بسم الله الرحمن الرحيم

تلخيص شبكات الحاسوب

٢٠٢٠

نقدم بين يديكم تلخيص كتاب شبكات الحاسوب

بالتعاون مع طلبة الفصل الصيفي الحالي وطلبة الفصل السابق

" اللهم علمنا ما ينفعنا، وانفعنا بما علمتنا، وزدنا علما، وأرنا الحق حقاً وارزقنا اتباعه، وأرنا الباطل باطلاً وارزقنا اجتنابه، واجعلنا ممن يستمعون القول فيتبعون أحسنه، وأدخلنا برحمتك يارب العالمين "

نسأل الله التوفيق للجميع، لا تنسونا من الدعاء

فهرس المحتويات

الوحدة الأولى

المخرجات التعليمية المقصودة (Intended Learning Outcomes ILOs) عزيزي الطالب، بعد الانتهاء من دراسة هذا المقرر، ينبغي أن تحقق المخرجات المبينة في الجدول أدنا موزعة على الوحدات الدراسية

مكونات المقرر (الوحدات الدراسية)

عزيزي الطالب، سنبدأ رحلتنا في دراسة هذا المقرر بإلقاء نظرة سريعة على مكوناته واضعين نصب أعيننا أن الوجهة النهائية هي الفهم العميق لماهية شبكات الحاسوب ولماذا وجدت وكيف نتعامل معها. ونبدأ بخارطة الطريق التي تتكون من سلسلة وحدات المقرر، وهي: .

١ـ الاتصالات الرقمية وشبكات الحاسوب والإنترنت(Digital

Communication

,

Computer Networks and the Internet):

تعتبر هذه الوحدة مقدمة المقرر، إذ تغطى المبادئ والمفاهيم الأساسية لشبكات الحاسوب، كأنواع الإشارات وطرق الترميز، ومفهومي التردد ومعدل الإرسال، بالإضافة إلى الفاقد والتأخير والإنتاجية. كما تغطي مفهوم الإنترنت، وأطراف الشبكة ونواتها التي تشكل الطبقة الفيزيائية، بما فيها وسائط النقل اللازمة لشبكات الحاسوب، وتقنيات تناقل البيانات. وأخيرة، فتناقش طبقات البروتوكولات ونماذج خدماتها.

٢ـ طبقة التطبيق(Application Layer):

تتناول هذه الوحدة مبادي تطبيقات الشبكات و الشبكة العنكبوتية، وبروتوكولات نقل النص التشعبي ونقل الملفات والبريد الإلكتروني وخادم اسم النطاق و كذلك تطبيقات النظير- للنظير، ولمحة حول برمجة المقابس.

٣. طبقة النقل(Transport Layer):

تناقش هذه الوحدة خدمات طبقة النقل، ومفهوم التجميع و فك التجميع وكذلك النقل بدون اتصال في بروتوكول المخطط البياني للمستخدم(UDP) ، والنقل الموجه بالاتصال في
بروتوكول التحكم بالنقل(TCP) ، كما تتناول مبادى النقل الموثوق وضبط الاحتقان الازدحام في بروتوكول
التحكم بالنقل.

٤. طبقة الشبكة(Network Layer):

تغطي هذه الوحدة المفاهيم المرتبطة بطبقة الشبكة، كالدارات الافتراضية، وشبكات رزم البيانات، ثم بروتوكول الإنترنت (IP) ومفهومي التمرير والعنونة، كما تتناول خوارزميات التوجيه، والتوجيه في الإنترنت

٥ طبقة الربط والشبكات المحلية(Link Layer and LANs):

تتناول هذه الوحدة أهم مفاهيم طبقة الربط والشبكات المحلية، فتغطى بروتوكولات الوصول المتعدد، والشبكات المحلية المحولة، وشبكة مركز البيانات، ثم نظرة شاملة متكاملة تتناول مثالا حول طلب صفحة ويب، والخطوات التي يمر بها حتى الاستجابة للطلب، كيوم في حياة هذا الطلب

٦. الشبكات اللاسلكية والنقالة(Wireless and Mobile Networks):

وتتناول المفاهيم المتعلقة باشبكات اللاسلكية والنقالة، وتشمل خصائص الوصلات والشبكات اللاسلكية، ثم تنتقل إلى الشبكات اللاسلكية المحلية، وأخيرا، الاتصال الخلوي بالإنترنت.

عزيزي الطالب، هناك مجموعة من أسئلة التقويم الذاتي والتدريبات في كل وحدة دراسية، وفرنا حلولها المفصلة جميعا في الأجزاء الختامية. أما الجانب العملي فله دليل خاص، يحتوي مجموعة من التجارب في المختبر، او من خلال برامج
المحاكاة مثل (Wireshark)

1 -الإشارات التناظرية والرقمية(Analog and Digital Signals)

شهد مجال تراسل البيانات في الفترة الأخيرة تطورا هائلا، وازدادت الحاجة إلى استخدام التقنيات والأدوات والوسائط المرتبطة بذلك، وتلبية للاحتياج المتزايد فقد ركزت الأبحاث والاستثمارات على تطوير وسائل تراسل البيانات بترقية الشبكات التقليدية السابقة و إدخال أنواع جديدة من الشبكات بتقنيات تتناسب مع السرعة العالية المطلوبة؛ والسعة العالية لأوساط النقل، وضمان خلو هذه الأوساط من معيقات التراسل؛ كالضجيج، والتخامد، والتداخل مع الإشارات الأخرى. كما تطورت وسائل التحكم بهذه الوسائط من شبكات ومراكز معالجة
تعريف:
يعرف تراسل البيانات بأنه التقنية التي تسمح بتبادل البيانات الرقمية كالصوت، والفيديو، والصور بين نقطتين تحويان تجهيزات مناسبة لاستقبالها أو معالجتها من خلال إشارات حاسوبية وإشارات تحكم وغيرها.

١ 1 - 2 - أنظمة تراسل البيانات

يتضمن مفهوم نظام تراسل البيانات كل التجهيزات الفيزيائية والإلكترونية و البرمجية التي تقوم بنقل البيانات وفيما ياتي توضح أهم المفاهيم المرتبطة بأنظمة تراسل البيانات

١. اوساط النقل (التجهيزات الفيزيائية)، وهي نوعان سلكية كالكوابل والألياف الضوئية، ولا سلكية عبر الأثير.

٢ .التجهيزات الإلكترونية الدارات والعناصر الالكترونية التي تحول الإشارة من شكل إلى آخر، من مستوى إلى آخر (زيادة الطاقة، التخلص من الإشارات المعيقة، التحويل من مجال ترددي إلى آخر, تغيير شكل الرموز الممثلة، نوع التضمين).

٣. البرمجيات التحكم في تراسل البيانات وتحصينها ضد الأخطاء وتحديد شكل رسائل البيانات وحجمها وأطرها وتزامنها.

٤. بنية نظام تراسل البيانات: يتكون نظام تراسل البيانات من مرسل ومستقبل وقناة تراسل البيانات كما يبين الشكل (١-١)

٥. إجراءات تراسل البيانات: وهي الخطوات التي تمر بها البيانات من لحظة إرسالها إلى لحظة استقبالها، كما يبين الشكل (١-٢) ص٤

٢ 1 - 2 - أنواع الإشارات(Signals)

الإشارة هي الشكل الذي تنتقل بوساطته البيانات ضمن وسط النقل، وهي التعبير المباشر عن المعلومات والبيانات التي يتم توليدها لتستطيع الانتقال عبر وسط النقل بشكل مناسب،

***- فالإشارات الكهربائية**

Electrical Signals تنتقل عبر أوساط النقل المعدنية

، *- والإشارات الضوئية Light Signals

تنتقل عبر الألياف الضوئية أو عبر الفراغ،

***- والإشارات الكهرومغناطيسية**Electromagnetic signals

تنتقل عبر الأثير.

ويمكن لأي من هذه الإشارات أن تحمل إشارات أخرى كما هو الحال في التضمين(Modulation) ، حيث تحمل الإشارات الجيبية التي تسمى إشارات الحامل Carrier Signals بإشارات البيانات لأسباب تقنية، أو تتحول الإشارات من شكل إلى آخر لتتلاءم مع مكونات وأجزاء نظام نقل البيانات، كان يتم تحويل الإشارات الكهربائية إلى إشارات كهرومغناطيسية أو ضوئية وبالعكس،

وبشكل عام هناك نوعان أساسيان من الإشارات، الإشارات التناظرية، والإشارات الرقمية، كما سنوضح فيما يلي

الإشارات التناظرية:(Analog Signals)

إشارات طبيعية كالصوت والفيديو، وقد تكون الإشارة التناظرية مستمرة مثل$s_{1(t)}$ ، أو منقطعة في القيمة (المطال Amplitudle مستمرة في الزمن مثل $s_{2(t)}$ أو منقطعة في الزمن مستمرة في القيمة مثل $s_{3(t)}$، كما هو موضح في الشكل (١-٣) ص٥،

وهناك ثلاث قيم أساسية تحدد شكل الإشارة

قيم تحديد شكل الاشارة

١) المطال Amiplitude: ويعبر عنه كقيم لحظية أو كقيم تابعة للزمن.
٢) الطيف الترددي Frequency spectrum: ويعطي فكرة واضحة عن المركبات الترددية للإشارة، ويؤدي دورا أساسيا في تحديد إمكانية إرسال الإشارة ضمن قناة تراسل معينة
٣) خصائص الطور Phase Characteristics: وتحدد الطور الابتدائي للمركبات الترددية

الإشارات الرقمية (Digital Signials):

مع تطور أنظمة الاتصالات، وزيادة متطلبات استخدامها، تم الاستعاضة عن الإشارات التناظرية بالإشارات المتقاطعة في بعض التطبيقات، وهي إشارات متقطعة في الزمن مستمرة في القيمة، كما يبين الشكل (١-٤) ص ٦

أهم أنواع الإشارات المتقطعة

هو الإشارات الرقمية، وتنتج عند الاستعاضة عن أهم عينات الإشارة بسلسلة من الرموز تشكل شيفرة معينة، تعبر بشكل أو بآخر عن القيم اللحظية للعينات، ويتم التعبير عن هذه السلسلة عادة بأرقام ثنائية،

كما يبين الشكل ص٦.(1-5)

ازاد استخدام الإشارات الرقمية في الأونة الأخيرة بشكل مضطرد، نتيجة للتطور الهائل في اساليب المعالجة الرقمية و أجهزتها، وتتحول الإشارة المتقطعة إلى رقمية بتكميم قيم العينات (Quantization)، اي بحصر قيم العينات

بعدد محدود من القيم، فتنتج إشارة المنقطعة في الزمن منقطعة في القيمة "
ولمعالجة الإشارات التناظرية الناتجة عن حوادث فيزيائية طبيعية باستخدام الحاسوب، فلا بد من تحويلها إلى رقمية ليتمكن من معالجتها وتخزينها ونقلها باستخدام الشبكات على شكل ملفات ورسائل رقمية

مفاهيم مهمة

تقاس جودة الإشارة بنسبة الإشارة إلى الضجيج بالديسيبل
Signal - to - Noise Ratin SNR =S/N dB

معدل الخطا (Error Rate):
هو تأثير الإشارات المعينة، ويساوي متوسط الأخطاء في وحدة الزمن

نسبة احتمال الخطا (Probability of Error):
هي عدد البتات الخاطئة المستقبلة في كل عدد من البتات
يمكنك إنقاص الأخطاء باختيار نوع مناسب من تعديل الإشارة (Modulation) والترميز وكشف الأخطاء

3 - 1 |ترميز الإشارات الرقمية(Digital Signal Encoding)

ترسل البيانات الرقمية الثنائية عن طريق ترميز كل بت بيانات إلى عناصر الإشارة، وفي ابسط الحالات، هناك علاقة واحدلواحد بين البتات وعناصر الإشارة، فمثلا كما يبين الشكل (١-٦)، يتم تمثيل الثنائيا بمستوى جهد منخفض، والثنائي ٠ بمستوى جهد عال، وسنعرض في هذا القسم مجموعة متنوعة من أنظمة الترميز

في البداية، دعنا، عزيزي الطالب، نعرف بعض المصطلحات:

مصطلحات مهمة

أ. الإشارة أحادية القطبية(Unipolar):

إذا كانت جميع عناصر الإشارة لها نفس العلامة الجبرية، أي أنها موجبة أو سالبة

ب. الإشارة المستقطبة(Polar):

يتم تمثيل حالة واحد المنطقي بمستوى جهد موجب، والأخرى بمستوى و جهد سالب.

ج محل بيانات الإشارة(Data signaling rate):

هو المعدل الذي ترسل به البيانات مقدرا بالبت في الثانية

د. مدة او طول البت(Bit duration or length):

هي مقدار الوقت الذي يستغرقه المرسل في إرسال البت، فإذا كان معدل إرسال البيانات$_R$ ، فإن مدة البت هي$_{1/R}$

ه.معدل التضمين او التباين(Modulation rate):

هو المعدل الذي يتغير عنده مستوى الإشارة، ويعتمد ذلك على طبيعة الترميز، ويعبر عنه بالبود(Baud) ، اي عنصر إشارة في الثانية (Signal elements per second)

و. العلامة والفراغ (Mark and Space):

يمثلان الأرقام الثنائية ٠، ١ على التوالي

يعتبر نظام ترميز الإشارات الرقمية أحد العوامل التي تؤثر في أداء مستقبل الإشارة دون حدوث أخطاء، بالاضافة إلى نسبة الإشارة إلى الضجيج، ومعدل الإرسال، وعرض الحزمة،

ونظام الترميز

هو ببساطة طريقة تحويل بتات البيانات إلى عناصر الإشارة، وهناك العديد من طرق الترميز، وستصف في هذا القسم أكثرها شيوعا، كما هو مبين في الجدول (١-١)ص٨ وفي الشكل (١-٧)ص٩

| 4 - 1 |تراسل البيانات(Data Transmission)

عزيزي الطالب، دعنا نبدأ هذا القسم بتعريف بعض المصطلحات المتعلقة بتراسل البيانات. كما تعلم، فإن البيانات تنتقل عبر أوساط النقل بين المرسل والمستقبل على شكل موجات كهرومغناطيسية، وفيما يأتي تعريف أهم المصطلحات التي ستحتاج إليها

الأوساط الموجهة(Guided media):

تنقل الإشارارت عبر ممرات محددة كالكوابل المجدولة (Twisted pair)و المحورية والألياف الضوئيةسلكية (Wired)

الأوساط غير الموجهة(Unguided media)

:تنقل الإشارات عبر الأثير أو الفضاء (لاسلكية Wireless).

الخط المباشر(Direct link):

مسار التراسل بين جهازين تنتقل فيه الإشارة من المرسل ى المستقبل مباشرة دون أجهزة وسيطة باستثناء المضخمات او المكررات اللازمة لتقوية الإشاره

تراسل نقطة-الى-نقطة (point- to - point)

:التراسل عبر خط مباشر بين جهازين هما الوحيدين اللذين يتشاركان الوسيط

التراسل البسيط(Simplex)

:ترسل الإشارات بين محطتين في اتجاه واحد فقط؛ إحداهما المرسل والأخرى في المستقبل .

التراسل أحادي الاتجاه(Half duplex)

، قد ترسل كلتا المحطتين بالاتجاهين، ولكن ترسل واحدة منها فقط في كل مرة .

التراسل باتجاهين

(Full-duplex)، قد ترسل كلتا المحطتين إشاراتهما معا عبر الوسيط في كلا الاتجاهين

١ 1 - 4 - التردد والطيف وعرض الحزمة : (Frequency , Spectrum ind Bandwidth)

سنهتم في بالإشارات الكهرومغناطيسية المستخدمة كوسيلة للنقل البيانات، ويتم توليد الإشارة في المرسل وتنتقل عبر الوسيط على شكل دالة بالنسبة للزمن، ولكن يمكن التعبير عنها أيضا كدالة بالنسبة للتردد frequency،

ويعرف التردد

(f) بانه معدل تكرار الإشارة مقدراً بالهيرتز (دورة في الثانية)، أي أن الدورة period(T=1/f)،

كما هو مبين في الشكل (١-٨). ص١٠

أما طيف الإشارة(Spectrum)

فهو مجموعة الترددات التي تحتويها،

و عرض النطاق الترددي المطلق(Absolute Bandwidth)

يعبر عن عرض هذا العطيف،

والعديد من الإشارات لها عرض نطاق ترددي لانهائي، ولكن

طاقة الإشارة

يتضمنها نطاق ضيق من الترددات يطلق عليه عرض النطاق الترددي (Bandwidth)

في الإشارة الرقمية يستعاض عن مفهوم عرض النطاق الترددي (Bandwidth) بمفهوم معدل البيانات (Data Rate) أو معدل الإرسال (Transmission Rate") ويرمز له بالرمز R ، ويقاس بالبت في الثانية bits per second(bps)

، ولكنهما مفهومان مرتبطان بشكل وثيق، حيث تحتاج الإشارة الرقمية إلى عرض حزمة يتناسب مع معدل إرسالها من أجل إرسالها في قناة تناظرية، كما تحتاج الإشارة التناظرية إلى معدل إرسال أدنى (بعد رقمنتها) ليتم ارسالها بشكل صحيح في قناة رقمية للدرس الإشارة المبينة في

الشكل (١-٥)، ونلاحظ تكرار رموزها (١ , ٠) في فترات زمنية متساوية كل منها T=1/R ثانية أو بمعدل R / Sec ، ويسمى الزمن T الفاصل الثنائي (Binary Interval)، ويعطي منيع المعلومات R بت(bit) في الثانية.

| 1 - 5 |مفهوم الإنترنت (The Internet)

عزيزي الطالب سنناقش في هذا القسم مفهوم الإنترنت من ناحيتين، المكونات المادية و البرمجية، والخدمات التي تقدمها

١ ـ ٥ ـ ١ المكونات المادية والبرمجية (Hardware and Software Componets) الإنترنت

هي شبكة حواسيب تربط مئات الملايين من الأجهزة المحوسبة حول العالم، وكانت هذه الأجهزة عبارة عن أجهزة حاسوب مكتبية تقليدية، ومحطات عمل لينكس تدعى الخوادم لتخزين المعلومات ونقلها مثل صفحات الويب ورسائل البريد الإلكتروني وتضاعفت هذه الأجهزة تدريجيا لتشمل أجهزة غير تقليدية مثل أجهزة الحاسوب المحمول، والهواتف الذكية والأجهزة اللوحية، وأجهزة التلفاز، ووحدات تحكم الألعاب، وكاميرات الويب، والسيارات، وأجهزة استشعار البيئة، والأنظمة الكهربائية و أنظمة الحماية المنزلية وفي لغة الإنترنت، تسمى جميع هذه الأجهزة المضيفين أو الأنظمة الطرفية.

ويبين الشكل (١-٩) عينة من الأجهزة المكونة لشبكة الإنترنت ترتبط الأنظمة النهائية ببعضها عن طريق شبكة من خطوط الأتصال (Communication Links) ومقسمت الحزم (Packet Switches).

وتستخدم خطوط الأتصال أنواع مختلفة من الأوساط المادية، كالكوابل المحورية، والأسلاك النحاسية، والألياف الضوئية، وطيف الراديو وتنتقل البيانات فيها بمعدلات ارسال مختلفة تقاس بالبت/ثانية،

ولإرسال البيانات يقوم المرسل بتقسيمها إلى شرائح و إضافة بايت لمقدمة كل شريحة لإنتاج الحزم (Packets) وإرسالها عبر الشبكة إلى المستقبل، وهناك يتم إعادة تجميعها لإنتاج البيانات الأصلية

بأخذ مقسم الحزم الحزمة الواردة عبر أحد خطوط الاتصال ويعيد توجيهها عبر أحد خطوط الاتصال الصادرة وتأتي مقسمات الحزم في اشكال عدة، ولكن أبرزها في هذه الأيام الموجهات (Routers) و مقسمات طبقة الارتباط (Link - Layer Switches)، وكلاهما يعمل على توجيه الحزم نحو وجهتها النهائية. عادة تستخدم المقسمات في شبكات النفاذ، بينما تستخدم الموجهات في الشبكة الأساسية

تعريف المسار:(Route Or Path)

تسلسل خطوط الاتصال والمقسمات التي تعبرها الحزمة عبر الشبكة من نظام الإرسال النهائي إلى نظام الاستقبال النهائي

تتيح الأنظمة النهائية النفاذ إلى الإنترنت من خلال مزودي خدمة الإنترنت (Intermet Service Providers "ISPs) ، مثل مزودي خدمات الإنترنت المنزلي من خلال الكوابل المحلية أو الهاتف، ومزودي خدمات الإنترنت للشركات ومزودي خدمات الإنترنت اللاسلكي (WiFi) في المطارات والفنادق والمقاهي والمتاجر والأماكن العامة كل مزود خدمة إنترنت هو بحد ذاته شبكة من المقسمات وخطوط الاتصال، ويوفر عدة أنواع من النفاد عبر الشبكة إلى الأنظمة النهائية، بما في ذلك النفاذ إلى النطاق العريض المنزلي مثل المودم السلكي أوDSL ، والنفاذ إلى الشبكة المحلية عالية السرعة، والنفاذ اللاسلكي، ومودم الطلب الهاتفي بسرعة ٥٦ كيلوبت في الثانية كما يوفر مزودو خدمات الإنترنت النفاذ مباشرة إلى الإنترنت لمزودي المحتوى ومواقع الويب، ويرتبط مزودو خدمات الإنترنت الذين يوفرون النفاذ إلى الأنظمة النهائية معا على المستويين الوطني والدولي، وتدار كل شبكة من مزودي خدمات الإنترنت بشكل مستقل، وتشغل بروتوكول الإنترنتIP ، وتتبع معاهدات تسمية وعنونة محددة. تعمل الأنظمة النهائية والمقسمات و غيرها من أجزاء الإنترنت من خلال تشغيل بروتوكولات تتحكم بإرسال المعلومات واستقبالها عبر الإنترنت، واهمها بروتوكول التحكم بالنقل (TCP) وبروتوكول الإنترنت (IP) الذي يحدد تنسيق الحزم التي يتم إرسالها واستقبالها بين الموجهات والأنظمة النهائية، وتعرف بروتوكولات الإنترنت الرئيسة مجتمعة باسم(TCP / IP)، ونظرا لأهميتها فإنها تتبع معايير محددة تحدد وظيفة كل بروتوكول وآلية عمله، حتى يتمكن المطورون من إنشاء انظمة ومنتجات تتفق في الية عملها.

١ 2 - 5 - خدمات الإنترنت (Internet Services)

عزيزي الطالب، يمكننا من وصف الإنترنت من زاوية مختلفة تماما على انها بنية تحتية توفر خدمات للتطبيقات مثل البريد الإلكتروني، وتصفح الويب، والشبكات الاجتماعية، والرسائل الفورية، وتدفق الفيديو، والالعاب الموزعة، ومشاركة الملفات من نظير إلى نظير(P2P) ، والتلفاز عبر الإنترنت، والنقاد عن بعد، وغيرها الكثير، وعلى الرغم من أن المقسمات تعمل على تسهيل تبادل البيانات بين الأنظمة النهائية، إلا أنها لا تهتم بالتطبيق الذي يصدر البيانات. ولنفترض أن لديك فكرة مثيرة لتطبيق انترنت تود تطويرها إلى منتج فعليه ستحتاج إلى كتابة برامج، ولنقل باستخدام لغة Java أو C أوPython ، تعمل على أنظمة نهائية مختلفة تتطلب تبادل البيانات فيما بينها، وهذا يقودنا إلى وصف آخر للأنترنت كمنصة للتطبيقات، أي كيف لبرنامج يعمل على أحد الأنظمة ان يوعز للإنترنت بنقل البيانات إلى برنامج آخر يعمل على نظام آخر؟ توفر الأنظمة المتصلة بالإنترنت واجهة برمجة تطبيقات (API) تؤدي هذه المهمة عبر البنية التحتية للأنترنت، وهي مجموعة من القواعد التي يجب أن يتبعها البرنامج المرسل حتى تتمكن الإنترنت من توصيل بياناته إلى البرنامج الوجهة.

