم بعض الأمثلة لتقنية تمرير العلامة ونعطي منظوراً تاريخياً مبسطاً من المفيد ذكر نبذة مختصرة عن شبكات حلقة العلامة.

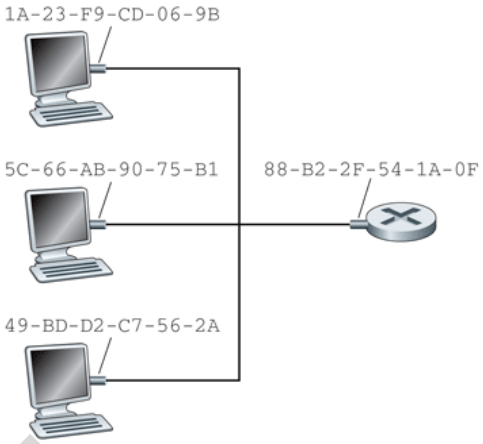
في شبكة بيانات محلية من نوع حلقة العلامة تُوصّل عُقد الشبكة (افترض أن عددها N وأنها تضم مضيفات وموجّهات) على شكل حلقة باستخدام وصلات مباشرة. تحدد طبوغرافية حلقة العلامة الترتيب المتّبع لتمرير العلامة. عندما تحصل عقدة على العلامة وترسل إطاراً، ينتقل الإطار حول الحلقة بأكملها، وبذلك تنشأ قناة إذاعة افتراضية. تقرأ العقدة المقصودة (الوجهة) الإطار من الوسط المادي لطبقة ربط البيانات أثناء مرور الإطار بها. تتحمّل العقدة التي ترسل الإطار مسؤولية إزالة الإطار من الحلقة. بهذا الأسلوب صُمّمت واجهة البيانات الموزعة عبر الألياف الضوئية (FDDI) لشبكات البيانات المحلية التي تمتد جغرافياً على مساحات أكبر، بما في ذلك شبكات المنطقة الحَضَرية (Metropolitan Area Networks (MANs)). في شبكات البيانات المحلية الممتدة جغرافياً عبر عدّة كيلومترات يقلل من كفاءة الشبكة ترك الإطار ينتقل مرةً أخرى إلى العقدة المُرسِلة بعد عبوره عقدة الوجهة. لذا ففي شبكات FDDI تقوم عقدة الوجهة نفسها بإزالة الإطار من الحلقة (وعليه فإن شبكة FDDI ليست بالضبط قناة إذاعة بالمعنى الحرفي، حيث إن كل عقدة لا تستلم كل إطار يتم إرساله).

4-5 العنونة في طبقة ربط البيانات

للعقد – أي المضيفات والموجّهات ـ عناوين في طبقة ربط البيانات. الآن قد تجد في هذا مفاجأة، بعد أن عرفت في الفصل الرابع أن العقد لها أيضاً عناوين بطبقة الشبكة. وقد تتساءل الآن لماذا نحتاج لأن يكون لدينا عناوين في كلٍّ من طبقة الشبكة وطبقة ربط البيانات؟ بالإضافة إلى وصف قواعد ووظائف عناوين طبقة ربط البيانات، نأمل أن نتمكن في هذا الجزء من توضيح كيف أن وجود طبقتين من العنونة هو أمر مفيد، بل وفي حقيقة الأمر لا غنى عنه. سنغطي أيضاً بروتوكول تحويل العناوين (Address Resolution Protocol (ARP))، والذي يوفّر آلية لترجمة عناوين طبقة الشبكة IP إلى عناوين طبقة ربط البيانات.

1-4-5 عناوين طبقة ربط البيانات

في الحقيقة، ليست العقدة ـ أي المضيف أو الموجّه ـ هي التي لها عنوان طبقة ربط البيانات ولكن موائم الشبكة بالعقدة هو الذي له عنوان طبقة ربط البيانات. يوضح هذا المفهوم الشكل 5-16. يُطلق على عنوان طبقة ربط البيانات أسماء مختلفة، كعنوان شبكة البيانات المحلية (LAN address)، والعنوان المادي (physical address)، أو عنوان طبقة ربط البيانات (عنوان الماك) (MAC address). ونظراً لأن التعبير الأخير يبدو أكثر تلك التعابير شهرة، فسوف نشير لعناوين طبقة ربط البيانات ابتداءً من الآن بعناوين الماك. في معظم شبكات البيانات المحلية (بما في ذلك الإيثرنت وشبكة البيانات المحلية اللاسلكية 802.11)، يتكون عنوان الماك من 6 بايتات، ومن ثم يسمح بـ 2^{48} عنوان ماك مختلف. كما هو مبين في الشكل 5-16، يُعبّر عن تلك العناوين المؤلفة من 6 بايتات عادةً بصيغة أعداد ستة عشرية (0-9, A-F)، حيث يمثل كل بايت من بايتات العنوان بزوج من الأعداد الستة عشرية. رغم أن عناوين الماك صمّمت لتكون ثابتة، فمن الممكن الآن تغيير عنوان الماك لموائم الشبكة عن طريق البرامج. على كل حال فإننا طوال هذا الجزء سنفترض أن عنوان الماك لموائم الشبكة هو عنوان ثابت.



الشكل 5-16 لكل موائم موصل بشبكة البيانات المحلية عنوان ماك فريد.

من الخواص الشائقة لعناوين الماك عدم وجود موائمين لهما نفس العنوان. قد يبدو ذلك مفاجأة لك. السؤال الآن: إذا كانت تلك الموائمات يتم إنتاجها في العديد من البلدان بواسطة العديد من الشركات، فكيف لشركة تنتج الموائمات في تايوان أن تتأكّد من أنها تستعمل عناوين مختلفة عن تلك التي تستخدمها شركة أخرى تنتج الموائمات في بلجيكا؟ الجواب على ذلك هو أن منظمة IEEE تدير فضاء عناوين الماك. وبتحديدٍ أكثر عندما تريد شركة صناعة موائمات، فإنها تشتري حيزاً من فضاء عناوين الماك يضم 2^{24} عنواناً مقابل أجر معين. تخصّص IEEE للشركة 2^{24} عنواناً بتثبيت الـ 24 بتاً الأولى من بتات عنوان الماك، وتترك للشركة الحرية لتكوين عناوين ماك فريدة تناظر التباديل المختلفة لقيم البتات الـ 24 الأخيرة من عنوان الماك لكل موائم.

عنوان الماك لموائم له تركيب مسطّح (flat) (في مقابل التركيب الهرمي hierarchical) ولا يتغيّر أينما ذهب الموائم. فحاسبٌ نقّال مزوّد ببطاقة إيثرنت يكون له نفس عنوان الماك دائماً أينما ذهب ذلك الحاسب. ومساعد شخصي رقمي (PDA) بموائم لاسلكي 802.11 يكون له نفس عنوان الماك دائماً أينما ذهب ذلك الـ PDA. تذكّر أنه على النقيض من ذلك يكون لعناوين طبقة الشبكة (IP addresses)

تركيب هرمي (أي أن العنوان يتكون من جزءٍ خاصٍ بالشبكة وجزءٍ خاصٍ بالمضيف)، وعليه فإن عنوان IP لمضيف ينبغي تغييره عند انتقال المضيف (أي عند تغيير الشبكة الموصّل بها). يشبه عنوان الماك الخاص بالموائم رقم الضمان الاجتماعي للشخص، والذي له أيضاً تركيب مسطح ولا يتغيّر أينما ذهب الشخص. أما عنوان IP فيماثل العنوان البريدي للشخص، والذي له تركيب هرمي ويلزم تغييره عندما ينتقل الشخص. تماماً كما يجد الشخص من المفيد أن يكون له عنوان بريدي ورقم ضمان اجتماعي، فمن المفيد للعقدة أن يكون لها عنوان بطبقة الشبكة (IP address) وعنوان ماك.

كما ذكرنا في بداية هذا الجزء، عندما يريد موائمٌ إرسال إطار إلى موائم وجهة، يقوم موائم المُرسِل بوضع عنوان الماك لموائم الوجهة بالإطار، وبعد ذلك يرسل الإطار إلى شبكة البيانات المحلية. إذا كانت الشبكة من نوع شبكات الإذاعة (كشبكة 802.11 والعديد غيرها من شبكات الإيثرنت المحلية) يتم استلام الإطار ومعالجته بواسطة كل الموائمات الأخرى الموصّلة على الشبكة المحلية. وبالتحديد يقوم كل موائم يتلقّى الإطار بالتأكد مما إذا كان عنوان الماك للوجهة والموجود في الإطار يوافق عنوان الماك الخاص بالموائم. إذا كان الأمر كذلك، ينتزع الموائم قطعة البيانات المرفقة بالإطار، ويدفع بها لأعلى عبر رصة البروتوكولات على عقدته الأم. إذا لم يحدث تطابق بين العنوانين، يهمل الموائم الإطار ولا يمرّر وحدة بيانات طبقة الشبكة لأعلى عبر رصة البروتوكولات. وهكذا فإن عقدة الوجهة فقط هي التي سيتم مقاطعتها عند استلام الإطار.

ومع ذلك ففي بعض الأحيان يريد موائم المُرسِل من كل الموائمات الأخرى على الشبكة المحلية أن تستلم وتعالج الإطار الذي سيرسله. في هذه الحالة يضع موائم الإرسال عنوان ماك مخصص لوظيفة الإذاعة (broadcast address) في حقل عنوان الوجهة بالإطار. في الشبكات المحلية التي تستخدم عناوين طولها 6 بايتات (كشبكات إيثرنت وشبكات تمرير العلامة يكون العنوان المخصص لإذاعة الإطار هو سلسلة من 48 بتاً قيمة كل منها 1 (أي FF-FF-FF-FF-FF-FF بالترقيم الست عشري).

المبادئ في الواقع العملي (Principles in Practice)

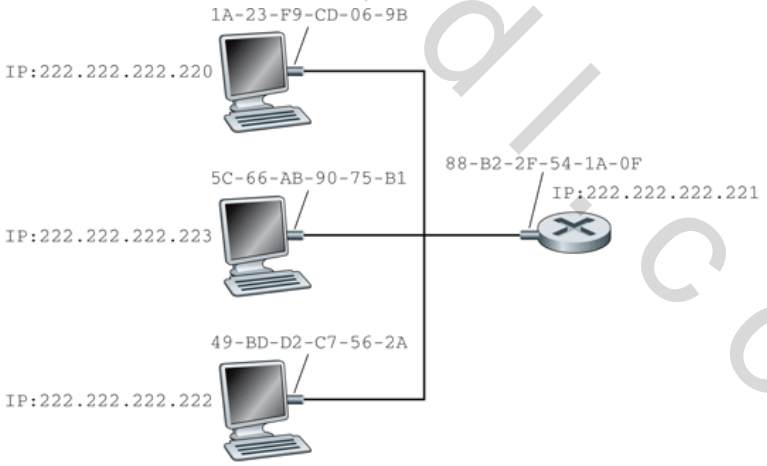
الحفاظ على استقلال الطبقات

هناك العديد من الأسباب لإعطاء العقد على الشبكة عناوين مادية (ماك) بالإضافة إلى عناوين طبقة الشبكة. أولاً: صممت شبكات البيانات المحلية (LANs) لبروتوكولات مختلفة لطبقة الشبكة وليست فقط لبروتوكولات الإنترنت. إذا خُصّصت للموائمات عناوين IP بدلاً من عناوين الماك "المحايدة"، فلن يكون من السهل عليها التعامل مع بروتوكولات طبقة الشبكة الأخرى (على سبيل المثال IPX أو DECnet). ثانياً: إذا كان على الموائمات استخدام عناوين طبقة الشبكة بدلاً من عناوين ماك، فسيتعين تخزين عنوان طبقة الشبكة في ذاكرة القراءة والكتابة (RAM) للموائم والتي ستحتاج بالتالي إلى إعادة تهيئتها في كل مرة يُنقل فيها الموائم إلى مكان جديد (أو يعاد تشغيله بعد إطفائه). هناك خيار آخر هو عدم استخدام أي عناوين للموائمات وجعل كل موائم يُمرّر البيانات (عادةً وحدة بيانات طبقة الشبكة) الموجودة في كل إطار يستلمه إلى أعلى عبر رصة البروتوكول. يمكن أن تقوم طبقة الشبكة في هذه الحالة بالتأكد من توافق عنوان طبقة الشبكة. من مشاكل هذا الخيار أنه ستتم مقاطعة المضيف عند وصول كل إطار يرسل على الشبكة المحلية، بما في ذلك الإطارات الموجّهة لعقد أخرى على نفس وصلة الإذاعة بالشبكة المحلية. الخلاصة هي أنه لكي تكون الطبقات وحدات بناء مستقلة بشكلٍ كبير في البنية المعمارية للشبكة، تحتاج الطبقات المختلفة لنظام عنونة خاص بها. لقد رأينا حتى الآن ثلاثة أنواع من العناوين: أسماء المضيفات في طبقة التطبيقات، وعناوين IP في طبقة الشبكة، وعناوين الماك في طبقة ربط البيانات.

5-4-2 بروتوكول تحويل العناوين (ARP)

نظراً لوجود عناوين لطبقة الشبكة (مثلاً عناوين IP الخاصة بالإنترنت) وعناوين لطبقة ربط البيانات (أي عناوين الماك)، هناك حاجة للتحويل بينهما. في حالة الإنترنت يضطلع بهذه المهمة بروتوكول تحويل العناوين (Address Resolution Protocol (ARP)) [RFC 826].

لفهم الحاجة إلى مثل هذا البروتوكول خذ في الاعتبار الشبكة المبيّنة في الشكل 5-17. في هذا المثال البسيط لكل عقدة عنوان IP واحد، ولكل موائم عنوان ماك واحد. كالمعتاد تبيّن عناوين IP بالصيغة العشرية المنقوطة، بينما تبيّن عناوين الماك بالترقيم الست عشري. افترض الآن أن العقدة بعنوان IP 222.222.222.220 تريد إرسال قطعة بيانات IP إلى العقدة 222.222.222.222 (على سبيل المثال قد تكون عقدة الوجهة 222.222.222.222 خادم ويب، وقد تكون عقدة الإرسال 222.222.222.220 قد حددت عنوان IP لخادم الويب بواسطة بروتوكول DNS). في هذا المثال تقع كل من عقدتي المصدر والوجهة في نفس شبكة البيانات المحلية حسب مفهوم العنونة الذي تناولناه في الجزء 4-4-2. لإرسال حزمة بيانات يجب على عقدة المصدر أن تعطي موائمها ليس فقط وحدة بيانات IP، ولكن أيضاً عنوان الماك لعقدة الوجهة 222.222.222.222. بتوفر وحدة بيانات IP ومعلومية عنوان الماك، يقوم موائم عقدة الإرسال بتكوين إطار طبقة ربط البيانات يحتوي على عنوان الماك لعقدة الوجهة ثم يرسل الإطار إلى الشبكة المحلية.



الشكل 5-17 لكل عقدة على شبكة البيانات المحلية عنوان IP، ولكل موائم عقدة عنوان ماك.

السؤال المهم الذي نتناوله في هذا الجزء هو: كيف تحدد عقدة الإرسال عنوان الماك لعقدة الوجهة التي لها عنوان IP 222.222.222.222؟ تقوم بذلك باستخدام بروتوكول تحويل العناوين (ARP)، حيث تأخذ وحدة بروتوكول ARP الموجودة على عقدة الإرسال أي عنوان IP على نفس الشبكة المحلية كمُدخل وتُرجع عنوان الماك المقابل. في المثال الذي نحن بصدده تزوّد عقدة الإرسال 222.222.222.220 وحدة ARP عليها بعنوان IP 222.222.222.222، فتُرجع لها وحدة بروتوكول ARP عنوان الماك المقابل 49-BD-D2-C7-56-2A.

وهكذا نرى أن بروتوكول ARP يحوّل عنوان IP إلى عنوان ماك. في الكثير من الجوانب يشبه ذلك بروتوكول خدمة الدليل لأسماء النطاقات (DNS) لتحويل أسماء المضيفات إلى عناوين IP، والذي سبق أن درسناه في الجزء 2-5. غير أن هناك فرقاً جوهرياً بين تحويل العناوين في الحالتين، فبينما يحوّل بروتوكول DNS أسماء المضيفات الموجودة في أي مكان على الإنترنت، يحوّل بروتوكول ARP عناوين IP إلى عناوين الماك فقط للعقد على نفس الشبكة الفرعية (subnet). إذا حاولت عقدة في كاليفورنيا استخدام بروتوكول ARP لتحويل عنوان IP لعقدة في ميسيسيبى، فإن بروتوكول ARP يُرجع تنبيهاً بحدوث خطأ.

الآن بعد أن وضّحنا الدور الذي يقوم به بروتوكول ARP لتحويل العناوين، دعنا ننظر كيف يؤدي البروتوكول هذا الدور. تحتوي كل عقدة (مضيف أو موجّه) في ذاكرة القراءة والكتابة بها على جدول لتحويل عناوين IP إلى عناوين الماك المقابلة. يبين الشكل 5-18 كيف يمكن أن يبدو جدول ARP على العقدة 222.222.222.220. يتضمن الجدول كذلك فترة العمر (Time-To-Live (TTL)) لكل مُدخل (صف) والتي تبين مدة الاحتفاظ بالصف في الجدول. لاحظ أن الجدول لا يحتوي بالضرورة على مُدخل لكل عقدة على الشبكة الفرعية، فبعض العقد ربما تكون قد انتهت صلاحية المُدخلات الخاصة بها، والبعض الآخر ربما لم يُسجّل في الجدول بعد. عادةً ما يكون وقت انتهاء صلاحية معلومة تحويل العناوين حوالي 20 دقيقة من وقت إيداع المُدخل في جدول بروتوكول ARP.

عنوان IP	عنوان الماك	فترة العمر (TTL)
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

الشكل 5-18 جدول محتمل لبروتوكول ARP على العقدة 222.222.222.220.[1]

افترض الآن أن العقدة 222.222.222.220 تريد إرسال وحدة بيانات معنونة بعنوان IP إلى عقدة أخرى على نفس الشبكة الفرعية. تحتاج عقدة الإرسال للحصول على عنوان الماك لعقدة الوجهة بمعلومية عنوان IP لتلك العقدة. تلك مهمة سهلة إذا كان جدول ARP لتحويل العناوين يتضمن المُدخل المطلوب لعنوان عقدة الوجهة. ولكن ماذا يحدث لو أن ذلك التحويل ليس مدرجاً حالياً في جدول ARP؟ بتحديد أكثر، افترض أن العقدة 222.222.222.220 بحاجة لإرسال وحدة بيانات إلى العقدة 222.222.222.222. في هذه الحالة تستخدم عقدة الإرسال بروتوكول تحويل العناوين لتحديد عنوان الماك. أولاً تُنشئ عقدة الإرسال رزمة خاصّة تسمى رزمة بروتوكول ARP. تتضمن تلك الرزمة عدّة حقول من بينها حقول لعناوين IP وعناوين الماك لكلٍّ من المُرسِل والمُستقبِل. تَستخدم رزم بروتوكول ARP نفس الصيغة للاستفسار والإجابة. الغرض من رزمة بروتوكول ARP للاستفسار هو سؤال كل العقد الأخرى الموصّلة على الشبكة الفرعية عن عنوان الماك المناظر لعنوان IP المراد تحديده.

عودةً إلى مثالنا الذي نحن بصدده، ترسل العقدة 222.222.222.220 رزمة استفسار ARP إلى الموائم مع إشارة تبين أن على الموائم إرسال الرزمة على عنوان الماك المخصص للإذاعة (أي FF-FF-FF-FF-FF-FF) . يغلّف الموائم رزمة استفسار ARP في إطار طبقة ربط البيانات، ويضع عنوان الإذاعة في حقل عنوان وجهة الإطار، ثم يرسل الإطار على الشبكة الفرعية. تذكّر التناظر الذي ذكرناه آنفاً

[1] يشار إلى بعض "الجداول" في الكتاب الأصلي بالأشكال، لذا تركنا الإشارة إليها "بالأشكال" من أجل عدم إحداث تغيير بتسلسل ترقيم الأشكال والجداول مما يسهل الرجوع للكتاب الأصلي (لمن أراد ذلك).

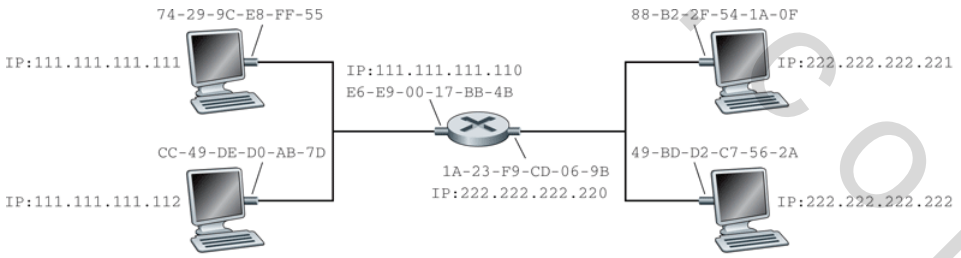
فيما يتعلق برقم الضمان الاجتماعي والعنوان البريدي حيث تمثل رزمة استفسار ARP شخصاً يصيح في غرفة مزدحمة بمقصورات المكاتب الصغيرة في شركةٍ ما (مثلاً شركة AnyCorp) قائلاً: "ما هو رقم الضمان الاجتماعي للشخص الذي عنوانه البريدي: مقصورة 13، غرفة 112، شركة AnyCorp، بالو ألتو، كاليفورنيا؟" يصل الإطار الذي يتضمن استفسار ARP إلى كل الموائمات الأخرى على الشبكة الفرعية، ونظراً لأن ذلك الإطار يحمل عنوان إذاعة، يقوم موائم كل عقدة بتمرير رزمة استفسار ARP التي استخلصها من الإطار إلى وحدة بروتوكول ARP الخاصة بتحويل العناوين على تلك العقدة. تفحص كل عقدة عنوان IP في رزمة استفسار ARP، وتقارنه بعنوان IP الخاص بها. تقوم العقدة التي تجد ذلك العنوان مطابقاً لعنوان IP الخاص بها بالرد على العقدة المستفسرة برزمة إجابة ARP تتضمن المطابقة المطلوبة بين عنوان IP المعروف وعنوان الماك المناظر. عندئذٍ يمكن للعقدة المستفسرة 222.222.222.220 تحديث جدول ARP لتحويل العناوين لديها ثم ترسل وحدة بيانات IP التي تود إرسالها بعد تغليفها في إطار طبقة ربط البيانات فيه عنوان الماك للوجهة هو نفسه عنوان الماك الخاص بالعقدة التي ردت على رزمة استفسار ARP السابقة.

هناك شيئان جديران بالملاحظة فيما يتعلق ببروتوكول ARP لتحويل العناوين. أولاً: في حين تُرسل رسالة استفسار ARP ضمن إطار إذاعة، تُرسل رسالة إجابة ARP ضمن إطار عادي (موجّه إلى عقدة واحدة). قبل مواصلة القراءة عليك أن تفكر في السبب وراء ذلك. ثانياً: يُعتبر بروتوكول ARP لتحويل العناوين من نوع "وصّل وشغّل" (plug-and-play)، بمعنى أن جدول ARP على العقدة يتم انشاؤه وتحديثه تلقائياً ـ أي لا يحتاج الأمر إلى تهيئته يدوياً بواسطة مدير النظام. وإذا حدث وفُصلت عقدة من الشبكة الفرعية، فإن المُدخل الخاص بها في تلك الجداول يتم حذفه في النهاية من جداول ARP على العقد المتبقية على الشبكة الفرعية.

إرسال وحدة بيانات إلى عقدة خارج نطاق الشبكة الفرعية

لعله يكون قد اتضح الآن كيف يعمل بروتوكول ARP لتحويل العناوين عندما تريد عقدة إرسال وحدة بيانات إلى عقدة أخرى تقع على نفس الشبكة الفرعية (تم تعريف الشبكة الفرعية بدقة في الجزء 4-4-2). دعنا الآن نناقش الحالة الأكثر تعقيداً عندما تريد عقدة على شبكة فرعية إرسال وحدة بيانات طبقة الشبكة إلى عقدة خارج نطاق الشبكة الفرعية (أي عبر موجّه إلى شبكة فرعية أخرى). سنناقش هذا الوضع في سياق الشكل 5-19، والذي يبين شبكة بسيطة تتكون من شبكتين فرعيتين موصلتين ببعضهما عن طريق موجّه.

هناك عدّة أشياء جديرة بالملاحظة فيما يتعلّق بالشكل 5-19. أولاً: هناك نوعان من العقد (مضيفات وموجّهات). لكل مضيف عنوان IP واحد وموائم واحد فقط. أما الموجّه ـ فكما لاحظنا في الفصل الرابع ـ فله عنوان IP لكل واجهة (interface) من واجهاته، ولكلٍّ منها هناك أيضاً موائم ووحدة بروتوكول ARP لتحويل العناوين. نظراً لأن الموجّه في الشكل 5-19 له واجهتان، فسيكون لديه عنوانان من عناوين IP، ووحدتا ARP، وموائمان. بالطبع يكون لكل موائم على الشبكة عنوان ماك خاص به.



الشكل 5-19 شبكتان فرعيتان موصّلتان عبر موجّه.

لاحظ أيضاً أن الشبكة الفرعية 1 لها العنوان 111.111.111/24، بينما الشبكة الفرعية 2 لها العنوان 222.222.222/24. وبالتالي تأخذ عناوين IP لكل الواجهات الموصلة بالشبكة الفرعية 1 الشكل 111.111.111.xxx، في حين تأخذ عناوين IP لكل الواجهات الموصلة بالشبكة الفرعية 2 الشكل 222.222.222.xxx.

لنناقش الآن كيف يقوم مضيف على الشبكة الفرعية 1 بإرسال وحدة بيانات إلى مضيف على الشبكة الفرعية 2. بالتحديد افترض أن المضيف 111.111.111.111 يريد إرسال وحدة بيانات IP إلى المضيف 222.222.222.222. يمرر المضيف المُرسِل وحدة البيانات إلى الموائم لديه كالعادة، غير أنه يتعين على المضيف المُرسِل أيضاً أن يبين للموائم عنوان ماك مناسب لوجهة تلك الوحدة. ما عنوان الماك الذي يمكن أن يستخدمه موائم المُرسِل؟ قد تتسرع بالتخمين بأن ذلك العنوان هو عنوان الماك لموائم مضيف الوجهة 222.222.222.222 أي 49-BD-D2-C7-56-2A، غير أن هذا التخمين خطأ للأسف! إذا استخدم موائم المُرسِل عنوان الماك ذلك، فلن يكترث أيٌّ من الموائمات على الشبكة الفرعية 1 برفع وحدة بيانات IP التي تصله إلى طبقة الشبكة الموجودة أعلاه لأن عنوان الماك لوجهة الإطار لن يطابق عنوان الماك لأيٍ منها. عندئذٍ ستموت وحدة البيانات تلك ويلفها النسيان.

أما إذا أمعنّا النظر في الشكل 5-19 فسنرى أنه لكي تتمكّن وحدة بيانات من الانتقال من العقدة 111.111.111.111 إلى عقدة على الشبكة الفرعية 2، ينبغي أن ترسل وحدة البيانات أولاً إلى واجهة الموجّه بعنوان IP 111.111.111.110. وهكذا يكون العنوان المناسب لوجهة الإطار هو عنوان الماك لواجهة الموجّه 111.111.111.110، أي E6-E9-00-17-BB-4B. ولكن كيف يحصل المضيف المُرسِل على عنوان الماك لـ 111.111.111.110؟ باستعمال بروتوكول ARP طبعاً! بمجرد حصول موائم المُرسِل على عنوان الماك هذا، يقوم بإنشاء إطار (يضم وحدة البيانات المعنونة إلى 222.222.222.222) ويرسل الإطار إلى الشبكة الفرعية 1. تكتشف واجهة الموجّه على الشبكة الفرعية 1 أن إطار طبقة ربط البيانات هذا موجّه إليها، فترفع الإطار إلى طبقة الشبكة على الموجّه. أخيراً انتقلت وحدة بيانات IP بنجاح من مضيف المصدر إلى الموجّه! لكنّ مهمتنا لم تنته بعد! لا يزال علينا نقل وحدة

البيانات من الموجّه إلى وجهتها النهائية. على الموجّه الآن تحديد الواجهة الصحيحة عليه والتي ينبغي إرسال وحدة البيانات إليها. كما بيّنا في الفصل الرابع، يتم ذلك باستشارة جدول التوجيه الموجود على الموجّه. يُخبر جدول التوجيه الموجّه أن وحدة البيانات سترسل عن طريق واجهة الموجّه التي لها عنوان IP 222.222.222.220. تدفع تلك الواجهة بعد ذلك بوحدة البيانات إلى موائمها، والذي يقوم بدوره بتغليف وحدة البيانات في إطار جديد ويرسل الإطار إلى الشبكة الفرعية 2. في هذه المرّة يكون عنوان الماك لوجهة الإطار هو في الحقيقة عنوان الماك للوجهة النهائية للإطار. وكيف يحصل الموجّه على عنوان الماك لهذه الوجهة؟ من بروتوكول ARP طبعاً!

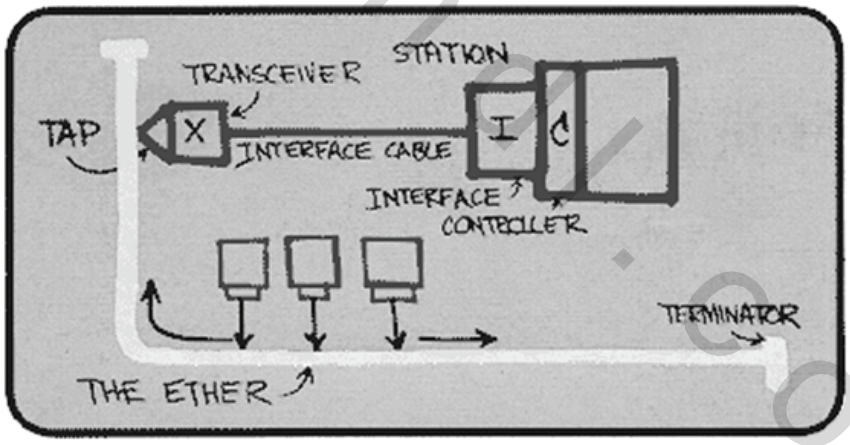
تم تعريف بروتوكول ARP للإيثرنت في طلب التعليقات RFC 826، كما توجد مقدمة لطيفة عن ARP في المقال التدريبي RFC 1180 عن بروتوكول TCP/IP. سوف نستكشف المزيد من تفاصيل بروتوكول ARP من خلال التمارين في نهاية الفصل.

5-5 شبكة الإيثرنت

لقد اكتسحت الإيثرنت تقريباً سوق شبكات البيانات المحلية السلكية. في الثمانينيات وأوائل التسعينيات واجهت الإيثرنت العديد من التحديات من التقنيات الأخرى لشبكات البيانات المحلية، بما في ذلك شبكات حلقة العلامة (token ring)، وشبكات واجهة البيانات الموزعة عبر الألياف الضوئية (FDDI)، وشبكات نمط النقل غير المتزامن (ATM). نجح البعض من تلك التقنيات في الاستحواذ على جزء من سوق الشبكات المحلية لبضع سنوات. غير أن الإيثرنت ومنذ اختراعها في أواسط السبعينيات واصلت نموها وتطورها وتمسّكت بمركزها المهيمن. واليوم تعتبر الإيثرنت إلى حد كبير أكثر تقنيات الشبكات المحلية انتشاراً، وهي مرشحة لتبقى كذلك في المُستقبل المنظور. قد يمكننا القول أن الإيثرنت كانت للشبكات المحلية بمثابة الإنترنت للشبكات العالمية.

هناك العديد من الأسباب التي ساهمت في نجاح الإيثرنت. أولاً: كانت الإيثرنت أول شبكة محلية سريعة قُدِّر لها الانتشار على نطاق واسع. ونظراً

لانتشارها المبكر، ألِفَ مشرفو الشبكات الإيثرنت عن كَثَب – بعجائبها والتواءاتها – ومن ثم كانوا يعارضون التحوّل إلى تقنيات الشبكات المحلية الأخرى عند ظهورها على الساحة. ثانياً: كانت التقنيات الأخرى – مثل: token ring، FDDI، ATM – أكثر تعقيداً وأغلى كلفةً من الإيثرنت، الأمر الذي ثبّط عزيمة مشرفي الشبكات أكثر عن ترك الإيثرنت والتحوّل إلى تلك التقنيات الجديدة. ثالثاً: كان السبب الأكثر إقناعاً للتحوّل إلى تقنية شبكة محلية أخرى (مثل: FDDI أو ATM) عادةً هو المعدّلات الأعلى لإرسال البيانات التي توفرها تلك التقنيات الجديدة، ولكن الإيثرنت كانت دائماً تستبسل في المقاومة منتجةً نسخاً جديدة تعمل بمعدلات إرسال تساوي أو تتجاوز تلك المعدّلات. وفي بداية التسعينيات ظهرت الإيثرنت المحوّلة (switched Ethernet)، مما أدى إلى زيادةٍ أكبر في معدلات الإرسال الفعلية. وأخيراً: نظراً لزيادة شعبية الإيثرنت وانتشارها، أصبحت أجهزة الإيثرنت (وبخاصة الموائمات والمحوّلات) سلعاً رائجة ورخيصة جداً.

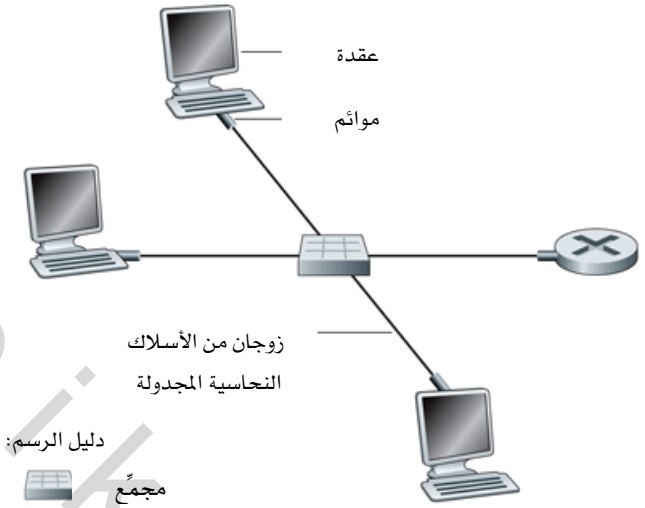


الشكل 5-20 تصميم ميتكالف الأصلي لمعيار BASE510 لشبكة الإيثرنت، والذي تضمّن كبل واجهة يصل موائم الإيثرنت بجهاز إرسال واستقبال خارجي.

اختُرعت شبكة الإيثرنت المحلية الأصلية في منتصف السبعينيات من قِبَل بوب ميتكالف وديفيد بوجز. يبين الشكل 5-20 رسماً تخطيطياً لميتكالف لهذا الاختراع. ستلاحظ في الشكل أن شبكة الإيثرنت المحلية الأصلية كانت تستخدم ناقلاً محورياً (coaxial bus) لربط العقد الموصّلة بالشبكة. في الواقع استمرت تقنية الناقل المحوري لطبوغرافية شبكة الإيثرنت على مدار الثمانينيات وحتى أواسط التسعينيات. جديرٌ بالذكر أن الإيثرنت بهيئة الناقل المحوري تمثل شبكة محلية بقناة إذاعة مشتركة، حيث تنتقل كل الإطارات المُرسَلة إلى كل الموائمات الموصّلة بالناقل وتتم معالجتها من قِبَلها.

بنهاية التسعينيات كانت معظم الشركات والجامعات قد استبدلت شبكاتها المحلية بتجهيزات إيثرنت تستخدم طبوغرافية النجمة (star topology) التي أساسها مجمِّع (hub). كما هو مبين في الشكل 5-21، في مثل هذه الترتيبة توصّل المضيفات (والموجّه) مباشرة إلى مجمِّع بزوج من الأسلاك النحاسية المجدولة. المجمِّع هو أداة تابعة للطبقة المادية تتعامل مع البتات المفردة وليس الإطارات. عندما يتلقى المجمِّع بتاً (يمثّل 0 أو 1) من إحدى واجهاته فإنه يقوم ببساطة بتكوين البت من جديد برفع طاقة إشارته الكهربية، ثم يرسله إلى كل الواجهات الأخرى. وهكذا فإن الإيثرنت بترتيبة نجمية ومجمِّع في المركز لاتزال شبكة إذاعة محلية. بتحديد أكثر إذا استلم المجمِّع إطارات من واجهتين مختلفتين في نفس الوقت سيحدث اصطدام، وسيتعين على العُقد التي أنشأت تلك الإطارات إعادة إرسالها.

في بداية القرن الجديد طرأ على الإيثرنت تطوير رئيس آخر. واصلت تجهيزات الإيثرنت استخدام طبوغرافية النجمة، ولكن مع استبدال المجمِّع الموجود في المركز بمحوّل (switch). سنفحص الإيثرنت المحوّلة بتفصيل أكثر لاحقاً في هذا الفصل. نكتفي الآن بالقول بأن المحوّل لا يمنع الاصطدام فقط، بل ويعتبر كذلك مثالاً أصيلاً لمحوّل الرزم بأسلوب "خزّن ومرّر" (store-and-forward). ولكن على خلاف الموجّه الذي يعمل حتى طبقة 3 في رصة البروتوكولات، فإن المحوّل يعمل حتى طبقة 2 فقط.



الشكل 5-21 طبوغرافية النجمة للإيثرنت. يتم توصيل العقد بعضها ببعض عن طريق مجمِّع.

5-5-1 صيغة إطار الإيثرنت

يمكننا تعلّم الكثير عن الإيثرنت بفحص إطار الإيثرنت والمبيَّن في الشكل 5-22. لإضفاء طابع واقعي على هذه المناقشة حول إطارات الإيثرنت، دعنا نأخذ في الاعتبار إرسال وحدة بيانات IP من مضيف إلى مضيف آخر يقع على نفس شبكة الإيثرنت المحلية (على سبيل المثال شبكة الإيثرنت المبينة في الشكل 5-21). رغم أن حمولة إطار الإيثرنت في حالتنا هذه هي وحدة بيانات IP، إلا أننا نذكر هنا بشكلٍ عابر أن إطار الإيثرنت يمكن أيضاً أن يحمل رزماً لأنواع أخرى من طبقة الشبكة. افترض أن موائم الإرسال A له عنوان الماك AA-AA-AA-AA-AA-AA وموائم الاستلام B له عنوان الماك BB-BB-BB-BB-BB-BB. يقوم موائم الإرسال بتغليف وحدة بيانات IP ضمن إطار إيثرنت ويدفع به لأسفل إلى الطبقة المادية. يستلم موائم الاستلام الإطار من الطبقة المادية أسفله، ويستخلص وحدة بيانات IP منه، ثم يمررها إلى طبقة الشبكة أعلاه. في هذا السياق دعنا الآن نفحص الحقول الستّة التي يتألف منها إطار الإيثرنت كما هو موضح في الشكل 5-22:

الشكل 5-22 صيغة إطار الإيثرنت.

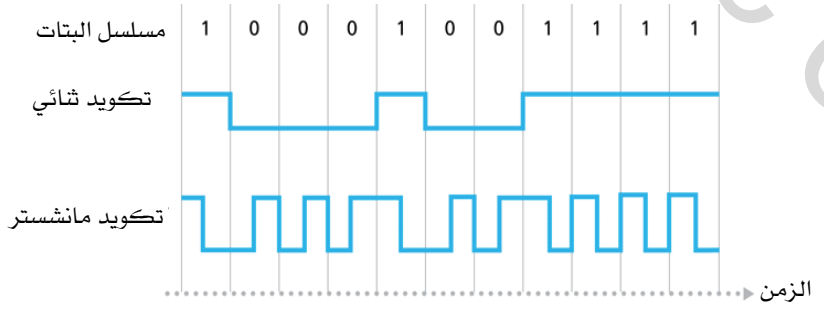
- حقل البيانات (يتكوّن من 46 بايتاً إلى 1500 بايت): يحمل هذا الحقل وحدة بيانات IP. يبلغ حجم وحدة الإرسال القصوى (Maximum Transmission Unit (MTU)) للإيثرنت 1500 بايت، وهذا يعني أنه إذا تجاوزت وحدة بيانات IP 1500 بايت فإن المضيف يضطر لتجزيء حزمة البيانات كما هو موضحٌ في الجزء 4-4-1. أما الحد الأدنى لحقل البيانات فهو 46 بايتاً، وهذا يعني أنه إذا كانت وحدة بيانات IP أقل من 46 بايتاً فإنه ينبغي "حشو" حقل البيانات لملئه حتى 46 بايتاً. في حالة استخدام الحشو (stuffing)، تتضمن البيانات التي تُرفع إلى طبقة الشبكة الحشو بالإضافة إلى وحدة بيانات IP الأصلية. في هذه الحالة تستخدم طبقة الشبكة حقل الطول في ترويسة وحدة بيانات IP لإزالة الحشو.
- عنوان الوجهة (6 بايتات): يحتوي هذا الحقل على عنوان الماك لموائم الوجهة، أي BB-BB-BB-BB-BB-BB في المثال الذي نحن بصدده. عندما يتلقى موائم B إطار إيثرنت يحمل في حقل عنوان الوجهة BB-BB-BB-BB-BB-BB أو عنوان الماك المخصص لعملية الإذاعة، فإنه يمرر محتويات حقل البيانات الموجود في الإطار إلى طبقة الشبكة أعلاه. أما إذا تلقى إطاراً بأي عنوان ماك آخر فإنه يستبعد ذلك الإطار ولا يعيره أي اهتمام.
- عنوان المصدر (6 بايتات): يحتوي هذا الحقل على عنوان الماك للموائم الذي يرسل الإطار على شبكة البيانات المحلية. في مثالنا الحالي يكون هذا العنوان AA-AA-AA-AA-AA-AA.
- النوع (بايتان): يسمح حقل النوع للإيثرنت بالقيام بعملية التجميع (multiplexing) لبروتوكولات مختلفة لطبقة الشبكة. لفهم هذه الحقيقة

تذكّر أن المضيفات يمكن أن تستخدم بروتوكولات أخرى لطبقة الشبكة بالإضافة إلى بروتوكول IP. في الواقع قد يدعم مضيف بعينه عدة بروتوكولات لطبقة الشبكة، حيث يستخدم المضيف بروتوكولات مختلفة مع التطبيقات المختلفة. لهذا السبب عندما يصل إطار إيثرنت إلى الموائم B يحتاج هذا الموائم لمعرفة بروتوكول طبقة الشبكة الذي يجب أن يمرر (أي يوزع demultiplex) محتويات حقل البيانات ضمن ذلك الإطار إليه. لكلٍّ من بروتوكول IP وغيره من بروتوكولات طبقة الشبكة الأخرى (على سبيل المثال: Novell ، وIPX، وAppleTalk) رقم النوع المعياري الذي يميِّزه. علاوةً على ذلك فإن بروتوكول تحويل العناوين ARP (والذي تناولناه في الجزء السابق) له أيضاً رقم النوع الخاص به. لاحظ أن حقل النوع يشبه حقل البروتوكول في وحدة بيانات طبقة الشبكة وحقل رقم المنفذ في قطعة طبقة النقل؛ والغرض من كل تلك الحقول وصل بروتوكول في طبقة ما ببروتوكول في طبقة تعلوها.

- شفرة فحص الفائض الدوري CRC (4 بايتات): كما تقدّم في الجزء 5-2-3، الغرض من حقل شفرة CRC هو تمكين موائم الاستقبال ـ الموائم B ـ من اكتشاف ما إذا كانت هناك أي أخطاء قد طرأت على الإطار أثناء انتقاله من موائم الإرسال، أي ما إذا كانت أيٌّ من بتات الإطار قد تغيرت (1 تحوّل إلى 0 أو 0 تحوّل إلى 1). تتضمّن أسباب وقوع أخطاء في البتات: الاضمحلال في قوة الإشارة، ووجود طاقة كهرومغناطيسية محيطة تتسرب إلى كبلات الإيثرنت وبطاقات المواءمة. يتم اكتشاف الأخطاء كالتّالي: عندما ينشئ مضيف A إطار الإيثرنت لإرساله، يقوم بتعيين قيمة حقل CRC بالإطار، والتي تحسب كدالةٍ في كل بتات الإطار الأخرى ما عدا بتات الديباجة (الاستهلال) (preamble). وعندما يستلم مضيف B الإطار يطبّق نفس الدالة على نفس الجزء من الإطار الذي وصله ليرى ما إذا كانت النتيجة مساويةً للقيمة الموجودة في حقل CRC بالإطار. يطلق على هذه العملية في مضيف الاستقبال تدقيق CRC. إذا كانت نتيجة ذلك الفحص سلبية (أي كانت

نتيجة تطبيق الدالة على بقية الإطار لا تساوي محتويات حقل CRC) فإن المضيف B يدرك أن خطأً قد طرأ على الإطار.

- الديباجة (8 بايتات): يبدأ إطار الإيثرنت بحقل ديباجة طوله 8 بايتات. البايتات السبع الأولى في الديباجة لها نفس القيمة وهي 10101010، في حين يكون البايت الأخير 10101011. تستخدم البايتات السبع الأولى لـ"إيقاظ" موائمات الاستقبال ولتحقيق التزامن بين ساعات التوقيت لديها وساعة التوقيت لدى المُرسِل. لماذا يمكن أن تكون الساعات غير متزامنة؟ تذكّر أن الموائم A يهدف لإرسال الإطار بمعدّل 10 ميجابت/ثانية، أو 100 ميجابت/ثانية، أو 1 جيجابت/ثانية حسب نوع شبكة الإيثرنت المحلية. ومع ذلك فنظراً لأنه لا يوجد شيءٌ مثاليٌ في هذا العالم، فلن يرسل الموائم A الإطار بنفس معدل الإرسال المستهدف بالضبط، بل سيكون هناك دائماً بعض الانحراف عن هذا المعدّل – انحراف لا يُعرف مقداره مسبقاً لدى الموائمات الأخرى على الشبكة المحلية. بوسع موائم الاستقبال أن يحقق المطابقة المطلوبة مع ساعة موائم الإرسال A ببساطة بالمطابقة على بتات البايتات السبع الأولى من الديباجة. أما البتان الأخيران من بتات البايت الثامن في الديباجة (بقيمة 1 لكلٍّ منهما) فتنبهان الموائم B إلى أن "الأشياء المهمة على وشك الوصول". عندما يرى المضيف B البتين المتتاليين بقيمة 1، فإنه يدرك أن البايتات الست القادمة هي عنوان الوجهة. يمكن لموائمٍ ما أن يعرف أن إطاراً قد انتهى ببساطة بملاحظة غياب التيار على الوصلة المادية.



الشكل 5-23 تكويد مانشستر.

تستخدم الإيثرنت إرسالاً في حيز التردد الأصلي (baseband transmission)، بمعنى أن الموائم يرسل الإشارة الرقمية مباشرة إلى قناة الإذاعة (أي لا تنقل بطاقة الواجهة الإشارة إلى نطاقٍ ترددي آخر كما يحدث في أنظمة خط المشترِك الرقمي غير المتماثل (ADSL) ونظام مودم الكبل (cable modem). تستخدم العديد من تقنيات الإيثرنت (مثلاً 10BASE-T) تكويد مانشستر (Manchester coding)، كما هو مبين في الشكل 5-23. في هذا الأسلوب تتضمن إشارة كل بت انتقالاً في مستوى الإشارة: يُمثّل البت 1 بانتقال من أعلى إلى أسفل بينما يُمثّل البت 0 بانتقال من أسفل إلى أعلى. يرجع السبب في استخدام كود مانشستر إلى أن ساعات التوقيت لدى موائمات الإرسال والاستقبال تكون غير متزامنة تماماً في واقع الأمر. يساعد وجود انتقال في الإشارة دائماً في منتصف كل بت مضيفَ الاستقبال في أن يزامن ساعته مع ساعة مضيف الإرسال. بمجرد تحقيق ذلك التزامن لساعة موائم الاستقبال سيكون بوسع المُستقبل تحديد موقع كل بت يتم استقباله وتعيين ما إذا كانت قيمته 1 أو 0. يُلاحَظ أن عملية تكويد البيانات بكود مانشستر تتم في الطبقة المادية وليس في طبقة ربط البيانات، ولكننا آثرنا الإلماح إليها سريعاً هنا لأنها تُستخدم على نطاق واسع في الإيثرنت.

الخدمة اللاتوصيلية غير الموثوقة

توفر كل تقنيات الإيثرنت خدمة لاتوصيلية (connectionless) لنقل البيانات لطبقة الشبكة. أي أنه عندما يريد الموائم A إرسال وحدة بيانات إلى الموائم B فإنه يغلّف وحدة البيانات في إطار إيثرنت، ويرسل الإطار على الشبكة المحلية، دون أن يسبق ذلك أي إجراءات مصافحة (handshaking) لإنشاء توصيلة مع الموائم B. إن هذه الخدمة اللاتوصيلية في الطبقة 2 تشبه خدمة IP لنقل وحدات البيانات في الطبقة 3 وخدمة UDP اللاتوصيلية في الطبقة 4.

دراسة حالة (Case Study)

بوب ميتكالف والإيثرنت

كطالب دكتوراه في جامعة هارفارد في أوائل السبعينيات، عمل بوب ميتكالف على شبكة أربانت (ARPAnet) في معهد ماسوشيستس للتكنولوجيا (MIT). ومن خلال دراساته اطّلع ميتكالف أيضاً على جهود أبرامسون في مجال تطوير بروتوكول ألوها وبروتوكولات الوصول العشوائي. وبعد إكماله دراسة الدكتوراه وقبل التحاقه مباشرةً بوظيفته الجديدة بمركز أبحاث زيروكس (Xerox) في بالو ألتو (Xerox PARC)، قام ميتكالف بزيارة أبرامسون وزملائه بجامعة هاواي لمدة ثلاثة أشهر، حيث اطلع عن كثب على شبكة ألوهانت. في مركز أبحاث Xerox PARC، تعامل ميتكالف مع حاسبات الألتو، والتي كانت تعتبر لأكثر من سبب الجيل المتقدم الذي سبق ظهور الحاسبات الشخصية في الثمانينيات. أيقن ميتكالف بالحاجة لتشبيك تلك الحاسبات بطريقة قليلة الكلفة. وهكذا بنى ميتكالف على معرفته بشبكات الأربانت والألوهانت وبروتوكولات الوصول العشوائي، ليتمكن مع زميله ديفيد بوجز من اختراع الإيثرنت.

عملت شبكة الإيثرنت الأصلية بمعدّل إرسال قدره 2.94 ميجابت/ثانية وربطت مضيفات وصل عددها إلى 256 مضيف فصلت بينها مسافات وصلت إلى ميل واحد. نجح ميتكالف وبوجز في تمكين أغلب الباحثين في معهد أبحاث Xerox PARC من الاتصال ببعضهم البعض من خلال حاسبات ألتو لديهم. بعد ذلك صاغ ميتكالف تحالفاً بين شركات Xerox و Digital و Intel لتأسيس الإيثرنت كشبكة معيارية بمعدّل إرسال 10 ميجابت/ثانية، والتي صدّقت عليها منظمة IEEE. لم تهتم Xerox كثيراً بالتطبيقات التجارية للإيثرنت. وفي عام 1979 أسس ميتكالف شركته الخاصة Com3، والتي طوّرت تقنيات الربط بالشبكات بما في ذلك تقنية الإيثرنت واهتمت بتطبيقاتها التجارية. في أوائل الثمانينيات طوّرت Com3 وسوّقت بطاقات الإيثرنت لحاسب IBM الشخصي ذائع الصيت آنذاك. وفي عام 1990 ترك ميتكالف Com3 عندما كان لديها 2,000 موظف وعائداتها 400 مليون دولار.

أيضاً توفر كل تقنيات الإيثرنت خدمة غير موثوقة (unreliable) لطبقة الشبكة. وبتحديدٍ أكثر عندما يستلم الموائم B إطاراً من الموائم A فإنه يُخضع الإطار لتدقيق CRC لاكتشاف الخطأ، ولكنه لا يرسل إشعار استلام عندما يجتاز الإطار عملية الفحص تلك، ولا إشعاراً سلبياً عندما لا يجتاز الإطار هذا الفحص. وعليه فعندما يفشل إطار في اجتياز تدقيق CRC لاكتشاف الأخطاء فإن الموائم B يكتفي فقط بإهمال ذلك الإطار. وهكذا لن تكون لدى الموائم A أي فكرة عما إذا كان إطاره الذي أرسله قد وصل إلى الموائم B واجتاز فحص اكتشاف الأخطاء أم لا. إن غياب إمكانيات النقل الموثوق (في طبقة ربط البيانات) تساعد في جعل الإيثرنت بسيطة ورخيصة الكلفة، غير أن ذلك يعني في المقابل أن سلسلة وحدات البيانات التي تمرّر إلى طبقة الشبكة يمكن أن تحدث بها فجوات.

إذا كانت هناك فجوات بسبب إهمال بعض إطارات الإيثرنت المعطوبة فهل يرى التطبيق على المضيف B تلك الفجوات هو الآخر؟ كما رأينا في الفصل الثالث يعتمد هذا على ما إذا كان التطبيق يستخدم بروتوكول UDP أو بروتوكول TCP. في حالة استخدام بروتوكول UDP فإن التطبيق على المضيف B سيلحظ فعلاً وجود فجوات في البيانات. وفي المقابل إذا استخدم التطبيق بروتوكول TCP فإن المضيف B لن يُرسل إشعارات باستلام البيانات المُرسِلة في الإطارات التي تم إهمالها، مما يجعل بروتوكول TCP على المضيف A يعيد إرسال تلك البيانات من جديد. لاحظ أنه عندما يعيد TCP إرسال البيانات فستعود البيانات في النهاية إلى موائم الإيثرنت الذي أهملها في السابق. وهكذا فإن الإيثرنت تعيد إرسال البيانات، ولكنها لا تدري ما إذا كانت تنقل وحدة بيانات جديدة محمّلة ببيانات جديدة أو وحدة بيانات تحتوي على بيانات سبق إرسالها مرة واحدة على الأقل.

2-5-5 بروتوكول الوصول المتعدد للإيثرنت: الوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام (CSMA/CD)

عندما تُوصّل العقد فيما بينها عن طريق مجمِّع (hub) (في مقابل محوّل طبقة ربط البيانات (switch))، كما هو مبين في الشكل 5-21، تكون شبكة الإيثرنت

شبكة إذاعة محلية بحق - بمعنى أنه عندما يرسل موائم إطاراً، فإن كل الموائمات الموصلة على شبكة البيانات المحلية تتلقى ذلك الإطار. نظراً لأن الإيثرنت يمكن أن تستخدم أسلوب الإذاعة، فإنها تحتاج ابتداءً إلى نظام وصول متعدد. تستخدم الإيثرنت البروتوكول الشهير للوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام (CSMA/CD). تذكّر من استعراضنا لذلك البروتوكول في الجزء 5-3 أن بروتوكول CSMA/CD يعمل كالتالي:

1. يمكن لموائم البدء في الإرسال في أي وقت يشاء، بمعنى أن البروتوكول لا يستخدم مفهوم الشرائح الزمنية.
2. لن يرسل الموائم إطاراً أبداً بمجرد إحساسه بأن موائماً آخر يرسل حالياً، بمعنى أن الموائم يستخدم أسلوب الإنصات للناقل.
3. يقوم الموائم بقطع إرساله بمجرد اكتشافه أن موائماً آخر يرسل أيضاً، بمعنى أن الموائم يستخدم أسلوب اكتشاف الاصطدام.
4. قبل محاولة إعادة الإرسال يقوم الموائم بالانتظار لوقت عشوائي عادةً ما يكون صغيراً مقارنةً بالوقت اللازم لإرسال إطار.

توفر تلك الآليات لبروتوكول CSMA/CD أداءً أفضل بكثير من أداء بروتوكول ألوها الشرائحي في بيئة الشبكة المحلية. في الحقيقة عندما يكون تأخير الانتقال الأقصى بين العقد صغيراً جداً، فإن كفاءة بروتوكول CSMA/CD يمكن أن تقترب من 100٪. لكن ينبغي ملاحظة أن الآليات رقم 2 و3 المذكورة أعلاه تتطلب من كل موائم إيثرنت أن يكون قادراً على: (1) الإحساس بما إذا كان هناك موائم آخر يرسل، و(2) اكتشاف وقوع اصطدام أثناء عملية الإرسال. تؤدّي موائمات الإيثرنت هاتين المهمّتين بقياس مستويات الجهد الكهربائي (الفولطية) قبل وأثناء الإرسال.

ينفّذ كل موائم بروتوكول CSMA/CD بدون تنسيق محدد مع الموائمات الأخرى على الإيثرنت. ضمن موائم بعينه يعمل بروتوكول CSMA/CD كالتّالي:

1. يحصل الموائم على وحدة بيانات من طبقة الشبكة، فينشئ إطار إيثرنت، ويضع الإطار في المخزن المؤقت على الموائم.

2. إذا أحس الموائم أن القناة شاغرة (أي أنه لا تدخل طاقة إشارة الموائم من القناة لفترة تبلغ مدة إرسال 96 بتاً)، فإنه يبدأ في إرسال الإطار. إذا أحس الموائم أن القناة مشغولة، فإنه ينتظر إلى أن تختفي أي طاقة إشارة (زائد مدة إرسال 96 بتاً) وبعد ذلك يبدأ في إرسال الإطار.
3. أثناء إرسال الإطار، يراقب الموائم القناة لاكتشاف وجود طاقة إشارة قادمة من الموائمات الأخرى. إذا تمكّن الموائم من إرسال الإطار كاملاً بدون اكتشاف طاقة إشارة من الموائمات الأخرى فإنه يكون قد نجح في إرسال ذلك الإطار.
4. إذا اكتشف الموائم طاقة إشارة من الموائمات الأخرى أثناء قيامه بالإرسال، فإنه يتوقف عن إرسال إطاره ويرسل بدلاً من ذلك إشارة تشويش طولها 48 بتاً.
5. بعد قطع الإرسال (وإرسال إشارة التشويش) يدخل الموائم مرحلة تراجع أسّي (exponential backoff). بالتحديد عندما تواجه عملية إرسال إطارٍ بعينه الاصطدام رقم n على التوالي، فإن الموائم يختار قيمة عشوائية للمتغير K من بين القيم $(0, 1, 2, \ldots, 2^m - 1)$، حيث $m = \min(n, 10)$. ينتظر الموائم مدة إرسال $K \times 512$ بتاً وبعدها يعود للخطوة 2.

من المفيد هنا ذكر بضعة تعليقات حول بروتوكول CSMA/CD. إن الغرض من بث إشارة التشويش التأكد من أن كل موائمات الإرسال الأخرى قد أدركت وجود الاصطدام. دعنا نأخذ هذا المثال. افترض أن الموائم A يبدأ في إرسال إطار، ولكن مباشرةً قبل وصول إشارة إطار A إلى B يبدأ الموائم B في الإرسال. لذا يكون B قد أرسل فقط بضعة بتات عندما يقطع إرساله. هذه البتات القليلة ستنتقل بالفعل إلى A، ولكنّها قد لا تشكّل طاقة إشارة كافية لتمكين A من اكتشاف وجود الاصطدام . للتأكد من أن A يكتشف الاصطدام (لكي يقوم هو الآخر بقطع إرساله)، يقوم B بإرسال إشارة تشويش طولها 48 بتاً.

لنأخذ في الاعتبار الآن خوارزمية التراجع الأسّي. أول ما نلاحظه هنا هو أن وقت البت (أي الوقت الذي يستغرقه إرسال بت واحد) قصيرٌ جداً، فعلى إيثرنت

سرعتها 10 ميجابت/ثانية يكون وقت البت 0.1 ميكروثانية. دعنا الآن نأخذ هذا المثال: افترض أن موائماً يحاول إرسال إطارٍ للمرة الأولى ولكنه يكتشف اصطداماً أثناء الإرسال. يختار الموائم $K = 0$ باحتمال 0.5 أو يختار $K = 1$ باحتمال 0.5. إذا اختار الموائم $K = 0$، فإنه يقفز فوراً لخطوة 2 بعد إرسال إشارة التشويش. إذا اختار الموائم $K = 1$ فإنه ينتظر 51.2 ميكروثانية قبل العودة لخطوة 2. بعد اصطدامٍ ثانٍ، يتم اختيار K باحتمالات متساوية من بين القيم (0، 1، 2، 3). بعد ثلاثة اصطدامات، يتم اختيار K باحتمالات متساوية من بين القيم (0، 1، 2، 3، 4، 5، 6، 7). بعد عشرة اصطدامات أو أكثر، يتم اختيار K باحتمالات متساوية من بين القيم (0، 1، 2، ...، 1023). وهكذا فإن حجم مجموعة الأعداد الذي تُختار منه قيمة K ينمو تصاعدياً مع عدد الاصطدامات (حتى $n = 10$)، ولهذا السبب تُدعى خوارزمية التراجع في الإيثرنت خوارزمية أُسّية.

يفرض معيار الإيثرنت حدوداً قصوى على المسافة بين أي عقدتين على الشبكة. تضمن تلك الحدود أنه إذا اختار الموائم A قيمة منخفضة للمتغير K عن كل الموائمات الأخرى التي اشتركت معه في الاصطدام، فإن الموائم A يكون بوسعه إرسال إطاره بدون مواجهة اصطدام جديد. سنستكشف تلك الخاصية بتفصيل أكثر في تمارين نهاية الفصل.

لماذا نستخدم تراجعاً أسّياً؟ لِمَ لا نختار K على سبيل المثال من بين 0، 1، 2، 3، 4، 5، 7، 6 بعد كل اصطدام؟ السبب أنه عندما يواجه موائم أول اصطدام له فإنه لا يدري كم عدد الموائمات المتورطة في ذلك الاصطدام. إذا كان هناك عدد صغير من تلك الموائمات، فإنه يكون من الحكمة اختيار K من مجموعة قليلة من القيم الصغيرة. وفي المقابل إذا كان هناك العديد من الموائمات المشتركة في الاصطدام، فمن الأفضل اختيار K من مجموعة أكبر من القيم الأكثر تفاوتاً (لماذا؟). لاحظ أنه بزيادة حجم المجموعة بعد كل اصطدام، يتكيّف الموائم بشكلٍ ملائم مع تلك السيناريوهات المختلفة.

نلاحظ هنا أيضاً أنه في كل مرة يقوم موائم بإنشاء إطار جديد للإرسال، فإنه يقوم بتنفيذ خوارزمية CSMA/CD المبينة أعلاه. وبشكلٍ خاص لا يأخذ الموائم في اعتباره أي اصطدامات ربما تكون قد وقعت في الماضي القريب. لذا فقد يتمكن موائم لديه إطار جديد من الانسلال بسرعة والنجاح في إرسال الإطار بينما تكون عدّة موائمات أخرى في حالة التراجع الأسّي.

كفاءة الإيثرنت

عندما يكون لدى عقدة واحدة فقط إطار للإرسال، يمكن لتلك العقدة أن ترسل بمعدل الإرسال الكامل لتقنية الإيثرنت المستخدمة (مثلاً 10 ميجابت/ثانية، أو 100 ميجابت/ثانية، أو 1 جيجابت/ثانية). ولكن إذا كان لدى العديد من العقد إطارات للإرسال، فإن معدل الإرسال الفعّال للقناة يمكن أن يكون أقل من ذلك بكثير. نُعرّف هنا كفاءة الإيثرنت (Ethernet efficiency) على أنها الكسر من الوقت على المدى البعيد الذي يتم فيه إرسال الإطارات على القناة بدون اصطدامات، وذلك في وجود عدد كبير من العقد النشطة لدى كلٍّ منها عدد كبير من الإطارات للإرسال. للحصول على معادلة تقريبية تمثل كفاءة الإيثرنت، افترض أن d_{prop} تمثل الوقت الأقصى الذي تستغرقه طاقة الإشارة للانتقال بين أي وصلتين، وd_{trans} الوقت اللازم لإرسال إطار إيثرنت له أقصى حجم ممكن (تقريباً 1.2 ميللي ثانية للإيثرنت بسرعة 10 ميجابت/ثانية). يقع اشتقاق كفاءة الإيثرنت خارج نطاق هذا الكتاب (انظر [Lam 1980] و[Bertsekas 1991])، ولكننا سنكتفي هنا ببساطة بذكر التقريب التالي للكفاءة:

$$Efficiency = \frac{1}{1 + 5d_{prop} / d_{tran}}$$

نرى من هذه المعادلة أنه عندما تقترب d_{prop} من 0، فإن الكفاءة تقترب من 1. إن هذا يتفق مع نظرتنا البدهية، حيث إنه إذا كان تأخير الانتقال صفراً، فإن العقد المتصادمة ستتوقف عن إرسالها فوراً بدون إهدار لوقت القناة. أيضاً كلما أصبحت d_{trans} كبيرة جداً، تقترب الكفاءة من 1. هذا بدهي أيضاً لأنه عندما يتمكن إطار

من الاستحواذ على القناة، فإنه سيتمسّك بها لوقت طويل جداً، أي أن القناة ستعمل عملاً منتجاً أغلب الوقت.

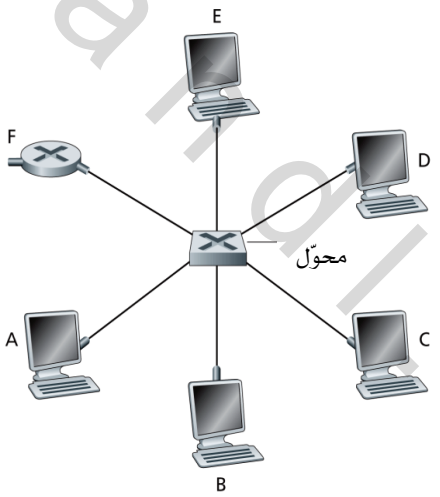
3-5-5 تقنيات الإيثرنت

في مناقشتنا أعلاه، كنا نشير إلى الإيثرنت كما لو كانت بروتوكولاً معيارياً واحداً. غير أنه في الواقع تأخذ الإيثرنت العديد من الأشكال المختلفة، وتستخدم بعض الاختصارات المحيّرة أحياناً مثل: 10BASE-T، 10BASE-2، 100BASE-T، 1000BASE-LX، 10GBASE-T. تم اعتماد هذه والعديد غيرها من تقنيات الإيثرنت الأخرى كمعايير قياسية على مرّ السنين من مجموعات العمل كمجموعة IEEE 802.3 CSMA/CD [IEEE 802.3 2007]. رغم أن هذه الاختصارات قد تبدو محيّرة بعض الشيء، إلا أنها تحمل في طياتها قدراً كبيراً من المنطق. فالجزء الأول من الاختصار يشير إلى سرعة الإرسال للمعيار: فالأرقام 10، و100، و1000، و10G تمثل 10 ميجابت/ثانية، و100 ميجابت/ثانية، و1 جيجابت/ثانية، و10 جيجابت/ثانية على الترتيب. تشير كلمة BASE إلى أن الإيثرنت ترسل في حيز التردد الأصلي (baseband)، بمعنى أن وسط الانتقال المادي يحمل فقط حركة بيانات الإيثرنت. كل معايير 802.3 تعرّف إيثرنت بحيز التردد الأصلي. يدل الجزء الأخير من الاختصار على وسط الانتقال المادي نفسه، فالإيثرنت تمثل مواصفات لكلٍّ من طبقة ربط البيانات والطبقة المادية، وهي تستخدم تشكيلة من الأوساط المادية لنقل الإشارات بما في ذلك الكبل المحوري، وأسلاك النحاس، والألياف الضوئية. عموماً ترمز T لزوج مجدول من الأسلاك النحاسية.

تاريخياً كانت الإيثرنت في البداية تقترن في المخيّلة على أنها قطعة (segment) من كبل محوري كما هو مبين في الشكل 5-20. تصف المعايير الأولى 10BASE-2 و10BASE-5 شبكة إيثرنت بمعدل إرسال قدره 10 ميجابت/ثانية على نوعين من أنواع الكبل المحوري، بطول يصل إلى 200 متر و500 متر على الترتيب. يمكن تغطية مسافات أطول من ذلك باستخدام مُكرِّر (repeater)، وهو جهاز يعمل في الطبقة المادية حيث يتلقى إشارة من ناحية المدخل ويعيد توليدها مجدداً على ناحية

المخرج. إن الكبل المحوري، كما يبدو في الشكل 5-20، يطابق بشكلٍ جيد مفهومنا عن الإيثرنت كوسط إذاعة- حيث يتم استقبال كل الإطارات التي ترسلها إحدى الواجهات بواسطة كل الواجهات الأخرى، ويحل بروتوكول الإيثرنت CSMA/CD مشكلة الوصول المتعددة بشكلٍ رائع. ما علينا إلا أن نربط العقد بالكبل ببساطة، فنحصل على شبكة بيانات محلية!

لقد مرّت الإيثرنت عبر سلسلة من التطورات على مرّ السنين، وإيثرنت اليوم تختلف كثيراً عن التصاميم الأصلية بترتيبة ناقل مشترك يأخذ شكل كبل محوري. في أكثر تجهيزات إيثرنت اليوم، توصّل العقد إلى محوّل (switch) عن طريق وصلات نقطة إلى نقطة مصنوعة من أسلاك النحاس المجدولة أو الألياف الضوئية كما هو مبيّن في الشكل 5-24.



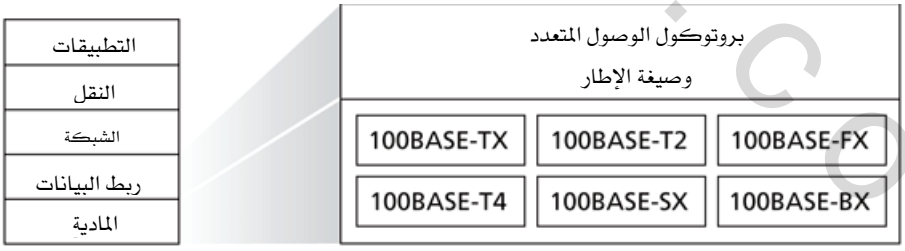
الشكل 5-24 محوّل طبقة ربط البيانات يربط بين ست عقد.

في منتصف التسعينيات ظهرت معايير إيثرنت بسرعة 100 ميجابت/ثانية، أي أسرع 10 مرات من المعيار السابق بسرعة 10 ميجابت/ثانية. تم الإبقاء على البروتوكول الأصلي للوصول المتعدد وصيغة إطار الإيثرنت، لكن وُصّفت سرعات أعلى للطبقة المادية للأسلاك النحاسية المجدولة (100BASE-T) والألياف الضوئية

(100BASE-FX, 100BASE-SX, 100BASE-BX). يبين الشكل 5-25 تلك المعايير المختلفة وبروتوكول الإيثرنت المشترك للوصول المتعدد وصيغة الإطار. يلاحَظ أن الإيثرنت بسرعة 100 ميجابت/ثانية محدودة بمسافة 100 متر فقط على زوج أسلاك النحاس المجدولة، وعدّة كيلومترات على الألياف الضوئية، مما يسمح بالتوصيل ما بين محوّلات الإيثرنت في بنايات مختلفة.

تعتبر إيثرنت الجيجابت امتداداً طبيعياً لمعايير الإيثرنت الناجحة جداً بسرعة 10 ميجابت/ثانية و100 ميجابت/ثانية. توفر إيثرنت الجيجابت معدل إرسال للبيانات قدره 1000 ميجابت/ثانية، وتحافظ على توافق كامل مع القاعدة العريضة من معدات شبكات الإيثرنت المستخدمة حالياً. يتسم معيار إيثرنت الجيجابت والمعروف بـ IEEE 802.3z بما يلي:

- يستخدم صيغة إطار الإيثرنت القياسي (الشكل 5-22) ويتوافق تراجعياً مع 10BASE-T و100BASE-T، مما يُسهّل تكامل أنظمة إيثرنت الجيجابت مع أجهزة الإيثرنت المستخدمة حالياً.
- يسمح بوصلات نقطة إلى نقطة بالإضافة إلى قنوات الإذاعة المشتركة. تستخدم وصلات نقطة إلى نقطة محوّلات (switches) بينما تستخدم قنوات الإذاعة مجمِّعات (hubs)، كما تقدّم وصفه. في مفردات إيثرنت الجيجابت يطلق على المجمِّعات موزّعات بمخازن مؤقتة (buffered distributors).



الشكل 5-25 معايير الإيثرنت 100 ميجابت/ثانية: طبقة ربط بيانات مشتركة، وطبقات مادية مختلفة.

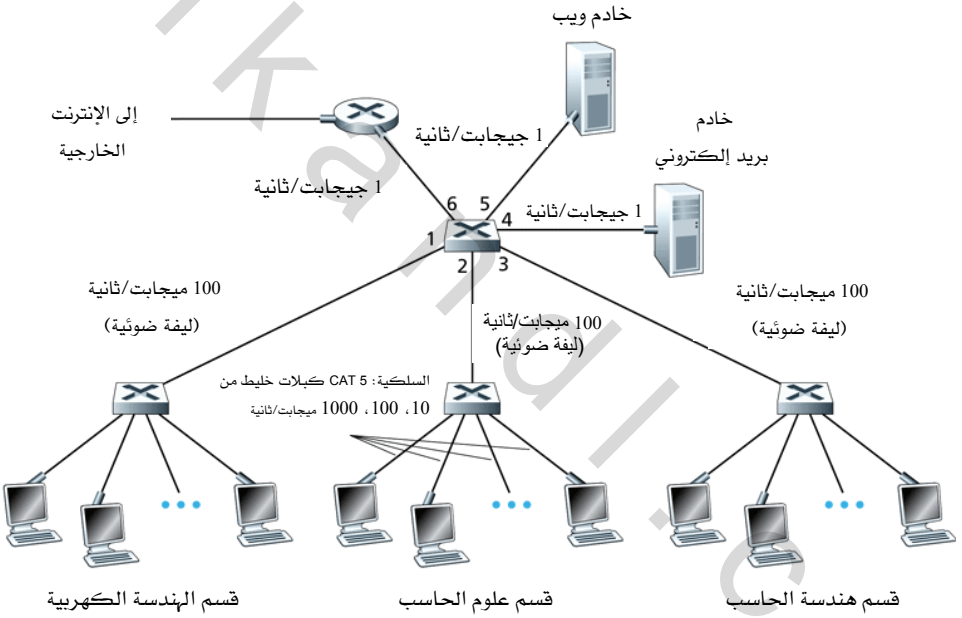
- يُستخدم بروتوكول CSMA/CD لقنوات الإذاعة المشتركة. ولتحقيق كفاءة مقبولة يجب الحد من المسافة القصوى بين العقد بشكل كبير.
- يُسمح باتصال مزدوج بالكامل (full-duplex) بمعدّل إرسال 1000 ميجابت/ثانية في كلا الاتجاهين لقنوات نقطة إلى نقطة.

في البداية كانت إيثرنت الجيجابت تتطلّب استخدام الألياف الضوئية كوسط مادي، أما الآن فيمكن استخدامها على أسلاك نحاس مجدولة من الفئة الخامسة (UTP 5). في صيف عام 2006 تم اعتماد معيار إيثرنت 10 جيجابت/ثانية (10GBASE-T)، مما يفتح المجال لشبكات إيثرنت بسعات أكبر في المُستقبل القريب.

لنختم مناقشتنا عن تقنيات الإيثرنت بطرح سؤال ربما يكون قد بدأ يلح عليك. في أيام طبوغرافية الناقل المحوري وطبوغرافية النجمة المبنية على استخدام مجمِّع، كانت الإيثرنت تمثل بوضوح وصلة إذاعة (كما عرّفناها في الجزء 5-3)، حيث تصطدم الإطارات عندما تقوم العقد بالإرسال في نفس الوقت. للتعامل مع تلك الاصطدامات تضمّن معيار الإيثرنت بروتوكول CSMA/CD، والذي يعتبر فعّالاً بصورة خاصة على شبكة بيانات محلية بوصلة إذاعة تمتدّ عبر نصف قطر صغير. لكن إذا كان الاستعمال السائد للإيثرنت اليوم يعتمد طبوغرافية نجمية مبنية على استخدام محوّل (switch)، ويطبق أسلوب "خزن ومرر" لتحويل الرزم، ألا زلنا حقاً بحاجة لبروتوكول الإيثرنت للوصول المتعدد؟ كما سنرى في الجزء 5-6 يُنسّق المحوّل إرساله بحيث لا يرسل أبداً أكثر من إطار واحد على نفس الواجهة في أي وقت. وعلاوة على ذلك فإن معظم المحوّلات الحديثة تعمل بطريقة الازدواج الكامل (full-duplex)، ومن ثم يمكن تبادل الإطارات بين المحوّل والعقدة في نفس الوقت بدون حدوث تداخل. وبمعنى آخر لا توجد اصطدامات في شبكة إيثرنت محلية مبنية على محوّل، ومن ثم فليست هناك حاجة لبروتوكول الوصول المتعدد!

كما رأينا تختلف إيثرنت اليوم جداً عن الإيثرنت الأصلية التي اخترعها ميتكالف وبوجز منذ أكثر من ثلاثين عاماً. فقد زادت سرعتها على ثلاث مراحل،

وتُنقل إطاراتها الآن على تشكيلة من أوساط النقل المادية، كما انتشرت شبكات الإيثرنت التي تستخدم محوّلات، والآن حتى بروتوكول الماك لم يعد ضرورياً في أغلب الأحيان! هل كل ذلك ما يزال إيثرنت؟ الجواب بالطبع "نعم، من حيث التعريف". من الجدير بالملاحظة أنه رغم كل هذه التغييرات، فإن ثمة شيئاً واحداً بقي بدون تغيير على مدى أكثر من ثلاثين عاماً: ألا وهو صيغة إطار الإيثرنت (قد تكون تلك هي العامل المشترك الوحيد في الواقع بين معايير الإيثرنت المختلفة).