عزيز الطالب، لقد قدمنا للتو وصفا للإنترنت من حيث المكونات المادية والبرمجية، والبنية التحتية لتقديم الخدمات التطبيقات الموزعة، وسنناقش واجهة برمجة تطبيقات الإنترنت وخدمات الإنترنت بالتفصيل في الوحدة الثانية .

٣ 1 - 5 - مفهوم البروتوكول (What Is a Protocol?)

يتولى بروتوكول الشبكة إدارة تبادل الرسائل واتخاذ الإجراءات اللازمة بين المكونات المادية أو البرمجية المتصلة بالشبكة (مثل الحاسوب أو الهاتف الذكي أو الجهاز اللوحي أو الموجه أو أي جهاز)، فجميع أنشطة الإنترنت التي تتضمن اثنين أو أكثر من الكيانات المتصلة تحكمها برتوكولات محددة مثلا، تتحكم البروتوكولات بتدفق البيانات بين بطاقتي الشبكة في جهازي حاسوب متصلين؛ كما تتحكم بروتوكولات التحكم بالازدحام بمعدل نقل الحزم بين المرسل والمستقبل؛ وتحدد البروتوكولات في الموجهات مسار الحزمة من المصدر إلى الوجهة، وتعمل البروتوكولات في كل جزء من أجزاء الإنترنت

يحدد البروتوكول شكل الرسائل المتبادلة وترتيبها بين كيانين متصلين أو أكثر، كما يحدد الإجراءات المتخذة شان ارسال و أو استلام رسالة معينة وكمثال مألوف على بروتوكول الشبكة، دعنا، عزيزي الطالبة تنظر فيما يحدث عند تقديم طلب إلى خادم الويب، أي عند كتابة عنوان صفحة ويب (URL)في مستعرض الويب. يوضح الشكل (١-١٠) السيناريو كما يأتي ص١٤:

ا- يرسل حاسوبك رسالة طلب اتصال إلى خادم الويب وينتظر الرد
ب- عندما يتلقى الخادم رسالة الطلب يرد برسالة موافقة
ج- يطلب حاسوبك مستند الويب بأرسال اسم مصلحة الويب التي ترغب بها من خادم الويب في رسالة GET.
د. يقوم خادم الويب بإرجاع صفحة الويب (الملف) إلى حاسوبك

1 - 6 | أطراف الشبكة (The Network Edge)

عزيزي الطالب، سنتعمق الأن في مكونات شبكة الحاسوب (وخاصة الإنترنت)، ولنبدأ في هذا القسم بأطراف الشبكة وننظر في المكونات المعروفة اكثر من غيرها، أي الحواسيب والهواتف الذكية والأجهزة التي نستخدمها يوميا، وسننتقل في القسم التالي إلى قلب الشبكة، ونناقش دور المقسمات والموجهات في شبكات الحاسوب تسمى الأجهزة المتصلة بالإنترنت أنظمة نهائية لأنها تقع على طرف شبكة الإنترنت كالحواسيب والخدمات والأجهزة المتنقلة، كما يطلق عليها مضيفات لأنها تستضيف وتشغل البرامج التطبيقية كمستعرض الإنترنت وخادم الويب أو البريد الإلكتروني، وتقسم إلى عملاء (Clients) كالحواسيب المكتبية و المتنقلة والهواتف الذكية، وخدمات (Servers) بمواصفات الى الأداء وظائف محددة، مثل تخزين صفحات الإنترنت و الفيديو والبريد الإلكتروني ونشرها وتوزيعها، بين الشكل (١-١١) تفاعل الأنظمة النهائية المتصلة بالإنترنت.

١ 1 - 06 - شبكات النفاذ (Access Networks)

شبكة النفاذ هي

الشبكة التي تربط نظاما نهائيا بأول موجه (الموجه الطرفي) على المسار بين نظام نهالي وآخر بعيد، وبين الشكل (١٢١) انواعا مختلفة من شبكات النفاذ ممثلة بالخطوط العريضة المظللة، والأوضاع و التي تستخدم فيها(المنزلية والشركات واللاسلكية الواسعة المتنقلة)

النقد المنزلي (Ionic Access)

توضح في هذا القسم طرق النفاذ المنزلي للإنترنت، وهي كثيرة سنذكرها، ونركز في الشرح أشهر طريقتين هما، خط المشترك الرقمي (Digital Subscriber Line: DSL) والكوابل (Cable)

خط المشترك الرقمي(Digital Subscriber Line: DSL)

عادة، يكون النفاذ المنزلي إلى الإنترنت سلكيا عبر مودم DSL من شركة الهاتف المحلية، وفي هذه الحالة من شركة الاتصالات هي أيضا مزود خدمة الإنترنت.

يبين الشكل (١-١٣) أن المودم الخاص بكل عميل يستخدلم خط الهاتف التقليدي (سلك نحاسي مزدوج مجدول) لتبادل البيانات مع مجمع نقاذ خط المشترك الرقمي (DSLAM) الموجود في المكتب المركزي المحلي لشركة الاتصالات، يستقبل المودم البيانات الرقمية يترجمها إلى درجات عالية التردد لنقلها عبر اسلاك الهاتف إلى شركة الاتصالات، ثم تعاد ترجمة الإشارات التناظرية من هذه المنازل إلى تنسيق رقمي في DSLAM يحمل خط الهاتف المنزلي السيارات الهاتف معا، ويتم ترميزها على ترددات مختلفة

قناة تنزيل عالية السرعة، ويتراوح نطاقها من50 khz الى 1MHz

قناة تحميل متوسطة السرعة، ويتراوح نطاقها من ٤ إلى50kHz

قناة هاتف عادية باتجاهين، يتراوح نطاقها من 0 إلى4 kHz

بهذه الطريقة، يظهر خط DSL الواحد كثلاثة خطوط منفصلة، حيث يمكن إجراء مكالمة هاتفية و الاتصال بالإنترنت مشتركة معا على جانب العميل، يقوم جهاز الفصل (Splitter) بفصل البيانات عن إشارات ال التي تصل إلى المنزل ويوجه إشارة البيانات إلى مودمDSL ، وعلى جانب شركة الاتصالات، يفصل DSLAM البيانات عن إشارات الهاتف ويرسل البيانات عبر الإنترنت، وقد تتصل مئات أو آلاف المنة المنازل بخطDSLAM واحد [Dischinger ٢٠٠٧]

كابل النفاذ إلى الإنترنت (Cable Internet Access)

يستخدم كابل النقد البنية التحتية لكوابل شركات التلفاز، فيحصل المنزل على الإنترنت عبر الكابل من الشركة نفسها التي توفر خدمة التلفاز كما هو موضح في الشكل (١-١٤)،

تقوم الألياف الضوئية بتوصيل طرف راس الكابل بالتقاطعات على مستوى الحي، والتي تستخدم الكابل المحوري التقليدي للنفاذ إلى المنازل، وكل تقاطع يدعم عادة ٥٠٠ إلى ٥٠٠٠ منزل. ونظرا لاستخدام كل من الألياف الضوئية والكوابل المحورية في هذا النظام، غالبا ما يشار إليها بالألياف

المحورية الهجينة .(HFC) يستخدم مودم كابل خارجى خاص يتصل بالحاسوب المنزلي عبر منفذ ايثرنت

وهناك طرق أخرى للوصل إلى الإنترنت المنزلي

طرق التوصيل المنزلي

نذكر منها الألياف الضوئية للمنازل(Fiber To The Hone : FTTH) ، والطلب الهاتفي(Dialup) ، والأقمار الصناعية(Sattellite) ، والإيثرنت(Ethernet) ، والاتصال اللاسلكي(WiFi) ، وكذلك الجيل الثالث عبر الأجهزة الخلوية (3G,4G,5G)

٢ 1 - 6 - الأوساط المادية (Physical Media)

عزيزي الطالب، في القسم الفرعي السابق، قدمنا نظرة عامة على بعض أهم تقنيات النفاذ إلى شبكة الإنترنت، كما وصفنا هذه التقنيات و اشرنا إلى الأوساط المادية المستخدمة فعلى سبيل المثال، ذكرنا أن HFC تستخدم مزيجا من الألياف الضوئية و الكوابل المحورية، وأن DSL والإيثرنت تستخدم الأسلاك النحاسية، وأن شبكات الوصول عبر الهاتف النقال تستخدم طيف الراديو. في هذا القسم الفرعي، تقدم نظرة عامة موجزة عن أوساط الإرسال والأوساط الأخرى الأكثر شيوعا في الإنترنت

لتحديد مفهوم الوسط المادي، دعنا نفترض انتقال بت من نظام نهائي إلى آخر من خلال سلسلة من خطوط الاتصال والموجهات. يقوم نظام المصدر بنقل الجزء الأول، وبعد ذلك بفترة وجيزة، يستقبل الموجه الأول في سلسلة الموجهات هذا البت ثم يقوم بنقله، بعد ذلك بوقت قصير يتلقاه الموجه الثاني، وهكذا. فعندما ينتقل البت من المصدر إلى الهدف، يمر عبر سلسلة أزواج من أجهزة الإرسال والاستقبال، وفي كل زوج، يتم إرسال البت بواسطة موجات كهرومغناطيسية منتشرة او نبضات ضوئية عبر وسط مادي قد يتخذ العديد من الأشكال والنماذج، وليس بالضرورة أن يكون من نفس النوع بين كل زوج من أجهزة الإرسال والاستقبال على طول المسار،

ومن الأمثلة على الأوساط المادية

ازواج الأسلاك النحاسية المجدولة(Twisted-pairs) او الكوابل المحورية (Coaxial Cables) أو الألياف الضوئية، أو طيف الراديو الأرضي او الفضائي، وتقع الأوساط المادية في فئتين: الأوساط الموجهة (guideal india)، و غير الموجهة (Unguided media)

فبالأوساط الموجهة

، تنتقل الموجات عبر وسط صلب، كالألياف الضوئية أو الأسلاك النحاسية المجدولة، أو الكوابل المحورية،

أما في الأوساط غير الموجهة،

فتنتشر الموجات في الغلاف الجوي وفي الفضاء الخارجي، كما هو الحال في الشبكات المحلية اللاسلكية أو القنوات الفضائية الرقمية غالبا ما تكون الكلفة الفعلية للشبكات التي تستخدم الأوساط المادية (كالأسلاك النحاسية والألياف الضوئية قليلة نسبيا مقارنة بتكلفة الشبكات الأخرى، وتكون كلفة العمالة المرتبطة بتركيبها أعلى بكثير من كلفة المادة.

امثلة على الأوساط الموجهه

الأزواج المجدولة(Twisted- Pair)

تعتبر الأزواج المجدولة من أوساط النقل الموجهة الأكثر شيوعا واستخداما، وخاصة في شبكات الهاتف اذ يستخدم أكثر من ٩٩٪ من التوصيلات السلكية بين سماعة الهاتف والهاتف المحلي السلك النحاسي مجدول

كما يبين الشكل (1-15-a) يتكون الزوج المجدول من سلكين نحاسيين معزولين سمك كل منها حوالي ١مم مرتبة بنمط حلزوني منتظم، وذلك للحد من التداخل الكهربائي، وعادة، يتم تجميع عدد من الأزواج معا في غلاف واق، ويشكل زوج الأسلاك خط اتصال واحد.

تستخدم شبكات الحاسوب الداخلية المحلية (مثل الانترنت المنزلي) الزوج المجدول غير المحمي(Unshielded Twisted Pair: UTP)

ويتراوح معدل البيانات الشيكات المحلية التي تستخدم الزوج المجدول من ١٠ ميغابت في الثانية إلى ١٠ جيجا بت في الثانية لمسافة تصل إلى ١٠٠ متر بين المرسل والمستقبل

الكوابل المحورية(Coaxial Cable)

تتكون الكوابل المحورية من موصلين نحاسيين بشكل متحد المركز لا متواز، كما يبين الشكل (١-١٥-b)، بهذه البنية بالإضافة إلى العزل والتغليف تحقق هذه الكوابل معدلات نقل بيانات عالية، وهي شائعة جدا في أنظمة التلفاز.

وكما أشرنا سابقا، دمج نظام تلفاز الكابل بأجهزة المودم لتوفير الإنترنت المنزلي بمعدل نقل يصل إلى عشرات الميغابايت في الثانية يرحل المرسل الإشارة الرقمية إلى نطاق ترددي معين، وترسل الإشارة التناظرية الناتجة من المرسل إلى مستقبل واحد أو أكثر.

وقد تستخدم الكوابل المحورية كوسط موجه مشترك، أي يمكن توصيل عدد من الأنظمة النهائية بالكابل مباشرة، بحيث يستقبل كل نظام نهائي ما يتم إرساله من الأنظمة النهائية الأخرى. ص١٩

الأوساط الموجهة الألياف الضوئية(Fiber Optics)

الالياف الضوئية هي عبارة عن وسط رفيع ومرن ينقل البيانات على شكل نبضات ضوئية كما يبين الشكل (١

٠(15 - ، كل بت تمثله نبضة، وتدعم الألياف الضوئية معدلات نقل هائلة تصل إلى عشرات او حتى مئات الجيغابت في الثانية. فهي محصلة من التداخل الكهرومغناطيسي، وترهين الإشارة فيها منخفض يصل إلى ١٠٠ كيلومتر، ويصعب جدا التنصت عليها هذه الخصائص جعلت من الألياف الضوئية أوساط النقل الموجهة المفضلة للمسافات البعيدة، وخاصة للخطوط الخارجية لذا، شاع استخدامها في العمود الفقري للإنترنت مع ذلك فان" الكلفة العالية لأجهزتها، كالمرسل والمستقبل والمقسمات، أعاقت انتشارها للمسافات القصيرة في

الشبكات المحلية أو المنزلية تتراوح السرعة القياسية الخطوط

الناقل الضوئي(Optical Carrier:OC)

51.8Mbps إلى 39.8Gbps ويشار إلى هذه المواصفات بالرمز OC-n، حيث تساوي سرعة الخط n x 51.8 Mbps

قنوات الراديو الأرضية والفضائية (Terrestrial and Satellite Radio Channels)

تحمل قنوات الراديو الإشارات في الطيف الكهرومغناطيسي، وتعتبر وسطا جاذبا لأنها لا تحتاج إلى تركيب أسلاك، ويمكنها اختراق العوائق كالجدران، وتوفر خطوط اتصال لمستخدمي الهاتف المحمول، وتستطيع نقل الإشارة لمسافات بعيدة. وتعتمد خصائص قناة الراديو بشكل كبير على بيئة الانتشار والمسافة التي ينبغي أن تحمل إليها الإشارة،

تتسبب بيئة الانتشار بما ياتي:

١. فقدان المسار (Path loss) **وتضاؤل الطيف**(Shadow fading) **، مما يقلل من قوة الإشارة عندما تنتقل مسافات طويلة، وكذلك حول أو عبر الأجسام المعيقة**

٢. التضاؤل متعدد المسار(Multipath fading) **، بسبب انعكاس الإشارة عن الأجسام المسببة للتداخل**

٣. التداخل(Interference) **، الذي ينتج عن الإشارات الكهرومغناطيسية، والإشارات المرسلة الأخرى**

تصنف قنوات الراديو الأرضية بشكل عام إلى ثلاث مجموعات:

- **قنوات قصيرة تعمل لمسافة قصيرة جدا من متر إلى مترين، وتستخدم في الأجهزة الشخصية مثل سماعات الأذن، ولوحات المفاتيح، والأجهزة الطبية اللاسلكية**

- قنوات لاسلكية محلية تعمل على المستوى المحلي من عشرة إلى بضع مئات من الأمتار، وتستخدم في تقنيات الشبكات المحلية اللاسلكية
- قنوات لاسلكية واسعة النطاق: تعمل لمسافات طويلة تمتد إلى عشرات الكيلومترات، وتستخدم في تقنيات النفاذ الخلوي

في قنات الراديو الفضائية، يربط القمر الصناعي بين اثنتين أو أكثر من المحطات الأرضية، أي أجهزة الإرسال والاستقبال الأرضية بالموجات الميكروية. ويستقبل الاتصالات على نطاق ترددي واحد، ويعيد توليد الإشارة باستخدام مكرر، ثم ينقل الإشارة على تردد أخر. ويستخدم نوعان من الأقمار الصناعية في الاتصالات: اقمار مستقرة بالنسبة إلى الأرض (Geostationary sattellites)، وأقمار تدور حول الأرض في مدارات منخفضة (Low-Earth Orbitting: LEO sattellites)

تبقى الأقمار الصناعية المستقرة بشكل دائم فرق نفس النقطة على الأرض، ويتحقق ذلك بوضع القمر في مداره على ارتفاع ٣٦٠٠٠ Km وهي مسافة طويلة عند الاتصال عبر القمر الصناعي بين محطتين ارضيتين، فينتج عنها تأخير كبير للإشارة يبلغ ms 280 وغالبا، تستخدم الاتصالات الفضائية، التي قد تصل سرعتها مئات الميجا بت في الثانية، في المناطق التي لا تصلها خدمة DSL أو النفاذ إلى الإنترنت عبر الكوابل، ويبين الشكل (١-١٦) انواع الاتصال عبر الأقمار الصناعية

اما الأقمار الصناعية المتحركة (LTO)، فيتم وضعها أقرب بكثير، وتدور حول الأرض كالقمر، ويمكنها أن تتواصل مع بعضها البعض، ومع المحطات الأرضية ولتوفير تغطية مستمرة لمنطقة معينة، يجب وضع العديد من الأقمار الصناعية في المدار، ويتم حاليا تطوير العديد من هذه الأنظمة، وقد يستخدم هذا النوع من الأقمار الصناعية في النفاذ إلى الإنترنت مستقبلا.

عزيزي الطالب، بعد دراسة أطراف شبكة الإنترنت في القسم السابق، دعنا ننتقل الأن نتعمق أكثر في نواة الشبكة (Network core)، أي شبكة تبديل الحزم

والخطوط التي تربط بين أنظمة الإنترنت النهائية بمين الشكل (١-١٧) نواة الشبكة بخطوط سميكة مظللة ص٢٣ .

١ 1 - 7 - تبديل الحزم (Packet Switching)

في تطبيقات الشبكة، تتبادل الأنظمة النهائية الرسائل فيما بينها، وقد تحتوي الرسائل على ما يريده مصمم التطبيق، فقد تؤدي وظيفة تحكم، وقد تحتوي على بيانات كرسالة بريد إلكتروني أو صورة بتنسيق JPEG أو ملف صوت MP3.ولإرسال رسالة يقوم المصدر بتجزئتها إلى أجزاء اصغر من البيانات تسمى الحزم (Packets) كما يبين الشكل (١-١٨)، وبين المصدر والوجهة، تنتقل كل حزمة عبر خطوط الاتصال ومقسمات الحزم (مثل الموجهات و المقسمات)، ترسل الحزم عبر كل خط اتصال بمعدل الإرسال الكامل، فإذا كان المصدر أو مقسم الحزم يرسل حزمة طولها L بت عبر خط اتصال بمعدل إرسال R بت/ثانية، يكون زمن إرسال الحزمة L/R ثانية

٢ ـ ٧ ـ ١ تبديل الدارات (Circuit Switching)

عزيزي الطالب، بعد أن غطينا شبكات تبديل الحزم في القسم الفرعي السابق، تنتقل الآن إلى شبكات تبديل الدارات. في هذا النوع من الشبكات، يتم حجز الموارد اللازمة على طول المسار(المخازن المؤقتة Buffers ، ومعدل إرسال الخط)لتأمين الاتصال بين الأنظمة النهائية طوال مدة جلسة الاتصال في شبكات تبديل الحزم، الا يتم حجز هذه الموارد، بل تستخدم عند الطلب، ونتيجة لذلك، قد تضطر إلى الانتظار في قائمة الانتظار للحصول على خط اتصال

وتعتبر شبكات الهاتف التقليدية مثالا على شبكات تبديل الدارات، فعندما يريد شخص إرسال معلومات (صوت او فاكس) إلى شخص أخر، وقبل أن يتمكن المرسل من إرسال المعلومات، يجب إنشاء اتصال بين المرسل والمستقبل، وتحافظ المقسمات في المسار بين المرسل والمستقبل على حالة الاتصال. في لغة الاتصال الهاتفي في هذا الاتصال دارة، فعندما تنشئ

الشيكة هذه الدارة، فإنها تحتفظ أيضا بمحل إرسال ثابت في خطوط الشبكة (يبين حصة كل خط من سعة الإرسال طوال) مدة الاتصال.
وبما أنه قد تم حجز معدل إرسال معين لهذا الاتصال بين المرسل والمستقبل، نضمن نقل البيانات بمعدل ثابت.

شبكة تبديل الدارات في هذه الشبكة، ترتبط المقسمات الأربعة من خلال أربعة خطون يحتوي كل خط على أربع دوائر ، ليتمكن كل خط من دعم أربعة اتصالات متزامنة يتم ربط كل مضيف (مثل أجهزة الحاسوب ومحطات العمل) مباشرة بأحد المقسمات، فعندما يرغب مضيفان بالاتصال، تنشئ الشبكة اتصالا متكاملا بين المضيفين ليتمكن المضيف من الاتصال بالمضيف ، يجب على الشبكة أولا حجز ادارة واحدة على كل خط في هذا المثال، يستخدم الاتصال الدارة الثانية في الخط الأول و الدارة الرابعة في الخط الثاني، ولأن كل خط يحتوي على أربع دوائر، يحصل كل خط يستخدمه الاتصال على ربع سعة الإرسال الإجمالية للخط طوال مدة الاتصال.
فمثلا، إذا كان معدل إرسال كل خط بين مقسمين متجاورين ١ ميجابت في الثانية، فإن كل خط تبديل يحصل على (٢٥٠ كيلوبت في الثانية من معدل الإرسال الإجمالي المخصص.

في المقابل، اعتبر أن مضيفا يريد إرسال حزمة إلى مضيف آخر عبر شبكة تبديل الحزم من الإنترنت، في هذه الحالة ستنتقل الحزمة عبر سلسلة من خطوط الاتصال، وخلافا لتبديل الدارات، ترسل الحزمة إلى الشبكة دون حجز موارد خط الاتصال على الإطلاق، فإذا كان أحد الخطوط مزدحمة بحزم أخرى ستنتقل عبر الحد ذاته في نفس الوقت، فعلى المضيف الانتظار ووضع الحزمة في مخزن مؤقت على جانب المرسل ما قد يتسبب التأخير أي أن الإنترنت تبذل قصارى جهدها لتسليم الحزم بأسرع وقت، ولكنها لا تقدم أي ضمانات.

٨ | 1 - التأخير والفاقد والإنتاجية في شبكات تبديل الحزمة
Delay, Loss, and Throughput in Packet-)
(Switched Networks

عزيزي الطالب، أشرنا في القسم الفرعي ١-٥ أن الإنترنت توفر بنية تحتية لخدمات التطبيقات التي تعمل على الأنظمة النهائية، وفي الحالة المثالية، يجب أن تكون خدمات الإنترنت قادرة على نقل أكبر قدر ممكن من البيانات فوراً بين نظامين نهائيين، دون فقدان للبيانات. ولكن هذا الهدف لا يمكن تحقيقه على أرض الواقع وبدلا من ذلك، فإن شبكات الحاسوب تقيد الإنتاجية بين الأنظمة النهائية، أي مقدار البيانات التي يمكن نقلها في الثانية، وقد يحدث تأخير أو فقدان للحزم بالفعل. فشبكات الحاسوب تعاني من هذه المشاكل، وهناك العديد من طرق التعامل معها. في هذا القسم، سنبدأ بتحديد مقدار التأخير والفاقد والإنتاجية في شبكات الحاسوب

١ 1 - 8 - التأخير في شبكات تبديل الحزمة (Delay in Packet-Switched Networks)

تبدأ حزمة البيانات رحلتها من مضيف (المصدر)، وتمر عبر سلسلة من الموجهات، وتنتهي في مضيف آخر (الوجهة). عندما تنتقل الحزمة من عقدة (المضيف أو الموجه) إلى العقدة اللاحقة (المضيف أو الموجه) على طول المسار، فإنها قد تعاني من عدة أنواع من التأخير في كل عقدة، وأهم هذه الأنواع هو تأخير معالجة العقدة(Nodal Processing Delay) ، وتأخير الطابور (Queuing Delay)، وتأخير الإرسال(Transmission Delay) ، وتأخير الانتشار (Propagation Delay)، وتتراكم هذه الأنواع لتعطي التأخير الكلي، ويمكن التعبير عن التأخير الكلي للعقدة رياضية بالمعادلة:

dnodal = dproc + dqueue + dtrans + dprop

ونشير هنا إلى الفاقد في الحزم (Packet loss) الناتج عن امتلاء الطابور وارتباطه بتأخير الطابور.

يتأثر أداء العديد من تطبيقات الإنترنت كالبحث وتصفح الويب والبريد الإلكتروني والخرائط والرسائل الفورية و اتصالات الصوت عبر بروتوكول الإنترنت بتأخير الشبكة، ولفهم تبديل الحزم وشبكات الحاسوب، يجب أن نفهم طبيعة هذه التأخيرات وأهميتها.

يبين الشكل (١-٢٠) التأخير في المسار بين المصدر والوجهة حيث تنتقل الحزمة من الموجه A إلى الموجه B ، وهدفنا هو تحديد تأخير العقدة في الموجه A ، لاحظ أن الموجه A يحتوي على خط صادر يؤدي إلى الموجه B ، يسبق هذا الخط طابور (Queue) يسمى المخزن المؤقت (Buffer). عندما تصل الحزمة إلى الموجه A ، فإنه يتفحص مقدمة الحزمة لتحديد الخط الصادر المناسب للحزمة، ثم يوجه الحزمة إلى هذا الخط في هذا المثال، يؤدي الخط الصادر للحزمة إلى الموجه B ، ولا يمكن إرسال الحزمة على هذا إلا إذا لم يكن هناك حزمة أخرى قيد الإرسال حاليا أو تسبقها في الطابور؛ وإلا ستقوم الحزمة التي وصلت حديثا بالانضمام إلى قائمة الانتظار في الطابور.

هنا، تتعرض الحزمة لأنواع عدة من التأخير، نوضحها بإيجاز فيما يأتي:

أنواع تأخير الحزم

تأخير المعالجة (Processing delay):

ويشمل الزمن اللازم لفحص مقدمة الحزمة للتعرف على وجهتها، وكذلك الزمن اللازم لفحص الخطأ على مستوى البت في الحزمة المرسلة، ولا يتجاوز تأخير المعالجة بضع ميكرو ثوان. وبعد معالجة العقدة يحول الموجه الحزمة إلى الطابور الذي يسبق الخط المؤدي إلى الموجه B

تأخير الطابور (Queuing delay):

في الطابور، تتعرض الحزمة إلى تأخير ناتج عن الانتظار على الخط وتعتمد فترة تأخير الحزمة في الطابور على عدد الحزم التي تصل قبلها إلى الطابور

انتظار الخطر فإذا كان الطابور فارغة ولم يكن هناك حزم أخرى قيد الإرسال، فسيكون تأخير الطابور صفرا، وإذا كانت الطابور مزدحما بالحزم التي تنتظر، سيكون التأخير طويلا، ويتراوح تأخير الطابور من١ميكرو ثانية إلى ١ميلي ثانية

تأخير الإرسال(Transmission delay):

هو الزمن اللازم لنقل جميع بتات الحزمة عبر خط الاتصال، فإذا افترضنا أن الحزمة تنتقل بأسلوب "من ياتي اولا يخدم أولا (First- comic - first served -) " الشائع في شبكات تبديل الحزم، فلا يمكن إرسال الحزمة إلا بعد كل الحزم التي وصلت قبلها، فإذا كان طول الحزمة (L) بت)،
ومعدل إرسال الخط من جهاز التوجيه A إلى جهاز التوجيه B (R بت/ثانية)،
فإن تأخير الإرسال هو (L\R ثانية)،
ويتراوح من ميكرو ثانية 1 إلى ميلي ثانية 1

تأخر الانتشار أو البث(Propagation delay):

هو الزمن اللازم لانتشار الحزمة من بداية الخط إلى الموجه B ، ويساوي (d/8)، أي المسافة بين الموجه A والموجه d
(B) مقسومة على سرعة انتشار الخط (٨).
ينتشر البت بسرعة التشار خط الاتصال، وهي تعتمد على نوع الوسط المادية
وتتراوح من ٢×١٠^8 إلى ٣*10^8 متر/ث، اي اقل من سرعة الضوء بقليل.

الفاقد في الحزم (Packet Loss)

عزيزي الطالب، يعتبر تأخير الطابور الأكثر تعقيدا، إذ يتباين من حزمة إلى أخرى اعتمادا على موقعها في الطابور حتى لو أرسلت هذه الحزم معا، لذا يقاس إحصائيا بالمتوسط والتباين والاحتمال. من ناحية أخرى، فإن اطول الغير محدود وقد يمتلئ في أي لحظة، فإذا وصلت الحزمة إلى الموجه وهو ممتلئ ولم تجد حيزاً التخزينها
في المخزن المؤقت، عندها يقوم الموجه بإهمالها(Drop) ، أي تضيع الحزمة فينتج الفاقد (Loss) في الحزم ويطلق على هذا السيناريو الفيضان (Overflow) من وجهة نظر النظام النهائي، يبدو فقدان الحزم وكأنه تم نقل حزمة إلى نواة الشبكة ولكنها لم تحصل آبنا من الشبكة إلى وجهتها، وقد يضطر المرسل إلى إعادة إرسال الحزم المفقودة لضمان نقل جميع البيانات في نهاية المطاف من المصدر إلى الوجهة، وتزداد نسبة الفاقد في الحزم بزيادة كثافة حركة المرور، لذا، غالبا ما يقاس أداء العقدة باحتمال فقدان الحزم إضافة إلى
زمن التأخير

٢ 1 - 8 - الإنتاجية في شبكات الحاسوب (Throughput in Computer Networks)

عزيزي الطالب، بالإضافة إلى التأخير والفاقد في الحزم، هناك مقياس أخر مهم لأداء الشبكات و الإنتاجية من نظام نهائي لأخر لتحديد سرعة النقل، سنأخذ بعين الاعتبار نقل ملف كبير من المضيف A إلى المضيف B عبر الشبكة، وقد يكون هذا الملف مقطع فيديو كبير من نظير لأخر عبر نظام مشاركة الملفات P2P الإنتاجية اللحظية هي المعدل الذي يستقبل فيه المضيف B الملف بالبت ثانية، فإذا كان الملف يتكون من F بت ويستغرق نقله T ثانية، فإن متوسط الإنتاجية في نقل الملف F/T بت ثانية بعض التطبيقات مثل الاتصال الهاتفي عبر الإنترنت، تتطلب أن يكون التأخير منخفضا و متوسط الإنتاجية اللحظية أكثر من قيمة محددة تسمى العتبة (أكثر من 24 kbps لبعض تطبيقات الاتصال الهاتفي عبر الإنترنت، وأكثر من ٢٥٦ kbps لبعض تطبيقات فيديو

الوقت الحقيقي).

لتوضيح مفهوم الإنتاجية،

دعنا نأخذ بعض الأمثلة يوضح الشكل (١-٢١) (a-نظامين نهائيين، خاتم و عمل، متصلان عبر خطي اتصال وموجه، لنحسب الإنتاجية لنقل ملف من الخادم إلى العميل، ولنفرض ان R. مدل النقل بين الخادم والموجه؛ وأن R معدل النقل بين الموجه والعميل، ولنفرض أن البنات الوحيدة التي يتم إرسالها عبر الشبكة بالكامل هي التي ترسل من الخادم إلى العميل. فما هو معدل نقل البيانات من الخادم إلى العميل؟ ستعتبر البنات في السائل وخطوط الاتصال في الأنابيب، فلا يمكن للخدم ضخ البنات عبر خطه بمعدل أسرع من Rc bps ، ولا يستطيع الموجه إعادة توجيه البنات بمعدل أسرع من Rc bps

مثال (١-٢) لنفترض أنك تقوم بتنزيل ملف MP3 بحجم ٣٢ مليون بت، ومعدل إرسال الخادم R=2 Mbps ، ولديك خط نقاد بمثل نفاذ بمعدل نقل Rc = 1 Mbps.

الحل :

الوقت اللازم لنقل الملف =حجم الملف / معدل النقل
32 =ثانية ص٢٩

| 1 - 9 |طبقات البروتوكولات ونماذج خدمتها(Protocol (Layers and Their Service Models

عزيزي الطالب، من الواضح أن الإنترنت نظام مكلف وغاية في التعقيد، وقد رأينا أن الإنترنت يتكون من العديد من المعدات والبرمجيات كالأنظمة النهائية، والملفات، والموجهات، والأوساط المادية والتطبيقات والبروتوكولات. سنركز في هذا القسم على بروتوكولات الشبكة، فقد نظم مصممو الشبكة البروتوكولات في طبقات تشمل أجهزة الشبكة و البرامج

التي تنفذها، بهدف توفير هيكل عام لتصميم بروتوكولات الشركة بروتوكول ينتمي إلى واحدة من هذه الطبقات، وسيمر معنا مصطلح نموذج خدمة الطبقة، أي الخدمات التي تقدمها طبقة إلى طبقة تعلوها، وتقدم كل طبقة ختمتها من خلال

١) تنفيذ إجراءات معينة داخل تلك الطبقة
٢) استخدام خدمات الطبقة التي تحتها مباشرة

على سبيل المثال، قد تتضمن الخدمات المقدمة من طبقة n تسليما موثوقا للرسائل من طرف الأخر، وقد ينفذ ذلك عن طريق خدمة تسليم غير موثوقة للرسائل من طرف الأخر للطبقة ١-n، وإضافة وظيفة للطبقة n لكشف الرسائل المفقودة وإعادة إرسالها.

تنفيذ طبقة البروتوكول في البرمجيات او في الأجهزة أو كليهما، فبروتوكولات طبقة التطبيقات مثل HTTP و SMTP تنفذ دائما في برمجيات النظم النهائية وكذلك الأمر في بروتوكولات طبقة النقل.

ولأن الطبقة المادية (الفيزيائية) وطبقة ربط البيانات مسؤولان عن التعامل مع الاتصالات عبر خط معين، فيتم تنفيذهما في بطاقة الشبكة المرتبطة بخط اتصال معين، سواء كانت Ethernet أو Wi-Fi ، و غالبا ما تنفذ بروتوكولات طبقة الشبكة في الأجهزة والبرمجيات معا. وتوزع بروتوكولات الطبقة n ما بين الأنظمة النهائية والمقسمات، ومكونات الشبكة الأخرى، أي أنه يوجد غاليا جزء من بروتوكول الطبقة n في كل من هذه المكونات

إن التنظيم البروتوكول في طبقات مزايا مفاهيمية وتنظيمية يوضحها المرجع [RFC ٣٤٣٩] ، حيث يوفر طريقة منظمة لمناقشة مكونات النظام، كما أن التجزيء (Modularity) يجعل تحديث مكونات النظام أسهل، ولكن هناك بعض العيوب مثل التكرار في وظائف الطبقات، كما أن وظائف الطبقة قد تحتاج إلى معلومات تتوفر في طبقة أخرى فقط، ما يخالف الهدف من فصل الطبقات. وعند النظر إليها كرزمة واحدة،

تسمى بروتوكولات الطبقات المختلفة بمكدس البروتوكل (Protocol Stack).

1 - 9 -طبقات مكدس بروتوكول الإنترنت(Internet Protocol Stack Layers)

يتكون مكدس بروتوكول الإنترنت (Internet Protocol Stack) من خمس طبقات: المادية(Physical) ، والارتباط(Link) ، والشبكة(Network) ، والنقل(Transport) ، والتطبيق(Application) ،

كما هو موضح في الشكل (١-٢٢-١)،

وقد قمنا، عزيزي الطالب، بتنظيم هذا الكتاب استنادا إلى طبقات مكدس بروتوكول الإنترنت، والتزمنا بمنهج يغطي الطبقات من أعلى إلى اسفل (Top- Down Approach)، فيغطي طبقة التطبيق أولا ثم يتجه نحو الأسفل

طبقة التطبيق (Application Layer)

طبقة التطبيق تتضمن تطبيقات الشبكة وبروتوكولات طبقة التطبيق الخاصة بها، مثل بروتوكول HTTP الذي يتولى طلب مستند ويب ونقله،

و SMTP الذي يتولى بنقل رسائل البريد الإلكتروني،

وبروتوكول نقل الملفات (FTP) الذي يتولى نقل الملفات بين الأنظمة النهاية

من الأمثة على بروتوكولات طبقة التطبيق نظام اسم النطاق (DNS) الذي يتولى ترجمة أسماء الأنظمة النهائية للإنترنت (مثل العنوان wWw. qou . edu) إلى عنوان شبكة ٣٢ بت.

يتوزع بروتوكول طبقة التطبيقات عبر أنظمة نهائية متعددة، ويستخدم لتبادل حزم المعلومات بين تطبيقين على نظام نهائي وأخر، وسنطلق على حزمة المعلومات في طبقة التطبيق "رسالة"(Message)

طبقة النقل(Transport Layer)

تتولى هذه الطبقة نقل رسائل طبقة التطبيق بين طرفي التطبيق، وهناك بروتوكول انقل في الإنترنت TCP وUDP ، وكلاهما يمكنه نقل رسائل طبقة التطبيق،

حيث يوفر TCP خدمة اتصال موجهة لتطبيقاته، وهي

خدمة تضمن تسليم رسائل طبقة التطبيق إلى الوجهة، والتحكم بالتدفق (أي، المواءمة بين سرعة المرسل والمستقبل)،
كما يقوم بتقسيم الرسائل الطويلة إلى أجزاء أقصر،
ويوفر ألية للتحكم باحتقان الشبكة من خلال تخفيض معدل الإرسال لدى المصدر،
أما بروتوكولUDP ، فيوفر خدمة بدون اتصال لتطبيقاته، وهي خدمة لا توفر أيا من الوظائف التي يقدمها TCP, في هذا الكتاب، سنطلق على حزمة طبقة النقل "شريحة(Segment)"

في طبقة الشبكة (Network Layer)

تتولى لينة الشبكة مسؤولية نقل حزم طبقة الشبكة "مخططات البيانات" (Datagrams)من مضيف إلى آخر، ويقوم بروتوكول مليئة النقل (TCP) أو (UDP) في المضيف المصدر بتمرير شريحة طبقة النقل وعنوان الوجهة إلى طبقة الشبكة، فتوفر طبقة الشبكة خدمة توصيل هذه الشريحة إلى طبقة النقل في المضيف الوجهة تتضمن طبقة الشبكة بروتوكول IP المشهور، الذي يحدد حقول مخطط البيانات وكيفية تصرف الأنظمة النهائية والموجهات بهذه الحقول. هناك بروتوكول IP واحد فقط وعلى جميع مكونات الإنترنت التي تحتوي على طبقة شبكة تشغيله،
كما تحتوي طبقة الشبكة على بروتوكولات التوجيه التي تحدد المسارات التي تتخذها وذات البيانات بين المصدر والوجهة.
ورغم أن طبقة الشبكة تحتوي على عدد من بروتوكولات التوجيه إضافة إلىIP ، إلا أنه يشار إليها بطبقةIP ، لأن IP هو الذي يربط الإنترنت ببعضها البعض.

طبقة الارتباط(Link Layer)

تقوم الارتباط بنقل حزمة البيانات من عدة (مضيف او موجه) إلى العقدة التالية في المسار، في كل عقدة الشبكة مخطط البيانات إلى أسفل نحو طبقة الارتباط، التي تنقل بدورها مخلط البيت إلى العدة دالة على طول المسار، وفي هذه العقدة (التالية)، تقوم طبقة الارتباط بتمرير مخطط البيانات إلى

أعلى نحو اقة الشبكة تعتمد الخدمات التي تقدمها طبقة الارتباط على البروتوكول المستخدم، فقد توفر بعض بروتوكولات طيقة الارتباط خدمة التسليم الموثوق من العادة المرسلة، عبر خط اتصال واحد، إلى العقدة المستقبلة وهي تختلف عن خدمة التسليم الموثوق التي يوفرها TCP من نظام إلى آخر

ومن الأمثلة على بروتوكولات طبقة الارتباط :

الإيثرنت (Ethernet) وبروتوكول WiFi ، وبروتوكول DOCSIS الخاص شبكة النفاذ عبر الكوابل.

ولأن مخططات البيانات قد تحتاج إلى اجتياز عدة خطوط للانتقال من المصدر إلى الوجهة، يتم التعامل معها من خلال بروتوكولات مختلفة عند الخطوط المختلفة على طول مسارها، فقد تم معالجة مخطط البيانات من خلال Ethernet على أحد الخطوط، ومن خلال PPP على الخط التالي فقد تتلقى طبقة الشبكة خدمة مختلفة من كل بروتوكول. في هذا الكتاب، سنطلق على حزم طبقة الارتباط "إطارات(Frames)."

الطبقة المادية (Physical Layer)

تتلخص مهمة الطبقة المادية بنقل كل بت ضمن الإطار المرسل من عقدة إلى أخرى، وتعتمد البروتوكولات في هذه الطبقة مرة أخرى على خط الاتصال وعلى وسط الإرسال الفعلي، مثل الأزواج المجدولة النحاسية والألياف الضوئية، وغيرها فعلى سبيل المثال، يحتوي الإيثرنت على العديد من بروتوكولات الطبقة المائية أحدها للزوج المجدول النحاسي، وأخر للكوابل المحورية، وأخر للألياف الضوئية، وهكذا، وفي كل حالة، يتم نقل البت عبر خط الاتصال بطريقة مختلفة

٢ 1 - 9 - نموذج ترابط الأنظمة المفتوحة (The OSI Model)

عزيزي الطالب، بعد أن ناقشنا طبقات مكدس بروتوكول الإنترنت بالتفصيل، ينبغي أن نذكر أنه ليس المكدس الوحيد، ففي اواخر السبعينيات، اقترحت المنظمة الدولية للمقاييس (ISO) نموذجا ينظم شبكات الحاسوب في سبع طبقات أطلقت عليه نموذج ترابط الأنظمة المفتوحة.[OSI] [ISO 2012]

تبلور نموذج OSI عنها بروتوكولات الإنترنت في مهدها، وكان مجرد واحد من مجموعات البروتوكولات قيد التطوير.

كما يبين دل (١-٢٢-b)، مهم جدا

الطبقات السبع من النموذج المرجعي (OSI) هي:

طبقة التطبيق، وطبقة العرض، وطبقه الجلسة وطبقة النقل والنقل، وطبقة الشبكة، وطبقة ربط البيانات، والطبقة المادية وظيفة خمسة من هذه الطبقات نفس نظائرها المسماة بالمثل في برتوكول الإنترنت تقريبا لذا، ستناقش الطبقين الإضافيتين في نموذجOSI

طبقة العرض:

توفر هذه الطبقة خدمات تسمح للتطبيقات المتصلة بتفسير معنى البيانات المتبادلة مثل ضغط البيانات وتشفيرها (واضحة التفسير)، بالإضافة إلى وصف البيانات (التحرير التطبيقات من التنسيق الداخلي لتمثيل البيانات أو تخزينها الذي يختلف من حاسوب لاخر).

طبقة الجلسة:

تتيح طبقة الجلسة تحديد تبادل البيانات وتزامنه، بما في ذلك وسائل بناء نظام التحقق البيانات واستعادتها.

إن حقيقة افتقار الإنترنت لطبقتين يوفرهما النموذج المرجعي (OSI) يطرح سؤالين مهمين: هل الخدمات اللاتي تقدمها هاتان الطريقان غير ضرورية؟

وهل تحتاج التطبيقات إلى هذه الخدمات؟ إن إجابة الإنترنت واضحة وهي نفسها دائما، فالأمر متروك لمطور التطبيق ليقرر ما إذا كانت الخدمة مهمة، وإذا كانت كذلك فإن الأمر متروك لمطور التطبيق لبناء هذه الوظيفة

٣ 1 - 9 - التغليف(Encapsulation)

عزيزي الطالب، من المفاهيم المهمة في نقل الحزم عبر الشبكات مفهوم التغليف، كما يوضح الشكل (١-٢٣).
في المضيف المرسل، يتم تمرير رسالة (Message) طبقة التطبيقات (M) إلى طبقة النقل، وفي أبسط الحالات، تأخذ طبقة النقل الرسالة وتضيف إليها معلومات مقدمة طبقة النقل (H) التي تستخدمها طبقة النقل في جانب المستقبل تشكل رسالة طبقة التطبيق ومعلومات مقدمة طبقة النقل معا شريحة (Segment) طبقة وبالتالي، فإن شريحة طبقة النقل علت رسالة طبقة التطبيقات.
قد تحتوي المعلومات المضافة على معلومات تسمح لطبقة النقل في جانب المستقبل بتسليم الرسالة إلى التطبيق المناسب في الأعلى، وقد تحتوى على بتات كشف الأخطاء التي تسمح للمستقبل بتحديد ما إذا كان قد تم تغيير محتوى الرسالة أثناء انتقالها عبر المسار ثم تمرر طبقة النقل الشريحة إلى طبقة الشبكة التي بدورها تضيف معلومات مقدمة طبقة الشبكة (Hn) وتشمل عنواني النظام النهائي المصدر والوجهة، لتشكل معا مخطط بيانات (Da tangram) طبقة الشبكة ثم يتم تمرير مخطط البيانات إلى طبقة الارتباط، والتي تضيف معلومات مقدمة طبقة الارتباط و انشاء اطار الارتباط اطار طبقة (Frame) طبقة الارتباط.

عزيزي الطالب، تحتوي الحزمة في كل طبقة على نوعين من الحقول:
حقول المقدمة وحقل الحمولة (Payload) أي حزمة البيانات الفعلية من الطبقة الأعلى من جانب آخر، قد يكون التغليف اكثر تعقيدا فمثلا، فلا تقسم الرسالة الكبيرة إلى عدة شرائح، وقد تقسم كل شريحة إلى عدة وحدات بيانات، وفي

جانب المستقبل، يجب إعادة بناء الشريحة من مخططات البيانات المكونة لها.