الشكل 5-26 شبكة مؤسّسة تتضمن مجموعة من المجمِّعات، ومحوّلات الإيثرنت، وموجّه.

6-5 محوّلات طبقة ربط البيانات

كما هو مبين في الشكل 5-26 تستخدم شبكات الإيثرنت المحلية الحديثة طبوغرافية نجمية، حيث توصّل كل عقدة بمحوّل مركزي (central switch). حتى الآن كان الأمر مبهماً فيما يتعلّق بماهية ذلك المحوّل: ماذا يفعل وكيف يعمل؟ يتلخص دور المحوّل في استلام إطارات طبقة ربط البيانات من الوصلات القادمة إليه وتوصيلها إلى الوصلات الخارجة منه، وسندرس وظيفة التوجيه تلك بالتفصيل بعد قليل. يعتبر المحوّل نفسه شفافاً (transparent) (أي كأنه غير موجود) بالنسبة للعقد، بمعنى أن عقدة الإرسال تعنون الإطار إلى عقدة الاستقبال (وليس إلى المحوّل) وترسِل الإطار إلى الشبكة المحلية، وهي لا تدري أن محوّلاً سيستلم الإطار ويوجّهه إلى العقدة الأخرى. بشكلٍ مؤقت قد يتجاوز معدّل وصول الإطارات إلى أيٍّ من الواجهات الخارجة من المحوّل سعة الإرسال لوصلة تلك الواجهة. للتعامل مع هذه المشكلة تتضمن واجهات المحوّل الخارجة مخازن مؤقتة (buffers)، تقريباً بنفس الطريقة التي تستخدم بها واجهات الموجّه الخارجة المخازن المؤقتة لتخزين وحدات بيانات طبقة الشبكة. دعنا الآن نلقي نظرة متفحصة أكثر على طريقة عمل المحوّلات.

1-6-5 الترشيح والتمرير (Filtering and Forwarding)

الترشيح (filtering) هو وظيفة المحوّل التي تحدد ما إذا كان الإطار سيتم إرساله إلى واجهةٍ ما، أو أنه ببساطة سيتم إسقاطه. أما التمرير (forwarding) فهو وظيفة المحوّل التي تحدد الواجهات التي ينبغي توجيه إطار إليها، وبعد ذلك نقل الإطار إلى تلك الواجهات. يتم تنفيذ عمليتي الترشيح والتمرير عن طريق جدول المحوّل. يحتوي جدول المحوّل على مُدخلات لبعض العقد على الشبكة المحلية، ولكن ليس بالضرورة كلها. يحتوي كل مُدخل في جدول المحوّل على: (1) عنوان ماك للعقدة، و(2) واجهة المحوّل التي تقود نحو العقدة و(3) الوقت الذي تم فيه إدراج المُدخل الخاص بالعقدة في الجدول. يبين الشكل 5-27 مثالاً لجدول على المحوّل الأعلى في الشبكة المبينة في الشكل 5-26. رغم أن هذا الوصف لتمرير

الإطارات قد يبدو مشابهاً لمناقشتنا لتوجيه وحدات البيانات في الفصل الرابع، فإننا سنكتشف بعد قليل وجود اختلافات مهمة. أحد تلك الاختلافات هو أن المحوّلات توجّه الرزم بناءً على عناوين الماك وليس على عناوين IP. سنرى أيضاً أن جدول المحوّل مبني بطريقة مختلفة جداً عن جدول التوجيه على الموجّه.

العنوان	الواجهة	الوقت
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
...	...	...

الشكل 5-27 جزء من جدول المحوّل الأعلى في الشبكة المبينة في الشكل 5-26.

لفهم كيف تتم عملية الترشيح والتمرير في المحوّل، افترض أن إطاراً بعنوان الوجهة DD-DD-DD-DD-DD-DD يصل إلى المحوّل على الواجهة x. يفحص المحوّل جدوله مستخدماً عنوان الماك DD-DD-DD-DD-DD-DD كمُدخل. هناك ثلاث حالات محتملة:

- لايوجد مُدخل في الجدول لعنوان الوجهة DD-DD-DD-DD-DD-DD. في هذه الحالة يرسل المحوّل نسخاً من الإطار إلى مخزن الخرج المؤقت الخاص بكل واجهة من واجهاته ماعدا الواجهة x التي وصل منها الإطار. بمعنى آخر إذا لم يكن هناك مُدخل بالجدول يناظر عنوان الوجهة، فإن المحوّل يذيع الإطار.
- يوجد مُدخل في الجدول يربط عنوان الوجهة DD-DD-DD-DD-DD-DD بالواجهة x. في هذه الحالة الإطار قادم من قطعة من الشبكة المحلية تضم الوجهة DD-DD-DD-DD-DD-DD. وعليه فلا حاجة لتوجيه الإطار إلى أيٍّ من الواجهات الأخرى، ومن ثم يقوم المحوّل بوظيفة الترشيح وذلك بإهمال الإطار.
- يوجد مُدخل في الجدول يربط عنوان الوجهة DD-DD-DD-DD-DD-DD بواجهة y مختلفة عن x. في هذه الحالة يلزم توجيه الإطار إلى قطعة الشبكة

المحلية الموصّلة بالواجهة y. يقوم المحوّل بوظيفة التمرير بوضع الإطار في مخزن الخرج المؤقت الخاص بالواجهة y.

دعنا نطبق هذه القواعد على المحوّل في أعلى الشكل 5-26 وجدول المحوّل الموجود عليه والمبين في الشكل 5-27. افترض أن إطاراً بعنوان الوجهة 62-FE-F7-11-89-A3 يصل إلى المحوّل من الواجهة 1. يفحص المحوّل جدوله ليجد أن وجهة الإطار تقع على قطعة الشبكة المحلية الموصلة بالواجهة 1 (أي قسم الهندسة الكهربية). هذا يعني أن الإطار كان قد أذيع على قطعة الشبكة المحلية التي تتضمن الوجهة ولذلك وصل إلى الواجهة 1 على المحوّل والتي تقع أيضاً على تلك القطعة. يقوم المحوّل بوظيفة الترشيح وذلك بإهمال هذا الإطار. افترض الآن أن إطاراً آخر بنفس عنوان الوجهة السابق يصل من واجهة 2. يفحص المحوّل جدوله ثانية فيجد أن الوجهة تتبع الواجهة 1، ومن ثم يرسل ذلك الإطار إلى مخزن الخرج المؤقت الذي يسبق الواجهة 1. يتضح من هذا المثال أنه طالما كان جدول المحوّل كاملاً ودقيقاً، فإن المحوّل يرسل بالإطارات نحو وجهتها المقصودة بدون اللجوء لإذاعة أيٍّ منها.

بهذا المعنى يعتبر المحوّل "أذكى" من المجمِّع. لكن كيف يتم تهيئة جدول المحوّل هذا في المقام الأول؟ هل هناك بروتوكولات في طبقة ربط البيانات تناظر بروتوكولات التوجيه في طبقة الشبكة؟ أم أنه يتعين على مشرف الشبكة القيام بتهيئة جداول المحوّلات يدوياً بنفسه؟

2-6-5 التعلم الذاتي

تتوافر للمحوّلات خاصية رائعة (خاصةً من منظور مشرف الشبكة المُجهَد!)، حيث يمكنها إنشاء وتحديث جداولها آلياً وذاتياً وبطريقة ديناميكية - بدون أي تدخل من مشرف الشبكة أو من بروتوكول خاص بالتهيئة. وبمعنى آخر، للمحوّلات قدرة ذاتية على التعلّم. ويتحقق ذلك كالتّالي:

1. يكون جدول المحوّل فارغاً في البداية.

2. لكل إطار قادم يتم استلامه على واجهة، يُخزّن المحوّل في جدوله: (1) عنوان الماك الموجود في حقل عنوان المصدر، (2) الواجهة التي وصل منها الإطار، (3) الوقت الحالي. بهذه الطريقة يسجّل المحوّل في جدوله قطعة الشبكة المحلية التي تقع عليها عقدة إرسال كل إطار يصله. إذا كانت كل عقدة في الشبكة المحلية سترسل في النهاية إطاراً، ففي النهاية سيتم تسجيل موقع كل عقدة في الجدول.
3. يحذف المحوّل عنواناً من الجدول إذا لم تصل إطارات بذلك العنوان كعنوان مصدر خلال فترة زمنية محددة (تسمى فترة العمر). بهذه الطريقة إذا تم استبدال حاسب شخصي على الشبكة بحاسب شخصي آخر (له موائم مختلف ومن ثم عنوان ماك مختلف)، فإن عنوان الماك للحاسب الأول سيتم حذفه في النهاية من جدول المحوّل.

دعنا نطبق خاصية التعلّم الذاتي للمحوّل الموجود في أعلى الشكل 5-26 وجدول المحوّل عليه في الشكل 5-27. افترض أنه في تمام الساعة 9:39 وصل إطار بعنوان المصدر 01-12-23-34-45-56 من الواجهة 2. افترض أن هذا العنوان ليس مدرجاً في جدول المحوّل. ومن ثم يضيف المحوّل مُدخلاً جديداً إلى جدوله، كما هو مبين في الشكل 5-28.

الوقت	الواجهة	العنوان
9:39	2	01-12-23-34-45-56
9:32	1	62-FE-F7-11-89-A3
9:36	3	7C-BA-B2-B4-91-10
…	…	…

الشكل 5-28 المحوّل يتعلّم موقع الموائم بعنوان الماك 01-12-23-34-45-56.

لنواصل مسيرتنا مع نفس المثال، افترض أن فترة العمر على هذا المحوّل هي 60 دقيقة، ولم تصل إلى المحوّل أي إطارات لها عنوان المصدر 62-FE-F7-11-89-A3 بين الساعة 9:32 والساعة 10:32. وبناءً على ذلك فبحلول الساعة 10:32 سيحذف المحوّل هذا العنوان من جدوله.

تُعدُّ المحوّلات أدوات من نوع "وصّل وشغّل" (plug-and-play)، بمعنى أنها لا تتطلب أي تدخل من مشرف الشبكة أو مستخدمها. فأي مشرف للشبكة يريد تركيب محوّل، ليس عليه إلا توصيل قطع الشبكة المحلية إلى واجهات المحوّل. لا يحتاج المشرف للقيام بتهيئة المحوّل عند تركيبه ولا عند إزالة مضيف من على إحدى قطع الشبكة المحلية. جدير بالذكر أيضاً أن المحوّلات تعمل بازدواج كامل (full-duplex)، بمعنى أنه على أي وصلة تربط عقدة بالمحوّل، يمكن لكلٍّ من العقدة والمحوّل أن يرسلا في نفس الوقت بدون حدوث أي اصطدامات.

3-6-5 خصائص التحويل في طبقة ربط البيانات

بعد أن انتهينا من وصف أساسيات تشغيل محوّلات طبقة ربط البيانات، دعنا الآن نتناول السمات والخصائص المميزة لتلك المحوّلات. بالرجوع إلى شبكة البيانات المحلية المبينة في الشكل 5-24، يمكننا التعرف على عدة مزايا لاستعمال المحوّلات بدلاً من وصلات الإذاعة التي تستخدم ناقلات (buses)، أو طبوغرافية نجمية مبنية على مجمِّع:

- تجنّب حدوث اصطدامات: في شبكة بيانات محلية مبنية باستخدام محوّلات (وبدون مجمِّعات)، لا يُفقد حيز ترددي (سعة إرسال) بسبب الاصطدامات! تقوم المحوّلات بتخزين الإطارات في المخزن المؤقت، ولا ترسل في أي وقت أبداً أكثر من إطار واحد إلى أي قطعة من قطع الشبكة. كما هو الحال مع الموجّه في طبقة الشبكة، الطاقة الإنتاجية الكلية القصوى لمحوّل هي مجموع معدلات الإرسال على كل واجهات المحوّل. وهكذا توفر المحوّلات تحسناً كبيراً في أداء شبكات البيانات المحلية مقارنةً بوصلات الإذاعة.

- إمكانية استخدام وصلات متباينة: نظراً لأن المحوّل يعزل كل وصلة من وصلاته عن الأخرى، يمكن للوصلات المختلفة في شبكة محلية أن تعمل بسرعات مختلفة وتستخدم أوساط نقل مادية مختلفة. فمثلاً على الشبكة المبينة في الشكل 5-24، يمكن توصيل المضيف A باستخدام أسلاك نحاسية بمعيار 10BASE-T بمعدّل إرسال 10 ميجابت/ثانية، في حين يوصل المضيف B بواسطة ليفة ضوئية بمعيار 100BASE-FX ومعدّل إرسال 100 ميجابت/ثانية، وC عبر أسلاك نحاسية بمعيار 1000BASE-T بمعدّل إرسال 1 جيجابت/ثانية. وهكذا تُعدُّ المحوّلات طريقةً مثاليةً للجمع ما بين الأجهزة القديمة والأجهزة الحديثة على نفس الشبكة.
- إدارة الشبكة: بالإضافة إلى تحسين أمن الشبكة (انظر المادة الجانبية بعنوان "نبذة عن الأمن")، تسهم المحوّلات كذلك في التخفيف من أعباء إدارة الشبكة. فعلى سبيل المثال إذا تعطل موائم على الشبكة وصار يرسل إطارات إيثرنت بشكلٍ مستمر (يطلق عليه عندئذٍ الموائم "الثرثار")، يمكن للمحوّل أن يكتشف هذه المشكلة تلقائياً ويفصل الموائم المعطوب عن الشبكة. بهذه الميزة لن يحتاج مشرف الشبكة لأن يغادر فراشه ليلاً ويقود سيارته إلى محل عمله لحل المشكلة. أيضاً إذا انقطع كبل فسيؤدي ذلك فقط إلى فصل تلك العقدة التي كانت تستخدم الكبل المقطوع للوصول إلى المحوّل. في أيام الكبل المحوري كان الكثير من مشرفي الشبكة يقضون الساعات لتتبع الكبل للعثور على مكان انقطاعه الذي عطّل الشبكة بكاملها. كما سنرى في الفصل التاسع (إدارة الشبكات)، تجمع المحوّلات أيضاً إحصائيات عن استغلال الحيز الترددي، ومعدّلات الاصطدام، وأنواع حركة البيانات. وتقدّم هذه المعلومات إلى مشرف الشبكة. يمكن استخدام تلك المعلومات لتحرّي الأعطال، وحل المشاكل، وللتخطيط من أجل تطوير الشبكة المحلية في المُستقبل.

نبذة عن الأمن (Focus on Security)

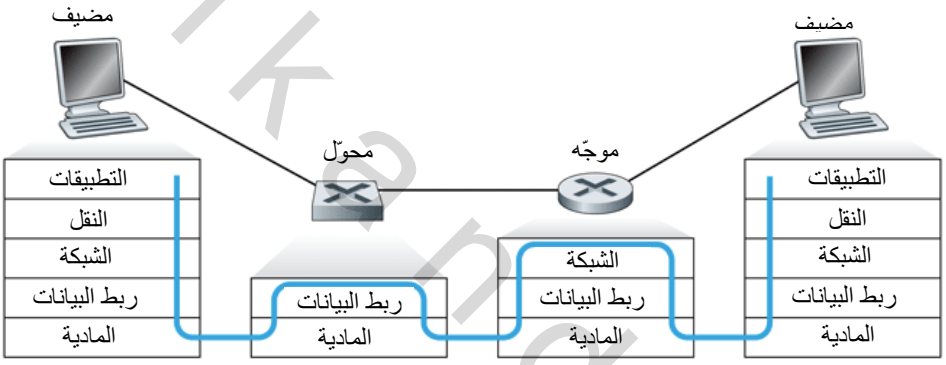
التقاط الرزم من الشبكات المحوّلة بتسميم المحوّل

عندما توصّل عقدة إلى محوّل فإنها تستلم عادةً الإطارات التي ترسل إليها على وجه التحديد فقط. على سبيل المثال خذ في الاعتبار شبكة البيانات المحلية في الشكل 5-24. عندما ترسل العقدة A إطاراً إلى العقدة B، ويكون هناك مُدخل للعقدة B في جدول المحوّل، فسيقوم المحوّل بإرسال ذلك الإطار فقط إلى العقدة B. إذا صادف وكانت العقدة C تشغّل برنامجاً لإلتقاط الرزم، فلن يتمكن ذلك البرنامج من التقاط ذلك الإطار من A إلى B. وهكذا ففي بيئة شبكة محلية محوّلة (LAN switched) (في مقابل بيئة شبكة محلية ذات وصلة إذاعة كـ 802.11 أو مبنية على استخدام مجمِّع)، يُعتبر التقاط الإطارات من قِبَل مهاجم أمراً أكثر صعوبة. ومع ذلك، فنظراً لأن المحوّل سيذيع الإطارات التي تكون عناوين الوجهة لها غير موجودة في جدول المحوّل، فلا يزال بوسع لاقط الرزم على C التقاط بعض الإطارات التي ليست معنونة إلى C بالتحديد. وعلاوة على ذلك سيكون بوسع لاقط الرزم التقاط كل إطارات الإيثرنت المذاعة التي تحمل العنوان المخصص للإذاعة (FF-FF-FF-FF-FF-FF كعنوان الوجهة). من أنواع الهجوم المشهورة ضد المحوّلات هجوم يعرف بتسميم المحوّل (switch poisoning). في هذا الهجوم يتم إرسال أطنان من الرزم إلى المحوّل تحمل العديد من عناوين الماك المختلفة والمزيفة للمصدر. يؤدي ذلك إلى ملء جدول المحوّل بمُدخلات مزيفة، بحيث لا يبقى ثمة مكان لعناوين الماك التي تستخدمها العقد الشرعية. يؤدي ذلك بالمحوّل إلى إذاعة أكثر الإطارات، وعندئذٍ يمكن التقاطها بواسطة لاقط الرزم [Skoudis 2006]. ونظراً لأن هذا الهجوم يُعد معقّداً حتى بالنسبة لمهاجم محنّك، فإن المحوّلات تعتبر أقل عرضة لالتقاط الرزم بدرجة كبيرة مقارنةً بالشبكات المحلية اللاسلكية وتلك المبنية على استخدام مجمِّعات.

5-6-4 المحوّلات في مقابل الموجّهات

كما رأينا في الفصل الرابع فإن الموجّهات هي محوّلات رزم تعمل بطريقة "خزّن ومرر" لتوجيه الرزم على أساس عنوان طبقة الشبكة الذي تحمله كل رزمة. رغم أن المحوّل يعتبر أيضاً محوّل رزم من نوع "خزّن ومرر" فإنه يختلف جوهرياً عن الموجّه، حيث إنه يوجّه الرزم مستخدماً عناوين ماك. وباختصار: الموجّه هو محوّل رزم في طبقة -3، أما المحوّل فهو محوّل رزم في طبقة -2.

رغم إن المحوّلات والموجّهات أدوات مختلفة بشكلٍ جوهري، فإنه غالباً ما يتعين على مشرفي الشبكات الاختيار بينهما عند تركيب أداة تشبيك. على سبيل المثال كان بوسع المشرف على الشبكة في الشكل 5-26 أن يستخدم بسهولة موجّهاً بدلاً من محوّل لتوصيل الشبكات المحلية للأقسام، والخادمات، وموجّه بوّابة الإنترنت. في الحقيقة سيسمح الموجّه بالاتصالات بين الأقسام بدون اصطدامات. ولمّا كانت كلٌّ من المحوّلات والموجّهات مرشّحة للاستخدام كأدوات تشبيك، يجدر بنا معرفة مزايا وعيوب كلٍّ منها.



الشكل 5-29 معالجة الرزم في المحوّلات، والموجّهات، والمضيفات.

لنتناول مزايا وعيوب المحوّلات أولاً. كما ذكرنا أعلاه فإن المحوّلات أجهزة من نوع "وصّل وشغّل"، وهي خاصية يقدّرها كل مشرفي الشبكات في العالم. المحوّلات يمكنها ترشيح وتوجيه الإطارات بمعدّلات عالية نسبياً. كما يوضح الشكل 5-29 يجب على المحوّلات معالجة الإطارات فقط حتى الطبقة 2، أما الموجّهات فيجب أن تعالج وحدات البيانات حتى الطبقة 3. من ناحية أخرى ولمنع دوران الإطارات المذاعة فإنه يجب ألا تتجاوز الترتيبة الفعّالة للشبكة المحوّلة شجرة اتصال ممتدة (spanning tree). أيضاً تتطلب شبكة محوّلة كبيرة جداول كبيرة في العقد لبروتوكول تحويل العناوين ARP، كما تولد حركة مرور ومعالجة كبيرة تتعلق بهذا البروتوكول. وعلاوة على ذلك لا توفر المحوّلات أي حماية ضد عاصفة

البث الإذاعي (broadcast storm) – فإذا أخذ مضيف على الشبكة يرسل سلسلة لانهائية من إطارات الإيثرنت المذاعة، فستقوم المحوّلات بتمرير كل تلك الإطارات – مما يؤدي إلى انهيار الشبكة بالكامل.

لنتناول الآن مزايا وعيوب الموجّهات. نظراً لأن عنونة الشبكة هرمية (hierarchical) في أغلب الأحيان وليست مسطّحة (flat) كما في عنونة الماك، فإن الرزم لا يتكرر دورانها خلال الموجّهات حتى عندما تتضمن الشبكة مسارات إضافية (لاحظ أن دوران الرزم قد يحدث إذا لم يتم تهيئة جداول التوجيه بشكلٍ جيد. ولكن كما رأينا في الفصل الرابع، يستخدم بروتوكول IP حقلاً خاصاً في ترويسة وحدة البيانات للحد من دوران الرزم). وعليه فلن يتم حصر الرزم في نطاق شجرة الاتصال الممتدة، وسيمكنها استخدام أفضل مسار بين المصدر والوجهة. ونظراً لأن الموجّهات لا تعاني من قيود شجرة الاتصال الممتدة، فقد سمح ذلك ببناء إنترنت بترتيبات غنية ـ تتضمّن على سبيل المثال وصلات متعددة نشطة بين أوروبا وأمريكا الشمالية. من المزايا الأخرى للموجّهات أنها توفر حماية ببرامج الـ firewall ضد عواصف الإذاعة في الطبقة 2. في المقابل لعل العائق الأساسي لاستخدام الموجّهات هو أنها ليست أجهزة من نوع "وصّل وشغّل"، فهي تحتاج مع المضيفات الموصّلة بها إلى تهيئة عناوين IP الخاصة بها يدوياً. كما أن الموجّهات غالباً ما تستغرق وقتاً أطول لمعالجة كل رزمة مقارنةً بالمحوّلات، نظراً لأن عليها المعالجة حتى الطبقة 3. وأخيراً هناك طريقتان مختلفتان لنطق اسم الموجّه (router) باللغة الإنجليزية، إمّا "rootor" أو "rowter"، ويضيّع الناس الكثير من الوقت في الجدل حول أيّ الطريقتين أصح [Perlman 1999].

الآن وبعد أن عرفنا مزايا وعيوب كلٍّ من المحوّلات والموجّهات، متى إذن يجدر بشبكة مؤسّسة (كشبكة في حرم جامعي أو شركة) استخدام محوّلات، ومتى يستحسن أن تستخدم موجّهات؟

عادةً ما تتألف الشبكات الصغيرة التي تضم بضع مئات من المضيفات من بضع قطع (segments) من الشبكات المحلية. تكفي المحوّلات لهذه الشبكات

الصغيرة، حيث تفيد في زيادة محلية حركة مرور البيانات وتزيد الطاقة الإنتاجية الكلية دون الحاجة لأي تهيئة لعناوين IP. أما الشبكات الأكبر التي تشمل آلاف المضيفات فعادةً ما تتضمّن موجّهات ضمن الشبكة (بالإضافة إلى المحوّلات). تحقق الموجّهات عزلاً أكثر متانة لحركة المرور، وتحكماً أفضل في عواصف الإذاعة، كما تستخدم مسارات "ذكية" أكثر بين المضيفات في الشبكة.

عرفنا في هذا الجزء أنه يمكن استخدام كلٍّ من المجمِّعات، والمحوّلات والموجّهات كأدوات لتشبيك قطع الشبكات المحلية والمضيفات. يلخّص الجدول 5-1 أبرز السمات التي تميز كل أداة من أدوات التشبيك تلك.

الخاصيّة	المجمِّعات	الموجّهات	المفاتيح
عزل حركة المرور	لا	نعم	نعم
سمة "وصّل وشغّل"	نعم	لا	نعم
التوجيه الأمثل	لا	نعم	لا
توفير طرق مختصرة	نعم	لا	نعم

الجدول 5-1 مقارنة بين الخصائص النمطية لأدوات التشبيك الشهيرة.

5-7 بروتوكول نقطة إلى نقطة (PPP)

تركزت أغلب مناقشاتنا لبروتوكولات طبقة ربط البيانات حتى الآن على بروتوكولات قنوات الإذاعة. سنتناول في هذا الجزء بروتوكولاً آخر لطبقة ربط البيانات مصمماً للتعامل مع الوصلات من نقطة إلى نقطة، وهو بروتوكول نقطة إلى نقطة (Point-to-Point Protocol (PPP)). نظراً لكون PPP هو البروتوكول المفضّل لوصلات المودم الهاتفي (dial-up links) من المضيفات السكنية، فإنه يعتبر بلا شك أحد أكثر بروتوكولات طبقة ربط البيانات انتشاراً اليوم. البروتوكول الآخر المهم لطبقة ربط البيانات والمستخدم اليوم هو بروتوكول المستوى العالي للتحكم في وصلة ربط البيانات (HDLC)؛ ويتضمن [Spragins 1991] مناقشة لبروتوكول HDLC. ستمكنّنا مناقشتنا هنا لبروتوكول PPP الأسهل من

استكشاف العديد من السمات الهامة لبروتوكولات طبقة ربط البيانات من نوع نقطة إلى نقطة.

كما يدل الاسم، بروتوكول نقطة إلى نقطة [RFC 1661; RFC 2153] هو بروتوكول لطبقة ربط البيانات يعمل على وصلة من نقطة إلى نقطة - أي وصلة تربط مباشرةً بين عقدتين، تقع كل عقدة على طرف من طرفي الوصلة. يمكن أن تكون وصلة النقطة إلى نقطة التي يعمل عليها بروتوكول PPP خطاً هاتفياً تسلسلياً بمودم (على سبيل المثال، وصلة مودم بسرعة 56 كيلوبت/ثانية، أو وصلة SONET/SDH، أو وصلة X.25 ، أو دائرة ISDN). وكما ذكرنا أعلاه أصبح PPP البروتوكول المفضّل لتوصيل المستخدمين السكنيين في منازلهم إلى موفري خدمة الإنترنت لهم على وصلات مودم هاتفية. قبل الخوض في تفاصيل بروتوكول PPP، من المفيد استعراض المتطلبات الأصلية التي حددها فريق عمل هندسة الإنترنت (IETF) لتصاميم PPP [RFC 1547]:

- تأطير الرزم: ينبغي أن يكون بوسع المُرسِل ببروتوكول PPP على وصلة ربط البيانات أخذ رزمة من مستوى الشبكة وتغليفها ضمن إطار PPP لطبقة ربط البيانات بحيث يمكن لمُستقبِل الإطار تحديد بداية ونهاية كلٍّ من إطار طبقة ربط البيانات ورزمة طبقة الشبكة المتضمنة في الإطار.
- الشفافية: لا ينبغي أن يفرض بروتوكول PPP أي قيود على البتات التي توضع في رزمة طبقة الشبكة (سواءً الترويسات أو البيانات). وعليه فلا يمكن لبروتوكول PPP مثلاً منع استعمال تسلسل معين من البتات في رزمة طبقة الشبكة. سنعود إلى هذه القضية بعد قليل أثناء مناقشتنا لموضوع حشو البايتات.
- دعم عدة بروتوكولات لطبقة الشبكة: يجب أن يكون بروتوكول PPP قادراً على دعم العديد من بروتوكولات طبقة الشبكة (مثل IP وDECnet) التي تستخدم نفس الوصلة المادية في نفس الوقت. تماماً كما يحتاج بروتوكول IP للقدرة على تجميع البيانات (multiplex) من بروتوكولات مختلفة بطبقة نقل البيانات (مثل TCP وUDP) على توصيلة واحدة من طرف

إلى طرف، يحتاج بروتوكول PPP أن يكون لديه القدرة على تجميع البيانات من عدة بروتوكولات طبقة شبكة مختلفة على وصلة واحدة من نقطة إلى نقطة. يعني هذا المتطلب أنه في الحد الأدنى ينبغي أن يتضمن بروتوكول PPP حقلاً أو آلية أخرى مماثلة لتحديد نوع بروتوكول طبقة الشبكة المستخدم، بحيث يتسنى لجانب الاستقبال من بروتوكول PPP توزيع (demultiplex) الإطار المستلَم إلى البروتوكول المناظر في طبقة الشبكة.

- دعم أنواع متعددة من الوصلات: بالإضافة إلى قدرته على التعامل مع عدة بروتوكولات في المستوى الأعلى، يجب أن يكون بوسع بروتوكول PPP العمل على تشكيلة كبيرة من الأنواع المختلفة من الوصلات، بما في ذلك الوصلات التسلسلية (التي ترسل البيانات في اتجاه معين على شكل بتات الواحد تلو الآخر) أو المتوازية (التي ترسل عدة بتات في نفس الوقت على التوازي)، وكذلك الوصلات المتزامنة (التي ترسل إشارة ساعة توقيت مع بتات البيانات) أو غير المتزامنة، وكذلك الوصلات منخفضة أو عالية السرعة، والوصلات الكهربية أو الضوئية.
- اكتشاف الأخطاء: يجب أن يكون لمُستقبِل بروتوكول PPP القدرة على اكتشاف أخطاء البتات في الإطار المستلَم.
- حيوية التوصيلة: يجب أن يكون لبروتوكول PPP القدرة على اكتشاف الأعطال على مستوى الوصلة (كعدم القدرة على نقل البيانات من جانب الإرسال إلى جانب الاستقبال من الوصلة) وإرسال إشارة بذلك إلى طبقة الشبكة.
- مفاوضات عنوان طبقة الشبكة: ينبغي أن يوفر بروتوكول PPP آلية لطبقات الشبكة المتصلة (على سبيل المثال IP) لمعرفة وتهيئة عنوان طبقة الشبكة لبعضها البعض.
- البساطة: كان على بروتوكول PPP تحقيق عدد من المتطلبات الأخرى بالإضافة لتلك المدرجة أعلاه، وكان على قمة كل تلك المتطلبات قبل كل شيء البساطة. تنص الوثيقة RFC 1547 على أن "الشعار الذي ينبغي أن يميّز

بروتوكول نقطة إلى نقطة PPP يجب أن يكون البساطة". وياله من مطلب صعب المنال في الواقع ـ إذا ما أخذنا في الاعتبار القائمة الطويلة من المتطلبات الأخرى لتصميم بروتوكول PPP. ظهر أكثر من خمسين من طلبات التعليقات (RFCs) حتى الآن لتعريف الجوانب المختلفة لهذا البروتوكول "البسيط"!

رغم أن قائمة المتطلبات التي وُضعت لتصميم بروتوكول PPP قد تبدو طويلة، إلا أن الوضع كان يمكن أن يكون أسوأ من ذلك! فمواصفات التصميم للبروتوكول نصت أيضاً على وظائف لم يكن مطلوباً من بروتوكول PPP أن يحققها، مثل:

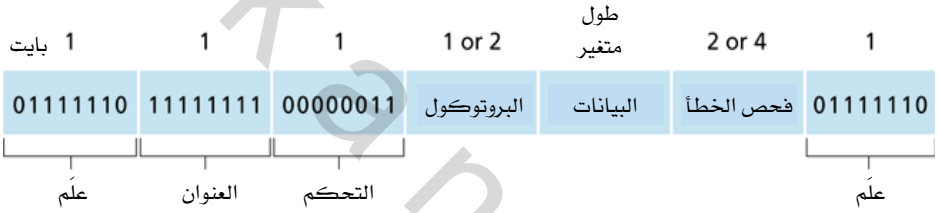
- تصحيح أخطاء البيانات: فبروتوكول PPP مطلوب منه اكتشاف أخطاء البتات ولكن ليس مطلوباً منه تصحيحها.
- ضبط التدفق: يُتوقع من مُستقبِل بروتوكول PPP أن يكون قادراً على استلام الإطارات عند إرسالها بمعدل الإرسال الكامل للطبقة المادية التحتية. إذا كانت طبقة أعلى لا تستطيع استلام الرزم بمعدل الإرسال هذا، فإن الطبقة الأعلى تتحمل مسؤولية إسقاط (إهمال) بعض الرزم أو "خنق" المُرسِل في الطبقة الأعلى. بمعنى أنه بدلاً من جعل مُرسِل PPP يخنق معدل إرساله بنفسه، يتحمل بروتوكول المستوى الأعلى مسؤولية خنق المعدل الذي يسلّم به مُرسِل ذلك البروتوكول الرزم إلى بروتوكول PPP لتوصيلها.
- تسلسل الإطارات: ليس مطلوباً من بروتوكول PPP توصيل الإطارات إلى مُستقبِل الوصلة بنفس الترتيب الذي أُرسِلَت به. من الجدير بالملاحظة أنه في حين تلائم تلك المرونة نموذج الخدمة لبروتوكول IP (والذي يسمح بتوصيل رزم IP من طرف إلى طرف بأي ترتيب)، فإن بروتوكولات أخرى لطبقة الشبكة والتي تعمل فوق بروتوكول PPP تتطلّب توصيل الرزم من طرف إلى طرف بالترتيب.
- الوصلات متعددة النقاط: المطلوب من بروتوكول PPP العمل فقط على الوصلات التي عليها مُرسِل واحد ومُستقبِل واحد. يمكن لبروتوكولات

أخرى لطبقة ربط البيانات (مثل بروتوكول HDLC) التعامل مع عدة مُستقبلين على وصلة (على سبيل المثال سيناريو شبيه بالإيثرنت) .

بعد أن تناولنا أهداف التصميم لبروتوكول PPP، دعنا نرى كيف استطاع تصميم هذا البروتوكول تحقيق هذه الأهداف.

1-7-5 تأطير البيانات في بروتوكول PPP

يبين الشكل 5-30 إطار بيانات PPP والذي يستخدم أسلوب تأطير مماثل لذلك المستخدم في بروتوكول HDLC [RFC 1662]. يتضمن إطار PPP الحقول التالية:



الشكل 5-30 صيغة إطار البيانات في بروتوكول PPP.

- حقل العَلَم (flag) : يبدأ كل إطار PPP وينتهي بحقل خاص طوله بايت واحد قيمته 01111110.
- حقل العنوان (address): القيمة الوحيدة المحتملة لهذا الحقل هي 11111111.
- حقل التحكم (control): القيمة المحتملة الوحيدة لهذا الحقل هي 00000011.

لمّا كان كلٌّ من حقلي التحكم والعنوان يأخذ قيمة واحدة (ثابتة) فقط، فقد تتساءل: لماذا تُعرّف تلك الحقول في المقام الأول. تنص مواصفات بروتوكول PPP [RFC 1662] على أنه قد يتم تعريف قيم أخرى في وقت لاحق، رغم أنه لم يتم شيء من ذلك حتى الآن. نظراً لأن هذه الحقول تأخذ قيماً ثابتة، فإن بروتوكول PPP يسمح للمُرسِل ببساطة بعدم إرسال بايتات العنوان والتحكم، ومن ثم يوفّر بايتين اثنين من العبء الإضافي في كل إطار PPP.

- حقل البروتوكول (protocol): يُخبر هذا الحقل مُستقبل PPP ببروتوكول الطبقة الأعلى الذي تنتمي له البيانات المغلّفة التي تم استلامها (أي محتويات حقل المعلومات في إطار PPP). عند استلام إطار PPP يقوم مُستقبل PPP بفحص الإطار للتأكد من صحته ثم يمرر البيانات المغلّفة إلى البروتوكول المناظر. يعرّف كلٌّ من RFC 1700 وRFC 3232 أرقام البروتوكولات التي يستخدمها بروتوكول PPP. إننا نهتم ببروتوكول IP في طبقة الشبكة (حيث تمثل البيانات المغلّفة في إطار PPP رزمة بيانات IP). يناظر بروتوكول IP القيمة 21 (بالصيغة الست عشرية) لحقل البروتوكول في إطار PPP. من بروتوكولات طبقة الشبكة الأخرى بروتوكول AppleTalk وبروتوكول DECnet وتُمثّل بالقيم 29 و27 على الترتيب.
- حقل المعلومات (information): يحتوي هذا الحقل على الرزمة المغلّفة (البيانات) التي يرسلها بروتوكول طبقة أعلى (مثلاً بروتوكول IP) على وصلة PPP. يبلغ الطول الأقصى المعتاد لحقل المعلومات 1500 بايت، مع أنه يمكن تغيير تلك القيمة عند تهيئة الوصلة في البداية كما سنبين لاحقاً.
- حقل المجموع التدقيقي (checksum): يُستخدم هذا الحقل لاكتشاف أخطاء البتات في الإطارات المُرسَلة. تُستعمل شفرة تدقيق إضافية دورية تبعاً لمعيار HDLC بطول بايتين أو 4 بايتات.

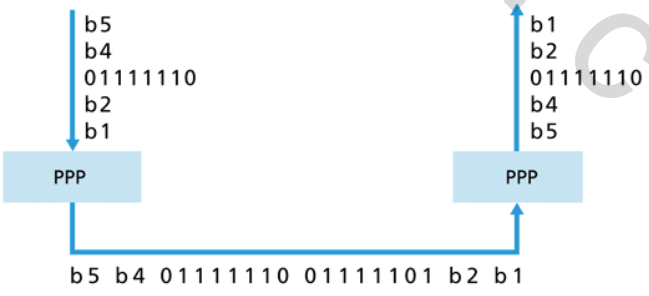
حشو البايتات (Byte Stuffing)

قبل أن نختم مناقشتنا لإطارات PPP، دعنا نتناول مشكلة تظهر عندما يستخدم بروتوكولٌ ما مسلسل بتات معين في حقل العَلَم لتحديد بداية أو نهاية الإطار. ماذا يحدث لو تكرر مسلسل بتات العَلَم في مكان آخر داخل الرزمة؟ على سبيل المثال ماذا يحدث لو ظهرت قيمة حقل العَلَم 01111110 في حقل المعلومات داخل الإطار؟ هل يتصوّر المستلم أنه اكتشف نهاية إطار PPP بشكلٍ خاطئ؟

يكمن أحد الطرق لحل هذه المشكلة في أن يمنع بروتوكول PPP بروتوكول الطبقة الأعلى من إرسال بيانات تحتوي على مسلسل بتات حقل العَلَم. غير أن متطلب

الشفافية في بروتوكول PPP والذي ذكرناه آنفاً يحول دون استخدام هذا الحل. هناك حل بديل، وهو المستخدم في بروتوكول PPP والعديد من البروتوكولات الأخرى، ويتلخص في استخدام التقنية المعروفة بحشو البايتات (byte stuffing).

يُعرّف PPP بايت تحكم خاص للهروب قيمته 01111101. إذا حدث وظهرت قيمة حقل العَلَم 01111110 في أي مكان في الإطار، باستثناء حقل العَلَم، يُدخل بروتوكول PPP قبل ذلك البايت بايت تحكم الهروب. بمعنى أنه "يحشو" (يضيف) بايت تحكم الهروب في سلسلة البيانات المُرسَلة، قبل 01111110، للإشارة إلى أن البايت التالي (01111110) ليس قيمة العَلَم ولكن في الحقيقة يمثّل بيانات فعلية. أي مُستقبِل يرى 01111110 مسبوقاً بـ 01111101 سيقوم بالطبع بإزالة بايت تحكم الهروب التي قام المُرسِل بحشوه وذلك لاستعادة سلسلة البيانات الأصلية. بنفس الطريقة، إذا ظهر بايت تحكم الهروب نفسه ضمن البيانات الفعلية، يجب أيضاً أن تُسبق ببايت تحكم هروب آخر يتم حشوه. وهكذا فعندما يرى المُستقبِل بايت تحكم هروب لوحده في سلسلة البيانات فإنه يعرف إن البايت تم حشوه في سلسلة البيانات. أما إذا ظهر زوج من بايتات تحكم الهروب (الواحد تلو الآخر مباشرةً) فهذا يعني أن البيانات الأصلية المُرسَلة تحتوي على بايت تحكم هروب واحد. يوضح الشكل 5-31 عملية حشو البايتات في بروتوكول PPP. (في الحقيقة يقوم PPP أيضاً بإجراء عملية "أو - الحصرية" (XOR)، بين بايت البيانات الذي يتم الهروب منه والرقم الست عشري 20، ولكن هذا تفصيلٌ آثرنا إهماله بهدف التبسيط).



الشكل 5-31 حشو البايتات في بروتوكول PPP.

نشير هنا إلى أن بروتوكول PPP يتضمن أيضاً بروتوكولاً للتحكم في الوصلة ((link control protocol (LCP والذي تتلخص وظيفته في تهيئة وصيانة وإغلاق وصلة PPP. تتضمن المواد الإضافية المرتبطة بهذا الكتاب على الإنترنت مناقشة عن بعض تفاصيل بروتوكول LCP.

8-5 الوصلة الافتراضية: الشبكة كطبقة ربط البيانات

لمّا كان هذا الفصل يتعلّق ببروتوكولات طبقة الوصلة، وبما أننا نقترب الآن من نهاية الفصل، دعنا نتأمل كيف تطوّر فهمنا للمصطلح "وصلة". لقد بدأنا هذا الفصل بالنظر إلى الوصلة كسلك مادي يصل ما بين مضيفين يتصلان فيما بينهما كما وضّح الشكل 5-2. في دراستنا لبروتوكولات الوصول المتعدد (الشكل 5-9)، رأينا أنه يمكن ربط عدة مضيفات ببعضها بواسطة سلك مشترك، وأن "السلك" الذي يربط المضيفات يمكن أن يكون حيز ترددات لاسلكية أو وسطاً مادياً آخر. بهذا المفهوم بدأنا ننظر إلى الوصلة بشيء من التجريد كـ "قناة"، بدلاً منها كـ "سلك". في دراستنا لشبكات الإيثرنت المحلية (الشكل 5-26) رأينا أن أوساط الربط المادية يمكن أن تكون في الحقيقة بنية نقل تحتية معقدة، ومع ذلك فعبر مراحل هذا التطور احتفظت المضيفات نفسها بالمفهوم ذاته ـ أن وسط التشبيك هو ببساطة قناة طبقة ربط بيانات تصل ما بين مضيفين أو أكثر. رأينا على سبيل المثال أن مضيفاً على الإيثرنت يمكن أن يكون غير مدرك لما إذا كان موصّلاً بالمضيفات الأخرى على الشبكة المحلية بواسطة قطعة واحدة قصيرة من شبكة محلية (الشكل 5-9) أو عبر شبكة محلية متسعة جغرافياً وتستخدم المحوّلات (الشكل 5-26).

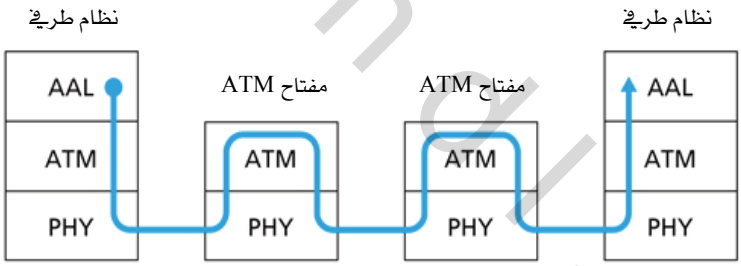
في الجزء 5-7 رأينا أن بروتوكول PPP يُستخدم غالباً عبر وصلة مودم بين مضيفين. في هذه الحالة، الوصلة التي تربط بين المضيفين هي في الحقيقة شبكة الهاتف ـ وهي شبكة اتصالات عالمية مستقلة منطقياً لها محوّلاتها، ووصلاتها، ورصات البروتوكولات الخاصة بها لنقل البيانات وإرسال إشارات التحكم (التأشير) (signaling). ولكن من وجهة نظر طبقة ربط البيانات في الإنترنت، يُنظر

إلى توصيلة المودم عبر شبكة الهاتف على أنها ببساطة سلك. بهذا المعنى فإن الإنترنت "تُجرّد" شبكة الهاتف، حيث تعتبرها بمثابة تقنية افتراضية لطبقة ربط البيانات توفر اتصالاً بين اثنين من مضيفي الإنترنت. تذكّر من مناقشتنا لمفهوم الشبكة الإضافية (overlay network) في الفصل الثاني أن الشبكة الإضافية تنظر إلى الإنترنت بنفس الطريقة كوسيلة لتوفير توصيلات بين عقد الشبكة الإضافية، بحيث تغطي (overlay) الإنترنت بنفس الطريقة التي تغطي بها الإنترنت شبكة الهاتف.

سنتناول في هذا الجزء شبكات نمط النقل غير المتزامن (ATM) وشبكات تحويل الوسمة متعدد البروتوكول (MPLS). على خلاف شبكة الهاتف بتحويل الدوائر تعتبر كلٌّ من ATM وMPLS بحكم تكوينهما شبكات تحويل رزم بدوائر افتراضية. لتلك الشبكات صيغ للإطارات وأساليب للتوجيه خاصة بها. وعليه فمن وجهة نظر تعليمية بحتة، من الملائم دراسة شبكات ATM وMPLS في سياق طبقة الشبكة أو طبقة ربط البيانات. غير أنه، من وجهة نظر الإنترنت، يمكن أن نعتبر شبكات ATM وMPLS مثل شبكة الهاتف وشبكات الإيثرنت المحوّلة، كتقنيات طبقة ربط بيانات توفر خدمة لتشبيك أجهزة IP. وعليه فسنتناول كلاً من شبكات ATM وMPLS في مناقشتنا لطبقة ربط البيانات. يمكن أيضاً استخدام شبكات ترحيل الإطارات (frame-relay) في تشبيك أجهزة IP على الرغم من أنها تمثل تقنيةً أقدم قليلاً (لكن لا تزال تُستخدم)، ولن نغطيها هنا وإنما ننصح بمراجعة الكتاب الجيد [Goralski 1999] للمزيد من التفاصيل. ستكون معالجتنا لشبكات ATM وMPLS مختصرة بالضرورة، فهناك كتب بكاملها تناولت تلك الشبكات. نوصي بمراجعة [Black 1995, Black 1997] و [Davie 2000] للمزيد من التفاصيل عن شبكات ATM وMPLS على الترتيب. سنركّز هنا بشكلٍ رئيس على الكيفية التي توفر بها تلك الشبكات خدمة تشبيك لأجهزة IP، مع أننا سنغوص أيضاً بعض الشيء في التقنيات التحتية المستخدمة.

5-8-1 شبكات نمط النقل غير المتزامن (ATM)

تم تطوير معايير شبكات نمط النقل غير المتزامن لأول مرة في منتصف الثمانينيات بهدف تصميم تقنية شبكات واحدة لنقل مواد الصوت والفيديو الفورية بالإضافة إلى النصوص، والبريد الإلكتروني، وملفات الصور. شاركت مجموعتان في تطوير معايير شبكات ATM، هما: منتدى ATM (والذي يُعرف الآن بمنتدى MFA Forum [MFA Forum 2007] والاتحاد الدولي للاتصالات [ITU 2007]. تم تحديد معيار كامل من طرف إلى طرف اشتمل على مواصفات تراوحت من واجهات التطبيقات مع شبكة ATM إلى تأطير بيانات ATM على مستوى البتات عبر مختلف الطبقات المادية بما في ذلك الألياف الضوئية، والأسلاك النحاسية، والراديو. عملياً استُخدمت شبكات ATM ضمن شبكات الهاتف وشبكات IP كتقنية لطبقة ربط البيانات مثلاً لتوصيل موجّهات IP كما بيّنا سابقاً.



الشكل 5-32 طبقات شبكة ATM الثلاث. توجد الطبقة AAL فقط على حواف شبكة ATM.

الخصائص الرئيسة لشبكات ATM

كما تقدم في الجزء 5-4-1، تدعم شبكات ATM عدّة نماذج خدمة، بما في ذلك خدمة معدّل البتات الثابت (Constant Bit Rate (CBR) ، وخدمة معدل البتات المتغير (Variable Bit Rate (VBR)، وخدمة معدّل البتات المتوفر (Available Bit)

((Rate (ABR ، وخدمة معدّل البتات غير المحدّد ((Unspecified Bit Rate (UBR)). تعتمد ATM بنيةً معمارية للشبكة أساسها تحويل الرزم والدوائر الافتراضية ((Virtual Circuits (VCs)). تذكّر أننا سبق أن استعرضنا موضوع الدوائر الافتراضية بشيء من التفصيل في الجزء 4-2-1. تم تنظيم البنية المعمارية الكلية لشبكات ATM على شكل ثلاث طبقات كما هو مبين في الشكل 5-32.

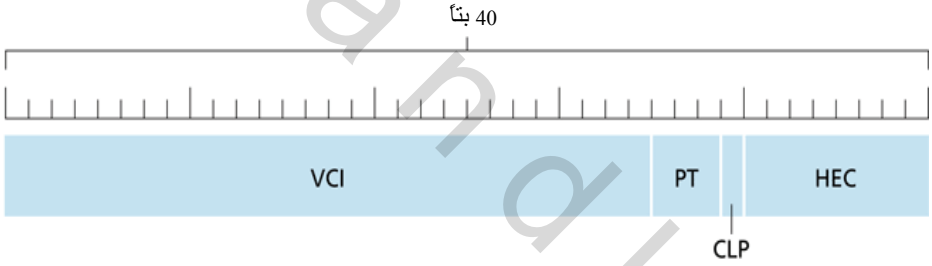
تشبه طبقة التكيّف بشبكة ((ATM Adaptation Layer AAL (ATM) تقريباً طبقة النقل في الإنترنت، وتوجد فقط في أجهزة ATM الموجودة على حافة الشبكة. على جانب الإرسال يتم تمرير البيانات إلى طبقة AAL من تطبيق أو بروتوكول في الطبقة الأعلى (مثل IP، إذا كانت شبكة ATM تستخدم لتشبيك أجهزة IP). على جانب الاستقبال ترفع طبقة AAL البيانات التي تم استلامها إلى البروتوكول أو التطبيق في الطبقة الأعلى. تم تعريف طبقات AAL مختلفة مثل AAL1 لخدمات معدّل البتات الثابت ومحاكاة الدوائر، وAAL2 لخدمات معدّل البتات المتغير (كالفيديو بمعدّل بتات متغير)، وAAL5 لخدمات البيانات (كنقل وحدات بيانات IP). من بين الخدمات التي تؤديها طبقة AAL اكتشاف الأخطاء، والتجزيء (segmentation) وإعادة التجميع (reassembly) . تعرف وحدة البيانات التي تتعامل معها طبقة AAL باسم عام هو وحدة بيانات بروتوكول AAL، وهي تكافئ تقريباً قطع بيانات UDP أو TCP.

يبين الشكل 5-33 وحدة بيانات بروتوكول AAL5. إن حقول وحدة البيانات بسيطة نسبياً. يضمن الحقل PAD أن وحدة البيانات تتكون من عدد صحيح من مضاعفات 48 بايتاً، لكي يسمح ذلك بتجزيء وحدة البيانات لتلائم حمولة بطول 48 بايتاً على رزم ATM التحتية (والتي تُعرف بخلايا ATM). يميّز حقل الطول حجم حمولة وحدة البيانات، بحيث يمكن إزالة الحقل PAD عند المُستقبل. يستخدم حقل CRC لاكتشاف أخطاء البتات بنفس أسلوب فحص الفائض الدوري المستخدم في الإيثرنت. يمكن أن يصل طول حقل الحمولة إلى 65535 بايت.

(بايت) 0-65535	0-47	2	4
الحمل الآجر CPCS-PDU	حشو	الطول	CRC

الشكل 5-33 وحدة بيانات بروتوكول AAL5.

دعنا الآن ننزل طبقة واحدة لأسفل لنتناول طبقة ATM، والتي تقع في قلب البنية المعمارية للشبكة. تعرّف طبقة ATM هيكل خلية ATM ومعنى كل حقل في الخلية. إن أهمية خلية ATM لشبكة ATM تماثل أهمية وحدة بيانات IP لشبكة IP. تشكّل البايتات الخمس الأولى من خلية ATM ترويسة ATM؛ بينما تشكّل البايتات الـ 48 الباقية حمولة ATM. يبين الشكل 5-34 صيغة ترويسة خلية ATM.



الشكل 5-34 صيغة ترويسة خلية ATM.

تؤدي الحقول المختلفة في خلية ATM الوظائف التالية:

- حقل معرّف القناة (أو الدائرة) الافتراضية (Virtual Channel Identifier ((VCI): يبين القناة الافتراضية التي تنتمي إليها الخلية. كما هو الحال في معظم تقنيات الشبكات التي تستخدم دوائر افتراضية، يتم ترجمة معرّف الخلية من وصلة إلى وصلة (انظر الجزء 4-2-1).
- حقل نوع الحمولة (Payload Type (PT)): يشير إلى نوع الحمولة الموجودة في خلية ATM . هناك عدة أنواع من حمولة البيانات، وعدة أنواع من حمولة

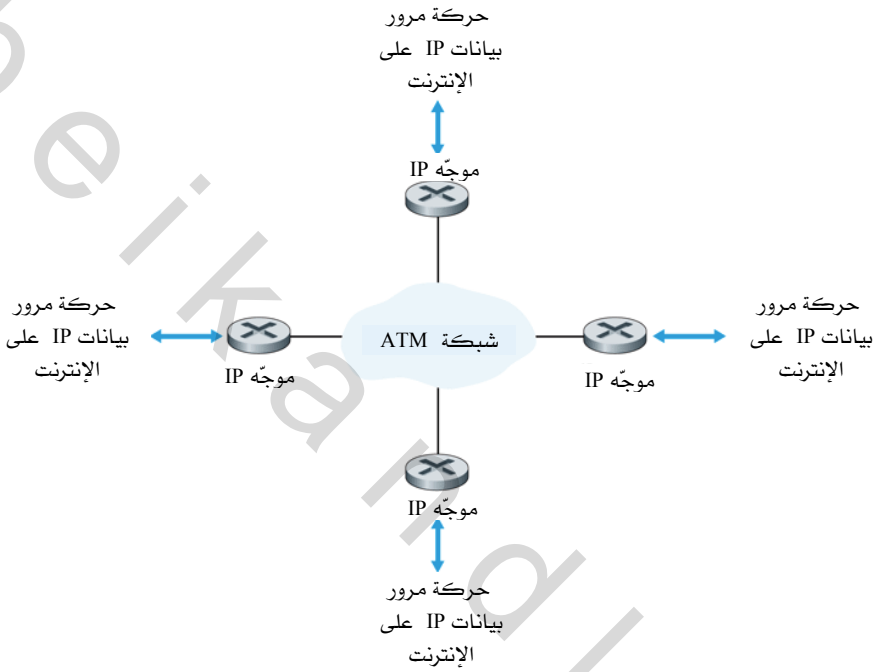
الصيانة، ونوع حمولة خلية شاغرة. يتضمّن حقل PT أيضاً بتاً لتمييز الخلية الأخيرة في وحدة بيانات بروتوكول AAL المجزّأة.

- بت أولوية الفقد للخلية (Cell-Loss Priority (CLP)). يمكن للمصدر إعطاؤها القيمة 1 للتفريق بين حركة مرور البيانات ذات الأولوية العالية وذات الأولوية المنخفضة. إذا حدث ازدحام وكان على محوّل ATM إهمال خلايا يمكن للمحوّل استخدام هذا البت للتخلص من حركة مرور البيانات ذات الأولوية المنخفضة.
- بايت التحكم في خطأ الترويسة (Header Error Control (HEC)). بتات اكتشاف الأخطاء التي تحمي ترويسة الخلية.

قبل أن يبدأ مصدر في إرسال خلايا إلى وجهة، يتعين على شبكة ATM أولاً تأسيس قناة افتراضية تمتد من المصدر إلى الوجهة. لا تعدو القناة الافتراضية كونها دائرة افتراضية كما وصفنا في الجزء 4-2-1. كل قناة افتراضية هي مسار يتألف من سلسلة وصلات بين المصدر والوجهة. يرتبط بكل وصلة على القناة الافتراضية مُعرّف القناة الافتراضية (VCI). في كل مرة يتم تأسيس أو فض قناة افتراضية، يتعين تحديث جداول الترجمة الخاصة بالقنوات الافتراضية (انظر الجزء 4-2-1). في حالة استخدام قناة افتراضية دائمة لن تكون هناك حاجة لتأسيس وفض القناة بطريقة ديناميكية. عند الحاجة لتأسيس وفض القناة بطريقة ديناميكية يوفر البروتوكول Q.2931 [Black 1997; ITU-T Q.2931 1994] عمليات التأشير اللازمة بين المحوّلات والأنظمة الطرفية في شبكة ATM.

تقع طبقة ATM المادية في أسفل القاع من رصة بروتوكولات ATM، وتتعامل مع الفولطيات، وتوقيت البتات، وتأطير البيانات على الوسط المادي. يعتمد جزء كبير من الطبقة المادية على خصائص الوصلة المادية. هناك صنفان أساسيان من الطبقات المادية: الطبقات التي لها هيكل محدد لإطار الإرسال (مثل: T1 وT3 وSONET وSDH)، والطبقات التي ليس لها هيكل محدد لإطار الإرسال. إذا كان للطبقة المادية هيكل إطار، تكون الطبقة مسؤولة عن توليد وتحديد الإطارات. ينبغي عدم الخلط بين كلمة "إطارات" المستخدمة هنا واستخدامنا لها في سياق

طبقة ربط البيانات (كما في الإيثرنت). يمثل إطار الإرسال هنا آلية خاصة بالطبقة المادية لتنظيم البتات المُرسِلة، كما في حالة إطارات الإرسال المتعدد بتقسيم الزمن (TDM).



الشكل 5-35 شبكة ATM في قلب العمود الفقري للإنترنت.

تشغيل بروتوكول IP فوق شبكة ATM

دعنا الآن ندرس كيف يمكن استخدام شبكة ATM للتشبيك ما بين أجهزة IP. يبين الشكل 5-35 شبكة عمود فقري ATM بأربع نقاط دخول وخروج لحركة بيانات الإنترنت IP. لاحظ أن كل نقطة دخول وخروج هي موجّه. يمكن أن تمتد شبكة العمود الفقري ATM لتغطي قارة بأكملها وتتضمن العشرات بل المئات من محوّلات ATM. تستخدم معظم شبكات الأعمدة الفقرية من نوع ATM قناة افتراضية دائمة بين كل زوج من نقاط الدخول والخروج. باستخدام قنوات افتراضية

دائمة يمكن توجيه خلايا ATM من نقطة دخول إلى نقطة خروج دون الحاجة لتأسيس أو فض قنوات افتراضية بطريقة ديناميكية. غير أن استخدام قنوات افتراضية دائمة يكون ممكناً فقط عندما يكون عدد نقاط الدخول والخروج قليلاً نسبياً. للتوصيل مباشرة بين n نقطة دخول وخروج نحتاج لـ $n(n - 1)$ قناة افتراضية دائمة.

ستحتاج كل واجهة على موجّه موصّل بشبكة ATM إلى عنوانين، تقريباً بنفس الطريقة التي يحتاج بها مضيف IP إلى عنوانين لوصلة إيثرنت: عنوان IP وعنوان ماك. بالمثل، يكون لواجهة ATM عنوان IP وعنوان ATM. خذ في الاعتبار الآن وحدة بيانات IP تعبر شبكة ATM المبينة في الشكل 5-35. في الحالة الأبسط تبدو شبكة ATM كوصلة منطقية واحدة تربط تلك الموجّهات الأربعة كما في حالة استخدام الإيثرنت لتوصيل أربعة موجّهات. دعنا نشير إلى الموجّه الذي تدخل منه أي وحدة بيانات إلى شبكة ATM بـ "موجّه دخول" والموجّه الذي تغادر منه وحدة البيانات الشبكة بـ "موجّه خروج". يقوم موجّه الدخول بما يلي:

1. فحص عنوان الوجهة لوحدة البيانات.
2. الدخول على جدول التوجيه لديه وتحديد عنوان IP لموجّه الخروج (أي الموجّه التالي في طريق وحدة البيانات).
3. لتوصيل وحدة البيانات إلى موجّه الخروج، يتعامل موجّه الدخول مع ATM كمجرد بروتوكول طبقة ربط بيانات آخر. لنقل وحدة البيانات إلى الموجّه التالي، علينا تحديد العنوان المادي لموجّه القفزة التالية. تذكّر من مناقشتنا في الجزء 5-4-2 إن هذا يتم باستخدام بروتوكول تحويل العناوين ARP. في حالة واجهة ATM يفحص موجّه الدخول جدول ATM ARP مستخدماً عنوان IP لموجّه الخروج ليحصل على عنوان ATM لموجّه الخروج. يوجد وصف لبروتوكول ATM ARP في [RFC 2225].
4. يقوم بروتوكول IP في موجّه الدخول بعد ذلك بتمرير وحدة البيانات مع عنوان ATM لموجّه الخروج إلى طبقة ربط البيانات بشبكة ATM.

بعد الانتهاء من تلك الخطوات الأربع، تخرج مهمة نقل وحدة البيانات إلى موجّه الخروج من أيدي بروتوكول IP وتنتقل إلى أيدي بروتوكول ATM. على ATM الآن نقل وحدة البيانات إلى عنوان ATM للوجهة والذي تم الحصول عليه في الخطوة 3 أعلاه. تنضوي تحت هذه المهمّة مهمّتان ثانويتان:

1. تحديد المعرّف VCI للقناة الافتراضية التي تؤدي إلى عنوان ATM للوجهة.
2. تجزئة وحدة البيانات إلى خلايا في جانب الإرسال على القناة الافتراضية (أي على موجّه الدخول)، ثم إعادة تجميع الخلايا للحصول على وحدة البيانات الأصلية في جانب الاستقبال على القناة الافتراضية (أي على موجّه الخروج).

المهمّة الثانوية الأولى سهلة. تحتوي الواجهة في جانب الإرسال على جدول للتحويل من عناوين ATM إلى معرّفات القنوات الافتراضية المناظرة. ونظراً لأننا افترضنا إن القنوات الافتراضية دائمة، فسيكون ذلك الجدول ثابتاً ومحدّثاً (بينما إذا كانت القنوات الافتراضية غير دائمة، فسيُستخدم بروتوكول التأشير ATM Q.2931 لتأسيس وفض القنوات الافتراضية بشكلٍ ديناميكي). أما المهمّة الثانية فتستحق تناولاً أكثر حذراً. أحد الطرق هو استخدام تجزئة IP كما تناولناه في الجزء 4-4. في هذه الحالة يقوم موجّه الإرسال أولاً بتجزئة وحدة البيانات الأصلية إلى أجزاء، بحيث لا يزيد كل جزء عن 48 بايتاً، ليتسنى وضع كل جزء كحمولة في خلية ATM. لكن هذه الطريقة في التجزئة تعاني من مشكلة كبيرة ـ فكل جزء IP له عادةً ترويسة تتكون من 20 بايتاً، وعليه فإن كل خلية ATM تحمل جزء IP ستحمل فقط 28 بايتاً من المعلومات المفيدة مقابل 25 بايتاً من العبء الإضافي (overhead). لهذا السبب تستخدم ATM بروتوكول AAL5 لتجزئة وإعادة تجميع وحدات البيانات بطريقة أكثر كفاءة.

بعد ذلك تنقل طبقة ATM كل خلية عبر الشبكة إلى عنوان ATM للوجهة. عند كل محوّل ATM بين مصدر ATM ووجهة ATM، يتم معالجة الخلية بواسطة طبقة ATM المادية وطبقات ATM الأخرى باستثناء طبقة AAL. في كل محوّل، يتم عادةً ترجمة معرّف القناة الافتراضية VCI (راجع الجزء 4-2-1) ويعاد حساب بايت التحكم في خطأ الترويسة (HEC). عندما تصل الخلايا إلى عنوان ATM للوجهة يتم

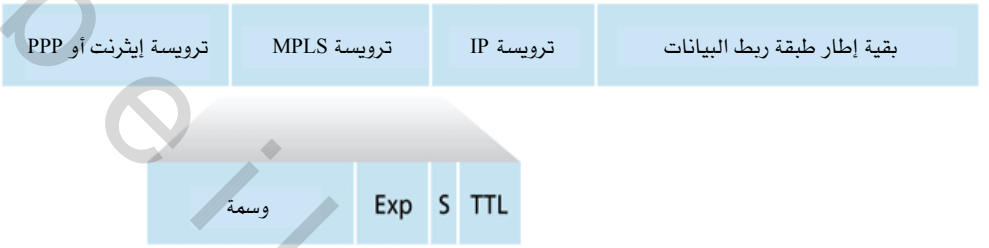
توجيهها إلى مخزن AAL مؤقت تم تخصيصه للقناة الافتراضية المستخدمة. بعد ذلك يعاد بناء وحدة بيانات بروتوكول AAL5 واستخراج وحدة بيانات IP وتمريرها عبر رصة البروتوكولات إلى طبقة IP.

2-8-5 تقنية تحويل الوسمة متعدد البروتوكول (MPLS)

تم تطوير تقنية تحويل الوسمة متعدد البروتوكول (Multi-Protocol Label Switching (MPLS)) من خلال جهود الصناعة في أواسط التسعينيات إلى أواخرها من أجل تحسين سرعة التوجيه في موجّهات IP، وذلك بتبنّي مفهوم أساسي من عالم شبكات الدائرة الافتراضية: استخدام وسمة (label) بطول ثابت. لم يكن الهدف الاستغناء عن البنية التحتية لتوجيه وحدات بيانات IP والمبني على أساس معرفة عنوان الوجهة النهائية واستبداله ببنية أخرى أساسها وسمات بأطوال ثابتة ودوائر افتراضية، ولكنه كان إدخال تحسينات على الوضع الحالي لنظام توجيه IP بوسم وحدات بيانات IP بشكلٍ اختياري والسماح للموجّهات بتوجيه حزم البيانات بناءً على الوسمات ثابتة الطول (بدلاً من عناوين IP للوجهة النهائية) كلما كان ذلك ممكناً. من المهم ملاحظة أن هذه الأساليب تعمل بالتعاون يداً بيد مع بروتوكول IP، مستخدمةً أنظمة IP للعنونة والتوجيه. قام فريق عمل هندسة الإنترنت بتوحيد تلك الجهود في بروتوكول MPLS [RFC 3031; RFC 3032]، والذي يدمج أساليب الدوائر الافتراضية في سياق شبكات توجيه وحدات البيانات.

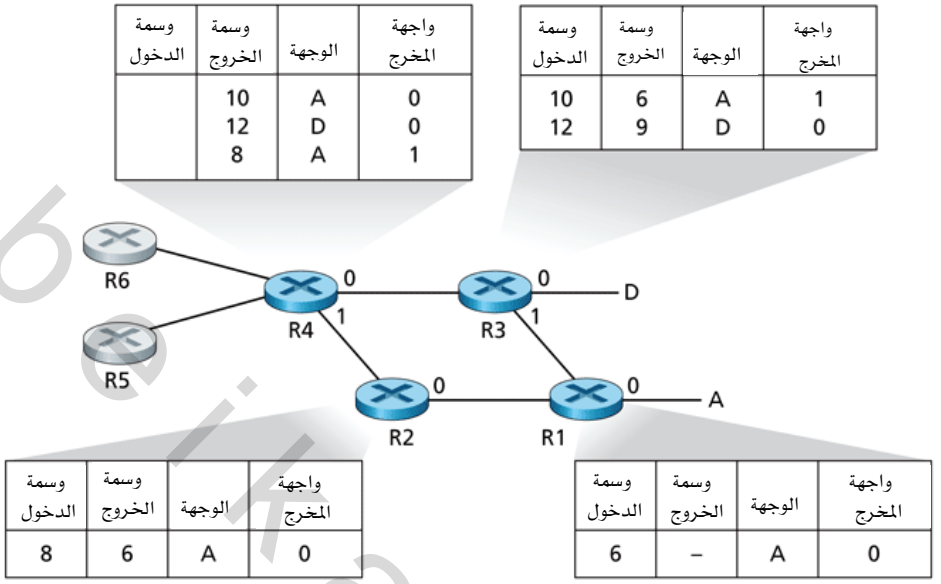
دعنا نبدأ دراستنا لبروتوكول MPLS باستعراض صيغة إطار طبقة ربط البيانات التي يعالجها موجّه مزوّد بإمكانيات التعامل مع MPLS. كما هو موضّح في الشكل 5-36، يتضمن إطار طبقة ربط البيانات المُرسَل على وصلة PPP أو شبكة محلية (كالإيثرنت) ترويسة MPLS صغيرة تضاف بين ترويسة الطبقة 2 (أي PPP أو الإيثرنت) وترويسة الطبقة 3 (أي IP). يُعرّف طلب الاقتراحات RFC 3032 صيغة ترويسة MPLS لتلك الوصلات؛ كما تم تعريف ترويسات MPLS لشبكات ATM وشبكات ترحيل الإطارات في وثائق RFC أخرى. تضم حقول ترويسة MPLS حقل الوسمة (label) (والتي تلعب دور مُعرّف الدائرة الافتراضية (VCI) الذي

استخدمناه في الجزء 4-2-1)، وحقلاً بطول 3 بتات محجوزة للاستعمال التجريبي، وحقلاً من بت واحد S يُستخدم للإشارة إلى نهاية سلسلة من ترويسات MPLS المرصوصة (stacked) (وهو موضوع متقدّم لن نغطيه هنا)، وأخيراً حقل يبين فترة العمر (TTL).



الشكل 5-36 ترويسة MPLS: والتي تقع بين ترويسة طبقة ربط البيانات وترويسة طبقة الشبكة.

يتضح مباشرةً من الشكل 5-36 أن الإطار المُحسّن بـ MPLS يمكن تبادله فقط بين موجّهين يكون لكلٍّ منهما القدرة على التعامل مع MPLS (حيث إن الموجّهات التي لا تفهم MPLS سترتبك تماماً عندما تجد ترويسة MPLS حيث تتوقّع وجود ترويسة IP!). غالباً ما يُطلق على الموجّه المزوّد بإمكانيات MPLS اسم موجّه التحويل بوسمة (label-switched router)، حيث إنه يقوم بتوجيه إطار MPLS باستخدام قيمة حقل الوسمة في ترويسة MPLS للدخول على جدول التوجيه الموجود عليه، ثم تمرير وحدة البيانات فوراً إلى واجهة الخرج المناسبة. وهكذا فإن الموجّه المزوّد بإمكانيات MPLS لا يحتاج لاستخراج عنوان IP للوجهة ثم تحديد مطابقة أطول بادئة بالرجوع إلى جدول التوجيه لديه تمهيداً لتوجيه الإطار. لكن كيف يعرف موجّه في الواقع ما إذا كان الموجّه المجاور له مجهزاً فعلاً للتعامل مع MPLS، وكيف يعرف الموجّه أي وسمة تقابل عنوان IP مُعطى لوجهة نهائية؟ للإجابة على هذه الأسئلة، نحتاج لإلقاء نظرة على التفاعل ما بين مجموعة موجّهات مجهزة للتعامل مع MPLS.



وسمة الدخول	وسمة الخروج	الوجهة	واجهة المخرج
	10	A	0
	12	D	0
	8	A	1

وسمة الدخول	وسمة الخروج	الوجهة	واجهة المخرج
10	6	A	1
12	9	D	0

وسمة الدخول	وسمة الخروج	الوجهة	واجهة المخرج
8	6	A	0

وسمة الدخول	وسمة الخروج	الوجهة	واجهة المخرج
6	–	A	0

الشكل 5-37 توجيه محسّن لوحدات بيانات IP باستخدام وسمات MPLS.

في المثال الموضح في الشكل 5-37، للموجّهات من R1 إلى R4 القدرة على التعامل مع MPLS، بينما R5 وR6 موجّهان IP عاديّان. افترض أن الموجّه R1 أعلن للموجّه R2 بأنه (أي R1) يمكنه أن يوجّه إلى الوجهة A، وأن الإطارات التي يتم استلامها بوسمات MPLS قيمتها 6 سترسل إلى الوجهة A. وكذلك أعلن الموجّه R3 لـ R4 بأنه يمكنه أن يوجّه إلى الوجهتين A وD، وأن الإطارات القادمة بوسمات MPLS قيمتها 10 و12 ستوجّه إلى هاتين الوجهتين على الترتيب. كما أعلن الموجّه R2 أيضاً للموجّه R4 بأنه يمكنه أن يصل إلى الوجهة A، وأن الإطارات بوسمات MPLS قيمتها 8 سيتم تحويلها نحو A. لاحظ أن الموجّه R4 أصبح الآن في وضعٍ فريد، حيث يتوافر لديه مساران من مسارات MPLS للوصول إلى A ـ عن طريق الواجهة 0 بوسمة خروج قيمتها 10، وعن طريق الواجهة 1 بوسمة خروج قيمتها 8. الصورة العامة التي نخرج بها من الشكل 5-37 هي أن أجهزة IP (الموجّهين R5 وR6 والمضيفين A وD) ترتبط مع بعضها عن طريق بنية تحتية بتقنية MPLS (الموجّهات من R1 إلى R4 والمزودة بإمكانيات MPLS)، تقريباً بنفس الطريقة التي يمكن بها

لشبكة بيانات محلية أو شبكة ATM تشبيك أجهزة IP سوية. وكما في حالة شبكة محلية محوّلة أو شبكة ATM، فإن الموجّهات من R1 إلى R4 والمزودة بإمكانيات MPLS تؤدي ذلك بدون أن تتعامل أبداً مع ترويسة IP في قطعة البيانات.

في مناقشتنا أعلاه، لم نحدّد البروتوكول المعيّن المستخدم في توزيع وسمات MPLS بين الموجّهات المزودة بإمكانيات MPLS؛ نظراً لأن تلك التفاصيل تقع خارج نطاق هذا الكتاب. ولكن نلاحظ هنا أن مجموعة العمل المنبثقة من IETF والمختصة بـ MPLS قد حدّدت في [RFC 3468] أن امتداداً لبروتوكول RSVP (والذي سندرسه في الفصل السابع)، ويعرف بـ RFC [RSVP-TE 3209] سيشكّل بؤرة الجهود لنظام التأشير باستخدام MPLS. وعليه فإننا نشجع القارئ المهتم بمراجعة RFC 3209.

حتى الآن ركزت مناقشتنا على أن MPLS يقوم بعملية التحويل بناءً على الوسمات، بدون حاجة لأخذ عنوان IP لوحدة البيانات في الاعتبار. غير أن الفوائد الحقيقية لـ MPLS والسبب وراء الاهتمام الكبير به حالياً لا يكمن في الزيادة المحتملة في سرعة تحويل الرزم فقط، ولكن بالأحرى في الإمكانيات الجديدة لإدارة حركة مرور البيانات والتي يوفرها MPLS. كما لاحظنا أعلاه، يتوافر للموجّه R4 مساران MPLS إلى المضيف A، إذا تم توجيه الرزم في طبقة IP الأعلى بناءً على عنوان IP، ستحدد بروتوكولات IP للتوجيه – والتي درسناها في الفصل الرابع – مساراً واحداً إلى A هو المسار الأقل كلفة. وهكذا يوفر MPLS إمكانية توجيه الرزم عبر مسارات قد لا تكون متاحة عند استخدام بروتوكولات توجيه IP القياسية. يعتبر هذا مجرد شكل واحد بسيط فقط من تطبيقات هندسة مرور البيانات الممكنة باستخدام MPLS [RFC 3346; RFC 3272; RFC 2702; Xiao 2000]، حيث يمكن لمشغّل الشبكة أن يتخطى توجيه IP المعتاد ويُجبر بعض حركة المرور المرسَلة إلى وجهةٍ ما على سلوك مسار بعينه، وحركة مرور أخرى إلى نفس الوجهة على سلوك مسار آخر (سواء لأسباب تتعلق بسياسة المرور، أو الأداء، أو أي سبب آخر).

يمكن أيضاً استخدام MPLS للعديد من الأغراض الأخرى، كالاستعادة السريعة لمسارات توجيه MPLS. مثلاً لإعادة توجيه المرور عند حدوث عطل في وصلة إلى مسار احتياطي محسوب مسبقاً [Kar 2000; Huang 2002; RFC 3469]. يمكن أيضاً استخدام MPLS لتحقيق هيكل الخدمة التفاضلية ("DiffSev") والتي سندرسها في الفصل السابع. وأخيراً نلاحظ أن MPLS يمكن أن يُستخدم أيضاً لتطبيق ما يسمّى بالشبكة الافتراضية الخاصة ((Virtual Private Network (VPN)
حيث يستخدم موفر خدمة الإنترنت شبكته المزوّدة بإمكانيات MPLS في توصيل الشبكات المختلفة الخاصة بعميلٍ ما ببعضها البعض، وبذلك يمكن عزل كلٍّ من الموارد، والعنونة المستخدمة بواسطة شبكة VPN للعميل عن المستخدمين الآخرين الذين يعبرون شبكة موفر الخدمة. لمزيد من التفاصيل انظر [DeClercq 2002].