مسرد المصطلحات

٢٦. التداخل (Interference)
٢٧. التراسل أحادي الاتجاه (Half - duplex) صفحة 10
٢٨. التراسل البسيط (Simplex) صفحة 10
٢٩. التراسل باتجاهين (Full - duplex) صفحة 10
٣٠. لترميز شبه الثلاثي
٣١. التردد والطيف وعرض الحزمة (Frequency , Spectrum and Bandwidth)
٣٢. التضاؤل متعدد المسار (Multipath fading)
٣٣. التضمين (Modulation)
٣٤. التغليف (Encapsulation)
٣٥. الحزم (Packets)
٣٦. الخط المباشر (Direct link)
٣٧. الزوج المجدول غير المحمي (Unshielded Twisted Pair : UTP)
٣٨. الطبقات من أعلى إلى أسفل (Top - Down Approach)
٣٩. الطبقة المادية (Physical Layer)
٤٠. الطلب الهاتفي (Dialup)
٤١. الطيف الترددي Frequency spectrum
٤٢. العلامة والفراغ (Mark and Space)
٤٣. الفاصل الثنائي (Binary Interval)
٤٤. الفاقد في الحزم (Packet loss)
٤٥. الفاقد في الحزم (Packet Loss)
٤٦. الفيضان (Overflow)
٤٧. الكوابل المحورية (Coaxial Cable)
٤٨. الكوابل المحورية (Coaxial Cables)
٤٩. اللاعودة إلى الصفر معكوس
٥٠. اللاعودة إلى مستوى الصفر
٥١. المخازن المؤقتة Buffers
٥٢. المخزن المؤقت (Buffer)
٥٣. المستقطبة (Polar)
٥٤. المطال Amplitude
٥٥. المكونات المادية والبرمجية (Hardware and Software Componets)

٥٦. المنظمة الدولية للمقاييس(ISO)
٥٧. الموجهات(Routers)
٥٨. النفاذ المنزلي(Home Access)
٥٩. بروتوكول الإنترنت(IP)
٦٠. بروتوكول التحكم بالنقل(TCP)
٦١. بروتوكول التحكم بالنقل(Transport Control Protocol : TCP)
٦٢. بروتوكول مخطط بيانات المستخدم(User Datagram Protocol : UDP)
٦٣. تأخير الإرسال(Transmission delay)
٦٤. تأخير الإرسال(Transmission Delay)
٦٥. تأخير الانتشار(Propagation delay)
٦٦. تأخير الانتشار(Propagation Delay)
٦٧. تأخير الطابور(Queuing delay)
٦٨. تأخير الطابور(Queuing Delay)
٦٩. تأخير المعالجة(Processing delay)
٧٠. تأخير معالجة العقدة(Processing Delay)
٧١. تبديل الحزم(Packet Switching)
٧٢. تبديل الدارات(Circuit Switching)
٧٣. تراسل نقطة إلى نقطة(point - to – point)
٧٤. ترميز مانشستر ترميز مانشستر التفاضلى تضاؤل الطيف(Shadow fading)
٧٥. تكميم قيم العينات(Quantization)
٧٦. ثنائي القطبية مع قلب العلامة بالتناوب جهاز الفصل(Splitter)
٧٧. خادمات(Servers)
٧٨. خدمات الإنترنت(Internet Services)
٧٩. خصائص الطور(Phase Characteristics)
٨٠. خط المشترك الرقمي(Digital Subscriber Line : DSL)
٨١. والكوابل(Cable)
٨٢. خطوط الاتصال(Communication Links)
٨٣. خطوط الناقل الضوئي(Optical Carrier : OC)
٨٤. رسالة(Message)
٨٥. شبكات النفاذ(Acces Networks)

٨٦. شريحة (Segment)
٨٧. طابور(Queue)
٨٨. طبقة الارتباط(Link Layer
٨٩. طبقة التطبيق (Application Layer)
٩٠. طبقة الشبكة(Network Layer)
٩١. طبقة النقل(Transport Layer)
٩٢. طيف الإشارة (Spectrum)
٩٣. عرض النطاق الترددي(Bandwidth)
٩٤. عرض النطاق الترددي المطلق(Absolute Bandwidth)
٩٥. عملاء(Clients)
٩٦. عنصر إشارة في الثانية(Signal elements per second)
٩٧. فقدان المسار(Path loss)
٩٨. قنوات الراديو الأرضية والفضائية (Terrestrial and Satellite Radio Channels)
٩٩. م كابل النفاذ إلى الإنترنت(Cable Internet Access)
١٠٠. مخطط بيانات(Datagram)
١٠١. مدة أو طول البت(Bit duration or length)
١٠٢. مزودي خدمة الإنترنت(Internet Service Providers ISPs ")
١٠٣. معدل الإرسال(Transmission Rate)
١٠٤. معدل التضمين أو التباين(Modulation rate)
١٠٥. معدل الخطأ(Error Rate)
١٠٦. معدل بيانات الإشارة(Data signaling rate)
١٠٧. مقسمات الحزم(Packet Switches)
١٠٨. مقسمات طبقة الارتباط(Link - Layer Switches
١٠٩. مكدس بروتوكول الإنترنت(Internet Protocol Stack)
١١٠. نظام تراسل البيانات(DTS Data Transmission System)
١١١. نموذج ترابط الأنظمة المفتوحة. (The OSI Model)

انتهت الوحدة

الوحدة الثانية

2 - 1 | المقدمة

2 - 1 - ١ تمهيد

تعتبر تطبيقات الشبكة سببا رئيساً لإيجاد شبكات الحاسوب، فلو لم تكن هناك تطبيقات مفيدة للشبكات، لما كان هناك حاجة إلى بروتوكولات الشبكة التي تدعم هذه التطبيقات، فمنذ تأسيس الإنترنت، ظهر العديد من التطبيقات المفيدة والمسلية، وكانت هذه التطبيقات القوة الدافعة وراء نجاح الإنترنت، وتحفيز الناس في المنازل والمدارس، والأعمال التجارية لجعل الإنترنت جزءا لا يتجزأ من أنشطتهم اليومية.

وتشمل تطبيقات الإنترنت التطبيقات المستندة إلى النصوص التي أصبحت أكثر انتشارا في سبعينات وثمانينيات القرن الماضي كالبريد الإلكتروني، والوصول إلى أجهزة الحاسوب عن بعد، ونقل الملفات، ومجموعات الأخبار، ثم ظهرت تطبيقات الشبكة العنكبوتية العالمية في منتصف التسعينات، والتي مكنت المستخدم من تصفح الشبكة، والبحث، والتجارة الإلكترونية، وانتهت الألفية الثانية بتطبيقي الرسائل الفورية ومشاركة الملفات.

منذ عام ٢٠٠٠، شهدنا انفجاراً في تطبيقات الصوت و الفيديو بما في ذلك:

تطبيقات الصوت والفيديو

١. الصوت عبر بروتوكول الإنترنت(Voice - over - IP (VoIP

2. المؤتمرات المرئية عبر بروتوكول الإنترنت Video - Conferencing over IP **مثل سكايب**(Skype)

٣. توزيع أو نشر الفيديوها التي يعدها المستخدم مثل موقع يوتيوب.(YouTube)

٤. الأفلام حسب الطلب مثل نيتفليكس (Netflix)**.**

كما شهدت هذه الفترة نفسها ظهور ألعاب الانترنت متعددة اللاعبين، بما في ذلك الحياة الأخرى وعالم الحروب، ثم ظهر مؤخراً جيل جديد من تطبيقات الشبكات الاجتماعية، مثل الفيسبوك وتويتر، التي خلقت شبكات بشرية ناشئة على شبكة الإنترنت عبر الموجهات وروابط الاتصال. ومن الواضح أنه لم يحدث أي تباطؤ في ظهور تطبيقات إنترنت جديدة ومثيرة، وقد تكون أنت مطور الجيل القادم من هذه التطبيقات.

ندرس في هذه الوحدة، الجوانب المفاهيمية والتنفيذية لتطبيقات الشبكة، ونبدأ بتعريف المفاهيم الرئيسة لطبقة التطبيقات، بما في ذلك خدمات الشبكة المطلوبة من قبل التطبيقات، والعملاء والخوادم، والعمليات، وواجهات طبقة النقل. كما نجرب العديد من تطبيقات الشبكة بالتفصيل، بما في ذلك الويب، والبريد الإلكتروني، ونظام أسماء النطاقات (DNS)، وتوزيع الملفات النظير للنظير (P2P)، ثم نقوم بتطوير تطبيقات الشبكة على بروتوكول التحكم بالنقل (TCP) و بروتوكول المخطط البياني للمستخدم (UDP). كما نركز على دراسة واجهة برنامج التطبيق للمقابس (Socket API) وبعض الأمثة البسيطة على تطبيقات العميل الخادم باستخدام لغة بابتون(Python)، وفي نهاية الوحدة، نقدم عددا من المهمات الممتعة والمثيرة حول برمجة المقابس.

تعتبر طبقة التطبيق مدخلا ملائمة للبدء بدراسة البروتوكولات، إذ أنها مألوفة وتعرفنا على العديد من التطبيقات اللي تعتمد على البروتوكولات، وتعطينا فكرة جيدة عنها وتقدم للعديد من القضايا التي نغطيها مرة أخرى عند دراسة: البروتوكولات الخاصة بطبقة النقل، وطريقة الشبكة، وطبقة ربط البيانات

21 - مبادئ تطبيقات الشبكة (Principles of Network Applications)

لنفترض أن لديك فكرة تطبيق شبكة جديد سيقدم خدمة كبيرة للبشرية، أو يجلب لك ثروة كبيرة، أيا كان الدافع سندرس في هذه الوحدة كيف يمكنك تحويل الفكرة إلى تطبيق حقيقي.

تعتبر كتابة البرامج لتعمل على أنظمة مختلفة وتتصل ببعضها البعض عبر الشبكة في صميم تطوير تطبيقات الشبكة، فعلى سبيل المثال، في تطبيقات الويب هناك نوعان من البرامج المميزة التي يتصل بعضها ببعض برنامج المتصفح (Browser) قيد التشغيل على جهاز المستخدم (سطح المكتب، أو الحاسوب المحمول، أو الجهاز اللوحي، أو الهاتف الذكي)؛ وبرنامج خادم الويب قيد التشغيل على الخادم. مثال آخر، في نظام تبادل الملفات النظير-للنظير(Peer - to - Peer : P2P) ، هناك برنامج على كل جهاز مشارك في الملفات، في هذه الحالة، تكون البرامج متشابهة أو متطابقة على مختلف الأجهزة.

لذا، عند تطوير تطبيقك الجديد، تحتاج إلى كتابة برنامج يعمل على أنظمة متعددة، ويمكنك كتابة هذا البرنامج باستخدام أي لغة برمجة مثلc ، أو جافا، أو بايثون، والأهم من ذلك، أنك لن تحتاج إلى كتابة البرنامج ليعمل على أجهزة الشبكة مثل الموجهات (Routers) أو المقسمات(Switches) ، حتى لو كنت تريد أن تكتب البرنامج لهذه الأجهزة الأساسية للشبكة، فلن تكون قادرة على ذلك.

كما تعلم عزيزي الطالب، فإن أجهزة الشبكة الأساسية لا تعمل في طبقة التطبيقات، بل تعمل في طبقات أدني مثل طبقة الشبكة، وهذا التصميم سهل وسرع تطوير البرامج التطبيقية، ونشر مجموعة واسعة من تطبيقات الشبكة كما هو مبين في الشكل (٢-١).ص٤٦

2 - 2 -بنية تطبيقات الشبكة (Network Application Architectures)

قبل الغوص في كتابة كود البرامج، يجب أن يكون لديك خطة معمارية موسعة للتطبيق الخاص بك، واضعا بالحسبان ان بنية التطبيق تختلف بشكل واضح عن بنية الشبكة، فمن وجهة نظر مطور التطبيق، معمارية بالحسبان أن بنية التطبيق تختلف بشكل واضح عن بنية الشبكة، فمن وجهة نظر مطور التطبيق معمارية الشبكة ثابتة وتوفر مجموعة محددة من الخدمات للتطبيقات. من جانب آخر، فإن معمارية التطبيق يصممها مطور التطبيق والتي تفرض بنية التطبيق على مختلف الأنظمة، مستندة إلى أحد النماذج المعمارية السائدة المستخدمة في تطبيقات الشبكة الحديثة: معمارية النظير- للنظير (Peer-to - Peer : P2P) ، أو العميل الخادم(Client-Server).

في معمارية النظير للنظير(P2P) ، هناك حد أدنى من الاعتمادية على خوادم مخصصة في مراكز البيانات، بل يستغل التطبيق الاتصال المباشر بين أزواج من المضيفين المتصلين بشكل متقطع يدعى كل منها النظير، وهي أجهزة غير مملوكة من مزود الخدمة، بل هي أجهزة حاسوب مكتبية أو محمولة يملكها المستخدمون ، ومعظم النظراء يقيمون في المنازل والجامعات والمكاتب، ويتواصلون مع نظرائهم دون المرور بخدمة مخصص. والعديد من التطبيقات الأكثر شيوعا هذه الأيام والتي تشهد حركة كثيفة تستند إلى هذه المعمارية، وتشمل مشاركة الملفات) مثل(BitTorrent ، ومسرعات تحميل الملفات) مثل(Xunlei ، والمهاتفة عبر الإنترنت) مثل(Skype ، والتلفاز عبر بروتوكول الإنترنت (مثل Kankan PPstream). ويوضح الشكل (٢-٢-أ) معمارية النظير للنظير.

ومن أهم سمات معمارية النظير للنظير قابلية التوسع الذاتي، فعلى الرغم من أن كل النظراء يضيفون عبئة جافية عند طلب الملفات في تطبيق مشاركة الملفات، فإن كل نظير يضيف طاقة جديدة للنظام لدى توزيع الملفات على نظرائهم، كما أن هذه المعمارية فعالة من حيث الكلفة، كونها عادة لا تتطلب بنية تحتية وعرض نطاق ترددي كبير للخادم (على عكس تصميم العميل الخادم ومراكز البيانات المستندة إليه)، ومع ذلك،

فإن تطبيقات النظير للنظير ستواجه ثلاثة تحديات رئيسة في المستقبل:

تحديات تطبيقات النظير

الألفة مع مزود خدمة الإنترنت(ISP Friendly):

معظم مقدمي خدمات الإنترنت يستخدمون عرض النطاق الترددي "غير المتماثل"، والذي يرتكز على أن تلقي البيانات (المصب Downstream): أكبر بكثير من رفعها (المنبع Upstream:)، ولكن تدفق الفيديو وتوزيع الملفات في تطبيقات النظير للنظير تركل حركة المرور على المنبع (Upstream Traffic) من الخوادم إلى مزودي خدمات الإنترنت المنزلي، مما يضيف ضغطة كبيرة على مزودي خدمات الإنترنت، لذا، فإن تصميم تطبيقات النظير للنظير المستقبلية يتطلب التركيز على الألفة مع مزودي خدمة الإنترنت

الأمن(Security) [Xie 2008].

بسبب طبيعتها المفتوحة والموزعة إلى حد كبير، فإن تطبيقات النظير للنظير تواجه تحديا كبيرا لتأمينها.

[Dhungel 2008; LeBlond 2011 ٢٠٠٦; Doucer 2002 ; Yu 2006 ; Liang 2006 ; Naoumov.]

الحوافز(Incentives)

يعتمد نجاح تطبيقات النظير للنظير في المستقبل إلى إقناع المستخدمين بالتطوع بعرض النطاق الترددي، وذاكرة التخزين، وموارد الحوسبة لهذه التطبيقات، ما يتطلب تصميم مزيد من الحوافز.

[Feldman 2005 ; Piatek 2008 ; Aperjis 2008 ; Liu ٢٠١٠]

اما في معمارية العميل الخادم، فهناك مضيف يدعى الخادم، يستجيب لطلبات الخدمة الواردة من المضيفين الآخرين، أي العملاء، مثل تطبيق الويب الذي يطلب خدمات من خلال المتصفح الذي يعمل على مضيف المقبل- من خادم (ملقم) الويب، فعندما يتلقى خادم الويب طلبة من العميل، فإنه يستجيب بإرسال الكائن المطلوب اسى مضيف العميل، لاحظ أن العملاء لا يتواصلون مع بعضهم مباشرة؛ ففي تطبيق الويب، لا يتصل متصفحان ت بشكل مباشر، وهناك سمة أخرى لمعمارية العميل الخادم، فالخادم لديه عنوان ثابت ومعروف، يدعى عنوان الانترنت (Internet Protocol: IP)، لذا، يمكن للعميل دائما الاتصال بالخادم عن طريق إرسال إلى عنوانه. ومن التطبيقات

المعروفة في معمارية العميل الخادم
e - Mail Telnet، FTP، Web ويبين الشكل (٢-٢-ب) معمارية العميل الخادم.

في الكثير من الأحيان لا يستطيع خادم واحد تلبية جميع طلبات العملاء، فعلى سبيل المثال، قد تنهار مواقع الشبكات الاجتماعية الشائعة إذا كان لديها خادم واحد فقط يتعامل مع جميع طلباتها، لذا، فإن مركز البيانات، الذي يستضيف عددا كبيرا من الأجهزة، يعمد إلى خلق خادم افتراضي قوي، كما أن المواقع الشائعة التي تقدم خدمات الإنترنت مثل محركات البحث (Bing، Google)ومواقع التجارة الإلكترونية (Amazon ، e – Bay)، ومواقع البريد الإلكتروني(Yahoo Mail Gmail) ، والشبكات الاجتماعية Twitter Facebook توظف مركز بيانات أو أكثر، فعلى سبيل المثال، لدى شركة غوغل ٣٠ إلى ٥٠ مركز بيانات موزعة في جميع أنحاء العالم، تتعاون جميعا لخدمة محرك البحث، واليوتيوب، والبريد الإلكترونيGmail ، ويحتوي كل مركز بيانات مئات الآلاف من الخوادم
ومن الجدير بالذكر، أن بعض التطبيقات ذات معمارية هجينة، أي تجمع بين معماريتي النظير- للنظير والعميل- الخادم ، فالعديد من تطبيقات المراسلة الفورية تستخدم الخوادم لتتبع عناوين الإنترنت IP للمستخدمين، ولكن يتم تبادل رسائل المستخدمين مباشرة بين النظراء (دون المرور بخوادم وسيطة).

٢ ـ ٢ ـ ٢ الاتصال بين العمليات (Processes Communicating)

قبل إنشاء تطبيق الشبكة، نحتاج إلى فهم كيفية تواصل البرامج التي تعمل في أنظمة نهائية (end systems) متعددة بعضها ببعض. في الواقع، واستنادا إلى أنظمة التشغيل، لا تتصل البرامج بحد ذاتها بل العمليات، ويمكن التفكير بأي عملية كبرنامج يعمل في نظام نهائي، وعند تشغيل العمليات على نفس النظام النهائي، تتواصل مع بعضها البعض من خلال الاتصال الداخلي بين العمليات باستخدام قواعد يحكمها نظام التشغيل، ولكننا سنركز على الاتصال بين العمليات التي تعمل على أجهزة (مضيفين) مختلفة ضمن أنظمة تشغيل مختلفة
تتواصل العمليات التي تنفذ على نظامين مختلفين بتبادل الرسائل عبر شبكة الحاسوب، حيث تخلق العملية (المرسل) رسائل وترسلها عبر الشبكة؛

تتلقى العملية (المستقبل) هذه الرسائل وتستجيب بالرد عليها، وكما نجحنا في الشكل (٢-١)، فإن العمليات التي تتصل بعضها ببعض تقيم في طبقة التطبيقات ضمن مكدس البروتوكول ذي الطبقات الخمس.

عمليات العميل والخادم

تكون تطبيق الشبكة من أزواج من العمليات التي تتبادل الرسائل عبر شبكة، فمثلا، في تطبيق الويب تتبادل عملية متصفح العميل الرسائل مع عملية خادم الويب، أما في نظام مشاركة الملفاتP2P ، ينتقل الملف من عملية في أحد النظراء إلى عملية في نظير آخر. ولكل زوج من العمليات المتصلة، نطلق على إحداهما العميل والأخرى الخادم، ففي تطبيق الويب، يكون المستعرض هو عملية العميل وخادم الويب هو عملية الخادم، وفي مشاركة الملفاتP2P ، يكون النظير الذي يحمل (Download)الملف يوصف بأنه العميل، والنظير الذي يرفع (Upload) الملف يوصف بأنه الخادم.

عزيزي الطالب، قد تكون لاحظت أنه في بعض التطبيقات، مثل مشاركة الملفاتP2P ، قد تكون العملية عميلا وخادمة على حد سواء. في الواقع يمكن للعملية في نظام مشاركة الملفات P2P تحميل أو رفع الملفات، مع ذلك، وفي سياق جلسة الاتصال بين زوج من العمليات، يمكنك أن تصف إحداهما كعميل والأخرى كخادم

تعريف: **عمليات العميل والخادم:**

في سياق جلسة اتصال بين زوج من العمليات،

العميل هو العملية التي تبدأ الاتصال (أي تبدأ الاتصال بالعملية الأخرى في بداية الجلسة)،

أما الخادم فهو العملية التي تنتظر الاتصال بها لبدء الجلسة.

الواجهة بين العملية وشبكة الحاسوب

The Interface between the Process and the Computer Network

تتكون معظم التطبيقات من أزواج من العمليات المتصلة، في كل زوج تتبادل العمليتان الرسائل، وأي رسالة يجب أن تمر عبر الشبكة الأساسية، ويتم تبادل الرسائل عبر الشبكة من خلال واجهة برنامج يدعى المأخذ أو المقلب (Socket)، ولفهم العمليات والمقابس، إذا اعتبرنا العملية هي المنزل فإن المقبس يمثل الباب، فعندما من عملية إرسال رسالة إلى عملية أخرى على مضيف آخر، فإنها توجه الرسالة من بابها (أي مقبسها)، وهنا العملية (المرسل) أن هناك بنية تحتية (وسيلة نقل على الجانب الآخر من بابها لنقل الرسالة إلى باب (الهدف)، وبمجرد وصولها إلى المضيف الهدف، يمرر الرسالة من باب العملية الهدف (أي المقبس) لتقوم بدورها بالرد على الرسالة وإجراء المطلوب.

كل (٢-٣) اتصال المقابس بين عمليتين عبر الإنترنت، ويفترض الشكل أن النقل الأساسي بين مليات يتم من خلال بروتوكول التحكم بالنقل TCP.

المقبس هو الواجهة بين طبقة التطبيقات وطبقة النقل داخل المضيف، ويشار إليه أيضا بأنه واجهة برامج التطبيق (API) بين التطبيق و الشبكة، لأنه يمثل واجهة البرمجة التي تبنى عليها تطبيقات الشبكة.

فمطور التطبيق لديه سيطرة كاملة على كل شيء من المقبس من جهة طبقة التطبيقات، ولكن لديه سيطرة طفيفة من جهة طبقة النقل، فهو يسيطر فقط على اختيار بروتوكول النقل، وضبط قليل من معاملات طبقة النقل مثل الحد الأقصى لحجم المخزن المؤقت (buffer) وحجم القطاع (segment).

وعند اختيار بروتوكول النقل (إذا كان متاحا)، يقوم المطور ببناء التطبيق باستخدام الخدمات التي يوفرها البروتوكول. لمزيد من التفصيل، سنتطرق إلى المقابس في القسم ٢-٨.