لقد كانت مناقشتنا لـ MPLS مختصرة بالضرورة، ولذا فنحن نشجّعك على الرجوع إلى المراجع التي ذكرناها للحصول على المزيد من التفاصيل. نلاحظ أنه مع ظهور العديد من الاستخدامات الممكنة لـ MPLS، يبدو أن هذا الأسلوب الجديد سيوفر حلاً للكثير من المشاكل في مجال هندسة حركة مرور الإنترنت!

5-9 الخلاصة

تناولنا في هذا الفصل طبقة ربط البيانات، حيث استعرضنا خدماتها، والمبادئ التي تحكم عملها، وعدداً من البروتوكولات المحددة والهامة التي تستخدم تلك المبادئ في تحقيق خدمات طبقة ربط البيانات.

رأينا أن الخدمة الأساسية لطبقة ربط البيانات تتلخص في نقل وحدة بيانات طبقة الشبكة من عقدة (موجّه أو مضيف) إلى عقدة مجاورة. وعرفنا أن كل بروتوكولات طبقة ربط البيانات تقوم بتغليف وحدة بيانات طبقة الشبكة ضمن إطار طبقة ربط البيانات قبل إرسال الإطار على الوصلة إلى العقدة المجاورة. وباستثناء وظيفة التأطير المشتركة تلك، وجدنا أن بروتوكولات طبقة ربط البيانات المختلفة توفر خدمات وتستخدم طرقاً مختلفة جداً للوصول للوصلة، ولتوصيل البيانات (الموثوقية واكتشاف وتصحيح الأخطاء)، ولضبط التدفق، وللإرسال

(مثلاً إرسال مزدوج تماماً أو نصف مزدوج). من أسباب هذه الاختلافات كثرة الأنواع المختلفة من الوصلات التي يتعيّن أن تعمل عليها بروتوكولات طبقة ربط البيانات. فوصلة نقطة إلى نقطة مثلاً وصلة بسيطة لها مُرسِل واحد ومُستقبِل واحد يتصلان عبر "سلك" واحد. أما وصلة الوصول المتعدد فمشتركة بين العديد من المُرسِلين والمُستقبِلين. لذلك فإن طبقة ربط البيانات لقناة وصول متعدد لها بروتوكول (هو بروتوكول الوصول المتعدد) لتنسيق الوصول للوصلة بين عدة مستخدمين. في حالة شبكات ATM وMPLS يمكن في الواقع أن تكون الوصلة التي تصل بين عقدتين متجاورتين (على سبيل المثال موجّهي IP متجاورين من منظور IP، أى يفصل بينهما قفزة واحدة على المسار نحو وجهةٍ ما) شبكة في حد ذاتها. من وجهة نظر معينة ينبغي ألاّ تبدو فكرة اعتبار الشبكة كوصلة فكرة مستغربة. فعلى سبيل المثال خطّ الهاتف الذي يوصل مودم بحاسب بيتي إلى مودم بموجّه بعيد هو في الحقيقة مسار عبر شبكة هاتف متطوّرة ومعقّدة.

تناولنا بعض المبادئ التي ينبني عليها الاتصال عبر طبقة ربط البيانات، ومنها: أساليب اكتشاف وتصحيح أخطاء البيانات، وبروتوكولات الوصول المتعدد، وعنونة طبقة ربط البيانات، وبناء شبكات بيانات محلية ممتدة باستخدام المجمِّعات والمحوّلات. أما فيما يتعلق باكتشاف وتصحيح الأخطاء، فقد رأينا كيف أن إلحاق بتات إضافية بترويسة إطار البيانات تمكننا من اكتشاف ـ وفي بعض الحالات تصحيح ـ أخطاء البتات التي قد تطرأ على الإطار أثناء انتقاله على الوصلة. كما غطّينا الأساليب البسيطة التي تستخدم بتات التكافؤ والمجموع التدقيقي، بالإضافة إلى أسلوب فحص الفائض الدوري الأكثر متانة. وانتقلنا بعد ذلك إلى موضوع بروتوكولات الوصول المتعدد، حيث درسنا ثلاثة طرق رئيسة لتنسيق الوصول إلى قناة إذاعة مشتركة: تقسيم القناة (مثل TDM و FDM)، والوصول العشوائي (مثل بروتوكولات ALOHA وبروتوكولات CSMA)، وأساليب التناوب على القناة (كأساليب الاستفتاء وتمرير العلامة). رأينا أنه نتيجة لجعل عدة عقد تشترك في قناة إذاعة واحدة، ظهرت الحاجة لعناوين العقد في طبقة ربط البيانات. كما عرفنا كيف أن العناوين المادية تختلف كثيراً عن عناوين طبقة الشبكة،

وأنه في حالة الإنترنت يُستخدم بروتوكول خاص (بروتوكول تحويل العناوين ARP) للترجمة بين هذين النوعين من العناوين. تناولنا بعد ذلك كيف تشكّل العقد التي تشترك في قناة إذاعة شبكة محلية، وكيف يمكن توصيل عدد من تلك الشبكات المحلية لتكوين شبكات محلية أكبر، كل ذلك بدون اللجوء إلى استخدام بروتوكولات التوجيه في طبقة الشبكة لتشبيك تلك العقد المحلية.

غطّينا أيضاً عدداً من البروتوكولات المحددة لطبقة ربط البيانات بالتفصيل، كبروتوكول الإيثرنت وبروتوكول PPP. ثم أنهينا دراستنا لطبقة ربط البيانات بالتركيز على كيفية قيام شبكات ATM وMPLS بخدمات طبقة ربط البيانات عند تشبيك موجّهات IP.

وبعد أن انتهينا من تغطية طبقة ربط البيانات تكون رحلتنا عبر رصة البروتوكولات قد انتهت! بالتأكيد تحت طبقة ربط البيانات توجد الطبقة المادية، ولكننا نرى أنه من الأفضل ترك تفاصيل الطبقة المادية لمقرر دراسي آخر (مثلاً في نظرية الاتصالات بدلاً من شبكات الحاسب). علماً بأننا مع ذلك قد لمسنا عدداً من جوانب الطبقة المادية في هذا الفصل (كمناقشتنا القصيرة لتشفير مانشستر في الجزء 5-5) وفي الفصل الأول (كمناقشتنا لأوساط النقل المادية في الجزء 1-2). سنأخذ الطبقة المادية بعين الاعتبار مرةً أخرى عند دراستنا لخصائص وصلة اللاسلكي في الفصل القادم.

وبالرغم من أن رحلتنا عبر رصة البروتوكولات قد انتهت، إلا أن دراستنا لشبكات الحاسب لم تنتهِ بعد. في الفصول الأربعة التالية سنغطّي الشبكات اللاسلكية، وشبكات الوسائط المتعددة، وأمن الشبكات، وإدارة الشبكات. لا ينضوي أيٌّ من هذه المواضيع الأربعة تحت طبقة واحدة. ففي الواقع يتوزع كل موضوع منها على عدة طبقات. لذلك فإن فهم تلك المواضيع (والتي وُصفت بكونها "مواضيع متقدّمة" في بعض كتب الشبكات) يتطلّب أساساً متيناً في كل طبقات رصة البروتوكولات ـ وهي المهمة التي قد انتهينا منها الآن عندما أكملنا دراستنا لطبقة ربط البيانات!

أسئلة وتمارين وتدريبات الفصل الخامس

❖ أسئلة مراجعة

- **الأجزاء 5-1 و 5-2**

1. لو أن كل الوصلات في الإنترنت وفّرت خدمة نقل موثوقة للبيانات، هل يعني ذلك أنه لن يكون هناك داعٍ لاستخدام خدمة TCP للنقل الموثوق؟ علل إجابتك.
2. اذكر بعض الخدمات التي يمكن لبروتوكول طبقة ربط البيانات توفيرها لطبقة الشبكة؟ أيٌّ من تلك الخدمات له نظير في بروتوكول IP؟ وبروتوكول TCP؟

- **الجزء 5-3**

3. افترض أن عقدتين تبدآن في إرسال رزمة طولها L بتاً في نفس الوقت على قناة إذاعة بمعدل R بت/ثانية. ليكن d_{prop} هو تأخير الانتقال بين العقدتين. هل سيحدث اصطدام لو كان $d_{prop} < L/R$؟ علل إجابتك.
4. في الجزء 5-3، ذكرنا أربع خواص مطلوبة في قناة الإذاعة. أي تلك الخواص تتوفر في بروتوكول ألوها الشرائحي؟ أي تلك الخواص تتوفر في بروتوكول تمرير العلامة؟
5. صف بروتوكولي الاستطلاع وتمرير العلامة مع التشبيه بتفاعل الناس في حفل.
6. لماذا يعاني بروتوكول تمرير العلامة من اتخفاض في كفاءته إذا كانت الشبكة المحلية تغطي منطقة جغرافية كبيرة؟

- **الجزء 5-4**

7. ماحجم حيز عنوان الماك؟، وعنوان IPv4؟، وعنوان IPv6؟
8. افترض أن كلاً من العقد A وB وC موصّلة بنفس شبكة إذاعة محلية (LAN) عن طريق موائم الشبكة الخاص بها. إذا أرسلت A الآلاف من قطع بيانات IP إلى B يتضمن كل إطار من الإطارات التي تغلف تلك القطع عنوان الماك الخاص بالعقدة . هل سيمرر موائم الشبكة الخاص بالعقدة C قطع بيانات IP ضمن تلك الإطارات إلى العقدة C؟ كيف ستتغير إجابتك إذا كانت A ترسل تلك الإطارات على عنوان الماك المخصص للإذاعة؟

9. لماذا يُرسل استفسار ARP ضمن إطار إذاعة؟ لماذا تُرسل إجابة ARP ضمن إطار يحمل عنوان الماك لوجهة محددة؟
10. للشبكة المبينة في الشكل 5-19، يتضمن الموجّه وحدتي ARP، لكلٍّ منهما جدول ARP الخاص بها. هل يمكن أن يظهر عنوان الماك نفسه في كلا الجدولين؟

- **الجزء 5-5**

11. قارن بين صيغة إطار الإيثرنت في كلٍّ من 10BASE-T و 100BASE-T والإيثرنت بسرعة جيجابت/ثانية.
12. في بروتوكول CSMA/CD، بعد خامس اصطدام، ماهو احتمال أن تختار عقدة $K = 4$؟ ماهو التأخير بالثانية المناظر لتلك القيمة لـ K على إيثرنت سرعتها 10 ميجابت/ثانية؟

- **الجزء 5-6**

13. بالرجوع إلى الشكل 5-26، كم عدد الشبكات الفرعية الموجودة، آخذاً في الاعتبار طريقة العنونة الواردة في الجزء 4-4؟

❖ تدريبات

1. افترض أن محتوى المعلومات في رزمة ما هو 1010101010101011 وأن نظام تكافؤ زوجي يجري استخدامه. ماهي قيمة الحقل الذي يتضمن بتات التكافؤ في حالة اتباع نظام في بعدين؟. يجب أن تكون إجابتك بحيث يُستخدم حقل المجموع التدقيقي بأقل طول ممكن.
2. بيّن (مستخدماً مثالاً غير المثال الموضح في الشكل 5-6) أن فحص التكافؤ ببعدين يمكن أن يكتشف ويصحح خطأ في بت واحد. بيّن مع التمثيل أن خطأ في بتّين سيمكن اكتشافه ولكن لن يمكن تصحيحه.
3. افترض أن جزء المعلومات في رزمة (D في الشكل 5-4) يضم 10 بايتات تمثل القيمة الثنائية للأعداد الصحيحة من 0 إلى 9. احسب المجموع التدقيقي للإنترنت لتلك البيانات.
4. خذ في الاعتبار التمرين السابق، ولكن بدلاً من احتواء البيانات على القيمة الثنائية للأعداد الصحيحة من 0 إلى 9، افترض أن البايتات العشرة تتضمن:

a. القيم الثنائية للأعداد من 1 إلى 10.
b. تمثيل الحروف الكبيرة من A إلى J بصيغة ASCII.
c. تمثيل الحروف الصغيرة من a إلى j بصيغة ASCII.

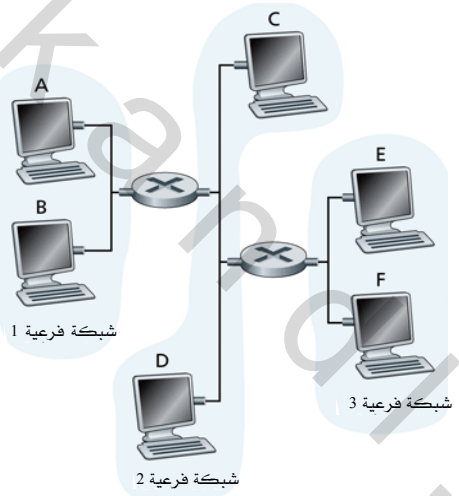
احسب المجموع التدقيقي للإنترنت لتلك البيانات.

5. خذ في الاعتبار المولد G من أربعة بتات والمبين في الشكل 5-8. بافتراض أن قيمة D هي 10101010، ما هي قيمة R؟
6. خذ في الاعتبار التمرين السابق، ولكن مع افتراض أن D لها القيمة:
   a. 10010001.
   b. 10100011.
   c. 01010101.
7. في الجزء 5-3 استعرضنا طريقة اشتقاق تعبير رياضي لكفاءة بروتوكول ألوها الشرائحي. في هذا التمرين سنكمل الاشتقاق.
   a. تذكّر أنه في وجود N عقدة نشطة، تكون كفاءة بروتوكول ألوها الشرائحي هي $Np(1-p)^{N-1}$. أوجد قيمة p التي تجعل قيمة هذا التعبير الرياضي نهاية عظمى.
   b. باستخدام قيمة p التي حصلتَ عليها في الجزء (a) أعلاه من هذا السؤال، أوجد كفاءة بروتوكول ألوها الشرائحي بجعل N تقارب مالانهاية. ملاحظة: $(1-1/N)^N$ تقارب $(1/e)$ عندما تقارب N ما لانهاية.
8. بيّن أن الكفاءة القصوى لبروتوكول ألوها الأصلي هي $(1/2e)$. ملاحظة: هذا التمرين سهل إذا كنت قد أكملت التمرين السابق!
9. افترض أن العقد الثلاث A وB وC تتنافس فيما بينها للوصول إلى قناة باستخدام بروتوكول ألوها الشرائحي. افترض أن كل عقدة لديها عدد لا نهائي من الرزم تود إرسالها. تحاول كل عقدة الإرسال في كل شريحة زمنية بالاحتمال p. يطلق على الشريحة الأولى شريحة 1، والثانية شريحة 2، وهكذا.
   a. ما هو احتمال نجاح العقدة A في الإرسال في أول محاولة في الشريحة 4؟
   b. ما هو احتمال نجاح العقدة أي عقدة (A أو B أو C) في الإرسال في الشريحة 2؟
   c. ما هو احتمال حدوث أول نجاح في الشريحة 4؟
   d. ماهي كفاءة هذا النظام الذي يضم ثلاث عقد؟
10. مثّل بالرسم كفاءة بروتوكول ألوها الشرائحي وبروتوكول ألوها الأصلي كدالة في p للقيم التالية لعدد العقد النشطة N في الحالات التالية:
    a. $N = 10$
    b. $N = 25$

c. $N = 50$

11. خذ في الاعتبار قناة إذاعة عليها N عقدة ولها معدل إرسال R بت/ثانية. افترض أن قناة الإذاعة تستخدم أسلوب الاستطلاع (بإضافة عقدة استطلاع خاصة) لتنظيم الوصول المتعدد. افترض أن الفترة الزمنية من انتهاء عقدة من الإرسال إلى السماح للعقدة التالية بالإرسال (أي تأخير الاستطلاع) هي d_{poll}. افترض أنه أثناء دورة استطلاع يتم السماح لعقدة بإرسال Q بتاً كحد أقصى. ما هي طاقة الإرسال الإنتاجية القصوى لقناة الإذاعة تلك؟

12. خذ في الاعتبار الشبكات المحلية الثلاث الموصّلة فيما بينها عن طريق موجّهين، كما هو مبين في الشكل 5-38.



الشكل 5-38 ثلاث شبكات فرعية موصّلة فيما بينها عن طريق موجّهين.

a. أعد رسم الشكل بحيث يتضمن موائمات الشبكة
b. عيّن عناوين IP لكل الواجهات. استخدم عناوين بالصيغة 111.111.111.xxx للشبكة الفرعية 1، و عناوين بالصيغة 122.222.222.xxx للشبكة الفرعية 2، و عناوين بالصيغة 133.333.333.xxx للشبكة الفرعية 3.
c. عيّن عناوين الماك لكل الواجهات.

d. خذ في الاعتبار إرسال قطعة بيانات IP من المضيف A إلى المضيف F. افترض أن كل جداول ARP محدّثة تماماً. اذكر جميع الخطوات اللازمة على نسق ما قمنا به في حالة موجّه واحد في الجزء 5-4-2.

e. كرر الجزء د أعلاه مع افتراض أن جدول ARP للمضيف المرسِل فارغ بينما جداول ARP الأخرى محدّثة تماماً.

13. خذ في الاعتبار التمرين السابق، ولكن افترض أن الموجّه بين الشبكة الفرعية 2 والشبكة الفرعية 3 قد تم استبداله بمحوّل. قم بالإجابة على الأسئلة a إلى e في التمرين السابق في هذا السياق الجديد.

14. تذكّر أنه في بروتوكول الوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام CSMA/CD ينتظر موائم الشبكة لمدة $K \times 512$ فترة بت بعد كل اصطدام، حيث K رقم يتم سحبه عشوائياً. في حالة $K = 100$، ماهي المدة التي ينتظرها الموائم قبل العودة للخطوة 2 (انظر البروتوكول) وذلك في حالة إيثرنت سرعتها 10 ميجابت/ثانية؟، وكذلك في حالة إيثرنت سرعتها 100 ميجابت/ثانية؟

15. افترض أن العقدتين A وB تقعان على نفس ناقل الإيثرنت بسرعة 10 ميجابت/ثانية، وأن تأخير الانتقال بين العقدتين هو 225 فترة بت. افترض أن العقدة A تبدأ بإرسال إطار، وقبل أن تنتهي بدأت العقدة B في إرسال إطار. هل يمكن للعقدة أ الانتهاء من إرسال إطارها قبل اكتشاف أن ب أخذت في الإرسال؟ علل إجابتك. إذا كانت الإجابة بنعم، فستظن أ مخطئةً أنها قد أرسلت إطارها بدون مشاكل. ملاحظة: افترض أنه عند الوقت t = صفر فترة بت، تبدأ A في إرسال إطار. في أسوأ الاحتمالات ترسل A إطاراً له أقل طول وقدره 512+64 فترة بت. وعليه ينبغي أن تنهي A إرسالها في اللحظة 512+64 فترة بت. ومن ثم فالإجابة تكون لا إذا وصلت إشارة B إلى A قبل الوقت 512+64 فترة بت. في أسوأ الاحتمالات، متى تصل إشارة B إلى A؟

16. افترض أن العقدتين A وB تقعان على نفس ناقل الإيثرنت بسرعة 10 ميجابت/ثانية، وأن تأخير الانتقال بين العقدتين هو 225 فترة بت. افترض أن كلاً من العقدتين A وB تبدآن بإرسال إطار في نفس الوقت، ويصطدم الإطاران، وتختار كلٌّ من العقدتين قيمة مختلفة لـ K في خوارزمية بروتوكول الوصول المتعدد بالإنصات للناقل مع اكتشاف الاصطدام CSMA/CD . افترض أنه لاتوجد عقد نشطة أخرى، هل يمكن أن يصطدم الإرسالان المعادان من A و B؟ يكفينا هنا أخذ هذا المثال بعين الاعتبار: افترض أن A وB يبدآن الإرسال عند الوقت t = صفر فترة بت. سيكتشف كلٌّ منهما حدوث اصطدام عند t = 225 فترة بت، وسينتهيا من إرسال إشارة التشويش عند t = 225+ 48 = 273 فترة بت. افترض أن $K_A = 0$ و$K_B = 1$. في أي وقت ستُجدول العقدة B لإرسالها

المعاد؟ في أي وقت ستبدأ A الإرسال؟ (ملاحظة: ينبغي على العقدتين الانتظار إلى أن تصبح القناة خالية بعد العودة إلى الخطوة 2 – انظر البروتوكول). في أي وقت تصل إشارة A إلى B؟ هل ستُحجم B عن الإرسال في وقت الإرسال الذي جدولته؟

17. خذ في الاعتبار إيثرنت 100BASE-T سرعتها 100 ميجابت/ثانية، حيث كل العقد عليها موصّلة إلى مجمِّع (hub). للحصول على كفاءة مقدارها 0.50، كم ينبغي أن تكون المسافة القصوى بين أيٍّ من العقد والمجمِّع ؟ افترض إطاراً طوله 64 بايتاً ولا توجد مكرِّرات. هل تضمن تلك المسافة القصوى أيضاً أن العقدة المرسِلة A يتسنى لها اكتشاف ما إذا كان هناك عقدة تقوم بالإرسال بينما A ترسل؟ علل إجابتك. كيف تبدو المسافة القصوى التي حسبتَها مقارنةً بتلك المسافة التي يحددها معيار 100 ميجابت/ثانية فعلاً.

18. في هذا التمرين سوف نشتق تعبيراً رياضياً لكفاءة بروتوكول للوصول المتعدد يشبه بروتوكول CSMA/CD. في ذلك البروتوكول يُقسّم الوقت إلى شرائح ويتم تزامن كل موائمات الشبكة مع الشرائح. غير أنه بخلاف بروتوكول ألوها الشرائحي، يكون طول الشريحة هنا أقل بكثير من زمن الإطار (أي الزمن اللازم لإرسال إطار). دع S تمثل طول فترة الشريحة. افترض أن كل الإطارات لها طول ثابت وقدره $L = kRS$، حيث R هو معدل الإرسال على القناة و k رقم صحيح كبير. افترض أن هناك N عقدة، لدى كلٍّ منها عدد لانهائي من الإطارات تود إرسالها. سنفترض أيضاً أن $S > d_{\text{prop}}$، بحيث تتمكّن كل العقد من اكتشاف وجود اصطدام قبل نهاية مدة الإطار. يمكن وصف البروتوكول كالتالي:

- في كل شريحة، إذا لم تكن هناك عقدة تستحوذ على القناة، تقوم كل العقد بمحاولة استخدام القناة للإرسال، وتقوم كل عقدة بالإرسال أثناء الشريحة باحتمال p. إذا قامت عقدة واحدة بالضبط بالإرسال في تلك الشريحة فإنها تستحوذ على القناة طوال الشرائح الـ (k-1) التالية لكي ترسل إطارها بأكمله.
- إذا كانت هناك عقدة تستحوذ على القناة، فستُحجم كل العقد عن الإرسال إلى أن تنتهي العقدة التي تستحوذ على القناة من إرسال إطارها. بمجرد إرسال تلك القناة لإطارها، تقوم كل العقد بمحاولة استخدام القناة للإرسال.

لاحظ أن القناة تراوح مابين حالتين: الحالة المنتجة، والتي تستمر لمدة k شريحة بالضبط، والحالة غير المنتجة، والتي تستمر لعدد عشوائي من الشرائح. واضح أن

كفاءة القناة هي النسبة $k/(k+x)$، حيث x هو العدد المتوقع للشرائح المتتابعة غير المنتجة.

a. لقيم ثابتة لـ N و p، أوجد كفاءة هذا البروتوكول.
b. لقيمة ثابتة لـ N، أوجد قيمة p التي تحقق الحد الأقصى للكفاءة.
c. مستخدماً قيمة p التي حصلت عليها في الخطوة (b) أعلاه (والتي هي دالة في N)، أوجد قيمة الكفاءة عندما تقارب N مالانهاية.
d. اثبت أن الكفاءة تقارب 1 عندما يصبح طول الإطار كبيراً.

19. افترض أن عقدتين A وB موصلتان على طرفي كبل طوله 900 متر وأنه لدى كلٍّ منها إطار طوله 1000 بت (بما في ذلك كل التراويس والديباجات) تريد إرساله إلى الأخرى. تحاول كلا العقدتين الإرسال عند $t = 0$. افترض وجود 4 مكرّرات بين A وB يتسبب كلٌّ منها في تأخير يكافىء 20 بتاً. افترض أن معدل الإرسال هو 10 ميجابت/ثانية وأننا نستخدم بروتوكول CSMA/CD بفترة تراجع قدرها 512 بتاً. بعد أول تصادم، تسحب A القيمة $K = 0$ بينما تسحب ب القيمة $K = 1$ تبعاً لبروتوكول التراجع الأسي. اهمل إشارة التشويش والتأخير لفترة 96 بتاً.
a. ما هو تأخير الانتقال في اتجاه واحد بالثانية بين العقدتين A وB (بما في ذلك التأخير في المكرّرات).
b. في أي وقت (بالثانية) يتم تسليم الرزمة بأكملها من A إلى B؟
c. افترض الآن أن A فقط لديها رزمة للإرسال وأن المكرّرات تم استبدالها بمحوّلات. افترض أن كل محول يتضمن تأخير معالجة قدره 20 بتاً بالإضافة إلى تأخير للتخزين والإرسال. في أي وقت (بالثانية) في هذه الحالة يتم تسليم الرزمة من A إلى B؟

20. خذ في الاعتبار الشكل 5-38 في تمرين 12. عيّن عناوين الماك وعناوين IP للواجهات على المضيف A، وكلا الموجّهين، والمضيف F. افترض أن المضيف A يرسل وحدة بيانات IP إلى المضيف F. أوجد عناوين ماك للمصدر والوجهة في الإطار الذي يغلف وحدة بيانات IP تلك عند: 1. إرسال الإطار من A إلى الموجّه على اليسار. 2. إرسال الإطار من الموجّه على اليسار إلى الموجّه على اليمين. 3. إرسال الإطار من الموجّه على اليمين إلى المضيف F. أوجد أيضاً عناوين IP للمصدر والوجهة في وحدة بيانات IP التي يغلفها ذلك الإطار في كل جزء من الأجزاء الثلاثة أعلاه من الرحلة.

21. افترض الآن أننا استبدلنا الموجّه على أقصى اليسار في الشكل 5-38 بمحوّل ووُصلت به كلٌّ من المضيفات A, B, C, D وكذلك الموجّه الأيمن على شكل نجمة. أوجد عناوين

ماك للمصدر والوجهة في الإطار الذي يغلف وحدة بيانات IP عند: 1. إرسال الإطار من A إلى الموجّه على اليسار. 2. إرسال الإطار من الموجّه على اليسار إلى الموجّه على اليمين. 3. إرسال الإطار من الموجّه على اليمين إلى المضيف F. أوجد أيضاً عناوين IP للمصدر والوجهة في وحدة بيانات IP التي يغلفها ذلك الإطار في كل جزء من الأجزاء الثلاثة أعلاه من الرحلة.

22. خذ في الاعتبار الشكل 5-26. افترض أن كل الوصلات تعمل بمعدل إرسال قدره 100 ميجابت/ثانية. ماهي الطاقة الإنتاجية الكلية للإرسال التي يمكن تحصيلها بين الأنظمة الطرفية الأربعة عشر في تلك الشبكة؟ ولماذا؟

23. افترض أن مفاتيح الأقسام الثلاثة في الشكل 5-26 تم استبدالها بمجمِّعات. كل الوصلات تعمل بمعدل إرسال قدره 100 ميجابت/ثانية. ماهي الطاقة الإنتاجية الكلية للإرسال التي يمكن تحصيلها بين الأنظمة الطرفية الأربعة عشر في تلك الشبكة؟ ولماذا؟

24. افترض أن كل المفاتيح في الشكل 5-26 تم استبدالها بمجمِّعات. كل الوصلات تعمل بمعدل إرسال قدره 100 ميجابت/ثانية. ماهي الطاقة الإنتاجية الكلية للإرسال التي يمكن تحصيلها بين الأنظمة الطرفية الأربعة عشر في تلك الشبكة؟ ولماذا؟

25. لنأخذ في الاعتبار طريقة عمل المحوّل المتعلم في سياق الشكل 5-24. افترض أن: (1) A ترسل إطاراً إلى D، (2) D ترد على A بإرسال إطار، (3) C ترسل إطاراً إلى D، (4) D ترد على C بإرسال إطار. افترض أن جدول المحوّل يكون خالياً في البداية. بيّن حالة جدول المحول قبل وبعد كلٍّ من تلك الخطوات الأربعة. لكل خطوة قم بتحديد الوصلات التي سيتم تمرير الإطار المرسل عليها، وعلل إجابتك باختصار.

26. تذكّر أن شبكات ATM تستخدم رزماً طولها 53 بايتاً تتألف من ترويسة طولها 5 بايتات وحمل آجر طوله 48 بايتاً. تعتبر 53 بايتاً قليلة بشكلٍ ملحوظ للرزم ثابتة الطول؛ فمعظم بروتوكولات الشبكات (مثل بروتوكول الإنترنت، والإيثرنت، وترحيل الإطارات، إلخ) تستخدم في المتوسط أطوالاً أكبر بكثير. أحد عيوب استخدام طول صغير للرزمة هو ضياع جزء كبير من سعة الإرسال (الحيز الترددي) للوصلة في إرسال بايتات العبء الإضافي؛ ففي هذه الحالة "تُهدر" 10٪ تقريباً من سعة الإرسال في إرسال ترويسة ATM. في هذا التمرين سنبحث في السبب وراء اختيار مثل هذا الطول القصير للرزمة. لهذا الغرض، افترض أن خلية ATM تتألف من L بايتاً (قد تختلف عن 48 بايتاً) وترويسة طولها 5 بايتات.

a. خذ في الاعتبار إرسال بيانات رقمية مكوّدة من مصدر صوت مباشرة على ATM. افترض أن المصدر يتم تكويده بمعدل 64 كيلوبت/ثانية. افترض أن كل خلية يتم ملؤها تماماً قبل أن يقوم المصدر بإرسالها إلى الشبكة. إن الوقت اللازم لملء الخلية هو تأخير الترزيم. احصل على تعبير رياضي لتأخير الترزيم (بالميللي ثانية) بدلالة L.

b. إذا زاد تأخير الترزيم عن 20 ميللي ثانية فقد يتسبب في حدوث صدى ملحوظ ومزعج. احسب تأخير الترزيم لـ $L = 1500$ (أي ما يناظر تقريباً أقصى طول ممكن لرزم الإيثرنت) وكذلك $L = 48$ (أي خلية ATM).

c. احسب تأخير "التخزين والإرسال" عند مفتاح ATM لوصلة معدل إرسالها R قيمته 155 ميجابت/ثانية (وتلك سرعة وصلة مفضلة في شبكات ATM) لكلٍّ من $L = 1500$ و$L = 48$.

d. علّق على ميزات استخدام خلية قصيرة.

27. خذ في الاعتبار شبكة MPLS المبينة في الشكل 5-37، وافترض أن الموجّهين R5 و R6 مزوّدان بإمكانيات للتعامل مع MPLS. افترض أننا نود استخدام هندسة حركة المرور بحيث يتم تحويل الرزم الخارجة من R6 قاصدةً A إلى A عبر R6-R4-R3-R1، وتحويل الرزم الصادرة من R5 قاصدةً A إلى A عبر R5-R4-R2-R1. وضّح جداول MPLS الموجودة في الموجّهين R5 و R6، وكذلك الجدول المعدّل في R4، واللازمة لتحقيق ذلك.

28. خذ في الاعتبار مرة أخرى نفس السيناريو في التمرين السابق، ولكن افترض أن الرزم الخارجة من R6 قاصدةً D يتم تحويلها عبر R6-R4-R3 ، بينما الرزم من R5 قاصدةً D يتم تحويلها عبر R4-R2-R1-R3. وضّح جداول MPLS الموجودة في كل الموجّهات واللازمة لتحقيق ذلك.

❖ أسئلة مناقشة

نحثك على تصفح الإنترنت بحثاً عن إجابات للأسئلة التالية:

1. ماهو المدى التقريبي لسعر: موائم شبكة إيثرنت بسرعة 10/100 ميجابت/ثانية؟ موائم شبكة جيجابت إيثرنت؟. قارن هذه الأسعار بأسعار مودم هاتف بسرعة 56 كيلوبت/ثانية؟ أو بمودم ADSL؟

2. يتم تسعير المحوّل عادةً بناءً على عدد الواجهات التي يتضمنها (والتي تُعرف بالمنافذ في مصطلحات شبكة الإيثرنت). ما هو مدى السعر التقريبي لكل واجهة لمحوّل يتضمن فقط واجهات بسرعة 100 ميجابت/ثانية.

3. يمكن القيام بالعديد من مهام موائم الشبكة بواسطة برامجيات تعمل على المعالج المركزي للعقدة. ماهي مزايا وعيوب نقل تلك المهام من موائم الشبكة إلى العقدة؟
4. ابحث في الويب عن أرقام البروتوكولات المستخدمة في إطار إيثرنت لوحدة بيانات IP و رزمة ARP.
5. اقرأ المراجع [Xiao 2000; Huang 2002; RFC 3346] حول هندسة حركة مرور البيانات باستخدام MPLS. اسرد أهداف هندسة حركة مرور البيانات. أيٌّ من هذه الأهداف يمكن تحقيقه فقط باستخدام MPLS وأيّها يمكن تحقيقه ببروتوكولات أخرى موجودة غير MPLS؟ في الحالة الثانية، ما هي المزايا التي يوفرها استخدام MPLS؟

❖ مختبر إيثريل

ستجد على موقع الويب المصاحب لهذا الكتاب (http://www.aw1.com/kurose-ross) مختبر إيثيريل لاستكشاف طريقة عمل بروتوكول IEEE 802.3 وصيغة إطار الإيثرنت.

[**3Com 2007**] 3Com Corporation, "White paper: Understanding IP addressing: Everything you ever wanted to know," http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf

[**3GPP 2007**] Third Generation Partnership Project, http://www.3gpp.org/

[**802.11 Security 2007**] The Unofficial 802.11 Security Web Page, http://www.drizzle.com/~aboba/IEEE/

[**Abitz 1993**] P. Albitz and C. Liu, *DNS and BIND,* O'Reilly & Associates, Petaluma, CA, 1993.

[**Abramson 1970**] N. Abramson, "The Aloha System—Another Alternative for Computer Communications," *Proceedings of Fall Joint Computer Conference, AFIPS Conference,* p. 37, 1970.

[**Abramson 1985**] N. Abramson, "Development of the Alohanet," *IEEE Transactions on Information Theory,* Vol. IT-31, No. 3 (Mar. 1985), pp. 119–123.

[**Adler 2002**] M. Adler, "Tradeoffs in Probabilistic Packet Marking for IP Traceback*," Proceedings of 34th ACM Symposium on Theory of Computing (STOC)*, May 2002. http://www.cs.umass.edu/~micah/pubs/traceback.ps

[**Adya 2004**] A. Adya, W. J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J. R. Douceur, J. Howell, J. R. Lorch, M. Theimer, R. P. Wattenhofer, "FARSITE: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment." *Proceedings of the 5th OSDI*, December 2002. http://research.microsoft.com/~adya/pubs/osdi2002.pdf

[**Ahn 1995**] J. S. Ahn, P. B. Danzig, Z. Liu, and Y. Yan, "Experience with TCP Vegas: Emulation and Experiment," *Proceedings of ACM SIGCOMM '95* (Boston, MA, Aug. 1995), pp. 185–195. http://www.acm.org/sigcomm/sigcomm95/papers/ahn.html

[**Akamai 2007**] Akamai homepage, http://www.akamai.com

[**Akella 2003**] A. Akela, S. Seshan, A. Shaikh, "An Empirical Evaluation of Wide-Area Internet Bottlenecks," *Proc. 2003 ACM Internet Measurement Conf.* (Miami FL, Nov. 2003).

[**Alvestrand 1997**] H. Alvestrand, "Object Identifier Registry," http://www.alvestrand.no/harald/objectid/top.html.

[**Anderson 1995**] J. B. Andersen, T. S. Rappaport, S. Yoshida, "Propagation Measurements and Models for Wireless Communications Channels," *IEEE Communications Magazine*, (Jan. 1995), pp. 42-49.

[**Appenzeller 2004**] G. Appenzeller, I. Kelassy, N. McKeown, "Sizing Router Buffers," *Proc. 2004 ACM SIGCOMM* (Portlan, OR, Aug. 2004).

[**Aprisma 2007**] Aprisma homepage, http://www.aprisma.com/

[**ARIN 1996**] ARIN, "IP allocation report," ftp://rs.arin.net/netinfo/ip_network_allocations

[**Ash 1998**] G. R. Ash, *Dynamic Routing in Telecommunications Networks,* McGraw Hill, NY, NY, 1998.

[**ASO-ICANN 2007**] The Address Supporting Organization home page, http://www.aso.icann.org

[**AT&T SLM 2006**] AT&T Business, "AT&T Enterprise Hosting Services Service Guide," http://www.att.com/abs/serviceguide/docs/eh_sg.pdf

[**Atheros 2006**] Atheros Communications Inc. "Atheros AR5006 WLAN Chipset Product Bulletins," http://www.atheros.com/pt/AR5006Bulletins.htm

[**ATM Forum 2007**] The ATM Forum Web site, http://www.atmforum.com/

[**Ayanoglu 1995**] E. Ayanoglu, S. Paul, T. F. La Porta, K. K. Sabnani, R. D. Gitlin, "AIR-MAIL: A Link-Layer Protocol for Wireless Networks," *ACM ACM/Baltzer Wireless Networks Journal*, 1: 47–60, February 1995. http://www.bell-labs.com/user/sanjoy/airmail.ps.Z

[**Bakre 1995**] A. Bakre, B. R. Badrinath, "I-TCP: Indirect TCP for Mobile Hosts," *Proceedings of the 15th International Conf. on Distributed Computing Systems (ICDCS)*, May 1995, pp. 136–143. ftp://paul.rutgers.edu/pub/badri/itcp-tr314.ps.Z

[**Balakrishnan 1995**] H. Balakrishnan, S. Seshan, R. H. Katz, "Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks," *ACM Wireless Networks*, 1, no. 4 (December 1995). http://nms.lcs.mit.edu/~hari/papers/winet.ps

[**Balakrishnan 1997**] H. Balakrishnan, V. Padmanabhan, S. Seshan, R. Katz, "A Comparison of Mechanisms for Improving TCP Performance over Wireless Links," *IEEE/ACM Transactions on Networking* 5, no. 6 (December 1997). http://nms.lcs.mit.edu/~hari/papers/ton.ps

[**Baptista 2003**] A. Baptista, T. Leen, Y. Zhang, A. Chawla, D. Maier, W. Feng, W. Feng, J. Walpole, C. Silva, J. Freire, "Environmental Observation and Forecasting Systems: Vision, Challenges and Successes of a Prototype," *Encyclopedia of Physical Science and Technology* (R. A. Meyers, Ed.), Academic Press, Third Edition, Vol. 5., pp 565-581.

[**Baran 1964**] P. Baran, "On Distributed Communication Networks," *IEEE Transactions on Communication Systems,* Mar. 1964. Rand Corporation Technical report with the same title (Memorandum RM-3420-PR, 1964). http://www.rand.org/publications/RM/RM3420/

[**Bardwell 2007**] J. Bardwell, "You Believe You Understand What You Think I Said … The Truth About 802.11 Signal And Noise Metrics: A Discussion Cclasifying Often-Misused 802.11 WLAN Terminologies," http://madwifi.org/attachment/wiki/UserDocs/RSSI/you_believe_D100201.pdf?format=raw

[**Baset 2006**] S. A. Baset and H. Schulzrinne, "An analysis of the Skype peer-to-peer Internet Telephony Protocol," *Proc. 2006 IEEE Infocom* (Barcelona, Spain, Apr. 2006).

[**BBC 2001**] BBC news online "A Small Slice of Design," April 2001, http://news.bbc.co.uk/1/low/sci/tech/1264205.stm

[**BBC Multicast 2007**] BBC, "BBC Multicast Trial," http://support.bbc.co.uk/multicast

[**Bender 2000**] P. Bender, P. Black, M. Grob, R. Padovai, N. Sindhushayana, A. Viterbi, "CDMA/HDR: A bandwidth-efficient high-speed wireless data service for nomadic users," *IEEE Commun. Mag.*, Vol. 38, No. 7 (July 200) pp. 70-77.

[**Berners-Lee 1989**] T. Berners-Lee, CERN, "Information Management: A Proposal," Mar. 1989, May 1990. http://www.w3.org/History/1989/proposal.html

[**Berners-Lee 1994**] T. Berners-Lee, R. Cailliau, A. Luotonen, H. Frystyk Nielsen, and A.Secret, "The World-Wide Web," *Communications of the ACM,* Vol. 37, No. 8 (Aug. 1994), Pages 76–82

[**Bernstein 2007**] D. Bernstein, "SYN Cookies," http://cr.yp.to/syncookies.html

[**Bertsekas 1991**] D. Bertsekas and R. Gallagher, *Data Networks, 2nd Ed.,* Prentice Hall, Englewood Cliffs, NJ, 1991.

[**Bhagwat 2003**] P. Bhagwat, B. Raman, D. Sanghi, "Turning 802.11 Inside Out," *Proceedings of the 2003 ACM Hotnets II Workshop*, Cambridge, MA (November 2003). http://nms.lcs.mit.edu/HotNets-II/papers/inside-out.pdf

[**Bhimani 1996**] Anish Bhimani: "Securing the Commercial Internet," *Communications of the ACM,* Vol. 39 No. 6: 29–35; March 1996

[**Biddle 2003**] P. Biddle, P. England, M. Peinado, B. Willman, "The Darknet and the Future of Content Distribution." 2002 ACM Workshop on Digital Rights Management, (Nov. 2002, Washington, D.C.) http://crypto.stanford.edu/DRM2002/darknet5.doc

[**Biersack 1992**] E. W. Biersack, "Performance evaluation of forward error correction in ATM networks," *Proceedings of ACM SIGCOMM'92* (Baltimore, MD 1992), pp. 248–257. http://www.acm.org/pubs/articles/proceedings/comm/144179/p248-biersack/p248-biersack.pdf

[**BIND 2004**] Internet Software Consortium page on BIND, http://www.isc.org/bind.html

[**Bisdikian 2001**] C. Bisdikian, "An Overview of the Bluetooth Wireless Technology," *IEEE Communications Magazine*, No. 12 (December 2001): 86–9 4.

[**Bishop 2003**] M. Bishop, *Computer Security: Art and Science,* Boston: Addison Wesley, Boston MA, 2003

[**BitTorrent 2007**] BitTorrent.org homepage, http://www.bittirrent.org

[**Black 1995**] U. Black, *ATM Volume I: Foundation for Broadband Networks*, Prentice Hall, 1995.

[**Black 1997**] U. Black, ATM, Volume II: Signaling in Broadband Networks, Prentice Hall, 1997.

[**Blaze 1996**] M. Blaze,W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," http://www.counterpane.com/keylength.html

[**Bluetooth 2002**] R. Morrow, *Bluetooth: Operation and Use*, New York: McGraw-Hill, 2002.

[**Blumenthal 2001**] M. Blumenthal, D. Clark, "Rethinking the Design of the Internet: The End-to-end Arguments vs. the Brave New World," *ACM Transactions on Internet Technology*, Vol. 1, No. 1, (August 2001) pp. 70-109.

[**Bochman 1984**] G. V. Bochmann and C. A. Sunshine, "Formal methods in communication protocol design," *IEEE Transactions on Communications,* Vol. COM-28, No. 4 (Apr. 1980), pp. 624–631.

[**Bolot 1994**] J-C. Bolot and T. Turletti, "A rate control scheme for packet video in the Internet," *Proceedings of IEEE Infocom,* 1994, pp. 1216–1223. ftp://ftp-sop.inria.fr/rodeo/bolot/94.Video_control.ps.gz

[**Bolot 1996**] J-C. Bolot and Andreas Vega-Garcia, "Control Mechanisms for Packet Audio in the Internet," *Proceedings of IEEE Infocom,* 1996, pp. 232–239. ftp://ftp-sop.inria.fr/rodeo/bolot/96.Audio_ctl.ps.gz

[**Boutremans 2002**] C. Boutremans, G. Iannaccone, C. Diot, "Impact of Link Failures on VoIP Performance," *12th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV),* Miami, May 2002. http://ipmon.sprint.com/pubs_trs/pubs/gianluca/voip.pdf

[**Bradner 1996**] S. Bradner, A. Mankin, *IPng: Internet Protocol Next Generation,* Addison-Wesley, Reading, MA, 1996.

[**Brakmo 1995**] L. Brakmo and L. Peterson, "TCP Vegas: End to End Congestion Avoidance on a Global Internet," *IEEE Journal of Selected Areas in Communications,* Vol. 13, No. 8, pp. 1465–1480, Oct. 1995. ftp://ftp.cs.arizona.edu/xkernel/Papers/jsac.ps.Z

[**Breslau 2000**] L. Breshlau, E. Knightly, S. Shenker, I. Stoica, H. Zhang, "Endpoint Admission Control: Architectural Issues and Performance," *Proc. 2000 ACM SIGCOMM* (Stockholm, Sweden, Aug. 2000)

[**Brodnik 1997**] A. Brodnik, S. Carlsson, M. Degemark, S. Pink, "Small Forwarding Tables for Fast Routing Lookups," *Proceedings of ACM SIGCOMM '97* (Cannes, France, Oct. 1997), pp. 3–15. http://www.acm.org/sigs/sigcomm/sigcomm97/papers/p192.html

[**Brown 1997**] K. Brown, S. Singh, "M-TCP: TCP for Mobile Cellular Networks," *ACM CCR* 27, no. 5 (1997). http://www.cs.pdx.edu/~singh/ftp/mtcp.ps.gz.

[**Bryant 1988**] B. Bryant, "Designing an Authentication System: A Dialogue in Four Scenes," http://web.mit.edu/kerberos/www/dialogue.html

[**Bush 1945**] V. Bush, "As We May Think," *The Atlantic Monthly,* July 1945. http://www.theatlantic.com/unbound/flashbks/computer/bushf.htm

[**Byers 1998**] J. Byers, M. Luby, M. Mitzenmacher, A Rege, "A digital fountain approach to reliable distribution of bulk data," *Proceedings of ACM SIGCOMM '98* (Vancouver, 1998, Aug. 1998), pp. 56–67. http://www.acm.org/sigcomm/sigcomm98/tp/abs_05.html

[**Cablelabs 2007**] CableLabs homepage, http://www.cablelabs.com

[**CacheLogic 2007**] CacheLogic homepage, http://www.cachelogic.com

[**Caesar 2005**] M. Caesar, J. Rexford, "BGP Routing Policies in ISP Networks," *IEEE Network Magazine*, vol. 19, no. 6 (Nov. 2005).

[**Caldwell 2007**] C. Caldwell, "The Prime Pages," http://www.utm.edu/research/primes/prove

[**Cardwell 2000**] N. Cardwell, S. Savage, T. Anderson, "Modeling TCP Latency," *Proceedings of the 2000 IEEE Infocom Conference*, (Tel-Aviv, Israel), March, 2000. http://www.cs.ucsd.edu/users/savage/papers/Infocom2000tcp.ps

[**CASA 2007**] Center for Collaborative Adaptive Sensing of the Atmosphere, http://www.casa.umass.edu

[**Casner 1992**] Casner, S., Deering, S., "First IETF Internet Audiocast," *ACM SIGCOMM Computer Communications Review,* Vol. 22, No. 3 (July 1992), pp. 92–97. http://citeseer.nj.nec.com/casner92first.html

[**Ceiva 2007**] Ceiva homepage, http://www.ceiva.com/

[**CENS 2007**] Center for Embedded Network Sensing, http://www.cens.ucla.edu/

[**Cerf 1974**] V. Cerf and R. Kahn, "A Protocol for Packet Network Interconnection," *IEEE Transactions on Communications Technology,* Vol. COM-22, No. 5, pp. 627–641.

[**CERT 1999-04**] CERT, "Advisory CA-1999-04: Melissa Macro Virus," http://www.cert.org/advisories/CA-1999-04.html

[**CERT 2001-09**] CERT, "Advisory 2001-09: Statistical Weaknesses in TCP/IP Initial Sequence Numbers," http://www.cert.org/advisories/CA-2001-09.html

[**CERT 2001-19**] CERT, "Advisory CA-2001-19: "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL," http://www.cert.org/advisories/CA-2001-19.html

[**CERT 2003-04**] CERT, "CERT Advisory CA-2003-04 MS-SQL Server Worm," http://www.cert.org/advisories/CA-2003-04.html

[**CERT 2003-04**] CERT, "CERT Advisory CA-2003-04 MS-SQL Server Worm," http://www.cert.org/advisories/CA-2003-04.html

[**CERT 2007**] CERT Coordination Center, http://www.cert.org/advisories

[**CERT Filtering 2007**] CERT, "Packet Filtering for Firewall Systems," http://www.cert.org/tech_tips/packet_filtering.html

[**CERT Smurf 1998**] CERT(r) Advisory CA-98.01, "smurf IP Denial-of-Service Attacks," http://www.cert.org/advisories/CA-1998-01.html

[**CERT SYN 1996**] CERT, "Advisory CA-96.21: TCP SYN Flooding and IP Spoofing Attacks," http://www.cert.org/advisories/CA-1998-01.html

[**CERT 2004 Summaries**] CERT, "CERT Summaries," http://www.cert.org/summaries/

[**Chao 2001**] H. J. Chao, C. Lam, E. Oki, Broadband Packet Switching Technologies—A Practical Guide to ATM Switches and IP Routers, John Wiley & Sons, 2001.

[**Chapman 1992**] B. Chapman, "Network (In)Security Through Packet Filtering," *Third UNIX Security Symposium, sponsored by USENIX Association*, (Baltimore, MD), 1992, http://www.greatcircle.com/pkt_filtering.html

[**Checkpoint 2004**] Checkpoint Web site, http://www.checkpoint.com.

[**Chen 2000**] G. Chen, D. Kotz, "A Survey of Context-Aware Mobile Computing Research," *Technical Report TR2000-381*, Dept. of Computer Science, Dartmouth College, November, 2000. http://www.cs.dartmouth.edu/~dfk/papers/chen:survey-tr.pdf

[**Chen 2006**] K.-T. Chen, C.-Y. Huang, P. Huang, C.-L. Lei, "Quantifying Skype User Satisfaction," *Proc. 2006 ACM SIGCOMM* (Pisa, Italy, Sept. 2006).

[**Cheswick 2000**] Bill Cheswick, Hal Burch, Steve Branigan, "Mapping and Visualizing the Internet," *Proc. 2000 Usenix Conference* (June 2000, San Diego) http://www.usenix.org/publications/library/proceedings/usenix2000/general/full_papers/cheswick/cheswick_html/ mapping.html

[**Chiu 1989**] D. Chiu and R. Jain, "Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks," *Computer Networks and ISDN Systems,* Vol. 17, No. 1, pp. 1–14. http://www.cis.ohio-state.edu/~jain/papers/cong_av.htm

[**Christiansen 2001**] M. Christiansen, K. Jeffay, D. Ott, F. D. Smith, "Tuning Red for Web Traffic," *IEEE/ACM Transactions on Networking*, Vol. 9, No. 3 (June 2001), pp. 249–264, http://www.cs.unc.edu/~jeffay/papers/IEEE-ToN-01.pdf

[**Chu 2000**] Y Chu, S. Rao, H. Zhang, "The Case for End System Multicast," *Proceedings of ACM SIGMETRICS 2000,* (Santa Clara, CA, Aug. 2000). http://www.cs.cmu.edu/~sanjay/Papers/sigmetrics-2000.ps.gz

[**Chuang 2005**] S. Chuang, S. Iyer, N. McKeown, "Practical Algorithms for Performance Guarantees in Buffered Crossbars," *Proc. 2005 IEEE Infocom*.

[**Cicconetti 2006**] C. Cicconetti, L. Lenzini, A. Mingozi, K. Eklund, "Quality of Service Support in 802.16 Networks," *IEEE Network Magazine*, Mar./Apr. 2006, pp. 50-55.

[**Cisco 12000 2007**] Cisco Systems, "Cisco 12000 Series Gigabit Switch Routers," http://www.cisco.com/univercd/cc/td/doc/pcat/12000.htm

[**Cisco 8500 2007**] Cisco Systems Inc., "Catalyst 8500 Campus Switch Router Architecture," http://www.cisco.com/univercd/cc/td/doc/product/l3sw/8540/rel_12_0/w5_6f/softcnfg/1cfg8500.pdf

[**Cisco CiscoWorks 2000**] Cisco Systems, Cisco Works2000 homepage, http://www.cisco.com/warp/public/cc/pd/wr2k/index.shtml

[**Cisco NAT 2007**] Cisco Systems Inc, "How NAT Works," http://www.cisco.com/warp/public/556/nat-cisco.shtml

[**Cisco NAPA 2007**] Cisco Systems Inc., "Cisco Network Application Performance Analysis (NAPA) Solution," http://www.cisco.com/en/US/products/sw/netmgtsw/index.html

[**Cisco QoS 2007**] Cisco Systems Inc, "Advanced QoS Services for the Intelligent Internet," http://www.cisco.com/warp/public/cc/pd/iosw/ioft/ioqo/tech/qos_wp.htm

[**Cisco Queue 2007**] Cisco Systems Inc., "Interface Queue Management," http://www.cisco.com/warp/public/614/16.html

[**Cisco Security 2007**] Cisco Systems Inc., "Why You Need a Firewall," http://www.cisco.com/en/US/products/sw/secursw/ps743/products_user_guide_chapter09186a008007f303.html

[**Cisco Switches 2007**] Cisco Systems Inc., "Cisco Catalyst 1900/2820 - Affordable Switching Solutions" http://www.cisco.com/warp/public/cc/pd/si/index.shtml

[**Cisco SYN 2007**] Cisco Systems Inc., "Defining Strategies to Protect Against TCP SYN Dential of Service Attacks," http://www.cisco.com/warp/public/707/4.html#tcpsyn

[**CISN 2004**] California Integrated Seismic Network, http://www.cisn.org/

[**Claffy 1998**] K. Claffy, G. Miller, and K. Thompson, "The Nature of the Beast: Recent Traffic Measurements from an Internet Backbone," *Proceedings of Inet '98,* (Geneva, Switzerland, July 1998), http://www.caida.org/outreach/papers/1998/Inet98/

[**Clark 1988**] D. Clark, " The Design Philosophy of the DARPA Internet Protocols, *Proceedings of ACM SIGCOMM'88,* (Stanford, CA), Aug. 1988, Vol. 18, No. 4, http://www.acm.org/sigcomm/ccr/archive/1995/jan95/ccr-9501-clark.html.

[**Clarke 2002**] I. Clarke, T. W. Hong, S. G. Miller, O. Sandberg, B. Wiley, "Protecting Free Expression Online with Freenet," *IEEE Internet Computing*, January–February 2002, pp. 40–49. http://freenet.sourceforge.net/papers/freenet-ieee.pdf

[**Cnet 2000**] Cnet news.com, "Leading Web Sites Under Attack," http://news.com.com/2100-1017-236683.html

[**Cohen 1977**] D. Cohen, "Issues in Transnet Packetized Voice Communication," *Proceedings of the Fifth Data Communications Symposium*, (Snowbird, Utah, September 1977) pp. 6-13.

[**Cookie Central 2007**] Cookie Central homepage, http://www.cookiecentral.com

[**CoolStreaming 2005**] X. Zhang, J. Liu, B. Li, Y. Yum, "CoolStreaming/DONet: a data-driven overlay network for peer-to-peer live media streaming," *Proc. IEEE Infocom*, (March 2005, Miami FL).

[**Cormen 2001**] T. H. Cormen, *Introduction to Algorithms, 2nd Ed.,* MIT Press, Cambridge, MA, 2001.

[**Crow 1997**] B. Crow, I. Widjaja, J. Kim, P. Sakai, "IEEE 802.11 Wireless Local Area Networks," *IEEE Communications Magazine,* Sept. 1997, pp. 116–126.

[**Crowcroft 1995**] J. Crowcroft, Z. Wang, A. Smith, J. Adams, *"A Comparison of the IETF and ATM Service Models," IEEE Communications Magazine,* Nov./ Dec. 1995, pp. 12–16. http://citeseer.nj.nec.com/crowcroft95rough.html

[**Crowcroft 1999**] J. Crowcroft, M. Handley, and I. Wakeman, *Internetworking Multimedia,* Morgan-Kaufman, San Francisco, 1999.

[**Culler 2004**] D. Culler, D. Estrin, M. Srivastava, "Overview of Sensor Networks," *IEEE Computer*, Vol. 37, No. 8, pp. 41-49, Aug. 2004.

[**Cusumano 1998**] M.A. Cusumano and D.B. Yoffie, *Competing on Internet Time: Lessons from Netscape and its Battle with Microsoft,* Free Press, NY, NY, 1998

[**Daemen 2000**] J. Daemen, V. Rijmen, "The Block Cipher Rijndael," in *Smart Card Research and Applications, LNCS 1820*, (J. J. Quisquater, B. Schneier, eds.), Springer-Verlag, 2000, pp. 288–296.

[**Daigle 1991**] J. N. Daigle, *Queuing Theory for Telecommunications,* Addison-Wesley, Reading, MA, 1991.

[**Dalal 1978**] Y. Dalal, R. Metcalfe, "Reverse Path Forwarding of Broadcast Packets," *Communications of the AC* M, Vol. 21, No. 12, (Dec. 1978), pp. 1040-1048.

[**Davie 2000**] B. Davie and Y. Rekhter, *MPLS: Technology and Applications*, Morgan Kaufmann Series on Networking, 2000.

[**Davies 2004**] G. Davies, M. Hardt and F. Kelly, "Network dimensioning, service costing and pricing in a packet switched environment," *Telecommunications Policy*, Vol. 28, pp. 391-412, 2004.

[**Danielyan 2001**] E. Danielyan, "Goodbye DES, Welcome AES," *Internet Protocol Journal* 4(2), June 2001.
http://www.cisco.com/en/US/about/ac123/ac147/ac174/about_cisco_ipj_archive_issues_list.html

[**DEC 1990**] Digital Equipment Corporation, "In Memoriam: J. C. R. Licklider 1915–1990," SRC Research Report 61, Aug. 1990. http://www.memex.org/licklider.pdf

[**DeClercq 2002**] J. DeClercq, O. Paridaens, "Scalability Implications of Virtual Private Networks," *IEEE Communications Magazin*e, 40(5), May 2002, pp. 151–157.

[**Deering 1990**] S. Deering, D. Cheriton, "Multicast routing in datagram internetworks and extended LANs," *ACM Transactions on Computer Systems,* Vol. 8, No. 2 (1990), pp. 85–110.

[**Deering 1996**] S. Deering, D. Estrin, D. Faranacci, V. Jacobson, C. Liu, L. Wei, "The PIM Architecture for Wide Area Multicasting," *IEEE/ACM Transactions on Networking,* Vol. 4, No. 2 (Apr. 1996), pp. 153–162.

[**Demers 1990**] A. Demers, S. Keshav, and S. Shenker, "Analysis and Simulation of a Fair Queuing Algorithm," *Internetworking: Research and Experience,* Vol. 1, No. 1, pp. 3–26, 1990..

[**Denning 1997**] D. Denning (Editor), P. Denning (Preface), *Internet Besieged: Countering Cyberspace Scofflaws,* Addison-Wesley, Reading, MA, 1997.

[**dhc 2007**] IETF Dynamic Host Configuration working group, http://www.ietf.org/html.charters/dhc-charter.html

[**Dialpad 2004**] Dialpad homepage, http://www.dialpad.com

[**Diffie 1976**] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory,* Vol IT-22 (1976), pp. 644–654.

[**Diffie 1998**] W. Diffie and S. Landau, *Privacy on the Line, The Politics of Wiretapping and Encryption,* MIT Press, Cambridge MA, 1998.

[**Digital Signature 2004**] Digital Signature Trust Company, http://www.trustdst.com/

[**Diggavi 2004**] S. N. Diggavi, N. Al-Dhahir, A. Stamoulis, and A. R. Calderbank, "Great Expectations: The Value of Spatial Diversity in Wireless Networks," *Proceedings of the IEEE*,vol. 92, no. 2, pp. 217-270, Feb. 2004.

[**Diot 2000**] C. Diot, B. N. Levine, B. Lyles, H. Kassem, D. Balensiefen, "Deployment Issues for the IP Multicast Service and Architecture," *IEEE Network,* Vol. 14, No. 1 (Jan./Feb. 2000), pp. 78–88, http://signl.cs.umass.edu/pubs/brian.ieeenetwork00.ps.gz

[**Dodge 2007**] M. Dodge, "An Atlas of Cyberspaces," http://www.cybergeography.org/atlas/isp_maps.html

[**Donahoo 2000**] M. Donahoo, K. Calvert, *TCP/IP Sockets in C: Practical Guide for Programmers*, Morgan Kaufman, 2000.

[**Dornan 2001**] A. Dornan, *The Essential Guide to Wireless Communications Applications: From Cellular Systems to WAP and M-Commerce*, Prentice Hall, Upper Saddle River, N.J., 2001.

[**Doucer 2002**] J. R. Douceur, "The Sybil Attack," *Proc. of the IPTPS'02 Workshop*, (Cambridge, MA, Mar. 2002).

[**Droms 1999**] R. Droms, T. Lemon, *The DHCP Handbook*, Macmillan Technical Publishing, Indianapolis, IN, 1999.

[**DSL 2007**] DSL Forum, http://www.dslforum.org/

[**EFF 1999**] Electronic Frontier Foundation, "Frequently Asked Questions (FAQ) About the Electronic Frontier Foundation's DES Cracker Machine," http://www.eff.org/pub/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html

[**Elgamal 2001**] A. Elgamal, F. Seible, F. Vernon, M. Trivedi, M. Fraser, "On-Line Structural Monitoring and Data Management," *Proceedings, 6th Seismic Research Workshop,* California Department of Transportation*,* Sacramento, California, June 12–13, 2001. http://www.calit2.net/eci/caltrans_health_monitoring_paper.pdf

[**Ellis 1987**] H. Ellis, "The Story of Non-Secret Encryption," http://www.cesg.gov.uk/site/publications/media/ellis.pdf

[**Ericsson 2007**] Ericsson, "EDGE: Introduction of High-Speed Data in GSM/GPRS Networks." http://www.ericsson.com/products/white_papers_pdf/edge_wp_technical.pdf

[**Estrin 1997**] D. Estrin, M. Handley, A. Helmy, P. Huang, D. Thaler, "A Dynamic Bootstrap Mechanism for Rendezvous-based Multicast Routing," *Proceedings of IEEE Infocom '98,* (New York, NY, April 1998). http://ceng.usc.edu/~helmy/infocom-bootstrap-99.pdf

[**Estrin 1998b**] Deborah Estrin, V. Jacobson, D. Farinacci, L. Wei, Steve Deering, Mark Handley, David Thaler, Ching-Gung Liu, Puneet Sharma, A. Helmy, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Motivation and Architecture," work in progress, http://netweb.usc.edu/pim/pimsm/PIM-Arch.ps.gz.

[**Estrin 2002**] D. Estrin, D. Culler, K. Pister, "Connecting the Physical World with Pervasive Networks," *IEEE Pervasive Computing*, 1,1 (Jan.–March 2002).

[**Ethereal 2007**] Ethereal homepage, http://www.ethereal.com

[**Faloutsos 1999**] C. Faloutsos, M. Faloutsos, P. Faloutsos, "What Does the Internet Look Like? Empirical Laws of the Internet Topology," *Proceedings of ACM SIGCOMM 1999*, Boston, MA, September 1999.

[**Feamster 2004**] N. Feamster, J. Winick, J. Rexford, "A Model for BGP Routing for Network Engineering," *Proceedings of 2004 ACM Sigmetrics,* NY, NY (June 2004). http://www.research.att.com/~jrex/papers/whatifatron.pdf

[**Feldmeier 1988**] D. Feldmeier, "Improving Gateway Performance with a Routing Table Cache," *Proc. 1988 IEEE Infocom Conference* (New Orleans LA, Mar. 1988).

[**Feldmeier 1995**] D. Feldmeier, "Fast Software Implementation of Error Detection Codes," *IEEE/ACM Transactions on Networking,* Vol. 3., No. 6 (Dec. 1995), pp. 640–652.

[**FIPS 1995**] Federal Information Processing Standard, "Secure Hash Standard," FIPS Publication 180-1. http://www.itl.nist.gov/fipspubs/fip180-1.htm

[**FIPS-46-1 1988**] US National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standard (FIPS) Publication 46-1, Jan. 1988. http://www.itl.nist.gov/fipspubs/fip46-2.htm

[**Fletcher 1982**] J. G. Fletcher, "An Arithmetic Checksum for Serial Transmissions," *IEEE Transactions on Communications,* Vol. 30, No. 1 (Jan. 1982), pp. 247–253.

[**Floyd 1999**] S. Floyd and K. Fall, "Promoting the Use of End-to-End Congestion Control in the Internet," *IEEE/ACM Transactions on Networking,* Vol. 6, No. 5 (Oct. 1998), pp. 458–472. http://www.icir.org/floyd/end2end-paper.html

[**Floyd 2000**] S. Floyd, M. Handley, J. Padhye, J. Widmer, "Equation-Based Congestion Control for Unicast Applications," Proceedings 2000 ACM Sigcomm Conference, (Stockholm, Sweden, Aug. 2000). http://www.icir.org/tfrc/tcp-friendly.pdf

[**Floyd 2001**] S. Floyd, "A Report on Some Recent Developments in TCP Congestion Control," *IEEE Communications Magazine* (April 2001), http://www.aciri.org/floyd/papers/report_Jan01.pdf

[**Floyd 2007**] S. Floyd, "References on RED (Random Early Detection) Queue Management," http://www.icir.org/floyd/red.html

[**Floyd Synchronization 1994**] S. Floyd, V. Jacobson, "Synchronization of Periodic Routing Messages," *IEEE/ACM Transactions on Networking,* Vol. 2, No. 2 (Apr. 1997), pp. 122–136. http://www.aciri.org/floyd/papers/sync_94.ps.Z

[**Floyd TCP 1994**] S. Floyd, "TCP and Explicit Congestion Notification," *ACM Computer Communication Review,* Vol. 24, No. 5, pp. 10–23, Oct. 1994. http://www.aciri.org/floyd/papers/tcp_ecn.4.ps.Z

[**Fluhrer 2001**] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, August 2002. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[**Fortz 2000**] B. Fortz, M. Thorup, "Internet Traffic Engineering by Optimizing OSPF Weights," *Proceedings of 2000 IEEE Infocom*. http://www.ieee-infocom.org/2000/papers/165.ps.

[**Fortz 2002**] B. Fortz, J. Rexford, M. Thorup, "Traffic Engineering with Traditional IP Routing Protocols," *IEEE Communication Magazine,* October 2002. http://www.research.att.com/~jrex/papers/ieeecomm02.ps

[**Foster 2002**] I. Foster, "The Grid: A New Infrastructure for 21st Century Science," *Physics Today*, 55(2):42–47, 2002, http://www.aip.org/pt/vol-55/iss-2/p42.html.

[**Freephone 2004**] "Freephone: Why use the Plain Old Telephone when you can get so much better on the Internet?" http://www-sop.inria.fr/rodeo/fphone/

[**Friedman 1999**] T. Friedman, D. Towsley "Multicast Session Membership Size Estimation," *Proc. IEEE Infocom '99* (New York, USA, March 1999) ftp://gaia.cs.umass.edu/pub/Friedman99_Infocom99.ps.gz

[**Frost 1994**] J. Frost, "BSD Sockets: A Quick and Dirty Primer," http://world.std.com/~jimf/papers/sockets/sockets.html

[**Gallager 1983**] R. G. Gallager, P. A. Humblet, P. M. Spira, "A Distributed Algorithm for Minimum Weight-Spanning Trees," *ACM Trans. on Programming Languages and Systems,* 1(5), (January 1983), pp. 66–77.

[**Gao 2001**] L. Gao, J. Rexford, "Stable Internet Routing Without Global Coordination," *IEEE/ACM Trans. Networking,* 9(6), pp. 681–692, December 2001. http://www.research.att.com/~jrex/papers/sigmetrics00.long.pdf

[**Garces-Erce 2003**] L. Garces-Erce, K. W. Ross, E. Biersack, P. Felber, G. Urvoy-Keller, "TOPLUS: Topology Centric Lookup Service," *Fifth International Workshop on Networked Group Communications (NGC'03*), Munich, September 2003. http://cis.poly.edu/~ross/papers/TOPLUS.pdf

[**Gartner 2003**] F. C. Gartner, "A Survey of Self-Stabilizing Spanning-Tree Construction Algorithms," *Technical Report IC/2003/38*, Swiss Federal Institute of Technology (EPFL), School of Computer and Communication Sciences, June 10, 2003. http://ic2.epfl.ch/publications/documents/IC_TECH_REPORT_200338.pdf.

[**Gauthier 1999**] L. Gauthier, C. Diot, and J. Kurose, "End-to-end Transmission Control Mechanisms for Multiparty Interactive Applications on the Internet," *Proceedings of IEEE Infocom '99,* (New York, NY, Apr. 1999). ftp://ftp.sprintlabs.com/diot/infocom99-mimaze.zip

[**Giacopelli 1990**] J. Giacopelli, M. Littlewood, W. D. Sincoskie "Sunshine: A high performance self-routing broadband packet switch architecture," *1990 International Switching Symposium.* An extended version of this paper appeared in *IEEE J. Sel. Areas in Common*., Vol. 9, No. 8 (Oct. 1991), pp. 1289–1298.

[**Girard 1990**] A. Girard, *Routing and Dimensioning in Circuit-Switched Networks,* Addison-Wesley, Reading, MA, 1990.

[**Glitho 1995**] R. Glitho and S. Hayes (eds.), special issue on Telecommunications Management Network, *IEEE Communications Magazine,* Vol. 33, No. 3 (Mar. 1995).

[**Glitho 1998**] R. Glitho, "Contrasting OSI Systems Management to SNMP and TMN," *Journal of Network and Systems Management,* Vol. 6, No. 2 (June 1998), pp. 113–131.

[**Gnutella 2007**] "The Gnutella Protocol Specification, v0.4" http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf

[**Goodman 1997**] David J. Goodman, *Wireless Personal Communications Systems*, Prentice-Hall, 1997.

[**Goodman 1997b**] D. Goodman (Chair), *The Evolution of Untethered Communications,* National Academy Press, Washington DC, Dec. 1997. http://www.nap.edu/readingroom/books/evolution/index.html

[**Goralski 1999**] W. Goralski, *Frame Relay for High-Speed Networks,* John Wiley, New York, 1999.

[**Goralski 2001**] W. Goralski, *Optical Networking and WDM,* Osborne/McGraw-Hill, Berkeley, CA, 2001.

[**Griffin 2002**] T. Griffin, "Interdomain Routing Links," http://www.research.att.com/~griffin/interdomain.html

[**Gummadi 2003**] K. P. Gummadi, R. J. Dunn, S. Saroiu, S. D. Gribble, H. M. Levy, J. Zahorjan, "Measurement, Modeling, and Analysis of a Peer-to-Peer File-Sharing Workload," *Proceedings of the 19th ACM Symposium on Operating Systems Principles (SOSP-19),* October 2003. http://www.cs.washington.edu/homes/tzoompy/publications/sosp/2003/abstract.html

[**Gupta 1998**] P. Gupta, S. Lin, N. McKeown. "Routing lookups in hardware at memory access speeds," *Proc. IEEE Infocom 1998* (San Francisco, CA, April 1998), pp. 1241–1248. http://tiny-tera.stanford.edu/~nickm/papers/Infocom98_lookup.pdf

[**Gupta 2001**] P. Gupta, N. McKeown, "Algorithms for Packet Classification," *IEEE Network Magazine,* Vol. 15, No. 2 (Mar./Apr. 2001), pp. 24–32, http://klamath.stanford.edu/~pankaj/paps/ieeenetwork_tut_01.pdf

[**Halabi 2000**] S. Halabi, *Internet Routing Architectures, 2nd Ed* ., Cisco Press, 2000.

[**Hamada 1997**] T. Hamada, H. Kamata, S. Hogg, "An Overview of the TINA Management Architecture," *Journal of Network and Systems Management,* Vol. 5. No. 4 (Dec. 1997). pp. 411–435.

[**Heidemann 1997**] J. Heidemann, K. Obraczka, and J. Touch, "Modeling the Performance of HTTP over Several Transport Protocols," *IEEE/ACM Transactions on Networking,* Vol. 5, No. 5 (Oct. 1997), pp. 616–630. http://www.isi.edu/~johnh/PAPERS/Heidemann96a.html

[**Held 2001**] G. Held, *Data Over Wireless Networks: Bluetooth, WAP, and Wireless LANs*, McGraw-Hill, 2001.

[**Hersent 2000**] O. Hersent, D. Gurle, J-P Petit, *IP Telephony: Packet-Based Multimedia Communication Systems*," Pearson Education Limited, Edinburgh, 2000.

[**Hinden 2007**] R. Hinden, "IP Next Generation (IPng)," http://playground.sun.com/pub/ipng/html/ipng-main.html

[**Holbrook 1999**] H. Holbrook, D. Cheriton, "IP Multicast Channels: EXPRESS Support for Large-Scale Single-Source Applications," *Proceedings of ACM SIGCOMM '99* (Boston, MA, Aug. 1999). http://www.acm.org/sigs/sigcomm/sigcomm99/papers/session2-3.html

[**Hollot 2002**] C.V. Hollot, V. Misra, D. Towsley, W. Gong, "Analysis and design of controllers for AQM routers supporting TCP flows," IEEE Transactions on Automatic Control, Vol. 47, No. 6 (June 2002), pp. 945-959. http://www1.cs.columbia.edu/~misra/pubs/TAC_special.pdf

[**Huang 2002**] C. Haung, V. Sharma, K. Owens, V. Makam, "Building Reliable MPLS Networks Using a Path Protection Mechanism," *IEEE Communications Magazine,* 40(3), March 2002, pp. 156–162.

[**Huitema 1998**] C. Huitema, *IPv6: The New Internet Protocol, 2nd Ed.,* Prentice Hall, Englewood Cliffs, NJ, 1998.

[**Huston 1999a**] G. Huston, "Interconnection, Peering, and Settlements—Part I," *The Internet Protocol Journal,* Vol. 2, No. 1, (March 1999). http://www.cisco.com/warp/public/759/ipj_2-1/ipj_2-1_ps1.html

[**Huston 1999b**] G. Huston, "Interconnecting, Peering, and Settlements—Part II," *The Internet Protocol Journal,* Vol. 2, No. 2 (June 1999). http://www.cisco.com/warp/public/759/ipj_2-2/ipj_2-2_ps1.html

[**Huston 2001**] G. Huston, "Analyzing the Internet BGP Routing Table," *The Internet Protocol Journal*, Vol. 4, No. 1 (Mar. 2001), http://www.cisco.com/warp/public/759/ipj_4-1/ipj_4-1_bgp.html

[**IAB 2007**] Internet Architecture Board, http://www.iab.org/iab/

[**IANA 2007**] Internet Assigned Number Authority homepage, http://www.iana.org/

[**ICANN 2007**] The Internet Corporation for Assigned Names and Numbers, http://www.icann.org

[**IEC Optical 2007**] IEC Online Education, "Optical Access," http://www.iec.org/online/tutorials/opt_acc/

[**IEEE 802 2007**] "IEEE 802 LAN/MAN Standards Committee," http://www.ieee802.org/

[**IEEE 802.11 1999**] IEEE 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Network—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[**IEEE 802.15 2007**] IEEE 802.15 Working Group for WPAN. http://grouper.ieee.org/groups/802/15/.

[**IEEE 802.1X**] IEEE Std 802.1X-2001 Port-Based Network Access Control, http://standards.ieee.org/reading/ieee/std_public/description/lanman/802.1x-2001_desc.html

[**IETF 2007**] Internet Engineering Task Force homepage, http://www.ietf.org

[**IETF dnsext 2004**] IETF DNS Extensions Working Group, http://www.ietf.org/html.charters/dnsext-charter.html

[**Interlinknetworks 2004**] Interlinknetworks, "Introduction to 802.1x for Wireless Local Area Networks," http://www.interlinknetworks.com/resource/wp5-1-1.htm

[**IMAP 2007**] The IMAP Connection, http://www.imap.org/

[**Interlinknetworks 2004**] Internlinknetworks, "Introduction to 802.1x for Wireless Local Area Networks," http://www.interlinknetworks.com/resource/wp5-1-1.htm

[**Ioannidis 2000**] S. Ioannidis, A. Keromytis, S. Bellovin, J. M. Smith, "Implementing a Distributed Firewall," *Proceedings of the ACM Computer and Communications Security (CCS)* 2000, (Athens, Greece), pp. 190–199, http://www.cis.upenn.edu/~strongman/Papers/df.pdf

[**Iren 1999**] S. Iren, P. Amer, P. Conrad, "The Transport Layer: Tutorial and Survey," *ACM Computing Surveys,* Vol 31, No 4, (Dec 1999). http://www.cis.udel.edu/~amer/PEL/survey/

[**ISC 2007**] Internet Systems Consortium, http://www.isc.org.

[**ISO 1987**] International Organization for Standardization, "Information processing systems — Open Systems Interconnection—,"International Standard 8824 (Dec. 1987). http://asn1.elibel.tm.fr/en/standards/index.htm

[**ISO X.680** 1998] International Organization for Standardization, "X.680: ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, Information Technology—Abstract Syntax Notation One (ASN.1): Specification of Basic Notation." http://asn1.elibel.tm.fr/en/standards/index.htm

[**ITU 2000**] International Telecommunication Union, "Recommendation X.509 (11/93) Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.509-200003-I

[**ITU 2007**] The ITU Web site, http://www.itu.int/

[ITU Statistics 2007] International Telecommunication Union, "ICT Statistics," http://www.itu.int/ITU-D/icteye/Reports.aspx

[**ITU-T Q.2931 1994**] "Broadband Integrated Service Digital Network (B-ISDN) Digital Subscriber Signaling System no.2 (DSS2) User Network Interface Layer 3 Specification for Basic Call/Connection Control," *ITU-T Recommendation Q.2931*, Geneva: International Telecommunication Union, 1994.