عمليات العنونة (Addressing Processes)

كما في البريد العادي، إذا أرادت عملية قيد التشغيل على مضيف معين إرسال الحزم إلى عملية قيد التشغيل على مضيف آخر، يجب أن يكون للعملية (المستقبل) عنوان محدد، ولتحديد العملية (المستقبل)، يلزم تحديد نوعين من المعلومات: عنوان المضيف، ومعرف يحدد العملية (المستقبل) في المضيف الهدف. في عالم الإنترنت، يتم تعريف المضيف بعنوان الإنترنت IP الخاص به، كما سنناقش في الوحدة الرابعة، وكل ما نحتاج إلى معرفته الآن هو أن

عنوان الإنترنت (IP Address) هو معرف فريد للمضيف طوله ٣٢ بت في الاصدار الرابع .(IPv4) بعد التعرف على عنوان المضيف الذي تم توجيه رسالة إليه، يجب على العملية (المرسل) أن تحدد العملية (المستقبل)، وخاصة المقبس المستقبل قيد التشغيل على المضيف، لأنه قد يتم تشغيل أكثر من تطبيق على مضيف واحد، ورقم المنفذ (Port number) هو الذي يعالج هذه المسألة، حيث يتم تعيين رقم منفذ لكل تطبيق
. فمثلا، يعرف خادم الويب بالمنفذ رقم ٨٠، والبريد الإلكتروني (باستخدام بروتوكول SMD) يعرف بالمنفذ رقم ٢٥،
وهذا ما سيتم عرضه بالتفصيل في الوحدة الثالثة يمكنك العثور على شانه أرقام المنافذ المعروفة لجميع بروتوكولات الإنترنت القياسية على الرابط
http : / / www . iana . org

٢-٢-٣ خدمات النقل المتوفرة للتطبيقات (Transport Services Available to Applications)

عزيزي الطالب، تذكر أن المقبس هو الواجهة بين عملية التطبيق و بروتوكول طبقة النقل، فالتطبيق من جهة المرسل يرسل الرسائل من خلال المقبس، ومن الجهة الأخرى، بروتوكول طبقة النقل هو المسؤول عن توصيل الرسائل إلى مقبس العملية الهدف.

توفر العديد من الشبكات، بما فيها شبكة الإنترنت، أكثر من بروتوكول طبقة نقل واحد، وعند تطوير تطبيق عليك اختيار أحد البروتوكولات المتاحة، وذلك بدراسة الخدمات التي تقدمها بروتوكولات طبقة النقل المتاحة ومن ثم اختيار البروتوكول الذي يقدم الخدمات التي تنطبق مع احتياجات تطبيقك، و يمكن تصنيف الخدمات الممكنة التي يقدمها بروتوكول طبقة النقل في أربعة محاور: النقل الموثوق للبيانات، والإنتاجية، والتوقيت، والأمن.

خدمات بروتوكول طبقة النقل

١ - النقل الموثوق للبيانات(Reliable Data Transfer)

قد تضيع الحزم في شبكة الحاسوب عندما تتجاوز حجم المخزن المؤقت للموجه(Router) ، أو قد يهملها المضيف أو الموجه إذا كانت بعض البنات تالفة، وفي العديد من التطبيقات مثل البريد الإلكتروني، ونقل الملفات، والوصول إلى المضيف عن بعد، ونقل وثائق الويب، والتطبيقات المالية، قد يكون لفقدان البيانات تبعات خطرة، ولدعم هذه التطبيقات، لا بد من التدخل لضمان أن البيانات المرسلة يتم تسليمها في الطرف الآخر من التطبيق صحيحة وكاملة، فإذا وفر البروتوكول مثل هذه الخدمة المضمونة لتسليم البيانات، يقال أنه يوفر نقلا موثوقة للبيانات، ومن الخدمات المهمة التي قد يقدمها بروتوكول طبقة النقل للتطبيق هو النقل الموثوق للبيانات من عملية إلى عملية، وفي هذه الحالة، ما على العملية (المرسل) إلا أن تمرر بياناتها إلى المقبس، ولديها الثقة الكاملة بأن البيانات ستصل العملية (المستقبل) دون أخطاء، وإلا فإن البيانات التي ترسلها عملية قد لا تصل أبدا إلى العملية الهدف. قد يكون هذا مقبولا في التطبيقات التي تسمح بذلك، كمعظم

الوسائط المتعددة التي قد تسمح بفقدان بعض البيانات، إذ تؤدي البيانات المفقودة إلى خلل بسيط في الصوت أو الفيديو لا يشكل فرقة واضحة في الجودة.

٢ـ الإنتاجية(Throughput)

عزيزي الطالب، مفهوم الإنتاجية المتاحة، في سياق جلسة اتصال بين عمليتين على مسار شبكة، هو معدل البنات التي تستطيع العملية (المرسل) تسليمها للعملية (المستقبل)، وكون الجلسات الأخرى ستتقاسم عرض النطاق الترددي على مسار الشبكة، وكونها تأتي وتذهب، فإن الإنتاجية المتاحة قد تتقلب مع مرور الوقت، وتقودنا هذه الملاحظات إلى خدمة طبيعية أخرى قد يوفرها بروتوكول طبقة النقل، وهي ضمان الإنتاجية الملاحة بمعدل محدد، عندها يمكن للتطبيق طلب معدل إنتاجية مضمون (r) بت/ ثانية، وبروتوكول النقل هو الذي ياكد ان الإنتاجية المتاحة دائمة (r بت/ثانية) على الأقل. هذه الإنتاجية المضمونة ستجذب العديد من التطبيقات ، فعلى سبيل المثال، إذا كان ترميز الصوت بمعدل ٣٢ كيلوبت في الثانية في أحد تطبيقات المهاتفة ، فإنه يرسل البيانات إلى الشبكة ليتم تسليمها إلى المتلقي بالمعدل ذاته، وإذا لم يتمكن البروتوكول فإن التطبيق يحتاج إلى تقليل معدل الترميز (وتلقي ما يكفي من الإنتاجية للحفاظ على هذا المعدل) أو قد يضطر إلى التوقف لأن استقبال نصف الإنتاجية اللازمة، مثلا، قلما يستخدمه تطبيق المها عبر الإنترنت.

عزيزي الطالب، يطلق على التطبيقات التي لديها متطلبات للإنتاجية تطبيقات حساسة لعرض النطاق الترددي (Bandwidth - sensitive applications)، والعديد من تطبيقات الوسائط المتعددة الحالية من هذا النه على الرغم أن بعضها قد يستخدم تقنيات ترميز تكيفية للصوت الرقمي أو الفيديو بمعدل يتناسب مع الإنتاجية المتاحة، أما التطبيقات المرنة (Elastic Applications) فقد تستنفد قدرا قليلا او كبيرا من الإنتاجية حسبما هو متاح، وكلما زادت الإنتاجية أفضل، مثل البريد الإلكتروني، ونقل الملفات، ونقل الويب.

٣- التوقيت(Timing)

قد يوفر بروتوكول طبقة النقل ضمانات التوقيت بأشكال عدة، كأن يضمن وصول كل بت يرسله المرسل عبر المقبس إلى مقبس المستقبل بما لا يزيد عن ١٠٠ ميلي ثانية. هذه الخاصية مهمة في تطبيقات الزمن الحقيقي التفاعلية، مثل المهاتفة عبر الإنترنت، والبيئات الافتراضية، والمؤتمرات عن بعد، والألعاب متعددة اللاعبين، وغيرها التي تتطلب الدقة في توقيت تسليم البيانات، فالتأخير في المهاتفة عبر الإنترنت مثلا قد يؤدي إلى انقطاع غير طبيعي في المحادثة، فيبدو التطبيق أقل فاعلية.
ورغم عدم وضع قيود صارمة على التأخير في غير تطبيقات الزمن الحقيقي، إلا أن زمن التأخير كلما قل كان أفضل.

٤- الأمن(Security)

يوفر بروتوكول النقل للتطبيق واحدة أو أكثر من خدمات الأمن، ففي المضيف المرسل مثلا، يمكن لبروتوكول النقل تشفير البيانات التي ترسلها العملية (المرسل)، وفك التشفير لدى المضيف المستقبل قبل تسليم البيانات للعملية المستقبل)، ومن شأن هذه الخدمة أن توفر السرية (Confidentiality) بين العمليتين حتى وإن كان يمكن ملاحظة البيانات بطريقة أو بأخرى بين العمليات المرسلة والمستقبلة، وقد يوفر بروتوكول النقل خدمات أخرى سلامة البيانات (Integrity) والمصادقة.(Authentication)

٤ ـ ٢ ـ ٢ خدمات النقل التي تقدمها الإنترنت (Transport Services Provided by the Interne)

عزيزي الطالب، حتى هذه اللحظة، ما زلنا نفكر في خدمات النقل التي توفرها شبكة الحاسوب بشكل عام، دعنا الآن نكون أكثر تحديدا ونختبر نوع خدمات النقل التي توفرها شبكة الإنترنت. توفر الإنترنت (أو شبكات TCP / IP بشكل عام للتطبيقات بروتوكولي نقل هما: بروتوكول مخطط بيانات المستخدم IIDD. User Datagram Proto) و برتوكول التحكم بالنقل (Transport Control Protocol: TCP)،

وعندما تقوم بإنشاء تطبيق شبكه جديد على الإنترنت، عليك أولا اتخاذ القرار باستخدام بروتوكول UDP من كل منهما يقدم مجموعة مختلفة من الخدمات للتطبيقات التي تطلبها، ويبين الشكل (٢-٤) متطلبات الخدمة لمجموعة من التطبيقات المختارة.

خدمات بروتوكول التحكم بالنقل TCP Services

عندما يستدعي أحد التطبيقات بروتوكول التحكم بالنقل(TCP) ، فإنه يتلقى نوعين من الخدمة حسب نموذج خدمة TCP كما يأتي:

الخدمة الموجهة بالاتصال (Connection - oriented Services):

لدى بروتوكول TCP يتبادل العميل والخادم معلومات التحكم الخاصة بطبقة النقل قبل أن تبدأ رسائل التطبيق بالتدفق، وهذا ما يسمى إجراء المصافحة (handshaking)الذي ينبه العميل والخادم ويسمح لهما بتحضير دفعة من الحزم. بعد مرحلة المصافحة، يدخل اتصال TCP حيز الوجود بين مقبسي العمليتين، وهو اتصال باتجاهين (full - duplex) يسمح للعمليتين بإرسال الرسائل إلى بعضها البعض في نفس الوقت، وعند انتهاء التطبيق من إرسال الرسائل ينتهي الاتصال. في الوحدة الثالثة سنناقش بالتفصيل الخدمة الموجهة بالاتصال وكيفية تنفيذها.

خدمة النقل الموثوق للبيانات(Reliable Data Transfer Services):

تستطيع العمليات المتصلة الاعتماد على بروتوكول TCP لتسليم جميع البيانات المرسلة خالية من الخطأ وبالترتيب السليم، فعندما يمرر أحد جانبي التطبيق دفعة من وحدات البايت في مقبس المرسل، فإنه يستطيع الاعتماد على TCP لتسليم الدفعة ذاتها إلى مقبس المستقبل دون فقدان أو تكرار

التركيز على الأمنFocus on Security

تأمين بروتوكول التحكم بالنقلTCP

لا يتوفر بروتوكول TCP او UDP أي تشفير، أي أن البيانات التي تمررها عملية ما من مقبسها هي نفس البيانات التي
تنتقل عبر الشبكة إلى وجهتها، لذلك، على سبيل المثال، فإذا أرسلت كلمة مرور في نص واضح (أي، غير مشفرة) فيمقبسها، فإنها ستنتقل عبر جميع الوصلات بين المرسل والمستقبل، وقد تكتشف في أي من هذه الوصلات، ولان الخصوصية وقضايا الأمن الأخرى أصبحت حاسمة في كثير من التطبيقات، فقد أجرى مجتمع الإنترنت تحسينات

لتعزيز بروتوكولTCP ، تدعي طبقة المقابس الآمنة(Secure Socket Layer: SSL)
فلم يعد بروتوكول TCP المعزز ب SSL يعمل بشكل تقليدي، بل أصبح يقدم خدمات أمنية حاسمة بين العمليات، بما في ذلك التشفير وسلامة البيانات، والمصادقة.

ونؤكد هنا أن SSL ليس بروتوكول نقل ثالث بنفس مستوى TCP وUDP ،
بل هو تعزيز ينفذ هذه التحسينات في طبقة التطبيقات، وخاصة إذا كان التطبيق يريد استخدام خدمات SSL ولتطبيق ذلك، يتم إدراج الكود الخاص بها

في التطبيق من جانب العمل والخادم على حد سواء (يتوفر الكود على شكل مكتبات برمجية مفتوحة).

لدي SSL مقبس API خاص يشبه ذلك الخاص ببروتوكول TCP التقليدي، فعندما يستخدم التطبيق طبقة SSL فإن المرسل يمرر النص الواضح للبيانات إلى مقبس SSL الذي يقوم بتشفير البيانات في المضيف المرسل، ثم يمرر البيانات المشفرة إلى مقبس TCP. تنتقل البيانات المشفرة عبر الإنترنت إلى مقبس TCP للمستقبل ويمررها إلى SSL الذي يقوم بدورة بفك تشف البيانات، وفي النهاية يمرر SSL النص الواضح للبيانات عبر مقبس SSL إلى العملية (المستقبل).

يوفر بروتوكول TCP أيضا آلية لضبط الازدحام(Congestion- control) ، وهي خدمة عامة لصالح الانترنت وليست لمنفعة العمليات المتصلة بشكل مباشر، وتعمل آلية ضبط الازدحام كصمام يقلص تدفق البيانات من عملية المرسل (العميل أو الخادم) عندما تكون الشبكة مزدحمة بين المرسل والمستقبل. وكما سنوضح في الوحدة الثالثة، فإن ضبط الازدحام من خلال TCP يحاول أيضا أن يحدد لكل اتصال TCP حصته العادلة من عرض النطاق الترددي للشبكة

خدمات بروتوكول مخطط بيانات المستخدم UDP Services

بروتوكول UDP هو بروتوكول نقل خفيف الوزن، ويوفر الحد الأدنى من الخدمات، وهو بروتوكول بدون اتصال، لذا، ليس هناك مصافحة قبل أن تبدأ العمليتان بالاتصال، كما يوفر خدمة نقل غير موثوق للبيانات، أي عندما ترسل عملية رسالة إلى مقبسUDP ، فلن تضمن أن الرسالة ستصل إلى العملية المستقبل، وإن وصلت فقد تكون بغير ترتيبها الأصلي.
من جانب آخر، لا يتضمن بروتوكول UDP آلية لضبط الازدحام، وبالتالي فإن المرسل من خلال UDP يمكنه ضخ البيانات نحو الطبقة التي تدنو (طبقة الشبكة) بأي معدل يحلو له، ومع ذلك، فإن الإنتاج الفعلي قد يكون أقل من هذا المعدل نظرا لمحدودية طاقة الإرسال أو نتيجة للازدحام.

الخدمات التي لا تقدمها بروتوكولات النقل عبر الإنترنت Services Transport Protocols Not Provided by Internet

لا بد انك لاحظت، عزيزي الطالب، أننا لم نشر في نقاشنا بشكل واضح إلى ضمان الإنتاجية أو التوقيت، لكن هذا يعني اننا لن نتمكن من تشغيل التطبيقات الحساسة للزمن، مثل المهاتفة عبر الإنترنت؟ بالطبع لا، بل هي

تعمل منذ سنوات عدة، ولكن هذه التطبيقات، غالبة، تعمل بشكل جيد لأنها مصممة للتعامل، إلى اقصى ممكن، مع هذا النقص في الضمان. وباختصار، فإن الإنترنت اليوم قد تقدم خدمة مرضية للتطبيقات للزمن في كثير من الأحيان، ولكن لا يمكنها أن توفر أي ضمانات على التوقيت أو الإنتاجية.

يشير الشكل (٢-٥)ص ٥٥
إلى بروتوكولات النقل المستخدمة في بعض تطبيقات الإنترنت الشائعة، حيث تجد أن البريد الإلكتروني، والوصول للحواسيب عن بعد، وشبكة الإنترنت، ونقل الملفات جميعها تستخدمTCP وذلك أن TCP ، في المقام الأول، يقدم نقلا موثوقة للبيانات، كما يضمن وصول جميع البيانات في نهاية المطاف إلى وجهتها. ولأن تطبيقات الاتصال الهاتفي عبر الإنترنت (مثل سكايب) قد تحتمل في كثير من الأحيان بعض الخسائر، ولكنها تتطلب حدا أدني لمعدل النقل لتكون فعالة، يفضل المطورون عادة تشغيل تطبيقاتهم الهاتفية على UDP للالتفاف على آلية ضبط الازدحام وبتات التحكم الإضافية في TCP، وكون العديد من الجدران النارية تمنع معظم أنواع حركة المرور عبر UDP، لذا فإن تطبيقات الاتصال الهاتفي عبر الإنترنت غالبا تصمم لاستخدام TCP احتياطا إذا فشل الاتصال عبر UDP .

٥ 2 - 2 - بروتوكولات طبقة التطبيقات)

(Application - Layer Protocols)لقد علمت للتو، عزيزي الطالب، أن عمليات الشبكة تتواصل مع بعضها البعض بإرسال الرسائل عبر المقابس، ولكن كيف يتم تنظيم هذه الرسائل؟ وما معاني الحقول المختلفة في الرسائل؟ ومتي ترسل العمليات هذه الرسائل؟ كل هذه الأسئلة تعيدنا إلى بروتوكول طبقة التطبيقات، والذي يحدد كيف تتمكن عمليات أحد التطبيقات، الذي يعمل على انظمة مختلفة، من تمرير الرسائل لبعضها البعض. بالتحديد، يحدد بروتوكول طبقة التطبيقات ما يأتي:

١. أنواع الرسائل المتبادلة، مثل رسائل الطلب ورسائل الاستجابة.
٢. صياغة الرسائل بأنواعها المختلفة، مثل حقول الرسالة وكيفية وصفها أو رسمها.

٣. دلالات الحقول، أي معاني المعلومات الواردة في الحقول.
٤. قواعد لتحديد متى وكيف يمكن لعملية أن ترسل الرسائل وتستجيب لها.

عزيزي الطالب، من المهم أن نميز بين تطبيقات الشبكة وبروتوكولات طبقة التطبيقات، يمثل بروتوكول طبقة واحدا من تطبيق الشبكة (مع ذلك، فهو جزء مهم جدا من التطبيق)، دعنا ننظر إلى بعض الأمثلة.

مثال (٢-١) ص٥٦

تطبيق الويب: هو تطبيق عميل-خادم يتيح للمستخدم الحصول على وثائق من خواد الطلب، وهو يتكون من العديد من العناصر، بما في ذلك معيار لتنسيق المستندات (أي،)متصفحات الويب (مثل، فاير فوكس ومايكروسوفت إنترنت إكسبلورر)، خوادم الويب (مثل، أي وخوادم مايكروسوفت)، وبروتوكول طبقة تطبيقات الويب (HTTP) الذي يحدد تنسية انمي المتبادلة وتسلسلها بين المتصفح وخادم الويب. لاحظ أن HTTP هو جزء واحد فقط ولكنه جزء مهم من تطبيق الويب.

مثال (٢-٢) ص٥٦

تطبيق البريد الإلكتروني عبر الإنترنت: يتكون التطبيق من عدة عناصر؛ خادم البريد الذي يحتوي على صناديق بريد المستخدمين؛ عملاء البريد (مثل مايكروسوفت أوتلوك) الذي يسمح للمستخدم بقراءة الرسائل وإنشائها؛ معيار يحدد بنية رسالة البريد الإلكتروني؛ وبروتوكول طبقة التطبيقات الذي يحدد كيف يتم تمرير الرسائل بين الخوادم، وكيف يتم تمرير الرسائل بين الخوادم وعملاء البريد الإلكتروني، وكيفية تفسير محتوى مقدمة الرسائل. بروتوكول طبقة التطبيقات الرئيس للبريد الالكتروني هو بروتوكول نقل البريد البسيط

(Simple Mail Transfer Protocol : SMTP) حسب المرجع رقم [RFC ٥٣٢١].

وهنا أيضا، لاحظ أن بروتوكول البريد الإلكتروني الأساس (SMTP) هو جزء واحد فقط، ولكنه جزء مهم من تطبيق البريد الإلكتروني.

2 - 2 -تطبيقات الشبكة التي يغطيها المقرر (Covered Network Applications)

في هذه الوحدة نناقش خمسة تطبيقات مهمة:

١. شبكة الإنترنت(Web) ،
٢. ونقل الملفات(FTP) ،
٣. والبريد الالكتروني (e - Mai) ،
٤. وخدمة الدليل(DNS) ،
٥. وتطبيقات النظير للنظير. (P2P)
٦.

علينا أولا أن نبحث في الويب، لا لانه تطبيق شائع فحسب، بل لأن بروتوكول طبقة التطبيقات، HTTPواضح و مباشر وسهل الفهم. ثم ندرس FTP بإيجاز، كونه لا يختلف كثيرا عن HTTP. ثم ننتقل لنناقش البري الإلكتروني، أول تطبيق إنترنت مهم، وهو أكثر تعقيدا من الويب، بمعنى أنه يوظف عدة بروتوكولات في ص التطبيقات ثم نغطي بعد ذلكDNS ، الذي يوفر خدمة دليل الإنترنت، إذ يلاحظ أن معظم المستخدمين يتفاعلون بشكل غير مباشر مع DNSمن خلال التطبيقات الأخرى (مثل شبكة الإنترنت، ونقل الملفات، والبرد الالكتروني)، فهو يوضح كيف يمكن لوظيفة جوهرية بسيطة (ترجمة اسم الشبكة إلى عنوان الشبكة) أن تناقش
طبقة التطبيقات في الإنترنت. واخيرا،

نناقش في هذه الوحدة تطبيقاتP2P ، مع التركيز على تصين مشاركة الملفات، وخدمات البحث الموزعة

2 الشبكة العنكبوتية وبروتوكول نقل النص التشعبي(The Web and HTTP)

حتى في أوائل التسعينات تم استخدام الإنترنت في المقام الأول من قبل الباحثين، والأكاديميين، وطلاب الجامعات التسجيل الدخول إلى الحاسوب (المضيف) عن بعد، ونقل الملفات من الحاسوب المحلي إلى البعيد، والعكس بالعكس، كما استخدم في تلقي الأخبار ورسائل البريد الإلكتروني وإرسالها، وعلى الرغم من أن هذه التطبيقات كانت (وما زالت مفيدة للغاية، لم يكن الإنترنت معروفة خارج الأوساط الأكاديمية والبحثية. وفي بداية التسعينات ظهر تطبيق جديد على المشهد وهو الشبكة العنكبوتية العالمية (World Wide Webd:

WWW) [Berners - Lee 1994]، وكان الويب من تطبيقات الإنترنت الأولى الملفتة للنظر، غير أنها تغيرت بشكل كبير ومستمر فيما يخص تفاعل الناس داخل بيئات عملهم وخارجها، ثم ارتقت الإنترنت من مجرد واحدة من العديد من شبكات البيانات إلى شبكة البيانات الأساسية الوحيدة.

ولعل أكثر ما يروق للمستخدمين أن الشبكة تعمل عند الطلب على عكس وسائل الإعلام التقليدية كالإذاعة والتلفاز، بالإضافة إلى العديد من الميزات الرائعة التي أحبها الناس، فمن السهل جدا لأي فرد توفير المعلومات عبر الإنترنت ونشرها بكلفة قليلة للغاية، وتساعدنا محركات البحث على التنقل في عدد لا حصر له من مواقع الإنترنت، والرسومات، والاستمارات، وسندات الجافا(JavaScript) ، وتطبيقات الجافا، والعديد من الأدوات التي تمكننا من التفاعل مع الصفحات والمواقع، كما وفر الويب منصة للعديد من التطبيقات الناشئة بعد عام ٢٠٠٣، بما في ذلك يوتيوبYouTube ، وبريد جوجلGmail ، والفيسبوك.Facebook

2 - 3 - 1لمحة حول بروتوكول نقل النص التشعبي (Overview of HTTP)

بروتوكول نقل النص التشعبيHTTP (HyperText Transfer Protocol:
هو بروتوكول طبقة الطبقات الويب، في قلب الشبكة العنكبوتية، وتم تعريفه في [١٩٤٥ RFC]و [٢٦١٦ RFC] ، ويطبق على المختلفة في برنامجين: برنامج العميل وبرنامج الخادم اللذان يتحادثان مع بعضهما البعض من خلال تبادل الرسائل HTTP، حيث يحدد HTTP بنية هذه الرسائل وكيفية تبادلها، وقبل الدخول في التفاصيل، لا بد لنا أن نستعرض بعض المصطلحات المهمة.