[**Iyer 2002**] S. Iyer, R. Zhang, N. McKeown, "Routers with a Single Stage of Buffering," *Proceedings 2002 ACM Sigcomm Conference,* http://www.acm.org/sigs/sigcomm/sigcomm2002/papers/routersingle.pdf.

[**Jacobson 1988**] V. Jacobson, "Congestion Avoidance and Control," *Proceedings of ACM SIGCOMM '88,* (Stanford, CA, Aug. 1988), pp. 314–329, ftp://ftp.ee.lbl.gov/papers/congavoid.ps.Z

[**Jain 1989**] R. Jain, "A Delay-Based Approach for Congestion Avoidance in Interconnected Heterogeneous Computer Networks," *ACM Computer Communications Review,* Vol. 19, No. 5 (1989), pp. 56–71. http://www.cis.ohio-state.edu/~jain/papers/delay.htm

[**Jain 1994**] R. Jain, *FDDI Handbook: High-Speed Networking Using Fiber and Other Media,* Addison-Wesley, Reading, MA, 1994.

[**Jain 1996**] R. Jain. S. Kalyanaraman, S. Fahmy, R. Goyal, and S. Kim, "Tutorial Paper on ABR Source Behavior," *ATM Forum*/96-1270, Oct. 1996. http://www.cis.ohio-state.edu/~jain/atmf/a96-1270.htm

[**Jaiswal 2003**] S. Jaiswal, G. Iannaccone, C. Diot, J. Kurose, D. Towsley, "Measurement and Classification of Out-of-Sequence Packets in a Tier-1 IP backbone," *Proceedings of 2003 INFOCO* M, ftp://gaia.cs.umass.edu/pub/Jaiswal03_oos.pdf.

[**Jakobson 1993**] G. Jacobson and M. Weissman, "Alarm Correlation," *IEEE Network Magazine,* 1993, pp. 52–59.

[**Ji 2003**] P. Ji, Z. Ge, J. Kurose, D. Towsley, "A Comparison of Hard-state and Soft-state Signaling Protocols," *Proceedings of 2003 ACM SIGCOMM*, http://www.acm.org/sigs/sigcomm/sigcomm2003/papers/p251-ji.pdf

[**Jiang 2001**] W. Jiang, J. Lennox, H. Schulzrinne, K. Singh, "Towards Junking the PBX: Deploying IP Telephony," *NOSSDAV'01* (Port Jefferson, NY, June 2001). http://www.cs.columbia.edu/~hgs/papers/Jian0106_Junking.pdf.

[**Jimenez 1997**] D. Jimenez, "Outside Hackers Infiltrate MIT Network, Compromise Security," *The Tech,* Vol. 117, No. 49 (Oct. 1997), p. 1. http://www-tech.mit.edu/V117/N49/hackers.49n.html

[**Jin 2004**] C. Jin, D. X. We, S. Low, "FAST TCP: Motivation, architecture, algorithms, performance," *Proc. IEEE Infocom*, Hong Kong, March 2004, http://netlab.caltech.edu/pub/papers/FAST-csreport2003.pdf.

[**Kaaranen 2001**] H. Kaaranen, S. Naghian, L. Laitinen, A. Ahtiainen, Valtteri Niemi*, UMTS Networks, Architecture, Mobility and Service* s, John Wiley &Sons, 2001.

[**Kahn 1967**] D. Kahn, *The Codebreakers, the Story of Secret Writing,* The Macmillan Company, 1967.

[**Kahn 1978**] R. E. Kahn, S. Gronemeyer, J. Burchfiel, R. Kunzelman, "Advances in Packet Radio Technology," *Proc. of the IEEE*, 66, 11 (November 1978).

[**Kangasharju 2000**] J. Kangasharju, K. W. Ross, and J. W. Roberts, "Performance Evaluation of Redirection Schemes in Content Distribution Networks ," *Proceedings of 5th Web Caching and Content Distribution Workshop, Lisbon*, Portugal, May 2000, Lisbon, Portugal. http://www.terena.nl/conf/wcw/Proceedings/S4/S4-2.ps

[**Kapoor 1997**] H. Kapoor, "CoreBuilder 5000 Switch Module Architecture," 3 Corporation, white paper, number 500645.

[**Kar 2000**] K. Kar, M. Kodialam, T. V. Lakshman, "Minimum Interference Routing of Bandwidth Guaranteed Tunnels with MPLS Traffic Engineering Applications," *IEEE J. Selected Areas in Communications*, December, 2000. http://www.bell-labs.com/org/11347A/paper/minint_jsac.pdf

[**Karol 1987**] M. Karol, M. Hluchyj, A. Morgan, "Input Versus Output Queuing on a Space-Division Packet Switch," *IEEE Transactions on Communications,* Vol. COM-35, No. 12 (Dec. 1987), pp. 1347–1356.

[**Katzela 1995**] I. Katzela, and M. Schwartz. "Schemes for Fault Identification in Communication Networks," *IEEE/ACM Transactions on Networking,* Vol. 3, No. 6 (Dec. 1995), pp. 753–764.

[**Kaufman 1995**] C. Kaufman, R. Perlman, M. Speciner, *Network Security, Private Communication in a Public World,* Prentice Hall, Englewood Cliffs, NJ, 1995.

[**KaZaA 2004**] KaZaA homepage, http://www.kazaa.com

[**Kelly 2003**] T. Kelly, *Scalable TCP: Improving Performance in Highspeed Wide Area Networks,* http://www-lce.eng.cam.ac.uk/~ctk21/papers/scalable_improve_hswan.pdf.

[**Kende 2000**] M. Kende, "The Digital Handshake: Connecting Internet Backbones," FCC Report, 2000, http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp32.pdf

[**Keshav 1998**] S. Keshav, R. Sharma, "Issues and Trends in Router Design," *IEEE Communications Magazine,* Vol. 36, No. 5 (May 1998), pp. 144–151.

[**Kilkki 1999**] K. Kilkki, *Differentiated Services for the Internet*, Macmillan Technical Publishing, Indianapolis, IN, 1999.

[**Kleinrock 1961**] L. Kleinrock, "Information Flow in Large Communication Networks," RLE Quarterly Progress Report, July 1961.

[**Kleinrock 1964**] L. Kleinrock, *1964 Communication Nets: Stochastic Message Flow and Delay,* McGraw-Hill, NY, NY, 1964.

[**Kleinrock 1975**] L. Kleinrock, *Queuing Systems, Vol. 1,* John Wiley, New York, 1975.

[**Kleinrock 1975b**] L. Kleinrock and F. A. Tobagi, "Packet Switching in Radio Channels: Part I—Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *IEEE Transactions on Communications,* Vol. COM-23, No. 12 (Dec. 1975), pp. 1400–1416.

[**Kleinrock 1976**] L. Kleinrock, *Queuing Systems, Vol. 2,* John Wiley, New York, 1976.

[**Kleinrock 2004**] L. Kleinrock, "The Birth of the Internet," http://www.lk.cs.ucla.edu/LK/Inet/birth.html

[**Kohler 2004**] E. Kohler, M. Handley, S. Floyd, J. Padhye, DCCP homepage, http://www.icir.org/kohler/dccp/

[**Korhonen 2003**] J. Korhonen, *Introduction to 3G Mobile Communications*, 2nd ed., Artech House, 2003.

[**Krishnamurthy 2001**] B. Krishnamurthy, and J. Rexford, *Web Protocols and Practice: HTTP/1.1, Networking Protocols, and Traffic Measurement*, Addison-Wesley, Boston, MA, 2001.

[**Kurose 1996**] J. F. Kurose, Unix Network Programming, http://manic.cs.umass.edu/~amldemo/courseware/intro.html

[**Labovitz 1997**] C. Labovitz, G. R. Malan, F. Jahanian, "Internet Routing Instability," *Proceedings of ACM SIGCOMM '97* (Cannes, France, 1997), Pages 115–126. http://www.acm.org/sigcomm/sigcomm97/papers/p109.html

[**Labrador 1999**] M. Labrador, S. Banerjee, "Packet Dropping Policies for ATM and IP Networks," *IEEE Communications Surveys*, Vol. 2, No. 3 (Third Quarter 1999), pp. 2–14, http://www.comsoc.org/livepubs/surveys/public/3q99issue/banerjee.html

[**Lakshman 1997**] T. V. Lakshman, U. Madhow, "The Performance of TCP/IP for Networks with High Bandwidth-Delay Products and Random Loss," *IEEE/ACM Transactions on Networking,* Vol. 5 No. 3 (1997). pp. 336–350. http://citeseer.ist.psu.edu/lakshman96performance.html

[**Lam 1980**] S. Lam, "A Carrier Sense Multiple Access Protocol for Local Networks," *Computer Networks,* Vol. 4 (1980), pp. 21–32, 1980.

[**Lamport 1981**] L. Lamport, "Password Authentication with Insecure Communication", *Communications of the ACM,* Vol. 24, No. 11 (Nov. 1981), pp. 770–772.

[**Larmouth 1996**] J. Larmouth, *Understanding OSI,* International Thomson Computer Press 1996. Chapter 8 of this book deals with ASN.1 and is available on-line at http://www.salford.ac.uk/iti/books/osi/all.html#head8

[**Larsen 1997**] A. Larsen, "Guaranteed Service: Monitoring Tools," *Data Communications,* June 1997, pp. 85–94.

[**Lawton 2001**] G. Lawton, "Is IPv6 Finally Gaining Ground?" *IEEE Computer Magazine* (Aug. 2001), pp. 11–15.

[**Leiner 1998**] B. Leiner, V. Cerf, D. Clark, R. Kahn, L. Kleinrock, D. Lynch, J. Postel, L. Roberts, and S. Woolf, "A Brief History of the Internet," http://www.isoc.org/internet/history/brief.html

[**Liang 2004**] J. Liang, R. Kumar, K.W. Ross, "Understanding KaZaA", http://cis.poly.edu/~ross/papers/.

[**Lin 2001**] Y. Lin, I. Chlamtac, *Wireless and Mobile Network Architectures*, John Wiley and Sons, New York, NY, 2001.

[**Liu 2002**] B. Liu, D. Goeckel, D. Towsley, "TCP-Cognizant Adaptive Forward Error Correction in Wireless Networks," *Proceedings of Globe Internet 2002.* ftp://gaia.cs.umass.edu/pub/wirelessTCPtech.pdf

[**Luotonen 1998**] A. Luotonen, *Web Proxy Servers,* Prentice Hall, Englewood Cliffs, New Jersey, 1998.

[**Lynch 1993**] D. Lynch, M. Rose, *Internet System Handbook,* Addison-Wesley, Reading, MA, 1993.

[**Macedonia 1994**] Macedonia, M. R., Brutzman, D. P., "MBone Provides Audio and Video Across the Internet," *IEEE Computer Magazine,* Vol. 27, No. 4 (Apr. 1994), pp. 30–36. ftp://taurus.cs.nps.navy.mil/pub/mbmg/mbone.html

[**Maconachy 2001**] W.V. Maconachy, C. Schou, D. Ragsdale, D. Welch, "A Model for Information Assurance: an Integrated Approach," *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, (West Point, NY), 2001, http://www.itoc.usma.edu/Documents/Workshop2001/paperW2C3(55).pdf

[**Maennel 2002**] O. Maennel, A. Feldmann, "Realistic BGP Traffic for Test Labs," *Proceedings. of 2002 ACM Sigcomm*, http://www.acm.org/sigs/sigcomm/sigcomm2002/papers/bgplab.pdf.

[**Mahdavi 1997**] J. Mahdavi and S. Floyd, "TCP-Friendly Unicast Rate-Based Flow Control," unpublished note, Jan. 1997. http://www.psc.edu/networking/papers/tcp_friendly.html

[**Mainwaring 2002**] A.Mainwaring, R. Szewczyk, D. Culler, J. Anderson "Wireless Sensor Networks for Habitat Monitoring" *ACM International Workshop on Wireless Sensor Networks and Applications (WSNA*), 2002. http://citeseer.ist.psu.edu/mainwaring02wireless.html

[**Manelli 2001**] T. Manelli, "What Happened to Internet Appliances?" *PC World,* (April 2001), http://www.pcworld.com/news/article/0,aid,47184,00.asp

[**manet 2007**] IETF Mobile Ad-hoc Networks (manet) Working Group, http://www.ietf.org/html.charters/manet-charter.html

[**Maymounkov 2002**] P. Maymounkov and D. Mazières. "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric." *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02*), pp. 53–65, March 2002.

[**McAuley 1994**] A. McAuley, "Weighted Sum Codes for Error Detection and Their Comparison with Existing Codes," *IEEE/ACM Transactions on Networking,* Vol. 2, No. 1 (Feb. 1994), pp. 16–22.

[**McCumber 1991**] J. McCumber, "Information Systems Security: A Comprehensive Model," *Proceedings of the 14th National Computer Security Conference*, (Baltimore, MD), 1991.

[MCI 2004] MCI, "Terms and Conditions: Service Level Agreement," http://global.mci.com/terms/sla/

[**McKeown 1997a**] N. McKeown, M. Izzard, A. Mekkittikul,W. Ellersick, M. Horowitz, "The Tiny Tera: A Packet Switch Core," *IEEE Micro Magazine,* Jan.–Feb. 1997. http://tiny-tera.stanford.edu/~nickm/papers/HOTI_96.ps.

[**McKeown 1997b**] N. McKeown, "A Fast Switched Backplane for a Gigabit Switched Router," *Business Communications Review,* Vol. 27, No. 12. http://www.bcr.com/bcrmag/12/mckeown.htm

[**McKusik 1996**] M. K. McKusick, K. Bostic, M. Karels, and J. Quarterman, *The Design and Implementation of the 4.4BSD Operating System,* Addison-Wesley, Reading, MA, 1996.

[**McQuillan 1980**] J. McQuillan, I. Richer, E. Rosen, "The New Routing Algorithm for the Arpanet," *IEEE Transactions on Communications,* COM-28(5) (May 1980), pp. 711–719.

[**Medhi 1997**] D. Medhi and D. Tipper (eds.), Special Issue: Fault Management in Communication Networks, *Journal of Network and Systems Management,* Vol. 5. No. 2 (June 1997).

[**Metcalfe 1976**] R. M. Metcalfe and D. R. Boggs. "Ethernet: Distributed Packet Switching for Local Computer Networks," *Communications of the Association for Computing Machinery,* Vol. 19, No. 7, (July 1976), pp. 395–404. http://www.acm.org/classics/apr96/

[**Microsoft Player Media 2007**] Microsoft Windows Media homepage, http://www.microsoft.com/windows/windowsmedia/

[**Miller 1997**] M.A. Miller, *Managing Internetworks with SNMP,* 2nd ed., M & T Books, New York, 1997.

[**Mockapetris 1988**] P. V. Mockapetris, K. J. Dunlap, "Development of the Domain Name System," *Proceedings of SIGCOMM '88*, Stanford, CA, 1988. http://citeseer.nj.nec.com/mockapetris88development.html

[**Molinero-Fernandez 2002**] P. Molinaro-Fernandez, N. McKeown, H. Zhang, "Is IP Going to Take Over the World (of Communications)?" *Proc. 2002 ACM Hotnets*, http://www.acm.org/sigcomm/HotNets-I/papers/fernandez.pdf

[**Molle 1987**] M. L. Molle, K. Sohraby, and A. N. Venetsanopoulos, "Space-Time Models of Asynchronous CSMA Protocols for Local Area Networks," *IEEE Journal on Selected Areas in Communications,* Vol. 5, No. 6, (1987) pp. 956–968.

[**Molva 1999**] R. Molva, "Internet Security Architecture," Computer Networks and ISDN Systems, Vol. 31, No. 8 (1999), pp. 787-804.

[**Moore 2003**] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, "Inside the Slammer Worm," http://www.caida.org/outreach/papers/2003/sapphire2/

[**Mouly 1992**] M. Mouly, M. Pautet, *The GSM System for Mobile Communications*, Cell and Sys, Palaiseau, France, 1992.

[**Moy 1998**] J. Moy, *OSPF: Anatomy of An Internet Routing Protocol*, Addison-Wesley, Reading, MA, 1998.

[**mrouted 1996**] "mrouted," v3.8 of DVMRP routing software for various workstation routing platforms, ftp://parcftp.xerox.com/pub/net-research/ipmulti

[**Mukherjee 1997**] B. Mukherjee, Optical Communication Networks, McGraw-Hill, 1997.

[**Murphy 2003**] S. Murphy, "BGP Security Vulnerabilities Analysis," draft-ietf-idr-bgp-vuln-00.txt, June 2003, ftp://ftp.rfc-editor.org/in-notes/internet-drafts/draft-ietf-idr-bgp-vuln-00.txt

[**Nahum 2002**] E. Nahum, T. Barzilai, D. Kandlur, "Performance Issues in WWWServers," *IEEE/ACM Transactions on Networking*, 10(1), February 2002, http://www.research.ibm.com/people/n/nahum/publications/ton02-www-camera.pdf.

[**Nesbitt 2002**] S. Nesbitt, "Network Appliances," Jan. 2002, About.com, http://netappliances.about.com/cs/settopboxes/.

[**Net2Phone 2004**] http://www.net2phone.com/

[**Netcraft 2004**] The Netcraft Web Server Survey, Netcraft Web Site, http://www.netcraft.com/survey/

[**Netscape Cookie 1999**] Netscape Communications Corp., "Persistent Client State http Cookies," http://home.netscape.com/newsref/std/cookie_spec.html

[**Netscape SSL 1998**] Netscape Communications Corps, "Introduction to SSL," http://developer.netscape.com/docs/manuals/security/sslin/

[**Neuman 1994**] B. Neuman and T. Tso, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communication Magazine,* Vol. 32, No. 9 (Sept. 1994), pp. 33–38.

[**Neumann 1997**] R. Neumann, "Internet Routing Black Hole," *The Risks Digest: Forum on Risks to the Public in Computers and Related Systems,* Vol. 19, No. 12 (May 1997). http://catless.ncl.ac.uk/Risks/19.12.html#subj1.1

[**Nielsen 1997**] H. F. Nielsen, J. Gettys, A. Baird-Smith, E. Prud'hommeaux, H. W. Lie, and C. Lilley, "Network Performance Effects of HTTP/1.1, CSS1, and PNG," *W3C Document,* 1997 (also appears in *Proceedings of ACM SIGCOMM '97,* Cannes, France, pp. 155–166). http://www.acm.org/sigcomm/sigcomm97/papers/p102.html

[**NIST 1993**] National Institute of Standards and Technology, "Federal Information. Data Encryption Standard," Processing Standards Publication 46-2, 1993. http://www.itl.nist.gov/fipspubs/fip46-2.htm

[**NIST 1999**] National Institute of Standards and Technology, "Data Encryption Standard Fact Sheet," http://csrc.nist.gov/cryptval/des/des.txt

[**NIST 1999b**] National Institute of Standards and Technology, "Draft Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES), and Request for Comments," http://csrc.nist.gov/cryptval/des/fr990115.htm

[**NIST 2001**] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," Federal Information Processing Standards 197, Nov. 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[**Nmap 2007**] Nmap homepage, http://www.insecure.com/nmap

[**Nonnenmacher 1998**] J. Nonnenmacher, E. Biersak, D. Towsley, "Parity-Based Loss Recovery for Reliable Multicast Transmission," *IEEE/ACM Transactions on Networking,* Vol. 6, No. 4 (Aug. 1998), pp. 349–361. ftp://gaia.cs.umass.edu/pub/NBT97:fec.ps.gz

[**Nortel 2004**] Nortel Networks, Optivity Portfolio, http://www.nortelnetworks.com/products/01/optivity

[**NTIA 1998**] National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce, "Management of Internet names and addresses," Docket Number: 980212036-8146-02. http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm

[**Odlyzko 2003**] A. Odlyzko, "Internet Traffic Growth: Sources and Implications," A. M. Optical Transmission Systems and Equipment for WDM Networking II, *Proc. SPIE*,. 5247, 2003, pp. 1–15. http://www.dtc.umn.edu/~odlyzko/doc/itcom.internet.growth.pdf.

[**OpenView2007**] HP OpenView homepage, http://www.openview.hp.com/

[**Overpeer 2004**] Overpeer Inc., http://www.overpeer.com..

[**OSS 2007**] OSS Nokalva, "ASN.1 Resources," http://www.oss.com/asn1/

[**Padhye 2000**] J. Padhye, V. Firoiu, D. Towsley, J. Kurose, "Modeling TCP Reno Performance: A Simple Model and its Empirical Validation," *IEEE/ACM Transactions on Networking,* Vol. 8 No. 2 (April 2000). pp. 133–145.

[**Padhye 2001**] J. Padhye, S. Floyd, "On Inferring TCP Behavior," In *Proceedings of ACM SIGCOMM,* 2001, (San Diego, CA), 2001v. http://www.aciri.org/floyd/papers/tbit.pdf

[**Pan 1997**] P. Pan and H. Schulzrinne, "Staged Refresh Timers for RSVP," In 2nd Global Internet Conference, Phoenix, 1997. http://www.cs.columbia.edu/~pingpan/papers/timergi.pdf

[**Parekh 1993**] A. Parekh and R. Gallager, "A generalized processor sharing approach to flow control in integrated services networks: the single-node case," *IEEE/ACM Transactions on Networking,* Vol. 1, No. 3 (June 1993), pp. 344–357.

[**Partridge 1992**] C. Partridge, S. Pink, "An Implementation of the Revised Internet Stream Protocol (ST-2)," *Journal of Internetworking: Research and Experience* 3(1), March 1992. http://www.sics.se/cna/publications/ST-2.ps

[**Partridge 1998**] C. Partridge, et al. "A Fifty Gigabit per second IP Router," *IEEE/ACM Transactions on Networking,* Vol. 6, No. 3 (Jun. 1998), pp. 237–248.

[**Paxson 1997**] V. Paxson, "End-to-end Internet packet dynamics," *Proceedings of ACM SIGCOMM '97,* (Sept. 1997, Cannes, France). http://www.acm.org/sigcomm/sigcomm97/papers/p086.html

[**Perkins 1994**] A. Perkins, "Networking with Bob Metcalfe," *The Red Herring Magazine,* Nov. 1994. http://www.herring.com/mag/issue15/bob.html

[**Perkins 1998a**] C. Perkins, O. Hodson and V. Hardman, "A Survey of Packet Loss Recovery Techniques for Streaming Audio," *IEEE Network Magazine,* Sept./ Oct. 1998, pp. 40–47.

[**Perkins 1998b**] C. Perkins, *Mobile IP: Design Principles and Practice*, Addison-Wesley, Reading, MA, 1998.

[**Perkins 2000**] C. Perkins, *Ad Hoc Networking*, Addison-Wesley, Reading, MA, 2000.

[**Perlman 1999**] R. Perlman, *Interconnections: Bridges, Routers, Switches, and Internet-working Protocols,* 2nd ed., Addison-Wesley Professional Computing Series, Reading, MA, 1999.

[**PGPI 2007**] The International PGP Home Page, http://www.pgpi.org

[**Phifer 2000**] L. Phifer, "The Trouble with NA *T," The Internet Protocol Journal,* Vol. 3, No. 4 (Dec. 2000), http://www.cisco.com/warp/public/759/ipj_3-4/ipj_3-4_nat.html

[**Pickholtz 1982**] R. Pickholtz, D. Schilling, L. Milstein, "Theory of Spread Spectrum Communication—a Tutorial," *IEEE Transactions on Communications,* Vol. COM-30, No. 5 (May 1982), pp. 855–884.

[**Piscatello 1993**] D. Piscatello and A. Lyman Chapin, *Open Systems Networking,* Addison-Wesley, Reading, MA, 1993.

[**Point Topic 2006**] Point Topic Ltd., *World Broadband Statistics Q1 2006*, http://www.point-topic.com

[**QuickTime 2007**] QuickTime homepage, http://www.apple.com/quicktime

[**Quittner 1998**] J. Quittner, M. Slatalla, *Speeding the Net: The Inside Story of Netscape and How it Challenged Microsoft,* Atlantic Monthly Press, 1998.

[**Ramakrishnan 1990**] K. K. Ramakrishnan and Raj Jain, "A Binary Feedback Scheme for Congestion Avoidance in Computer Networks," *ACM Transactions on Computer Systems,* Vol. 8, No. 2 (May 1990), pp. 158–181.

[**Raman 1999**] S. Raman, S. McCanne, "A Model, Analysis, and Protocol Framework for Soft State-based Communication," *Proceedings of ACM SIGCOMM '99* (Boston, MA, Aug. 1999). http://www.acm.org/sigs/sigcomm/sigcomm99/papers/session1-2.html

[**Ramaswami 1998**] R. Ramaswami, K. Sivarajan, *Optical Networks: A Practical Perspective,* Morgan Kaufman Publishers, 1998

[**Ramjee 1994**] R. Ramjee, J. Kurose, D. Towsley, and H. Schulzrinne, "Adaptive Playout Mechanisms for Packetized Audio Applications in Wide-Area Networks," *Proceeding IEEE Infocom 94.* ftp://gaia.cs.umass.edu/pib/Ramj94:Adaptive.ps.Z

[**Rao 1996**] K. R. Rao and J. J. Hwang, *Techniques and Standards for Image, Video and Audio Coding,* Prentice Hall, Englewood Cliffs, NJ, 1996.

[**RAT 2007**] Robust Audio Tool, http://www-mice.cs.ucl.ac.uk/multimedia/software/rat/

[**Ratnasamy 2001**] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A Scalable Content-Addressable Network," *In Proceedings of ACM SIGCOMM,* 2001, (San Diego, CA), 2001. http://www.acm.org/sigcomm/sigcomm2001/p13.html

[**RealNetworks 2007**] RealNetworks homepage, http://www.realnetworks.com

[**Reid 2003**] N. Reid and R. Seide, *802.11 (Wi-Fi) Networking Handbook*, McGraw-Hill/ Osborne, New York, 2003.

A note on Internet Request for Comments (RFCs): Copies of Internet RFCs are maintained at multiple sites. The RFC URLs below all point into the RFC archive at the Information Sciences Institute (ISI), maintained at the RFC Editor of the Internet Society (the body that oversees the RFCs). Other RFC sites include http://www.faqs.org/rfcs, http://www.pasteur.fr/other/computer/RFC (located in France), and http://www.csl.sony.co.jp/rfc/ (located in Japan). Internet RFCs can be updated or obsoleted by later RFCs. We encourage you to check the sites listed above for the most up-to-date information. The RFC search facility at ISI, http://www.rfc-editor.org/rfc.html, will allow you to search for an RFC and show updates to that RFC.

[**RFC 001**] S. Crocker, "Host Software," RFC 001 (the *very first* RFC!). http://www.rfc-editor.org/rfc/rfc1.txt

[**RFC 741**] D. Cohen, "Specifications for the Network Voice Protocol NVP", RFC 741, Nov. 1977. ftp://ftp.rfc-editor.org/in-notes/rfc741.txt

[**RFC 768**] J. Postel, "User Datagram Protocol," RFC 768, Aug. 1980. http://www.rfc-editor.org/rfc/rfc768.txt

[**RFC 789**] E. Rosen, "Vulnerabilities of Network Control Protocols," RFC 789. http://www.rfc-editor.org/rfc/rfc789.txt

[**RFC 791**] J. Postel, "Internet Protocol: DARPA Internet Program Protocol Specification," RFC 791, Sept. 1981. http://www.rfc-editor.org/rfc/rfc791.txt

[**RFC 792**] J. Postel, "Internet Control Message Protocol," RFC 792, Sept. 1981. http://www.rfc-editor.org/rfc/rfc792.txt

[**RFC 793**] J. Postel, "Transmission Control Protocol," RFC 793, Sept. 1981. http://www.rfc-editor.org/rfc/rfc793.txt

[**RFC 801**] J. Postel, "NCP/TCP Transition Plan," RFC 801 Nov. 1981. http://www.rfc-editor.org/rfc/rfc801.txt

[**RFC 821**] J. Postel, "Simple Mail Transfer Protocol," RFC 821, Aug. 1982. http://www.rfc-editor.org/rfc/rfc821.txt Obsoleted by RFC 2821.

[**RFC 822**] D. H. Crocker, "Standard for the Format of ARPA Internet Text Messages," RFC 822, Aug. 1982. http://www.rfc-editor.org/rfc/rfc822.txt

[**RFC 826**] D. C. Plummer, "An Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," RFC 826, Nov. 1982. http://www.rfc-editor.org/rfc/rfc826.txt.

[**RFC 829**] V. Cerf, "Packet Satellite Technology Reference Sources," *RFC 829*, November 1982. http://www.rfc-editor.org/rfc/rfc829.txt

[**RFC 854**] J. Postel and J. Reynolds, "TELNET Protocol Specification," RFC 854. May 1993. http://www.rfc-editor.org/rfc/rfc854.txt

[**RFC 904**] D. Mills, "Exterior Gateway Protocol Formal Specification," RFC 904, Apr. 1984. http://www.rfc-editor.org/rfc/rfc904.txt

[**RFC 950**] J. Mogul, J. Postel, "Internet Standard Subnetting Procedure," RFC 950, Aug. 1985. http://www.rfc-editor.org/rfc/rfc950.txt.

[**RFC 959**] J. Postel and J. Reynolds, "File Transfer Protocol (FTP)," RFC 959, Oct. 1985. http://www.rfc-editor.org/rfc/rfc959.txt

[**RFC 977**] B. Kantor and P. Lapsley, "Network News Transfer Protocol," RFC 977, Feb. 1986. http://www.rfc-editor.org/rfc/rfc977.txt

[**RFC 1028**] J. Davin, J.D. Case, M. Fedor, M. Schoffstall, "A Simple Gateway Monitoring Protocol," RFC 1028, Nov. 1987, http://www.rfc-editor.org/rfc/rfc1028.txt.

[**RFC 1034**] P. V. Mockapetris, "Domain Names—Concepts and Facilities," RFC 1034, Nov. 1987. http://www.rfc-editor.org/rfc/rfc1034.txt

[**RFC 1035**] P. Mockapetris, "Domain Names—Implementation and Specification," RFC 1035, Nov. 1987. http://www.rfc-editor.org/rfc/rfc1035.txt

[**RFC 1058**] C. L. Hendrick, "Routing Information Protocol," RFC 1058, June 1988. http://www.rfc-editor.org/rfc/rfc1058.txt

[**RFC 1071**] R. Braden, D. Borman, and C. Partridge, "Computing The Internet Checksum," RFC 1071, Sept. 1988. http://www.rfc-editor.org/rfc/rfc1071.txt

[**RFC 1075**] D. Waitzman, C. Partridge, S. Deering, "Distance Vector Multicast Routing Protocol," RFC 1075, Nov. 1988. http://www.rfc-editor.org/rfc/rfc1075.txt.

[**RFC 1112**] S. Deering, "Host Extension for IP Multicasting," RFC 1112, Aug. 1989. http://www.rfc-editor.org/rfc/rfc1112.txt

[**RFC 1122**] R. Braden, "Requirements for Internet Hosts—Communication Layers," RFC 1122, Oct. 1989. http://www.rfc-editor.org/rfc/rfc1122.txt

[**RFC 1123**] R. Braden, ed., "Requirements for Internet Hosts—Application and Support," *RFC-1123*, October 1989. ftp://ftp.rfc-editor.org/in-notes/rfc1123.txt.

[**RFC 1142**] D. Oran, "OSI IS-IS Intra-domain Routing Protocol," RFC 1142, Feb. 1990, ftp://ftp.rfc-editor.org/in-notes/rfc1142.txt

[**RFC 1180**] T. Socolofsky and C. Kale, "A TCP/IP Tutorial," RFC 1180, Jan. 1991. http://www.rfc-editor.org/rfc/rfc1180.txt

[**RFC 1190**] C. Topolcic, "Experimental Internet Stream Protocol: Version 2 (ST-II)," RFC 1190, October 1990. ftp://ftp.rfc-editor.org/in-notes/rfc1190.txt

[**RFC 1191**] J. Mogul, S. Deering, "Path MTU Discovery," RFC 1191, November 1990, ftp://ftp.rfc-editor.org/in-notes/rfc1191.txt

[**RFC 1213**] K. McCloghrie, M. T. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II," RFC 1213, Mar. 1991. http://www.rfc-editor.org/rfc/rfc1213.txt

[**RFC 1256**] S. Deering, "ICMP Router Discovery Messages," RFC 1256, Sept. 1991. http://www.rfc-editor.org/rfc/rfc1256.txt.

[**RFC 1320**] R. Rivest, "The MD4 Message-Digest Algorithm," RFC 1320, Apr. 1992. http://www.rfc-editor.org/rfc/rfc1320.txt

[**RFC 1321**] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, Apr. 1992. http://www.rfc-editor.org/rfc/rfc1321.txt

[**RFC 1323**] V. Jacobson, S. Braden, and D. Borman, "TCP Extensions for High Performance," RFC 1323, May 1992. http://www.rfc-editor.org/rfc/rfc1323.txt

[**RFC 1332**] G. McGregor, "The PPP Internet Protocol Control Protocol (IPCP)," RFC 1332, May 1992. http://www.rfc-editor.org/rfc/rfc1332.txt

[**RFC 1378**] B. Parker, "The PPP AppleTalk Control Protocol (ATCP)," RFC 1378, Nov. 1992. http://www.rfc-editor.org/rfc/rfc1378.txt

[**RFC 1422**] S. Kent, "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management," RFC 1422, Feb. 1993. http://www.rfc-editor.org/rfc/rfc1422.txt

[**RFC 1510**] J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, Sept. 1993. http://www.rfc-editor.org/rfc/rfc1510.txt

[**RFC 1519**] V. Fuller, T. Li, J. Yu, K. Varadhan, "Classless inter-domain routing (CIDR)," RFC 1519, Sept. 1993. http://www.rfc-editor.org/rfc/rfc1519.txt

[**RFC 1542**] W. Wimer, "Clarifications and Extensions for the Bootstrap Protocol," RFC 1542, Oct. 1993. http://www.rfc-editor.org/rfc/rfc1542.txt

[**RFC 1547**] D. Perkins, "Requirements for an Internet Standard Point-to-Point Protocol," RFC 1547, Dec. 1993. http://www.rfc-editor.org/rfc/rfc1547.txt

[**RFC 1584**] J. Moy, "Multicast Extensions to OSPF," RFC 1584, Mar. 1994. http://www.rfc-editor.org/rfc/rfc1584.txt

[**RFC 1631**] K. Egevang, P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May 1994. http://www.rfc-editor.org/rfc/rfc1631.txt

[**RFC 1633**] R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture: an Overview," RFC 1633, June 1994. http://www.rfc-editor.org/rfc/rfc1633.txt

[**RFC 1636**] R. Braden, D. Clark, S. Crocker, C. Huitema, "Report of IAB Workshop on Security in the Internet Architecture," RFC 1636, Nov. 1994. http://www.rfc-editor.org/rfc/rfc1636.txt

[**RFC 1661**] W. Simpson (ed.), "The Point-to-Point Protocol (PPP)," RFC 1661, July 1994. http://www.rfc-editor.org/rfc/rfc1661.txt

[**RFC 1662**] W. Simpson (ed.), "PPP in HDLC-like framing," RFC 1662, July 1994. http://www.rfc-editor.org/rfc/rfc1662.txt

[**RFC 1700**] J. Reynolds and J. Postel, "Assigned Numbers," RFC 1700, Oct. 1994. http://www.rfc-editor.org/rfc/rfc1700.txt

[**RFC 1730**] M. Crispin, "Internet Message Access Protocol—Version 4," RFC 1730, Dec. 1994. http://info.internet.isi.edu/in-notes/rfc/files/rfc1730.txt.

[**RFC 1752**] S. Bradner, A. Mankin, "The Recommendations for the IP Next Generation Protocol," RFC 1752, Jan. 1995. http://www.rfc-editor.org/rfc/rfc1752.txt

[**RFC 1760**] N. Haller, "The S/KEY One-Time Password System," RFC 1760, Feb. 1995. http://www.rfc-editor.org/rfc/rfc1760.txt

[**RFC 1762**] S. Senum, "The PPP DECnet Phase IV Control Protocol (DNCP)," RFC 1762, Mar. 1995. http://www.rfc-editor.org/rfc/rfc1762.txt.

[**RFC 1771**] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, Mar. 1995. http://www.rfc-editor.org/rfc/rfc1771.txt

[**RFC 1772**] Y. Rekhter and P. Gross, "Application of the Border Gateway Protocol in the Internet," RFC 1772, Mar. 1995. http://www.rfc-editor.org/rfc/rfc1772.txt

[**RFC 1773**] P. Traina, "Experience with the BGP-4 protocol," RFC 1773, Mar. 1995. http://www.rfc-editor.org/rfc/rfc1773.txt.

[**RFC 1779**] S. Kille, "A String Representation of Distinguished Names," RFC 1779, Mar. 1995. http://www.rfc-editor.org/rfc/rfc1779.txt .Obsoleted by RFC 2253

[**RFC 1810**] J. Touch, "Report on MD5 Performance," RFC 1810, June 1995. http://www.rfc-editor.org/rfc/rfc1810.txt

[**RFC 1812**] F. Baker, ed., "Requirements for IP Version 4 Routers*," RFC-1812*, June 1995. ftp://ftp.rfc-editor.org/in-notes/rfc1812.txt.

[**RFC 1884**] R. Hinden, S. Deering, "IP Version 6: addressing architecture," RFC 1884, Dec. 1995. http://www.rfc-editor.org/rfc/rfc1884.txt. . Obsoleted by RFC 2373

[**RFC 1906**] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)," RFC 1906, Jan. 1996. http://www.rfc-editor.org/rfc/rfc1906.txt

[**RFC 1907**] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)," RFC 1907, Jan. 1996. http://www.rfc-editor.org/rfc/rfc1907.txt

[**RFC 1911**] G. Vaudreuil, "Voice Profile for Internet Mail," RFC 1911, Feb. 1996. http://www.rfc-editor.org/rfc/rfc1911.txt. Obsoleted by RFC 2421.

[**RFC 1918**] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, "Address Allocation for Private Internets," RFC 1918, February 1996. ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt

[**RFC 1930**] J. Hawkinson, T. Bates, "Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)," RFC 1930, March 1996. ftp://ftp.rfc-editor.org/in-notes/rfc1930.txt

[**RFC 1938**] N. Haller, C. Metz, "A One-Time Password System," RFC 1938, May 1996, ftp://ftp.rfc-editor.org/in-notes/rfc1938.txt

[RFC 1939] J. Myers and M. Rose, "Post Office Protocol—Version 3," RFC 1939, May 1996. http://www.rfc-editor.org/rfc/rfc1939.txt

[**RFC 1945**] T. Berners-Lee, R. Fielding, H. Frystyk, "Hypertext Transfer Protocol— HTTP/1.0," RFC 1945, May 1996 http://www.rfc-editor.org/rfc/rfc1945.txt

[**RFC 1994**] W., Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)," RFC 1994, Aug. 1996, ftp://ftp.rfc-editor.org/in-notes/rfc1994.txt

[**RFC 2001**] W. Stevens, "TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms," RFC 2001, Jan. 1997. http://www.rfc-editor.org/rfc/rfc2001.txt. Obsoleted by RFC 2581.