صفحة الويب تتكون من مجموعة من الكينونات، والكائن هو مجرد ملف مثل ملفHTML ، أو صورة - برنامج جافا، او مقطع فيديو، قابلة للعنونة بعنوان أو رابط واحد يطلق عليه موقع المعلومات العالمي (Universal Resource Locator: URL). معظم صفحات الويب تتكون من ملفHTML أساس يشير إلى كائنات متعددة، فمثلا، إذا كانت صفحة الويب تحتوي على نصHTML و خمسة صور JPEG ، فإنها تتكون من ستة كائنات: ملف HTML أساس وخمس صور، ويشير ملف HTML إلى مراجع الكائنات الأخرى في الصفحة مع عناوينهاURLs ، و يتكون كل عنوان للخادم الذي يضم الكائن و اسم مسار الكائن

.

مثال (٢-٣) ص ٥٨

حدد مكونات عنوان URL الآتي:
http://www.someSchool.edu/some Department/picture.gif
الإجابة: اسم مضيف الخادم هو:
http://www.someSchool.edu
اسم المسار: /some Department/picture.gif

ولأن متصفحات الويب (مثل إنترنت إكسبلورر وفايرفوكس) تنفذ ما يخص العميل من HTTP في سباق الويب، سنستخدم الكلمات المتصفح والعميل بشكل متناوب. أما خوادم الويب، التي تنفذ ما يخص الخادم منHTTP ، فتستضيف الكائنات كل بعنوانه الخاص، وأكثر خوادم الويب شعبية أباتشي (Apache) وخادم

معلومات الإنترنت

- (Internet Information Server: IIS)

يحدد بروتوكول HTTP كيف يطلب العملاء صفحات الويب من الخوادم، وكيف تنقل الخوادم صفحات الويب للعملاء.
ويبين الشكل (٢-٦) ص٥٩
الفكرة العامة، فعندما يقوم المستخدم بطلب صفحة ويب (بالنقر على ارتباط تشعبي) يرسل المتصفح إلى الخادم رسائل طلب HTTP لكائنات محددة من الصفحة، فيتلقى الخادم الطلبات ويستجيب لها برسائل استجابة HTTP تحتوي الكائنات المطلوبة.
يستخدم بروتوكول HTTP بروتوكول النقل الأساس TCP، فيبادر عميل HTTP بداية بإنشاء اتصال TCP مع الخادم، وبمجرد إنشاء الاتصال، تصل عمليات المتصفح والخادم إلى TCP من خلال واجهات مقابسها، وكما أوضحنا في القسم ٢-٢ ، فعلى جانب العميل تمثل واجهة المقبس الباب بين عملية العميل والاتصال ببروتوكول TCP،
و على جانب الخادم تمثل الباب بين عملية الخادم والاتصال ببروتوكول TCP.
يرسل العميل رسائل طلب HTTP إلى واجهة مقبسه،
ويتلقى رسائل استجابة HTTP منها، وبالمثال، يتلقى الخادم رسائل طلب HTTP من واجهة مقبسه و يرسل رسائل الاستجابة إليها، فعندما يرسل العميل يرسل العميل رساله الى واجهة مقبسه، تخرج الرسالة من العميل إلى بروتوكول TCP الذي يوفر لبروتوكول HTTP خدمة نقل موثوق للبيانات، وهذا يعني أن كل رسالة طلب HTTP أرسلتها عملية العميل ستصل سليمة إلى الخادم، وبالمثل ، فان كل رسالة استجابة HTTP أرسلتها عملية الخادم ستصل في نهاية المطاف سليمة إلى العميل، وهنا نلاحظ واحدة من أهم

مزايا معمارية الطبقات؛ إذ لا داع للقلق لدى HTTP من فقدان البيانات او اي تفاصيل حول كيفية استردادها أو إعادة ترتيبها داخل الشبكة، فهذه وظيفة بروتوكول TCP و بروتوكولات الدنيا من مكدس البروتوكول.

لاحظ، عزيزي الطالب، أن الخادم يرسل الملفات المطلوبة للعملاء دون تخزين أي معلومات عن حالة العميل، فإذا طلب عميل معين نفس الكائن مرتين في بضع ثوان، يعيد إرسال الكائن، وكأنه نسي ما فعله سابقا، وكونه لا يحتفظ بمعلومات حول حالة العملاء، يقال أن بروتوكول HTTP عديم الحالة. لاحظ أيضا أن شبكة الإنترنت تستخدم معمارية العميل الخادم كما هو موضح في القسم ٢-٢، فخادم الويب يعمل دائما، وله عنوان انترنت IP ثابت، كما يقدم الخدمة لجميع الطلبات من ملايين المتصفحات المختلفة.

٢ 2 - 3 - الاتصالات الدائمة وغير الدائمة (Non - Persistent and Persistent Connections) .

في العديد من تطبيقات الإنترنت، يتواصل العميل والخادم لفترة من الزمن، يطلب العميل سلسلة من الطلبات والخادم يستجيب. واعتمادا على التطبيق وعلى كيفية استخدامه، يمكن تنفيذ سلسلة من الطلبات دوريا على فترات منتظمة أو متقطعة. وعندما يأخذ تفاعل العميل الخادم مجراه عبر TCP ، يحتاج مطور التطبيق إلى اتخاذ القرار: هل ينبغي لكل زوج (طلب/استجابة) أن يرسل عبر اتصال TCP مستقل، أم أن ترسل جميع الطلبات والاستجابات المتعلقة بها عبر نفس الاتصال؟ تسمى الطريقة الأولى أعلاه الاتصال غير الدائم أو المتقطع (Non - Persistent Connection)، والثانية يطلق عليها الاتصال الدائم أو الثابت (Persistent Connection).

ولفهم هذه المسألة في التصميم، دعنا نختبر مزايا وعيوب الاتصال الدائم في تطبيق محدد البروتوكول HTTP، حيث أنه يستخدم الطريقتين؛ الاتصال

الدائم في الوضع الافتراضي، ويمكن إعداد العميل والخادم لاستخدام الاتصال غير الدائم.

بروتوكول نقل النص التشعبي والاتصالات الغير الدائمة HTTP with Non-Persistent Connections

عزيزي الطالب، دعنا نتتبع خطوات نقل صفحة ويب من الخادم إلى العميل لحالة الاتصالات غير الدائمة فلنفترض أن الصفحة تتكون من ملف HTML و ١٠ صور من نوع JPEG ، أي ١١ كائن وافترض أن عنوان URL لملف HTML الأساس هو:

http://www.someSchool.edu/some Department/home.index

خطوات نقل صفحة ويب

فيما يلي أهم الخطوات من البداية إلى النهاية

١ . تنشئ عملية العميل HTTP اتصال TCP بالخادم WWW . SomeSchool . edu على المنفذ (port) رقم ٨٠، وهو المنفذ الافتراضي لبروتوكول HTTP. ويصحب اتصال TCP تفعيل مقبسى العميل والخادم.

٢ . يرسل عميل HTTP رسالة طلب إلى الخادم عبر مقبسه تتضمن اسم المسار على النحو الآتي.

someDepartment/home.index

٣ .تتلقى عملية الخادم HTTP رسالة الطلب عبر مقبسها، وتسترجع الكائن

SomeDepartment / home . index

من وسط التخزين (الذاكرة المؤقتة أو القرص)، وتغلف الكائن في رسالة استجابةHTTP ، وترسلها إلى العميل عن طريق المقبس.

٤. تبلغ عملية الخادم بروتوكول TCP ليقوم بإغلاق الاتصال، ولكن بروتوكول TCP لا ينهي الاتصال فعلا حتى يتأكد أن العميل تلقى رسالة استجابة سليمة.

٥. يتلقى العميل رسالة الاستجابة، وينتهي اتصالTCP ، وتشير الرسالة إلى أن الكائن المغلف هو ملف
HTML، فيقوم العميل باستخراج ملف HTML وفحصه ليجد مراجع لعشرة كائنات JPEG.

٦. يتم تكرار الخطوات (١-٤) لكل كائن من كائنات JPEG المشار إليها.
بمجرد حصول المتصفح على صفحة الويب، فإنه يعرضها للمستخدم، ولا علاقة لبروتوكول HTTP كيف يفسر العميل صفحة الويب، توضح الخطوات أعلاه الاتصال غير الدائم، حيث يغلق كل اتصال TCP بعد ارسال كل كائن، ففي هذا المثال، عندما يطلب المستخدم صفحة الويب، يتم إنشاء ١١ اتصال.TCP

في الواقع، يمكن للمستخدمين إعداد المتصفحات الحديثة للتحكم بعدد الاتصالات التي يمكن إنشاؤها على التوازي، في الوضع الافتراضي، أكثر المتصفحات تفتح ٥-١٠ اتصالاتTCP ، كل اتصال له حركة طلب. استجابة، ويمكن للمستخدم تحديد العدد الأقصى بقيمة (١)، أي على التوالي، وكما سنر في الوحدة التالية فإن الاتصالات المتوازية تقلل زمن الاستجابة.

التقدير الوقت المستغرق من لحظة طلب العميل ملف HTML حتى استلامه، لا بد من قياس زمن الذهاب الإياب

زمن الاستجابة (Round - Trip Time : RTTT).

، وهو الزمن الذي تستغرقه حزمة صغيرة للانتقال من العميل إلى الخادم ثم العودة إلى العميل،

ويتضمن التأخير في انتشار الرزم، وتأخير الاصطفاف معالجة الرزم (حسبما ناقشنا في القسم ١-٨). لنتأمل الآن ما يحدث عندما ينقر المستخدم على ارتباط تشعبي الشكل (٢-٧) ص٦١، ينشئ المتصفح اتصال TCP مع خادم الويب وتحدث مصافحة ثلاثية – فيرسل
العميل مقطع TCP صغير للخادم، فيقر الخادم بالاستلام ويستجيب بمقطع TCP آخر، وأخيرا، يقر العميل للخادم بالاستلام.
أول جزأين يحتاجان RTT واحدة، ثم يرسل العميل رسالة طلب HTTP مع الجزء الثالث من المصافحة الثلاثية الاعتراف) في اتصالTCP ،
وفور وصول رسالة الطلب إلى الخادم، يبدأ بإرسال ملف HTML عبر اتصال TCP، وبذلك يكون مجموع زمن الاستجابة هو 2RTTsبالإضافة إلى زمن إرسال ملف HTML لدى الخادم.

بروتوكول نقل النص التشعبي والاتصالات الدائمة HTTP with Persistent Connections

للاتصالات غير الدائمة بعض نقاط الضعف، أولا، يجب إنشاء اتصال جديد والاحتفاظ به لكل كائن، لكل منها بحب حجز مخازن والاحتفاظ بمتغيرات TCP لدي كل من العميل والخادم، مما يضيف عبئا كبيرا على خادم الويب الذي يخدم مئات العملاء في نفس الوقت. ثانيا، كما وصفنا للتو، كل كائن يعاني من زمن تأخير بقيمة 2RTTs.
أما الاتصالات الدائمة، يبقي الخادم اتصال TCP مفتوحا بعد إرسال الاستجابة لتبادل الطلبات والاستجابات اللاحقة مع نفس العميل عبر الاتصال نفسه، ففي المثال أعلاه، يمكن إرسالها ملف HTML و١٠ صور عبر اتصال TCP دائم واحد. علاوة على ذلك، يمكن إرسال صفحات ويب متعددة من نفس الخادم لنفس العميل عبر اتصال TCP دائم واحد.

في العادة، يغلق خادم HTTP الاتصال إذا لم يستخدم لفترة معينة (timeout interval)، و في الوضع الافتراضي يستخدم HTTP الاتصالات الدائمة مع خط الأنابيب (pipelining). سنقوم بمقارنه

أداء الاتصالات غير الدائمة والدائمة في واجبات الوحدتين الثانية والثالثة، ولمزيد من التفاصيل أن على الاطلاع على المرجعين [Nielsen 1997 ، ١٩٩٧ Heidemann. ١٩٩٧

٣ 2 - 3 - تنسيق رسائل النص التشعبي(HTTP Message Format)

تشمل مواصفات[HTTP RFC 1945] ، و [RFC ٢٦١٦تعريفات لصيغة رسالةHTTP ، وهناك نوعان. من رسائلHTTP ،

١. رسائل الطلب

٢. ورسائل الرد (الاستجابة)،

سنناقشهما حالا.

رسالة الطلب HTTP Request Message

أولا، نلاحظ أن الرسالة مكتوبة بنص ASCII العادي حيث يمكن لشخص غير خبير بالحاسوب قراءتها. ثانيا، تتألف الرسالة من خمسة أسطر، ومع ذلك يمكن أن يكون عدد الأسطر أكثر من ذلك أو أقل لغاية سطر واحد فقط، ويطلق على السطر الأول سطر الطلب(request line) ، وتسمى السطور التالية سطور المقدمة .(header lines) يحتوي سطر الطلب على ثلاثة حقول: حقل الطريقة، وحقل عنوانURL ، وحقل إصدار .HTTP قد يحمل حقل الطريقة عدة قيم مختلفة، بما في ذلك

DELETE، PUT HEAD، POST GET ومعظم رسائل الطلب تستخدم طريقة GET التي تستخدم عندما يطلب المتصفح كائن معرف في حقل .URL في هذا المثال، المتصفح يطلب الكائنsomedir / page . html حسب الإصدار ١.١ /HTTP ننتقل إلى سطور المقدمة، يحدد السطرHost : Www . someschool. edu المضيف الذي يتواجد فيه الكائن، والذي تطلبه الذاكرة المخبأة لوكيل الويب (Proxy cache).

ويعني السطر Connection: close آن المتصفح يبلغ الخادم أن بإمكانه إغلاق الاتصال بعد إرسال الكائن المطلوب، إذ لم يعد بحاجة إليه. أما سطر المقدمة User - agent : Mozilla ٥ . 0/ فيشير إلى وكيل المستخدم، أي نوع المتصفح الذي طلب الخدمة، وهو في المثال متصفح موزيلا ٥ . ٠ من فايرفوكس، وهذا السطر مفيد لأن الخادم قد يرسل إصدارات مختلفة من نفس الكائن إلى أنواع مختلفة من الوكلاء. أخيرا، فإن السطر

Accept : - language يشير أن المستخدم يفضل الحصول على النسخة الفرنسية من الكائن إن وجدت على الخادم، وإلا سيرسل الخادم النسخة الافتراضية عزيزي الطالب، دعنا ننظر الآن في الشكل العام لرسالة الطلب كما هو مبين في الشكل (٢-٨) ص ٦٣ مهم جدا

، نلاحظ أنه يتواءم مع المثال السابق.

بالإضافة إلى نص الكيان(entity body) ، ويكون فارغا مع طريقة GET ، ولكنه يستخدم مع POST. غالبا ما يستخدم عميل HTTP طريقة POST عندما يملا المستخدم نموذجة مثل إدخال كلمات مفتاحية لمحرك البحث، وهنا لا يزال المستخدم يطلب صفحة ويب من الخادم، ولكن محتواها يعتمد على ما أدخله المستخدم في حقول النموذج.

طريقة Head تشبه طريقة GET ، فعندما يتلقى الخادم طلبة بطريقة Head ، فإنه يستجيب برسالة HTTP دون الكائن المطلوب، وغالبا، يستخدم مطور التطبيق هذه الطريقة لفحص الأخطاء .(Debugging) ويقترن استخدام طريقة PUT بأدوات النشر على الويب، فتتيح للمستخدم أو التطبيق رفع كائن إلى مسار معين (Directory) على خادم الويب. وأخيرا، فإن طريقة DELETE تسمح للمستخدم أو التطبيق بحذف كائن عن خادم الويب.

رسالة الاستجابة HTTP Response Message

فيما يلي رسالة استجابة HTTP نموذجية، وقد تكون رد على رسالة الطلب ص٦٣

تتكون رسالة الاستجابة من ثلاثة أقسام: سطر الحالة الابتدائي، ستة سطور مقدمة، ثم نص الى .(body . يحتوي نص الكيان على الكائن المطلوب نفسه ممثلة بالسطر data data data ...) دم ويتكون سطر الحالة من ٣ حقول: إصدار البروتوكول، ورمز حالة، ورسالة الحالة المقابلة في هنا يشير سطر الحالة إلى أن الخادم يستخدم ١ . ١ HTTP/وأن كل شيء على ما يرام (أي أن الخادم من ويرسل الكائن المطلوب). الآن سنناقش سطور المقدمة، يستخدم الخادم السطرConnection: close
ليخبر العميل بأنه سيغلق ات TCP بعد إرسال الرسالة، ويدل سطر التاريخ Date:على وقت وتاريخ إنشاء الاستجابة وإرسالها من الخان ولا يتعلق بوقت إنشاء الكائن نفسه أو آخر تعديل. يشير السطر Server: أن الخادم الذي أنشأ الرسالة هو خادم الويب .Apache ويشير السطر Last - Modified : إلى وقت إنشاء الكائن أو آخر تعديل، وهو أمر بالغ الأهمية في التخزين المخبأ (الكاش) للكائن، سواء كان محلية لدى العميل أو لدي خادمات الكاش التي تسمى بروكسي .(Proxy servers) يشير سطر طول المحتوى Content- Length : إلى عدد بايتات الكائن المرسل. وأخيرا، يشير سطر نوع المحتوى Content - Type : إلى نوع الكائن الموجود في نص الكيان، وهو في هذا المثال HTML نصي.
)لاحظ أن Content - Type : هو الذي يحدد نوع الكائن وليس امتداد الملف .(يبين الشكل (٢-٩) الشكل العام لرسالة الاستجابة، وهو يتفق مع ما شرحنا في مثالنا أعلاه. في البداية، دعنا نتحدث قليلا عن رموز الحالة والعبارات المرتبطة بها والتي تشير إلى نتيجة الطلب، وفيما يأتي بعض الرموز والعبارات الشائعة

OK 200: . :نجح الطلب ويتم إرجاع المعلومات في الاستجابة
Moved Permanently ٣٠١ :تم نقل الكائن المطلوب بشكل دائم، يتم تحديد عنوان URLالجديد
في السطر Location: في مقدمة رسالة الاستجابة، ويقوم برنامج العميل باسترداده تلقائية
Bad Request ٤٠٠ :هو رمز خطأ عام يشير أن الطلب غير مفهوم للخادم
Not Found ٤٠٤ :المستند المطلوب لا يتوفر على هذا الخادم
HTTP Version Not Supported ٥٠٥: الخادم لا يدعم الإصدار الخاص ببروتوكول HTTP المطلوب.

كيف يمكنك مشاهدة رسالة استجابة HTTP على أرض الواقع؟ الأمر مهم ويمكنك القيام به بسهولة.
قم بعمل Telnet على خادم الويب الذي ترغب، ثم اكتب رسالة طلب من سطر واحد لكائن متوفر على هذا الخادم.
عزيزي الطالب، ناقشنا في هذا القسم عددا قليلا من مجمل سطور المقدمة التي يمكن استخدامها في رسائل الطلب أو الاستجابة، وهناك المزيد من سطور المقدمة التي قد تدرجها المتصفحات وخوادم الويب، سنغطي بعضا منها أدناه، والبعض الآخر في القسم ٢-٣-٥. هناك شرح واف ومبسط حول بروتوكول HTTP بما في ذلك مقدماته ورموز الحالة في المرجع [Krishnamurthy ٢٠٠١].

2 - 3 -التفاعل بين المستخدم والخادم: الكوكيز (User - Server Interactions (Cookies

يستخدم بروتوكول HTTP الكوكيز(Cookies) ، غالبة، حتى يتمكن موقع الويب من التعرف على مستخدميه، إما لتقييد وصول المستخدم أو لتقديم المحتوى للمستخدم استنادا إلى هويته. والكوكيز معرفة في [RFC ٦٢٦٥] بأنها السماح للمواقع بتتبع المستخدمين ومعظم مواقع الويب التجارية الكبرى تستخدم الكوكيز هذه الأيام.

مثال: لنفترض أن سعاد دائما تستخدم متصفح Internet Explorer للوصول إلى الويب من حاسوبها ال. ودخلت إلى Amazon . Corn لأول مرة، ولنفترض أنها زارت موقع e- Bay سابقة، تتبع كيف ستعمل من استنادا إلى الشكل (٢-١٠)، عندما يصل الطلب إلى خادم الويب الخاص بالأمازون، فإنه ينشى رقم هوية فريد وينشئ قيدا في قاعدة البيانات الخلفية مفهرسة بهذا الرقم، ثم يستجيب

خادم الويب إلى متصفح سعاد باستجابة تتضمن سطر المقدمة Set - Cookie : الذي يحتوي رقم الهوية، وقد يكون السطر:

Set-cookie: 1678

عندما يتلقى متصفح سعاد رسالة الاستجابة، يقرأ السطر Set- Cookie : فيضيف سطرا يشمل اسم الخادم ورقم الهوية إلى ملف الكوكي الذي يديره. تذكر أن ملف الكوكي لديه قيد لموقع e- Bay عندما زارته سعاد سابقا. مع استمرار سعاد بتصفح موقع الأمازون، في كل مرة تطلب صفحة ويب، يرجع المتصفح إلى ملف الكوكي، ويسترجع رقم هويتها لهذا الموقع، ويضع سطر كوكي يتضمن رقم الهوية في الطلب، وعلى وجه التحديد، كل الطلبات الموجهة إلى خادم الأمازون تشمل سطر المقدمة ١٦٧٨ .Cookie: بهذه الطريقة، يتمكن خادم الأمازون من تتبع نشاط سعاد في موقع الأمازون، على الرغم من أنه لا يعرف بالضرورة اسم سعاد، بل يعرف بالضبط الصفحات التي زارها المستخدم ١٦٧٨، ومتى وبأي ترتيب. يستخدم الأمازون الكوكيز لتوفير خدمة عربة التسوق، إذ يستطيع الموقع الإبقاء على قائمة بجميع مشتريات سعاد حتى تتمكن من دفع الكلفة الإجمالية في نهاية الجلسة. إذا عادت سعاد إلى موقع أمازون، بعد أسبوع، سيستمر متصفحها بوضع سطر ١٦٧٨ Cookie: في رسائل الطلب، وسيعرض الأمازون بعض المنتجات على سعاد بناء على صفحات الويب التي زارتها سابقا. وإذا قامت سعاد بالتسجل في موقع الأمازون بتوفير الاسم الكامل، والبريد الإلكتروني، والعنوان البريدي، ومعلومات بطاقة الائتمان، يمكن للأمازون إدراج هذه المعلومات في قاعدة البيانات الخاصة بها، وربط اسم سعاد برقم هويتها (وجميع الصفحات التي زارتها في الموقع سابقا)، وبهذه الطريقة توفر مواقع التجارة الإلكترونية خدمة التسوق بنقرة واحدة

(One - click shopping).

وعلى سبيل المثال، عندما تسجل الدخول إلى البريد الإلكتروني عبر الويب (مثل Hotmail)، يرسل المتصفح

من الدخول عبر الكوكي إلى الخادم، ويسمح للخادم بالتعرف على المستخدم حتى نهاية الجلسة. ورغم ر ك

ن من الأحيان، تسهل التسوق عبر الإنترنت، إلا أن الكوكيز مثيرة للجدل فيما يعتبر انتهاكا اللخصوصية.