[**RFC 2003**] C. Perkins, "IP Encapsulation within IP," RFC 2003, Oct. 1996. http://www.rfc-editor.org/rfc/rfc2003.txt

[**RFC 2004**] C. Perkins, "Minimal Encapsulation within IP," RFC 2004, Oct. 1996. http://www.rfc-editor.org/rfc/rfc2004.txt.

[**RFC 2011**] K. McCloghrie, "SNMPv2 Management Information Base for the Internet Protocol using SMIv2," RFC 2011, Nov. 1996. http://www.rfc-editor.org/rfc/rfc2011.txt

[**RFC 2012**] K. McCloghrie, "SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2," RFC 2012, Nov. 1996. http://www.rfc-editor.org/rfc/rfc2012.txt

[**RFC 2013**] K. McCloghrie, "SNMPv2 Management Information Base for the User Data-gram Protocol using SMIv2," RFC 2013, Nov. 1996. http://www.rfc-editor.org/rfc/rfc2013.txt

[**RFC 2018**] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, "TCP Selective Acknowledgment Options," RFC 2018, Oct. 1996. http://www.rfc-editor.org/rfc/rfc2018.txt

[**RFC 2021**] S. Waldbusser, "Remote Network Monitoring Management Information Base Version 2 using SMIv2," RFC 2021, Jan. 1997. http://www.rfc-editor.org/rfc/rfc2021.txt

[**RFC 2045**] N. Freed, N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies," RFC 2045, Nov. 1996. http://www.rfc-editor.org/rfc/rfc2045.txt

[**RFC 2046**] N. Freed, N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types," RFC 2046, Nov. 1996. http://www.rfc-editor.org/rfc/rfc2046.txt

[**RFC 2048**] N. Freed, J. Klensin, J. Postel "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures," RFC 2048, Nov. 1996. http://www.rfc-editor.org/rfc/rfc2048.txt

[**RFC 2050**] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg, J. Postel, "Internet Registry IP Allocation Guidelines," RFC 2050, Nov. 1996. http://www.rfc-editor.org/rfc/rfc2050.txt

[**RFC 2060**] R. Crispin, "Internet Message Access Protocol—Version 4rev1," RFC 2060, Dec. 1996. http://www.rfc-editor.org/rfc/rfc2060.txt

[**RFC 2068**] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee, "Hypertext Transfer Protocol—HTTP/1.1," RFC 2068, Jan. 1997. http://www.rfc-editor.org/rfc/rfc2068.txt. Obsoleted by RFC 2616.

[**RFC 2104**] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, Feb. 1997. http://www.rfc-editor.org/rfc/rfc2104.txt

[**RFC 2109**] D. Kristol and L. Montulli, "HTTP State Management Mechanism," RFC 2109, Feb. 1997. http://www.rfc-editor.org/rfc/rfc2109.txt

[**RFC 2131**] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131, Mar. 1997. http://www.rfc-editor.org/rfc/rfc2131.txt

[**RFC 2136**] P. Vixie, S. Thomson,Y. Rekhter, and J. Bound, "Dynamic Updates in the Domain Name System," RFC 2136, Apr. 1997. http://www.rfc-editor.org/rfc/rfc2136.txt

[**RFC 2153**] W. Simpson, "PPP Vendor Extensions," RFC 2153, May 1997. http://www.rfc-editor.org/rfc/rfc2153.txt

[**RFC 2186**] K. Claffy and D. Wessels, "Internet Caching Protocol (ICP), version 2," RFC 2186, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2186.txt

[**RFC 2189**] A. Ballardie, "Core Based Trees (CBT version 2) Multicast Routing: Protocol Specification," RFC 2189, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2189.txt

[**RFC 2201**] A. Ballardie, "Core Based Trees (CBT) Multicast Routing Architecture," RFC 2201, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2201.txt.

[**RFC 2205**] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification," RFC 2205, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2205.txt

[**RFC 2210**] J. Wroclawski, "The Use of RSVP with IETF Integrated Services," RFC 2210, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2210.txt

[**RFC 2211**] J. Wroclawski, "Specification of the Controlled-Load Network Element Ser-vice," RFC 2211, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2211.txt

[**RFC 2212**] S. Shenker, C. Partridge, R. Guerin, "Specification of Guaranteed Quality of Service," RFC 2212, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2212.txt

[**RFC 2215**] S. Shenker, J. Wroclawski, "General Characterization Parameters for Integrated Service Network Elements," RFC 2215, Sept. 1997. http://www.rfc-editor.org/rfc/rfc2215.txt

[**RFC 2225**] M Laubach, J. Halpern, "Classical UP and ARP over ATM," RFC 2225, April 1998. http://www.rfc-editor.org/rfc/rfc2225.txt

[**RFC 2246**] T. Dierks and C. Allen, "The TLS Protocol," RFC 2246, Jan. 1998. http://www.rfc-editor.org/rfc/rfc2246.txt

[**RFC 2253**] M. Wahl, S. Kille, T. Howes, "Lightweight Directory Access Protocol (v3)," RFC 2253, Dec. 1997. http://www.rfc-editor.org/rfc/rfc2253.txt

[**RFC 2284**] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP," RFC 2284, March 1998, ftp://ftp.rfc-editor.org/in-notes/rfc2284.txt

[**RFC 2326**] H. Schulzrinne, A. Rao, R. Lanphier, "Real Time Streaming Protocol (RTSP)," RFC 2326, Apr. 1998. http://www.rfc-editor.org/rfc/rfc2326.txt

[**RFC 2328**] J. Moy, "OSPF Version 2," RFC 2328, Apr. 1998. http://www.rfc-editor.org/rfc/rfc2328.txt

[**RFC 2362**] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification," RFC 2362, June 1998. http://www.rfc-editor.org/rfc/rfc2362.txt

[**RFC 2373**] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture," RFC 2373, July 1998. http://www.rfc-editor.org/rfc/rfc2373.txt

[**RFC 2400**] J. Postel, J. Reynolds, "Internet Official Protocol Standards," RFC 2400, Sept. 1998. http://www.rfc-editor.org/rfc/rfc2400.txt. Obsoleted by RFC 2500.

[**RFC 2401**] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2401.txt

[**RFC 2402**] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2402.txt

[**RFC 2405**] C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm with Explicit IV," RFC 2405, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2405.txt

[**RFC 2406**] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2406.txt

[**RFC 2407**] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2407.txt

[**RFC 2408**] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2408.txt.

[**RFC 2409**] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2409.txt

[**RFC 2411**] R. Thayer, N. Doraswamy, R. Glenn, "IP Security Document Road Map," RFC 2411, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2411.txt

[**RFC 2420**] H. Kummert, "The PPP Triple-DES Encryption Protocol (3DESE)," RFC 2420, Sept. 1998. http://www.rfc-editor.org/rfc/rfc2420.txt

[**RFC 2421**] G. Vaudreuil, G. Parsons, "Voice Profile for Internet Mail—version 2," RFC 2421, Sept. 1998. http://www.rfc-editor.org/rfc/rfc2421.txt

[**RFC 2427**] C. Brown, A. Malis, "Multiprotocol Interconnect over Frame Relay," RFC 2427, Sept. 1998. http://www.rfc-editor.org/rfc/rfc2427.txt

[**RFC 2437**] B. Kaliski, J. Staddon, "PKCS #1: RSA Cryptography Specifications, Version 2," RFC 2437, Oct. 1998. http://www.rfc-editor.org/rfc/rfc2437.txt

[**RFC 2453**] G. Malkin, "RIP Version 2," RFC 2453, Nov. 1998. http://www.rfc-editor.org/rfc/rfc2453.txt.

[**RFC 2460**] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998. http://www.rfc-editor.org/rfc/rfc2460.txt

[**RFC 2463**] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)," RFC 2463, Dec. 1998. http://www.rfc-editor.org/rfc/rfc2463.txt

[**RFC 2474**] K. Nicols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474, Dec. 1998. http://www.rfc-editor.org/rfc/rfc2474.txt

[**RFC 2475**] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang,W. Weiss, "An Architecture for Differentiated Services," RFC 2475, Dec. 1998. http://www.rfc-editor.org/rfc/rfc2475.txt

[**RFC 2481**] K. K. Ramakrishnan and S. Floyd, "A Proposal to Add Explicit Congestion Notification (ECN) to IP," RFC 2481, Jan. 1999. http://www.rfc-editor.org/rfc/rfc2481.txt

[**RFC 2500**] J. Reynolds, R. Braden, "Internet Official Protocol Standards," RFC 2500, June 1999. http://www.rfc-editor.org/rfc/rfc2500.txt.

[**RFC 2535**] D. Eastlake, "Domain Name System Security Extensions," RFC 2535, Mar. 1999, ftp://ftp.rfc-editor.org/in-notes/rfc2535.txt

[**RFC 2578**] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)," RFC 2578, Apr. 1999. http://www.rfc-editor.org/rfc/rfc2578.txt

[**RFC 2579**] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Textual Conventions for SMIv2," RFC 2579, Apr. 1999. http://www.rfc-editor.org/rfc/rfc2579.txt

[**RFC 2580**] K. McCloghrie, D. Perkins, J. Schoenwaelder, "Conformance Statements for SMIv2," RFC 2580, Apr. 1999. http://www.rfc-editor.org/rfc/rfc2580.txt

[**RFC 2581**] M. Allman, V. Paxson,W. Stevens, " TCP Congestion Control," RFC 2581, Apr. 1999. http://www.rfc-editor.org/rfc/rfc2581.txt

[**RFC 2582**] S. Floyd, T. Henderson, "The NewReno Modification to TCP's Fast Recovery Algorithm," RFC 2582, April 1999.. ftp://ftp.isi.edu/in-notes/rfc2582.txt

[**RFC 2597**] J. Heinanen, F. Baker,W. Weiss, J. Wroclawski, "Assured Forwarding PHB Group," RFC 2597, June 1999. http://www.rfc-editor.org/rfc/rfc2597.txt.

[**RFC 2598**] V. Jacobson, K. Nichols, K. Poduri, "An Expedited Forwarding PHB," RFC 2598, June 1999. http://www.rfc-editor.org/rfc/rfc2598.txt

[**RFC 2616**] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, R. Feilding, "Hypertext Transfer Protocol—HTTP/1.1," RFC 2616, June 1999. http://www.rfc-editor.org/rfc/rfc2616.txt

[**RFC 2638**] K. Nichols, V. Jacobson, L. Zhang, "A Two-bit Differentiated Services Architecture for the Internet," RFC 2638, July 1999. http://www.rfc-editor.org/rfc/rfc2638.txt

[**RFC 2644**] D. Senie, "Changing the Default for Directed Broadcasts in Router," RFC 2644, Aug. 1999. http://www.rfc-editor.org/rfc/rfc2644.txt

[**RFC 2663**] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663. http://www.rfc-editor.org/rfc/rfc2663.txt

[**RFC 2715**] D. Thaler, "Interoperability Rules for Multicast Routing Protocols," RFC 2715, Oct. 1999. http://www.rfc-editor.org/rfc/rfc2715.txt

[**RFC 2716**] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol," RFC 2716, Oct. 1999, ftp://ftp.rfc-editor.org/in-notes/rfc2716.txt

[**RFC 2733**] J. Rosenberg, H. Schulzrinne, "An RTP Payload Format for Generic Forward Error Correction," RFC 2733, Dec. 1999. http://www.rfc-editor.org/rfc2733.txt

[**RFC 2821**] J. Klensin, Eed., "Simple Mail Transfer Protocol," RFC 2821, April 2001, http://www.rfc-editor.org/rfc/rfc2821.txt

[**RFC 2827**] P. Ferguson, D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing," RFC 2827. May 2000. http://www.rfc-editor.org/rfc/rfc2827.txt

[**RFC 2893**] R. Gilligan, E. Nordmark "Transition Mechanisms for IPv6 Hosts and Routers," RFC 2893, Aug. 2000. http://www.rfc-editor.org/rfc/rfc2893.txt

[**RFC 2961**] L. Berger, D. Gan, G. Swallow, P. Pan, F. Tommasi, S. Molendini, "RSVP Refresh Overhead Reduction Extensions," RFC 2961, April 2001, ftp://ftp.rfc-editor.org/in-notes/rfc2961.txt

[**RFC 2988**] V. Paxson, M. Allman, "Computing TCP's Retransmission Timer," RFC 2988, Nov., 2000. ftp://ftp.isi.edu/in-notes/rfc2988.txt

[**RFC 3022**] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," RFC 3022, Jan. 2001. http://www.rfc-editor.org/rfc/rfc3022.txt

[**RFC 3031**] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031, Jan. 2001. ftp://ftp.rfc-editor.org/in-notes/rfc3031.txt.

[**RFC 3032**] E. Rosen, D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li, A. Conta, "MPLS Label Stack Encoding," RFC 3032, Jan. 2001. ftp://ftp.rfc-editor.org/in-notes/rfc3032.txt

[**RFC 3052**] M. Eder, S. Nag, "Service Management Architectures Issues and Review," RFC 3052, Jan. 2001, http://www.rfc-editor.org/rfc/rfc3052.txt

[**RFC 3139**] L. Sanchez, K. McCloghrie, J. Saperia, "Requirements for Configuration Management of IP-Based Networks, RFC 3139, June 2001, http://www.rfc-editor.org/rfc/rfc3139.txt

[**RFC 3209**] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC 3209, Dec. 2001. ftp://ftp.rfc-editor.org/in-notes/rfc3209.txt.

[**RFC 3221**] G. Huston, "Commentary on Inter-Domain Routing in the Internet," RFC 3221, December 2001. ftp://ftp.rfc-editor.org/in-notes/rfc3221.txt

[**RFC 3232**] J. Reynolds, "Assigned Numbers: RFC 1700 is Replaced by an Online Database," RFC 3232, January 2002, http://www.rfc-editor.org/rfc/rfc3232.txt

[**RFC 3260**] D. Grossman, "New Terminology and Clarifications for Diffserv," RFC 3260, April 2002. ftp://ftp.rfc-editor.org/in-notes/rfc3260.txt

[**RFC 3261**] J. Rosenberg, H. Schulzrinne, G. Carmarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, July 2002. http://www.rfc-editor.org/rfc/rfc3261.txt

[**RFC 3344**] C. Perkins, ed., "IP Mobility Support for IPv4," *RFC 3344*, October 2002. ftp://ftp.rfc-editor.org/in-notes/rfc3344.txt

[**RFC 3346**] J. Boyle, V. Gill, A. Hannan, D. Cooper, D. Awduche, B. Christian, W. S. Lai, "Applicability Statement for Traffic Engineering with MPLS," RFC 3346, Aug. 2002. ftp://ftp.rfc-editor.org/in-notes/rfc3346.txt

[**RFC 3376**] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, "Internet Group Management Protocol, Version 3," RFC 3376, October 2002. ftp://ftp.rfc-editor.org/in-notes/rfc3376.txt

[**RFC 3390**] M. Allman, S. Floyd, C. Partridge, "Increasing TCP's Initial Window," RFC 3390, October 2002, ftp://ftp.rfc-editor.org/in-notes/rfc3390.txt.

[**RFC 3410**] J. Case, R. Mundy, D. Partain, D. Partain, "Introduction and Applicability Statements for Internet Standard Management Framework," RFC 3410, December, 2002, ftp://ftp.rfc-editor.org/in-notes/rfc3410.txt

[**RFC 3411**] D. Harrington R. Presuhn B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," RFC 3411, December 2002, ftp://ftp.rfc-editor.org/in-notes/rfc3411.txt

[**RFC 3414**] U. Blumenthal, U. Blumenthal, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," RFC 3414, December 2002,

[**RFC 3415**] B. Wijnen, R. Presuhn, K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)," RFC 3415, December 2002. ftp://ftp.rfc-editor.org/in-notes/rfc3415.txt

[**RFC 3416**] R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)," December 2002, ftp://ftp.rfc-editor.org/in-notes/rfc3416.txt

[**RFC 3468**] L. Andersson, G. Swallow, "The Multiprotocol Label Switching (MPLS) Working Group Decision on MPLS Signaling Protocols," RFC 3468, Feb. 2003. ftp://ftp.rfc-editor.org/in-notes/rfc3468.txt

[**RFC 3469**] V. Sharma, Ed., F. Hellstrand, Ed, "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery," RFC 3469, Feb. 2003. ftp://ftp.rfc-editor.org/in-notes/rfc3469.txt

[**RFC 3550**] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: ATransport Protocol for Real-Time Applications," RFC 3550, July 2003, ftp://ftp.rfc-editor.org/in-notes/rfc3550.txt

[**RFC 3569**] S. Bhattacharyya (ed.), "An Overview of Source-Specific Multicast (SSM)," RFC 3569, July 2003, ftp://ftp.rfc-editor.org/in-notes/rfc3569.txt.

[**RFC 3588**] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol," Sept. 2003, ftp://ftp.rfc-editor.org/in-notes/rfc3588.txt

[**RFC 3600**] J. Reynolds, 6 S. Ginoza, 6, "Internet Official Protocol Standards," RFC 3600, November 2003, ftp://ftp.rfc-editor.org/in-notes/rfc3600.txt

[**RFC 3649**] S. Floyd, "HighSpeed TCP for Large Congestion Windows," RFC 3649, December 2003, ftp://ftp.rfc-editor.org/in-notes/rfc3649.txt.

[**Rhee 1998**] I. Rhee, "Error Control Techniques for Interactive Low-bit Rate Video Transmission over the Internet," *Proceedings ACM SIGCOMM'98,* Vancouver BC, (Aug. 31–Sept. 4, 1998). http://www.acm.org/sigcomm/sigcomm98/tp/abs_24.html

[**Roberts 1967**] L. Roberts, T. Merril, "Toward a Cooperative Network of Time-Shared Computers," *AFIPS Fall Conference,* Oct. 1966.

[**Rom 1990**] R. Rom, M. Sidi, *Multiple Access Protocols: Performance and Analysis,* Springer-Verlag, New York, 1990.

[Root Servers 2007] http://www.root-servers.org/

[**Rose 1996**] M. Rose, *The Simple Book: An Introduction to Internet Management, Revised Second Edition,* Prentice Hall, Englewood Cliffs, NJ, 1996.

[**Rosenberg 2000**] J. Rosenberg, L. Qiu, H. Schulzrinne, "Integrating Packet FEC into Adaptive Playout Buffer Algorithms on the Internet," *IEEE INFOCOM 2000* (Tel Aviv, 2000).

[**Ross 1995**] K. W. Ross, *Multiservice Loss Models for Broadband Telecommunication - Networks,* Springer, Berlin, 1995.

[**Ross 2007**] K. W. Ross, PowerPoint slides on network security, http://cis.poly.edu/~ross/.

[**Rowston 2001**] A. Rowston, and P. Druschel, "Pastry: Scalable, Distributed Object Location and Routing for Large-Scale Peer-to-Peer Systems," in *Proceedings of IFIP/ACM Middleware 2001*, 2001, Heidelberg, Germany, 2001.

[**RSA 1978**] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* Vol. 21, No. 2, pp. 120–126, Feb. 1978.

[**RSA Challenge 2002**] RSA Data Security Inc., "What is the RSA Secret Key Challenge?" http://www.rsasecurity.com/rsalabs/faq/2-4-4.html

[**RSA FAQ 2007**] RSA Inc., "RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1," http://www.rsasecurity.com/rsalabs/faq

[**RSA Fast 2007**] RSA Laboratories, "How fast is RSA?" http://www.rsasecurity.com/rsalabs/faq/3-1-2.html

[**RSA Key 2007**] RSA Laboratories, "How large a key should be used in the RSA Crypto system?" http://www.rsasecurity.com/rsalabs/faq/3-1-5.html

[**Rubenstein 1998**] D. Rubenstein, J. Kurose, D. Towsley "Real-Time Reliable Multicast Using Proactive Forward Error Correction," *Proceedings of NOSSDAV '98* (Cambridge, UK, July 1998). http://gaia.cs.umass.edu/pub/Rubenst98:proact.ps.gz

[**Rubin 2001**] A. Rubin, White-Hat Security Arsenal: Tackling the Threats, Addison-Wesley, 2001.

[**Saltzer 1984**] J. Saltzer, D. Reed, D. Clark, "End-to-End Arguments in System Design," *ACM Transactions on Computer Systems (TOCS),* 2(4) (November 1984)..

[**Saroiu 2002**] S. Saroiu, K. Gummadi, R. Dunn, S. Gribble, H. Levy, "An Analysis of Internet Content Delivery Systems," *Proc. Usenix OSDI 2002*, pp. 315–328. http://www.usenix.org/events/osdi02/tech/saroiu/saroiu_html/index.html

[**Savage 1999**] S. Savage, A. Collins, E. Hoffman, J. Snell, T. Anderson, "The End-to-End Effects of Internet Path Selection," in *Proceedings of 1999 ACM SIGCOM* M, Boston, MA, September 1999

[**Savage 2000**] S. Savage, D. Wetherall, A. Karlin, T. Anderson, "Practical Network Support for IP Traceback, *Proceedings of the 2000 ACM SIGCOMM Conference*, (Stockholm, Sweden), August 2000, pp. 295–306, http://www.cs.washington.edu/homes/savage/papers/Sigcomm00.pdf

[**Saydam 1996**] T. Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management," *Journal of Networks and System Management,* Vol. 4, No. 4 (Dec. 1996), pp. 345–348.

[Schneier 1995] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* John Wiley and Sons, 1995.

[**Schulzrinne 1997**] H. Schulzrinne, "A Comprehensive Multimedia Control Architecture for the Internet," *NOSSDAV'97 (Network and Operating System Support for Digital Audio and Video),* St. Louis, Missouri; May 19, 1997.
http://www.cs.columbia.edu/~hgs/papers/Schu9705_Comprehensive.ps.gz

[**Schulzrinne-RTP 2007**] Henning Schulzrinne's RTP site, http://www.cs.columbia.edu/~hgs/rtp

[**Schulzrinne-RTSP 2007**] Henning Schulzrinne's RTSP site,
http://www.cs.columbia.edu/~hgs/rtsp

[**Schulzrinne-SIP 2007**] Henning Schulzrinne's SIP site, http://www.cs.columbia.edu/~hgs/sip

[**Schurmann 1996**] G. Schurmann, "Multimedia Mail," *ACM Multimedia Systems,* Oct. 1996, pp. 281–295.

[**Schwartz 1977**] M. Schwartz, *Computer-Communication Network Design and Analysis*, Prentice-Hall, Englewood Cliffs, N.J., 1997.

[**Schwartz 1980**] M. Schwartz, *Information, Transmission, Modulation, and Noise,* McGraw Hill, NY, NY 1980.

[**Schwartz 1982**] M. Schwartz, "Performance Analysis of the SNA Virtual Route Pacing Control," *IEEE Transactions on Communications,* Vol. COM-30, No. 1, (Jan. 1982), pp. 172–184.

[**Schwiebert 2001**] L. Schwiebert, S. Gupta, J. Weinmann, "Research Challenges in Wireless Networks of Biomedical Sensors," *ACM Mobicom 2001*, 2001, pp. 151-165.
http://citeseer.ist.psu.edu/schwiebert01research.html

[**Scourias 2001**] J. Scourias, T. Farley, "Overview of the Global System for Mobile Communications: GSM." http://www.privateline.com/PCS/GSM0.html

[**Segaller 1998**] S. Segaller, *Nerds 2.0.1, A Brief History of the Internet,* TV Books, New York, 1998.

[**Semeria 1996**] C. Semeria, "Understanding IP addressing: Everything you ever wanted to know," http://www.3com.com/nsc/501302s.html

[**Shacham 1990**] N. Shacham, P. McKenney, "Packet Recovery in High-Speed Networks Using Coding and Buffer Management," *Proc. IEEE Infocom Conference* (San Francisco, 1990), pp. 124–131..

[**Sharma 1997**] Puneet Sharma, Deborah Estrin, Sally Floyd, Van Jacobson, "Scalable Timers for Soft State Protocols," *Proc. IEEE Infocom '97 Conference,* Apr. 1997 (Kobe, Japan).

[**Shipley 2001**] P. Shipley, "Open WLANS: The Early Results of War Driving,"
http://www.dis.org/filez/openlans.pdf

[**Sidor 1998**] D. Sidor, "TMN Standards: Satisfying Today's Needs While Preparing for Tomorrow," *IEEE Communications Magazine,* Vol. 36, No. 3 (Mar. 1998), pp. 54–64.

[**Singh 1999**] S. Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scotsto Quantum Cryptography,* Doubleday Press, 1999.

[**SIP Software 2007**] H. Schulzrinne Software Package site, http://www.cs.columbia.edu/IRT/software

[**Skype 2007**] Skype homepage, www.skype.com

[**SMIL 2007**] W3C Synchronized Multimedia homepage, http://www.w3.org/AudioVideo

[**Snoeren 2001**] A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, S. Kent, W. T. Strayer, "Hash-Based IP Traceback," *Proceedings of the 2001 ACM Sigcomm*, http://www.acm.org/sigcomm/sigcomm2001/p1-snoeren.pdf

[**Snort 2007**] Sourcefire Inc., Snort homepage, http://www.snort.org/

[**Solari 1997**] S. J. Solari, *Digital Video and Audio Compression,* McGraw Hill, NY, NY, 1997.

[**Solensky 1996**] F. Solensky, "IPv4 Address Lifetime Expectations," in *IPng: Internet Protocol Next Generation* (S. Bradner, A. Mankin, ed), Addison-Wesley, Reading, MA, 1996.

[**Spragins 1991**] J. D. Spragins, *Telecommunications Protocols and Design,* Addison-Wesley, Reading, MA, 1991.

[**Sprint 2007**] Sprint Corp., "Dedicated Internet Access Service Level Agreements," www.sprint.com/business/resources/dedicated_internet_access.pdf

[**Spurgeon 2002**] C. Spurgeon, "Charles Spurgeon's Ethernet Web Site," http://wwwhost.ots.utexas.edu/ethernet/ethernet-home.html

[**Srinivasan 1999**] V. Srinivasan and G. Varghese, "Fast Address Lookupp Using Controlled Prefix Expansion," *ACM Transactions Computer Systems*, Vol. 17, No. 1 (Feb 1999), pp. 1–40.

[**Stallings 1993**] W. Stallings, *SNMP, SNMP v2, and CMIP The Practical Guide to Network Management Standards,* Addison-Wesley, Reading, MA, 1993.

[**Stallings 1999**] W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2,* Addison-Wesley, Reading, MA, 1999.

[**Steinder 2002**] M. Steinder, A. Sethi, "Increasing robustness of fault localization through analysis of lost, spurious, and positive symptoms," in *Proc. IEEE INFOCOM*, 2002. http://www.ieee-infocom.org/2002/papers/665.pdf

[**Stevens 1990**] W. R. Stevens, *Unix Network Programming,* Prentice-Hall, Englewood Cliffs, NJ.

[**Stevens 1994**] W. R. Stevens, *TCP/IP Illustrated, Vol. 1: The Protocols,* Addison-Wesley, Reading, MA, 1994.

[**Stevens 1997**] W.R. Stevens, *Unix Network Programming, Volume 1: Networking APIs-Sockets and XTI,* 2nd edition, Prentice-Hall, Englewood Cliffs, NJ, 1997.

[**Stewart 1999**] J. Stewart, *BGP4: Interdomain Routing in the Internet,* Addison-Wesley, 1999..

[**Stoica 2001**] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," In *Proceedings of ACM SIGCOMM,* 2001, (San Diego, CA), 2001. http://www.acm.org/sigcomm/sigcomm2001/p12.html

[**Stoll 1995**] C. Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Pocket Books, 1995.

[**Stone 1998**] J. Stone, M. Greenwald, C. Partridge, and J. Hughes, "Performance of Check-sums and CRC's Over Real Data," *IEEE/ACM Transactions on Networking,* Vol. 6, No. 5 (Oct. 1998), pp 529–543

[**Stone 2000**] J. Stone, C. Partridge, "When Reality and the Checksum Disagree," *Proceedings of ACM SIGCOMM '00,* (Stockholm, Sweden, Aug. 2000).

[**Strayer 1992**] W. T. Strayer, B. Dempsey, A. Weaver, *XTP: The Xpress Transfer Protocol,* Addison-Wesley, Reading, MA, 1992.

[**Stubblefield 2002**] A. Stubblefield, J. Ioannidis, A. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," *Proceedings of the 2002 Network and Distributed Systems Security Symposium* (2002), 17–22. http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

[**Subramanian 2000**] M. Subramanian, *Network Management: Principles and Practice,* Addison-Wesley, Reading, MA, 2000.

[**Subramanian 2002**] L. Subramanian, S. Agarwal, J. Rexford, R. Katz, "Characterizing the Internet Hierarchy from Multiple Vantage Points," *Proc. 2002 IEEE Infocom*.

[**Sun 2007**] Sun Microsystems, "Solistice Enterprise Manager," http://www.sun.com/software/solstice/sem/

[**Sunshine 1978**] C. Sunshine and Y. K. Dalal, "Connection Management in Transport Protocols," *Computer Networks,* North-Holland, Amsterdam, 1978.

[**T-Mobile 2004**] T-Mobile HotSpot US Location Map, http://locations.hotspot.t-mobile.com

[**Tangmunarunkit 2001**] H. Tangmunarunkit, R. Govindan, D. Estrin, S. Shenker, "The Impact of Routing Policy on Internet Paths," *Proceedings 2001 IEEE INFOCOM*, Alaska, April 2001. http://www.isi.edu/~hongsuda/publication/info2001.ps

[**TechnOnLine 2004**] TechOnLine, "Protected Wireless Networks," online webcast tutorial, http://www.techonline.com/community/tech_topic/internet/21752

[**Teleography 2002**] Teleography—a research division of Pirmetrica, "WorldCom Controls the Most Internet Bandwidth, Connections, and Revenue," http://www.telegeography.com/press/releases/2002/10-jul-2002.html.

[**Thaler 1997**] D. Thaler and C. Ravishankar, "Distributed Center-Location Algorithms," *IEEE Journal on Selected Areas in Communications,* Vol. 15, No. 3, (Apr. 1997), pp. 291–303.

[**Think 2007**] Technical History of Network Protocols, "Cyclades," http://www.cs.utexas.edu/users/chris/think/Cyclades/index.shtml

[**Thinplanet 2002**] Thinplanet homepage, http://www.thinplanet.com/

[**Thottan 1998**] M. Thottan and C. Ji, "Proactive Anomaly Detection Using Distributed Intelligent Agents," *IEEE Network Magazine,* Vol. 12, No. 5 (Sept./ Oct. 1998), pp. 21–28.

[**Tobagi 1990**] F. Tobagi, "Fast Packet Switch Architectures for Broadband Integrated Networks," *Proc. of the IEEE,* Vol. 78, No. 1 (Jan. 1990), pp. 133–167..

[**Turner 1986**] J. Turner, "New Directions in Communications (or Which Way to the Information Age?)," *Proceedings of the Zürich Seminar on Digital Communication,* (Zurich, Switzerland, Mar. 1986), pp. 25–32.

[**Turner 1988**] J. S. Turner "Design of a Broadcast packet switching network," *IEEE Transactions on Communications,* Vol. 36, No. 6 (June 1988), pp. 734–743.

[**Utah 2004**] Utah Division of Corporations and Commercial Codes, Digital Signature Licensing Information, http://www.commerce.state.ut.us/corporat/dsmain.htm

[**Varghese 1997**] G. Varghese and A. Lauck, "Hashed and Hierarchical Timing Wheels: Efficient Data Structures for Implementing a Timer Facility," *IEEE/ACM Transactions on Networking,* Vol. 5, No. 6, (Dec. 1997), pp. 824–834.

[**Verisign 2007**] http://www.verisign.com

[**Verizon 2007**] Verizon Communication, *Verizon Broadband Anytime.* http://www.verizon.net/wifi/

[**Verma 2001**] D.C. Verma, *Content Distribution Networks: An Engineering Approach,* John Wiley, 2001.

[**Viterbi 1995**] A. Viterbi, *CDMA: Principles of Spread Spectrum Communication,* Addison-Wesley, Reading, MA, 1995.

[**VON 2004**] Voice on the Net, http://www.von.com

[**von Lohmann 2003**] F. von Lohmann, "Peer-to-Peer File Sharing and Copyright Law: A Primer for Developers," *2nd International Workshop on Peer-to-Peer Systems (IPTPS '03),* Berkeley, 2003. http://iptps03.cs.berkeley.edu/final-papers/copyright.pdf

[**Voydock 1983**] V. L. Voydock, and S.T. Kent, "Security Mechanisms in High-Level Net-work Protocols," *ACM Computing Surveys* Vol. 15, No. 2 (June 1983), pp. 135–171.

[**W3C 1995**] The World Wide Web Consortium, "A Little History of the World Wide Web," 1995. http://www.w3.org/History.html

[**WAP 2004**] WAP Forum, "WAP 2.0 Technical White Paper," http://www.wapforum.org/what/whitepapers.htm.

[**Wakeman 1992**] Ian Wakeman, Jon Crowcroft, Zheng Wang, and Dejan Sirovica, "Layering Considered Harmful," *IEEE Network,* Jan. 1992, pp. 20–24.

[**Waldvogel 1997**] M. Waldvogel et al., "Scalable High Speed IP Routing Lookup," *Proceedings of ACM SIGCOMM '97* (Cannes, France, Sept. 1997). http://www.acm.org/sigs/sigcomm/sigcomm97/papers/p182.html

[**Walker 2000**] J. Walker, "IEEE P802.11 Wireless LANs, Unsafe at Any Key Size; An Analysis of the WEP Encapsulation," Oct. 2000, http://www.drizzle.com/~aboba/IEEE/0-362.zip

[**Weatherspoon 2000**] S. Weatherspoon, "Overview of IEEE 802.11b Security," *Intel Technology Journal,* (2nd Quarter 2000), http://developer.intel.com/technology/itj/q22000/articles/art_5.htm

[**Web ProForum 1999**] Web ProForum, "Tutorial on H.323," 1999. http://www.webproforum.com/h323/index.html

[**Wei 2004**] W. Wei, B. Wang, J. Kurose, D. Towsley, "Detecting and Distinguishing Wired and Wireless Packet Losses in an End-End Connection," *Technical Report*, Dept. Computer Science, University of Massachusetts, 2004.

[**Wei 2006a**] W. Wei, C. Zhang, H. Zang, J. Kurose, and D. Towsley "Inference and Evaluation of Split-Connection Approaches in Cellular Data Networks," *Proc. Active and Passive Measurement Workshop,* (Adelaide, Australlia, Mar. 2006).

[**Wei 2006b**] D. X. Wei, C. Jin, S. H. Low, S. Hegde, "FAST TCP: Motivation, Architecture, Algorithms, Performance," IEEE/ACM Transactions on Networking, Vol.14, No.6, pp.1246-1259, Dec. 2006.

[**Weinstein 2002**] S. Weinstein, "The Mobile Internet:Wireless LAN vs. 3G Cellular Mobil *e," IEEE Communications Magazine* (February 2002). pp. 26–28.

[**Weiser 1991**] M. Weiser, "The Computer for the Twenty-First Century," *Scientific American* (September 1991): 94–10. http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

[**Wessels 2001**] D. Wessels, *Web Caching*, O'Reilly, Sebastopol, CA, 2001.

[**Wimba 2004**] Wimba homepage, http://www.wimba.com

[**Woo 1994**] T. Woo, R. Bindignavle, S. Su, and S. Lam. SNP: an interface for secure network programming. In Proceedings of 1994 Summer USENIX, pages 45—58, Boston, MA, June 1994. http://www.cs.utexas.edu/users/lam/Vita/Cpapers/WBSL94.pdf

[**Wood 2007**] L. Wood, "Lloyds Satellites Constellations," http://www.ee.surrey.ac.uk/Personal/L.Wood/constellations/iridium.html

[**Xiao 2000**] X. Xiao, A. Hannan, B. Bailey, L. Ni, "Traffic Engineering with MPLS in the Internet," *IEEE Network*, March/April 2000. http://www.cse.msu.edu/~xiaoxipe/papers/mplsTE/mpls.te.pdf

[**Youtube 2007**] Youtube homepage, www.youtube.com

[**Yahoo-MIME 1999**] Yahoo MIME WWWpage, http://dir.yahoo.com/Computers_and_ Internet/Multimedia/MIME/

[**Yeager 1996**] N. J. Yeager and R. E. McGrath, *Web Server Technology,* Morgan Kaufmann Publishers, San Francisco, 1996.

[**Zegura 1997**] E. Zegura, K. Calvert, M. Donahoo, "A Quantitative Comparison of Graph-based Models for Internet Topology," *IEEE/ACM Transactions on Networking,* Vol. 5, No. 6, (Dec. 1997). http://www.cc.gatech.edu/fac/Ellen.Zegura/papers/ton-model.ps.gz.

[**Zhang 1991**] L. Zhang, S. Shenker, and D. D. Clark, "Observations on the Dynamics of a Congestion Control Algorithm: The Effects of Two Way Traffic," *Proceedings of ACM SIGCOMM '91,* Zürich, 1991. http://www1.acm.org/pubs/citations/proceedings/comm/115992/p133-zhang/

[**Zhang 1993**] L. Zhang, S. Deering, D. Estrin, S. Shenker, D. Zappala, "RSVP: A New Resource Reservation Protocol," *IEEE Network Magazine,* Vol. 7, No. 9 (Sept. 1993), pp. 8–18.

[**Zhang 1998**] L. Zhang, R. Yavatkar, Fred Baker, Peter Ford, Kathleen Nichols, M. Speer, Y. Bernet, "A Framework for Use of RSVP with Diffserv Networks," <draft-ietf-diffservrsvp-01.txt>, 11/20/1998. Work in progress.

[**Zhao 2004**] B. Y. Zhao, L. Huang, J. Stribling, S. C. Rhea, A. D. Joseph, J. Kubiatowicz, "Tapestry: A Resilient Global-scale Overlay for Service Deployment," *IEEE Journal on Selected Areas in Communications,* Vol. 22, No. 1 (Jan. 2004). http://www.cs.berkeley.edu/~adj/publications/paper-files/tapestry_jsac.pdf

[**Zimmermann 1980**] H. Zimmermann, "OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection," IEEE Transactions on Communications, Vol. 28, No. 4 (Apr. 1980), pp. 425-432.

[**Zimmermann 2007**] P. Zimmermann, "Why do you need PGP?" http://www.pgpi.org/doc/whypgp/en/.