يمكنك الرجوع إلى [Cookie Central ٢٠١٢] لمزيد من المعلومات

الذاكرة المخبأة في الشبكة العنكبوتية (Web Caching)

ذاكرة الويب المخبأة (Web cache) وتسمى أيضا خادم وكيل (Proxy server)، هي أحد مكونات الشبكة يعمل على تلبية طلبات HTTP نيابة عن خادم الويب، ولديه قرص تخزين خاص يحتفظ فيه بنسخ من الأشياء المطلوبة مؤخرة. كما هو مبين في الشكل (٢-١١)ص ، يمكنك إعداد متصفحك بحيث يتم توجيه الطلبات إلى خادم الوكيل أولا.

مثال: لنفرض أن المتصفح طلب الكائن http : / / www . Someschool . edu / campus . gif إليك ما سيحدث.

١ . ينشئ المتصفح اتصال TCP مع خادم الوكيل، ويرسل له طلب HTTP للحصول على كائن.

٢ . يتحقق خادم الوكيل فيما إذا كان لديه نسخة من الكائن مخزنة محلية، فإذا كان كذلك، يرد الوكيل برسالة استجابة تتضمن إلى المتصفح العميل.

٣ . إذا لم يكن الكائن لدى الوكيل، يفتح اتصال TCP مع الخادم الأصل . www Someschool . edu ، ثم يرسل طلب HTTP للحصول عليه، فيرد الخادم الأصل برسالة استجابة للوكيل تتضمن الكائن.

٤ . عندما يتلقى خادم الوكيل الكائن، فإنه يخزن نسخة محلية، ويرسل نسخة ضمن رسالة استجابةHTTP إلى متصفح العميل) عبر اتصال TCP القائم بين متصفح العميل وخادم الوكيل)

.شهد التخزين المخبا للويب (Web caching) انتشارا في الإنترنت لسببين:

أسباب انتشار الانترنت

١) يمكنه أن يقلل وقت الاستجابة الطلب العميل بشكل كبير، وخاصة إذا كان عرض النطاق الترددي بين العميل والخادم الأصل أقل بكثير منه بين العميل وخادم الوكيل، وكان الكائن المطلوب لدي خادم الوكيل.

٢) يمكنه أن يقلل بشكل كبير حركة المرورعلى خط اتصال المؤسسة بشبكة الإنترنت، وبذلك لا تضطر المؤسسة إلى ترقية عرض النطاق الترددي بسرعة، مما يخفض التكاليف.

عزيزي الطالب، للحصول على فهم أعمق لفوائد الذاكرة المخبأة (cache)، دعنا نناقش مثالا استنادا إلى الشكل (١٢ - ٢ ص ٦٩) الذي يظهر شبكتين؛ شبكة المؤسسة وشبكة الإنترنت العامة، شبكة المؤسسة هي شبكة محلية (LAN) عالية السرعة، وهناك موجه في شبكة المؤسسة وموجه آخر في شبكة الإنترنت متصلان عبر وصلة (خط) سرعتها ١٥ Mbps.

تصل الخوادم الأصل بشبكة الإنترنت ولكن تقع في جميع أنحاء العالم.

لنفترض أن متوسط حجم الكائن عنا ١M، وأن المتوسط معدل الطلبات من متصفحات المؤسسة إلى الخوادم الأصل هو ١٥ طلبا في الثانية ولنفترض أن رسائل طلب HTTP صغيرة ولا تشكل حركة المرور تذكر في الشبكات أو في خط النفاذ الرئيس، ولنفترض أيضا أن مقدار الوقت اللازم لتوجيه طلب HTTP من موجه الإنترنت على خط النفاذ الرئيس في الشكل (٢-١٢ ص٦٩) إلى أن يتلقى ردا هو ثانيتين بالمتوسط، ودعنا نطلق عليه، تأخير الإنترنت (Internet delay)

وقت الاستجابة الإجمالي، أي من لحظة طلب كائن من قبل المتصفح حتى استلامه، هو مجموع تأخير الشبكة المحلية(LAN) ، وتأخير الوصول (أي، التأخير بين الموجهين)، وتأخير الإنترنت. دعنا الآن نقوم بحسبة بسيطة لتقدير هذا التأخير. كثافة حركة المرور على الشبكة المحلية (انظر القسم ١-٨) هي:

(15 requests/sec). (1 Mbits/request)/(100 Mbps) = 0.15

في حين أن كثافة حركة المرور على خط النفاذ الرئيس (بين الموجهين) هي:

(15 requests/sec). (1 Mbits/request)/(15 Mbps) = 1

عادة، ينتج عن كثافة حركة المرور على الشبكة المحلية بقيمة 0.15، عشرات الميلي ثانية من التأخير على الأكثر؛ أي يمكن إهماله. وكما ناقشنا في القسم ١-٨، عند اقتراب كثافة حركة المرور إلى ١ (كما في حالة خط النفاذ الرئيس) يصبح التأخير على الخط كبيرة جدا، وينمو بلا حد. وهكذا، فإن متوسط زمن الاستجابة لتلبية الطلبات سيكون بضع دقائق، وهو أمر غير مقبول لمستخدمي المؤسسة ولا بد من علاج

أحد الحلول الممكنة هو زيادة معدل الوصول من ١٥ Mbps إلى، فلنقل، ١٠٠ Mbps، وهذا يقلل من كثافة حركة المرور على خط النفاذ إلى 0.15، وهو

تأخير ضئيل بين الموجهين، وعليه، تكون الاستجابة الكلية ثانيتين تقريبا، وهي تأخير الإنترنت. لكن هذا الحل يعني أن على المؤسسة ترقية الخط، فهو حل مكلف هناك حل بديل بتركيب مخبأ الويب،
أي خادم الوكيل(proxy server) ، في شبكة المؤسسة كما في الشكل (١٣ - ٢)ص ٧٠
. وتتراوح معدلات الإصابة(Hit rates) ، أي نسبة الطلبات التي يلبيها الوكيل، عادة بين٠,٧-٠,٢ في الواقع العملي للتوضيح، دعنا نفترض أن معدل الإصابة٠,٤ لهذه المؤسسة. بما أن العملاء والوكيل
ص٦٨+٦٩

يتصلان عبر شبكة محلية عالية السرعة، ٤٠٪ من الطلبات تلبي على الفور تقريبا، ولنقل، في غضون ١٠ميلى ثانية. مع ذلك، هناك ٦٠٪ من الطلبات يجب أن تلبيها الخادمات الأصل، ولكن فقط ٦٠٪ من الطلبات ستمر عبر خط النفاذ، فتقل كثافة حركة المرور عليه من ١,٠ إلى ٠,٦ .عادة، كثافة حركة المرور التي تقل عن ٠,٨ يقابلها تأخير قليل، أي عشرات الميلي ثانية على خط ١٥ .Mbpsوهذا التأخير لا يكاد يذكر مقارنة مع تأخير الإنترنت الذي يبلغ ٢ ثانية. ونظرة لهذه الاعتبارات، يكون متوسط التأخير هو

٠,٤ (0.01 seconds) +0.6 (2.01 seconds)

وهو أكبر قليلا من ١,٢ ثانية، وبالتالي، فإن هذا الحل له وقت استجابة أقل من الحل الأول، ولا يتطل من المؤسسة رفع سرعة خط الإنترنت، بل عليها، بالطبع، شراء خادم الوكيل وتثبيته، ولكن كلفته أقل، وخاصة عند استخدام برنامج نطاق عام يعمل على أجهزة حاسوب غير مكلفة.
من خلال استخدام شبكات توزيع المحتوى(Content Distribution Networks: CDNs) ، بدأت مخابئ الويب بشكل متزايد تلعب دورا مهما في شبكة الإنترنت، وتعمل شركة CDN على تثبيت العز من المخابئ الموزعة جغرافية عبر الإنترنت، وبالتالي، توطين الكثير من حركة المرور. هناك شبكات توزيع مشتركة (مثل أكاماي ولايملايت) وشبكات مخصصة (مثل جوجل ومايكروسوفت)

الدالة الشرطيةGET (The Conditional GET) ص٧١

أن ذاكرة الويب المخبأة (web caching) تقلل زمن الاستجابة الذي يشعر به المستخدم، فقد تكون ت المخبأة قديمة، أي تم تعديل نسخة الكائن في خادم الويب بعد حفظها في الذاكرة المخبأة لدى العميل، ولكن آلية للتحقق من أن هذا الكائن هو الأحدث، وتسمى الدالة الشرطية conditional بروتوكول HTTP يقدم الية للتحقق من أن هذا الكائن هو الأحدث، تسمى رسالة الطلب رسالة GETالشرطية إذا كانت (١) رسالة الطلب تستخدم دالة GET أو (٢) تتضمن مقدمة

رسالة الطلب السطر

":If - Modified - Since"

مثال:

آلية عمل دالة GET الشرطية

أولاً يرسل مخبأ الوكيل رسالة طلب إلى خادم الويب نيابة عن المتصفح

ثانيا، برسيل خادم الويب رسالة استجابة تتضمن الكائن المطلوب لمخبأ الوكيل الذي يقوم بدوره بتحويل الكائن إلى المتصفح الذي طلبه، ويخزن نسخة محلية مع تاريخ آخر تعديل:

ثالثا، إذا طلب متصفح آخر نفس الكائن عبر الوكيل بعد أسبوع، وكان لا يزال في الذاكرة المخبأة، فيقوم الوكيل بفحص تاريخ آخر تعديل للتأكد أن الكائن لم يعدل في خادم الويب عن طريق إصدار دالة GET الشرطية بارسال الرسالة

يستمر خادم الويب بإرسال رسالة استجابة لا تتضمن الكائن المطلوب، وذلك لتجنب ضياع عرض النطاق الترددي، وتجنب زيادة زمن الاستجابة، وخاصة إذا كان حجم الكائن كبيرة.

لاحظ أن رسالة الرد السابقة تحتوي Not Modified ٣٠٤ في سطر الحالة، الذي يخبر مخبأ الوكيل بأنه يمكنه المضي قدما بتحويل النسخة المخبأة لديه من الكائن إلى المتصفح الذي طلبه.

| 2 - 4 |بروتوكول نقل الملفات (File Transfer
(Protocol: FTP

في جلسة بروتوكول نقل الملفات (File Transfer Protocol FTP) النموذجية، يطلب المستخدم نقل ملفاته من وإلى مضيف بعيد(Remote host) ، ويمكنه الوصول إليه عن طريق اسم مستخدم وكلمة مرور، وبذلك يمكن للمستخدم نقل الملفات من نظام الملفات المحلي إلى البعيد والعكس بالعكس. وكما يبين الشكل
(٢-١٤)ص ٧٤ مهم ،
يتفاعل المستخدم مع FTP عن طريق وكيل.FTP
حيث تنشئ عملية عميل FTP اتصال TCP مع عملية خادم FTP في المضيف البعيد، فيطلب الخادم تحديد اسم المستخدم وكلمة المرور، ويتم إرسالهما كجزء من أوامر FTP عبر اتصال TCP.
وعندما يأذن الخادم للمستخدم، يمكنه نسخ واحد أو أكثر من الملفات المخزنة في المضيف المحلي إلى البعيد أو العكس. يتشابه FTP و HTTP بأنهما بروتوكولان لنقل الملفات بين أنظمة الملفات المحلية والبعيدة، وكلاهما يعمل عبر TCP. ومع ذلك، فإن بينهما اختلافات مهمة، الفرق الأول هو أن FTP يستخدم اتصالي TCP متوازيين
اتصال التحكم و اتصال البيانات، كما هو موضح في الشكل (٢-١٥).
يتم استخدام اتصال التحكم الإرسال مرات التحكم مثل اسم المستخدم وكلمة المرور، وأوامر تغيير الدليل البعيد، وأوامر وضع الملفات (out) الحصول عليها (get). أما اتصال البيانات فيستخدم لإرسال الملفات.

عندما يبدأ المستخدم جلسة FTP مع مضيف بعيد، ينشئ العميل اتصال تحكم TCP مع الخادم (المضيف البعيد) على رقم المنفذ ٢١.
يرسل العميل اسم المستخدم وكلمة المرور وكذلك أوامر تغيير الدليل البعيد عبر هذا الاتصال. عندما يتلقى الخادم أمراً لنقل الملفات ينشئ اتصال بيانات TCP مع العميل، يرسل بروتوكول FTP ملف واحدة عبر اتصال البيانات ثم يغلقه، وإذا، أراد المستخدم نقل ملف آخر خلال الجلسة نفسها، عليه إنشاء اتصال بيانات آخر. لاحظ أن اتصال التحكم يبقى مفتوحة طوال مدة الجلسة، بينما يتم إنشاء اتصال بيانات جديد النقل كل ملف في نفس الجلسة، أي أن اتصال البيانات غير دائم
(non- persistent). على عكس HTTP ، يجب أن يحتفظ FTP بحالة (state) المستخدم طوال الجلسة، فعلى الخادم أن يقرن اتصال التحكم بحساب مستخدم معين، وأن يتتبع مسار الدليل الحالي للمستخدم طالما هو يتنقل في شجرة الدليل البعيد، وهذا بالطبع يحد بشكل كبير من عدد الجلسات التي يستطيع FTP الإبقاء
عليها معا.

٢ 1 - 4 - أوامر نقل الملفات وردودها (FTP Commands and Replies)

في نهاية هذا القسم، نقدم مناقشة موجزة لبعض أوامر FTP الأكثر شيوعا والردود عليها. يتم إرسال الأوامر من العميل إلى الخادم، والردود من الخادم إلى العميل، عبر اتصال تحكم بشكل .bit ASCII-7 ولفصل الأوامر المتتالية، نحتاج إلى حرف إرجاع (carriage return) نهاية كل أمر. كل أمر يتكون من أربعة
أحرف ASCII كبيرة، وفيما يلي بعض الأوامر الأكثر شيوعا:-

١- USER username:
يستخدم لإرسال اسم المستخدم إلى الخادم

٢- PASS password:

يستخدم لإرسال كلمة المرور إلى الخادم

.

٣- LIST:

يستخدم ليطلب من الخادم عرض قائمة بجميع الملفات في الدليل البعيد، ويتم إرسال قائمة الملفات عبر اتصال بيانات جديد، وليس عبر اتصال التحكم.TCP

٤- RETR filename:

يستخدم للحصول على (get) ملف من الدليل الحالي على المضيف البعيد، فيأمر المضيف البعيد بإنشاء اتصال البيانات وإرسال الملف المطلوب عبره.

٥- :STOR filename:

يستخدم لتخزين (put) ملف على الدليل الحالي في المضيف البعيد.
هناك تراسل واحد لواحد بين الأمر الذي يصدره المستخدم وأمر FTP الذي يرسل عبر اتصال التحكم، فكل امر يتبعه رد من الخادم الى العمل، وتكون الرد على شكل أرقام من ثلاثة منازل مع رسالة اختيارية تتبع

5 - 2 | البريد الإلكتروني عبر الإنترنت (Electronic Mail' e-Mail' in the Internet)

ظهر البريد الالكتروني منذ بداية الإنترنت، وكان ما زال الأكثر شعبية وأهمية واستخدام بين تطبيقات الإنترنت
[Segaller-1998] ، وكما هو الحال في البريد العادي، فإن البريد الإلكتروني وسيلة اتصال غير متزامن الإرسال الرسائل وقراءتها في الوقت المناسب دون الحاجة إلى تنسيق بين المرسل والمستقبل، وما يميزه عن البريد العادي هو السرعة وسهولة التوزيع بكلفة قليلة إن لم تكن مجانية، كما أن البريد الإلكتروني الحديث يوفر العديد من الميزات، بما في ذلك تضمين

المرفقات، والروابط، والصور، وتنسيق النصوص.
الطالب، يغطي هذا القسم بروتوكولات طبقة التطبيقات الخاصة بالبريد الإلكتروني عبر الإنترنت) وقال التعمق في هذه البروتوكولات، سنلقي نظرة عامة على هذا النظام ومكوناته الرئيسة، كما هو مبين في الشكل

هناك ثلاثة عناصر رئيسة؛

١. وكلاء المستخدم
٢. ، خادم البريد،
٣. وبروتوكول نقل البريد البسيط(Simple Mail

Transfer Protocol : SMTP)،

وفي هذا السياق سيكون المرسل "أليسA "، والمستلم "بوب .B "يسمح الوكلاء للمستخدم بقراءة الرسائل، والرد عليها، وتحويلها، وحفظها، وكتابتها، ومن الأمثلة على وكلاء المستخدم برنامج Microsoft Outlook وبرنامج Apple Mail. عندما تنتهي أليس من كتابة رسالتها، يقوم وكيلها بإرسالها إلى خادم البريد الذي يضعها في طابور الرسائل الصادرة(outgoing message queue) ، وعندما يريد بوب قراءة الرسالة، يتلقى وكيلة الرسالة من صندوق بريده في خادم البريد.

يشكل خادم البريد جوهر البنية التحتية للبريد الإلكتروني، فكل مستلم لديه صندوق بريد في أحد خوادم البريد، ويعمل صندوق البريد على إدارة الرسائل التي أرسلت له وحفظها.

تبدأ رحلة أي رسالة نموذجية من وكيل المستخدم الخاص بالمرسل، وتنتقل إلى خادم البريد المرسل، ثم إلى خادم البريد المستلم، حيث يتم ايداعها في صندوق بريد المستلم

عندما يريد بوب الوصول إلى رسائله في صندوق البريد، فإنه بحاجة إلى مصادقة خادم البريد الذي يحتوي صندوق بريده من خلال اسم المستخدم وكلمة المرور، وعلى خادم البريد الخاص بأليس التعامل مع حالات الخطأ او الفشل في خادم البريد الخاص ببوب، فإذا لم يستطع خادم اليس تسليم البريد

إلى خادم بوب، يقوم خادم اليس بالاحتفاظ بالرسالة في طابور الرسائل (message queue)ويحاول نقل الرسالة في وقت لاحق، وغالبا المحاولة كل ٣٠ دقيقة؛ فإذا نجح خلال بضعة أيام، فإنه يحذف الرسالة ويعلم المرسل (أليس).

يعد SMTP بروتوكول طبقة التطبيق الأساسي للبريد الإلكتروني عبر الإنترنت، ويستخدم خدمة نقل البيانات الموثوقة من TCP لنقل البريد من خادم البريد المرسل (جانب العميل) إلى خادم البريد المستلم (جانب الخادم). بعبارة أخرى، كلا الجانين، العميل و الخادم، يعملان على كل خادم للبريد، فعندما يرسل الخادم بريدة إلى خادم آخر، فإنه يعمل كعميلSMTP ، و عندما يتلقي الخادم بريدا من خادم آخر، فإنه يعمل كخادم.SMTP

٢ 5 - 2 - بروتوكول نقل البريد البسيط (Simple Mail Transfer Protocol: SMTP)

يعتبر بروتوكولSMTP ، المعرف في ٥٣٢١RFC ، في صميم البريد الإلكتروني عبر الإنترنت، فهو بعمل على نقل الرسائل من خادم البريد المرسل إلى خادم البريد المستلم، وهو أقدم بكثير منHTTP ، وعلى الرغم من العديد من المزايا، يستند SMTP إلى تقنيات وخصائص بانت قديمة. فعلى سبيل المثال، هناك قيود على محتوى الرسالة (وليس المقدمة فقط) لجميع رسائل البريد نحو استخدام الأسكي البسيط7-bit ASCII ، فقد كان هذا منطقية في وقت مبكر عندما كانت الرسائل بسيطة بلا مرفقات ضخمة من صور وصوت وفيديو، أما اليوم، في عصر الوسائط المتعددة، أصبحت هذه القيود تشكل عبئة، حيث ينبغى ترميز بيانات الوسائط المتعددة الثنائية إلى اسكي قبل إرسالها عبرSMTP ، ومن ثم فك الترميز إلى ثنائي في الطرف المقابل بعد النقل.

لتوضيح آلية عمل SMTP الأساسية، دعنا نأخذ السيناريو الذي يلخصه الشكل (٢-١٧) ص٧٨

لنفترض أن أليس تريد إرسال رسالة أسكي بسيطة إلى بوب، كما يبين الشكل (٢-١٧)ص٧٨، عندها تنتقل الرسالة بالخطوات الآتية:

١ تستدعى أليس وكيل المستخدم الخاص بها للبريد الإلكتروني، وتدخل عنوان البريد الإلكتروني لبوابة . (مثلاbob @ someschool . edu)، وتنشئ رسالة ثم تطلب من وكيل المستخدم إرسال الرسالة
٢. يرسل وكيل أليس الرسالة إلى خادم بريدها، حيث يقوم بوضعها في طابور الرسائل
٣. عندما يجد عميل SMTP الذي يعمل على خادم بريد أليس في طابور الرسائل، يفتح اتصال TCP إلى خادم SMTP الذي يعمل على خادم بريد بوب.
٤. بعد المصافحة الأولية، يرسل عميل SMTP رسالة أليس عبر اتصال TCD يتلقى خادم SMTP الرسالة على خادم بريد بوب، ثم يضع الرسالة في صندوق بريد بوب.
٦. يستدعي بوب وكيل المستخدم الخاص به لقراءة الرسالة في الوقت الذي يناسبه

لاحظ أن وكيل المستخدم لا يمكنه استخدام SMTP لسحب (pull) الرسائل بل لدفعها(push) ، فلا بد من بروتوكول آخر يمكن المستلم من تلقي الرسائل من صندوق البريد على خادم بريده إلى جهازه الشخصي المحلي. وهناك عدد من البروتوكولات الشائعة للوصول إلى البريد الإلكتروني، بما في ذلك بروتوكول مكتب البريد الإصدار ٣ (Post Office Protocol- Version 3 : POP3) وبروتوكول الوصول إلى البريد عبر الإنترنت (Internet Mail Access Protocol: IMAP) ، بالإضافة إلى بروتوكول HTTP. ويلخص الشكل

(٢-١٨) البروتوكولات التي تستخدم في بريد الإنترنت.

بروتوكول مكتب البريد POP3 | POP3

هو بروتوكول وصول إلى البريد تم تعريفه في [RFC١٩٣٩]، و هو في غاية البساطة، ووظائفه محدودة، ويبدا عمله عندما يفتح وكيل المستخدم (العميل) اتصال TCP إلى خادم البريد (الخادم) على المنفذ ١١٠،

وبتقدم العمل في ثلاث مراحل:
١ ـ المصادقة أو التفويض (Autherization): يرسل وكيل المستخدم اسم المستخدم وكلمة المرور (نص واضح) للمصادقة.
٢ ـ الحركة او المعاملات (Transaction): يتلقى وكيل المستخدم الرسائل، وفي هذه المرحلة، يمكنه الحديد الرسائل للحذف، وإزالة علامات الحذف، والحصول على إحصائيات حول البريد.
٣ ـ التحديث (Update): ويحدث عندما يصدر العميل أمر التوقف (quit) وإنهاء جلسة بروتوكولPOP3 عندها ، يقوم خادم البريد بحذف الرسائل التي تم تحديدها للحذف.

بروتوكول الوصول إلى البريد عبر الإنترنتIMAP

ي ملها بروتوكولPOP3 ، كما ذكرنا آنفا، جاء بروتوكول IMAP الذي تم تعريفه في
RFC ٣٥٠١] كبروتوكول وصول إلى البريد. ولديه العديد من المميزات التي لا يوفرها POP3، ولكنه بشكل ملحوظ أكثر تعقيدة، ما يعني أن تنفيذ برمجة العميل والخادم أكثر تعقيدة أيضا.
يربط خادم IMAP كل رسالة بمجلدها؛ فعندما تصل الرسالة إلى الخادم لأول مرة، ترتبط بمجلد البريد الوارد للمستلم، الذي يمكنه بعد ذلك نقلها إلى مجلد جديد أنشأه، أو قراءتها أو حذفها. ويسمح بروتوكول IMAP للمستخدمين بإنشاء المجلدات ونقل الرسائل من مجلد إلى آخر، كما يسمح بالبحث عن الرسائل على المجلدات البعيدة
لاحظ أنه، على عكسPOP3 ، يحتفظ خادم IMAP بمعلومات عن حالة المستخدم طوال الجلسة، مثل أسماء المجلدات والرسائل التي ترتبط بها.
:هامة أخرى من IMAP هي أنه يسمح لوكيل المستخدم بالحصول على مكونات الرسائل، مثل مقدمة الرسالة فقط أو جزء من رسالة MIME متعددة الأجزاء.
وهي ميزة مفيدة عندما يكون الاتصال ضعيفة (مودم بطيئة) بين وكيل

المستخدم وخادم البريد، فقد لا ترغب في تحميل الرسائل كافة في صندوق البريد، ولا سيما الرسائل الطويلة التي قد تحتوي على مقاطع صوت أو فيديو.

البريد الإلكتروني عبر الإنترنت Web - Based E - Mail

أصبح البريد الإلكتروني المعتمد على الإنترنت أكثر شيوعا هذه الأيام، إذ يتم توفير البريد الإلكتروني من قبل هوتميل، وجوجل، وياهو، فضلا عن الجامعات والشركات وغيرها. في هذه الحالة، وكيل المستخدم هو متصفح ويب عادي، ويصل المستخدم إلى صندوق بريده البعيد عبر HTTP، فعندما يريد المستلم، مثل بوب، الوصول إلى رسالة في صندوق بريده، يتم إرسال رسالة البريد الإلكتروني من خادم البريد إلى متصفحه باستخدام بروتوكول HTTP بدلا من POP3 أو IMAP. وعندما يريد مرسل، مثل أليس، إرسال رسالة البريد الإلكتروني، يتم إرسالها من متصفحها لخادم بريدها عبر HTTP بدلا من SMTP، مع ذلك، يبقى خادم البريد الخاص بأليس، يرسل الرسائل ويتلقاها من وخوادم البريد الأخرى باستخدام SMTP.

|نظام اسم النطاق(DNS_The Internets
(Directory Service

يمكن التعرف على كل مضيف على الشبكة بطريقة عدة واحده من الطرق هذا المعرفات هي اسم المضيف (hostname)مثل Www . yahoo . com، www . qou . edu ولكن اسم المضيف لا يقدم إلا قليلا من المعلومات عن موقع المضيف على مثلا، اسم المضيف www . eurecom . fr ، الذي ينتهي برمز الدولةfr ، يبين أن المضيف هو على فرنسا لا أكثر)، وعلاوة على ذلك، فإن أسماء المضيفين تتكون من حروف متغيرة الطول، فيصعب اليه جهات معالجتها. لهذه الأسباب، يتم تعريف المضيف بما

يسمى عنوان الإنترنت : IP Address.

عناوين الإنترنت بشيء من التفصيل في الوحدة الرابعة، ولكن دعنا نذكر بعض المعلومات المهمة هنا ايمان، بتكون عنوان الإنترنت، بإصداره الرابع

(IPv4)، من ٤ بايت تفصل بين كل بايت منها نقطة، وتمثل النظام العشري من ٠ إلى ٢٥٥، مثل الرقم: ١٢١ . 83 . 106 . 7 .وكلما انتقلنا في قراءته من اليسار إلى اليمين، تحصل على المزيد من المعلومات المحددة حول موقع المضيف على الإنترنت (أي في أي شبكة ضمن شبكة الشبكات).

١ 2 - 6 - الخدمات التي يقدمها نظام اسم النطاق (Services Provided by DNS)

يفضل المستخدم معرف اسم المضيف للتذكر، بينما الموجهات تفضل معرفات ذات طول ثابت، أي عناوين الإنترنت المنظمة بشكل هرمي. ومن أجل التوفيق بينهما، فإننا بحاجة إلى خدمة الدليل الترجمة أسماء المضيفين إلى عناوين إنترنت، وهذه هي الخدمة الرئيسة التي يقدمها نظام اسم النطاق(Domain - Name System DNS:) ، فهو: (١) يوفر قاعدة بيانات موزعة ضمن تسلسل هرمي من خوادمDNS ، (2)يسمح للمضيفين بالاستعلام في قاعدة البيانات الموزعة.

غالبة، تعمل خوادم DNS على أجهزة UNIX وتشغل برنامج نطاق اسم الإنترنت من بيركليBerkley)

[BIND 2012] (Internet Name Domain : BIND)، ويعمل بروتوكول DNS عبر بروتوكول UDP
ويستخدم المنفذ ٥٣. وعادة، يستخدم DNS من قبل بروتوكولات أخرى في طبقة التطبيقات، بما في ذلك
FTP، SMTP، HTTPلترجمة أسماء المضيفين التي يضعها المستخدم إلى عناوين إنترنت. فمثلا، عندما يقوم المتصفح) اي عميل (HTTP بطلب العنوانWWW . Someschool . edu / index . html، وحتى يتمكن تضيق المستخدم من إرسال طلب HTTP إلى خادم الويبWWW . Someschool . edu

، عليه الحصول أولا على عنوان الإنترنت الخاص بخادم الويب كما يأتي:

١ .يعمل عميل تطبيق DNS على جهاز المستخدم نفسه.
٢ . يستخرج المتصفح اسم المضيفWww . Someschool . edu
من عنوان URL ويمرره إلى جانبالعميل.
٣ .يرسل عميل DNS استعلامة يحتوي اسم المضيف إلى خادمDNS
٤ .يتلقى عميل DNS الرد، والذي يتضمن عنوان الإنترنت الخاص باسم المضيف.

ص ٨٦ لمحة عن الية عملDNS

وبالتحديد اسم المضيف المنوي ترجمته) في العديد من الأجهزة المستندة إلىUNIX ، تستخدم مات الدالة gethostbvname()لطلب الترجمة(، وعندها يتولى DNSفي المضيف المستخدم إرسال استعلام الى الشبكة. يتم إرسال جميع رسائل الاستعلام والرد عبر مخططات UDP إلى المنفذ ٥٣. بعد ما قد يصل إلى ثانية، يتلقىDNS في مضيف المستخدم رسالة الرد التي توفر الترجمة المطلوبة ليتم تمريرها للتطبيق الذي استدعاها.
من منظور التطبيق المستدعي يعتبر DNS صندوقا أسود يوفر خدمة ترجمة ب ات واضحة في الواقع، هذا الصندوق معقد، ويتالف من عدد كبير من خوادم DNS الموزعة في جميع أنحاء العالم، كما أن هناك بروتوكول طبقة تطبيقات يحدد كيفية تواصل خوادم DNS والمضيفين الذين يطلبون الخدمة.

قد يكون التصميم مركزية، أي خادم DNS واحد يحتوي على جميع السجلات، وترسل جميع استعلامات العملاء مباشرة إلى هذا الخادم، الذي يستجيب مباشرة لاستعلامات العملاء، وعلى الرغم من بساطة هذا التصميم، فإنه لا يناسب الإنترنت هذه الأيام، مع العدد الكبير والمتزايد من المضيفين،

وتتضمن مشاكل التصميم المركزي:

.نقطة واحدة للفشل: إذا تعطل خادمDNS ، تعطلت شبكة الإنترنت بالكامل. .
حجم حركة المرور. لن يتمكن خادم DNS واحد من التعامل مع جميع الاستعلامات من طلباتHTTP ورسائل البريد الإلكتروني الصادرة من مئات الملايين من الأجهزة أو المضيفين.
. قاعدة بيانات مركزية بعيدة. خادم DNS واحد لا يمكن أن يكون قريبة من جميع العملاء، فإذا كان
خادم DNS واحد في مدينة رام الله، وجاءت جميع الاستعلامات من نيوزيلندة فإن عليها أن تنتقل إلى الجانب الآخر من الأرض، عبر وصلات قد تكون بطيئة ومزدحمة، ما قد يؤدي إلى تأخير كبير.
الصيانة. احتفاظ خادم DNS واحد بسجلات جميع المضيفين على الإنترنت لا يشكل قاعدة بيانات مركزية ضخمة فحسب، بل لا بد من تحديثها باستمرار

لكل مضيف جديد. وباختصار. نتيجة لذلك، يتم تصميم DNS بشكل قاعدة بيانات موزعة على الإنترنت.

قاعدة بيانات هرمية موزعة Distributed Hierarchical

- Database من أجل التعامل مع مسألة حجم الطلبات، يستخدم DNS عددا كبيرة من الخوادم الموزعة بطريقة هرمية في جميع أنحاء العالم، إذ لن يتمكن خادم DNS واحد من احتواء جميع المضيفين في شبكة الإنترنت، بل توزع على هذه الخوادم. هناك ثلاث فئات من خوادم DNS: خوادم الجذر، وخوادم النطاق عالي المستوى (TLD)، والخوادم الموثوقة، نظمت جميعا بتسلسل هرمي كما يبين الشكل (٢-١٩).

كيف يمكن لهذه الفئات الثلاث من الخوادم أن تتفاعل، لنفترض أن عميل DNS يريد تور للمضيف www . amazon . com
، في البداية يتصل العميل بأحد خوادم الجذر، الذي يرد بعناوين TLD ٠ للنطاق عالي المستوى من نوع com ، فيتصل العميل بأحد خوادم TLD ، الذي يرد بعنوان D موثوق لدى amazon . com . وأخيرا، يتصل العميل بأحد الخوادم الموثوقة لدى amazon.com ، الن بعنوان IP للمضيف

عزيزي الطالب، سنفحص عملية البحث DNS lookup من www . amazon . com التفاصيل في الأقسام الفرعية التالية، ولكن دعنا الأن نلقي نظرة فاحصة على فئات خوادم DNS الثلاث: .
خوادم الجذر Root DNS servers. في الانترنت هناك ١٣ نوع من خوادم الجذر (من A إلكل خادم هو في الواقع شبكة من الخوادم المتكررة، لأغراض الأمن والموثوقية على حد سواء، وذ خريف ٢٠١١ بلغ مجموع خوادم الجذر ٢٤٧ خادمة.
خوادم النطاق عالي المستوى Top - Level Domain (TLD) servers هذه الخادمات مسؤولة عن المستوى الأعلى للنطاقات مثل (com , org , net , edu , gov) ، كما أنها مسؤولة عن نطاقات الدول مثل (uk , fr , ca , jp).

الخوادم الموثوقة (المخولة Authoritative DNS servers.)كل مؤسسة لديها مجموعة متاحة من المضيفين على شبكة الإنترنت (مثل خوادم الويب و البريد الإلكتروني) يجب أن تتيح سجلات DNS التي تترجم أسماء هؤلاء المضيفين إلى عناوين إنترنتIP ، ويضم الخادم الموثوق للمؤسسة هذه السجلات. وللمؤسسة أن تختار ما بين حفظ هذه السجلات على خادم موثوق خاص بها، أو أن تدفع مقابل حفظها في خوادم موثوقة لدى مزود الخدمة.

هناك نوع آخر مهم من خوادم DNS يدعى الخادم المحلي أو الافتراضي local DNS server، ورغم أنه لا ينتمي للتسلسل الهرمي إلا أنه مركزي في بنية DNS لدى مزود الخدمة، فعندما يتصل مضيف بمزود الخدمة، يزوده بعناوين الإنترنت لواحد أو أكثر من خوادمه المحلية) عادة من خلال(DHCP ، وقد يكون خادم DNS المحلي قريبة من المضيف، أي على نفس الشبكة المحليةLAN ، فعندما يقوم المضيف باستعلام DNS فإنه يرسل إلى خادم DNS المحلي الذي يعمل، بدوره كوكيل، على توجيه الاستعلام إلى خادم DNS ضمن التسلسل الهرمي.

مثال:

لنفترض أن المضيف cis. poly . edu يرغب بالحصول على عنوان gaia . cs . umass . edu ، وأن خادم DNS المحلي لبوليتكنيك يدعى dns. poly . edu ، وأن الخادم الموثوق لدى

gaia . cs . umass . edu يسمى dns . umass . edu ، كما هو مبين في الشكل (٢-٢٠).

بين آلية الحصول على العنوان المطلوب. يقوم المضيف cis. poly . edu أو بإرسال رسالة استعلام DNS إلى خادمه المحليdns

. poly .edu نحو اسم المضيف المراد ترجمته، أيgaia . cs . umass . edu

، فيقوم الخادم المحلي بتوجيه رسالة الاستعداد للخادم الجذر الذي يستجيب بدوره للخادم المحلي ويزوده بقائمة من عناوين الإنترنت لخوادم النطق المستوى TLD المسؤولة عن(edu) ، فيعيد الخادم المحلي إرسال رسالة الاستعلام إلى واحد من TLD الذي يقوم بدوره بتسجيل المقطع النهائي umass.edu، ويستجيب بعنوان الإنترنت للخادم الجامعة ماساشوستس، أي dns . umass . edu وأخيرة، يعيد الخادم المحلى إرسال رسالة الاستعلم dns . umass * edu .، الذي يستجيب بعنوان الإنترنت للمضيف gaia . cs . umass . edu في هذاالة الاستعلام مباشرة إلى gaia . cS . umas . في هذا المثال، تم رسائل استعلام و ٤ رسائل استجابة.

وسنرى في الفقرات التالية كيف يمكن تقليص حركة مرور الاستعلامات من خلال التخزين المؤقت DNS caching:

مثالنا المبين في الشكل (٢-٢٠) ص٨٩ كلا من استعلامات الإعادة (Iterative Queries)و التكرار(Recursive Queries) ، فالاستعلام المرسل من cis. poly . edu إلى dns. poly .edu هو استعلام تكرار، إذ أنه يطلب من dns poly . edu .الحصول على الترجمة نيابة عنه، بينما الاستعلامات الثلاثة التالية فهي استعلامات إعادة، لأن كل الردود تعود مباشرة إلى dns . poly . edu . من الناحية النظرية، يمكن لأي استعلام DNS أن يكون استعلام إعادة أو تكرار. فعلى سبيل المثال، فإن سلسلة استعلامات DNS المبينة في الشكل (٢-٢١) كلها استعلامات تكرار. أما في الممارسة العملية، فتتبع الاستعلامات النمط المبين في الشكل (٢٠ - ٢)، أي أن الاستعلام من المضيف الطالب إلى خادم DNS المحلي هو استعلام تكرار، والبقية هي استعلامات إعادة.

الذاكرة المخبأة (التخزين المؤقت)DNS Caching

عزيزي الطالب، لغاية الآن لم نتطرق إلى مفهوم الذاكرة المخبأة في نظام DNS، إذ أنها ميزة بالغة حيث تستغل الذاكرة المخبأة على نطاق واسع لتحسين الأداء وللحد من التأخير، وتقليص عدد رسائل عن المرتدة عبر شبكة الإنترنت. وفكرة الذاكرة المخبأة هي في غاية البساطة، فعندما يتلقى الخادم في سال الاستعلام استجابة(DNS قد تحتوي على ترجمة من اسم

المضيف إلى عنوان الإنترنت(IP) ، فإنه يمكن تخزين هذه الترجمة في الذاكرة المحلية، فمثلا، في الشكل (٢-٢٠)، في كل مرة يتلقى خادم DNS المحل . dns poly . edu الرد من أحد خوادم DNS ، فإن بإمكانه تخزين أي من المعلومات الواردة في الرد. فإذا ت تخزين الزوج (اسم المضيف، عنوان الإنترنت في خادم DNS ، ووصل استعلام آخر لخادم DNS لنفس المضيف، فإن هذا الخادم يوفر عنوان الإنترنت IP المطلوب، حتى لو لم يكن هو الخادم الموثوق لهذا المضيف. ولأن ترجمة أسماء المضيفين إلى عناوين إنترنت هي عملية دائمة، فإن خوادم DNS تتجاهل المعلومات المخزنة في الذاكرة المخبأة بعد فترة تحدد غالبا بيومين.

وكمثال على ذلك، افترض أن المضيف apricot . poly . edu يستعلم من dns. poly .edu عن عنوان الإنترنت للمضيف cnn . com ، ولنفرض أن مضيفا آخر من جامعة بوليتكنيك kiwi. poly .fr ، استعلم أيضاً من dns . poly . edu عن نفس المضيف بعد بضع ساعات، ونتيجة للتخزين في الذاكرة المخبأة، يستطيع خادم DNS المحلي فورة استرجاع عنوان المضيف cnn . com في المرة الثانية دون الحاجة إلى الاستعلام من أي خوادم DNS أخرى، كما يستطيع الخادم المحلي تخزين عناوين خوادم TLD، مما يتيح لخادم DNS المحلي تجاوز خوادم الجذر في سلسلة الاستعلام (وهذا ما يحدث في كثير من الأحيان).

سجلات DNS ورسائله(DNS Records and Messages)

عزيزي الطالب، تعمل خوادم DNS التي تشكل معة قاعدة بيانات موزعة على الاحتفاظ بسجلات الموارد(Resource Records(RRs) ، بما في ذلك الترجمة من اسم المضيف إلى عنوان الإنترنت IP ، وكل رسالة استجابة تحمل واحدة أو أكثر من سجلات الموارد. في هذا القسم، نقدم لمحة موجزة عن سجلات موارد DNS ورسائله، ويمكنك الاستزادة من [Abitz 1993] أو من مراجع RFC 1034; RFC [1035، .[DNS

يتكون سجل المورد من أربعة أجزاء تحتوي على حقول (الاسم، القيمة، النوع، زمن الحياة . (, NameValue Type , TTL) ويحدد زمن الحياة (TTL : Time to Live) الفترة الزمنية المتاحة قبل إزالة سجل المورد من الذاكرة المخبأة. وتبين النقاط الآتية أمثلة على سجل المورد، حيث تجاهلنا حقل زمن الحياة(TTL) ، كما أن معنى كل من الاسم (Name) والقيمة (Value) يعتمد على النوع (Type): :

إذا كان النوع Type = A ، سيكون الاسم (Name) هو اسم المضيف، والقيمة (Value)

هي عنوان الإنترنت IP ، وكمثال على ذلك، السجل (relay1 . bar . foo . com , 145 . 37 . 93 . 126 , A)
(هو سجل من نوع Type A. .
إذا كان النوع Type = NS ، يمثل الاسم (Name نطاقاً (domain) مثل foo. com ، وتمثل القيمة (Value) اسم المضيف لخادم DNS موثوق يعرف كيف يحصل على عناوين المضيفين في هذا النطاق، ويستخدم هذا السجل لتوجيه استعلامات DNS في سلسلة الاستعلام، فعلى سبيل المثال، السجل (foo . com , dns . foo . com , NS) هو سجل من نوع Type NS.
إذا كان النوع Type = CNAME، تمثل القيمة (Value) اسم المضيف الأساسي، ويمثل الاسم (Name) اسم المضيف المستعار، ويمكنك هذا السجل من الاستعلام عن الاسم الأساسي للمضيف. مثال على ذلك)
foo . com , relay1 . bar . foo . com , CNAME) هو سجل CNAME.
إذا كان النوع Type = MX ، تمثل القيمة (Value) الاسم الأساسي لخادم البريد الإلكتروني الذي له اسم مستعار يمثل الاسم(Name ، وكمثال على ذلك، السجل (foo . com , mail . bar . foo . com MX) من نوع MX ، وتتيح سجلات MX للمضيفين في خوادم البريد أن يكون لهم أسماء مستعارة بسيطة، كما يمكنك سجل MX من استخدام نفس الاسم المستعار لخادم البريد وخوادم أخرى (مثل خادم الويب). للحصول على الاسم الأساسي لخادم البريد، يستعلم عميل DNS عن سجل MX وللحصول على الاسم الأساسي للخوادم الأخرى، يستعلم عميل DNS عن سجل CNAME
رسائل اسم النطاق DNS Messages اشرنا سابقا، عزيزي الطالب، إلى رسائل استعلام DNS ورسائل الاستجابة، وهناك نوعان فقر DNS، وسواء كانت رسائل استعلام أو استجابة فإن لها نفس الشكل ص٩٢ مهم

صيغة رسائل DNS وتكون صيغة الحقول المختلفة في رسالة DNS كما يأتي: :
مقدمة الرسالة 12 بايت (Header Section) الأولى، ويحتوي هذا المقطع عددا من الحقول، الحقل

الأول هو رقم طوله ١٦ بت يعرف الاستعلام، حيث يتم نسخ هذا المعرف في رسالة الرد على استعلام مما يتيح للعميل ربط الردود المستقبلة بالاستعلامات المرسلة، وهناك عدد من الرايات في حقل الراية(Flag) ، راية الاستعلام / الرد" طولها ١ بت، وتحدد فيما إذا كانت الرسالة هي استعلام (٠) أو رد (١)، راية "الخادم الموثوق" طولها ١ بت، وتحدد في رسالة الرد إذا كان خادم DNS موثوقا لرسم المستعلم عنه، راية "الإعادة مرغوبة" طولها ١ بت، وتحدد عندما يرغب العميل (مضيف او خادم DNS بأن يقوم خادم DNS بإعادة الطلب عندما لا يكون السجل متوفرة لديه. راية "حقل الإعاد متوفر " طولها ١بت، ويحدد في رسالة الرد إذا كان خادم DNS يدعم الإعادة. في المقدمة، هناك ايه أربعة حقول رقمية، وتشير هذه الحقول إلى عدد مرات حدوث الأنواع الأربعة من مقاطع البيانات اللي تتبع المقدمة.

المسألة أو الاستعلام .(Question section) يحتوي هذا المقطع معلومات حول الاستعلام الحالي ويتضمن (١) حقل الاسم، ويحتوي على الاسم الذي يجري الاستعلام عنه (٢) حقل النوع، ويشير مي نوع السؤال المطروح حول الاسم، مثلا عنوان مضيف يرتبط بالاسم من نوع (Type A) او البريد الاسم من نوع. (Type MX)

الإجابة أو الرد .(Answer Section) يحتوي هذا المقطع سجلات المورد للاسم الذي تم الاستعلام عنه أصلا. تذكر أنه في كل سجل مورد هناك النوع CNAME ، NS، Type (A، و(MX ، والقيمةValue ، ووقت الحياة .TTL الرد قد يعود بسجلات موارد متعددة في الجواب،

إذ أن المضيف قد يكون له عناوين إنترنت IP متعددة.

عناوين المضيف

١. السلطة أو التخويل (Authority Section). يحتوي هذا المقطع سجلات الخوادم الموثوقة الأخرى.
٢. مقطع إضافي (Additional section). يحتوي هذا المقطع سجلات أخرى مفيدة. على سبيل المثال، فإن حقل الجواب في الرد على استعلام MX يحتوي سجل
٣. مورد يزودك باسم المضيف الأساسي لخادم البريد، وهنا يحتوي المقطع الإضافي سجلا نوعه Type A يزودك بعنوان IP للمضيف الأساسي الخادم البريد.

السؤال الذي يدور في ذهنك عزيزي الطالب، كيف ترسل رسالة استعلام DNS مباشرة من المضيف الذي تعمل عليه إلى خادم DNS ؟ يتم ذلك باستخدام برنامج NSLOOKUP الذي يتوفر في معظم أنظمة تشغيل ويندوز ويونيكس. للاختبار من نظام Windows ، افتح موجه الأوامر ثم قم باستدعاء NSLOOKUP ببساطة عن طريق كتابة الأمر "NSLOOKUP" ، عندها يمكنك إرسال استعلام DNS إلى أي خادم DNS بعد تلقي رسالة الرد من خادم DNS ، سوف يعرض لك برنامج NSLOOKUP السجلات المدرجة في الاستجابة. سيتناول الجانب العملي الخاص بهذه الوحدة خادم DNS بالتفصيل من خلال مختبر وير شارك. DNS Wireshark lab
إدراج سجلات DNS في قاعدة البيانات Inserting Records into the DNS Database ركزنا في المناقشة أعلاه على كيفية استرجاع السجلات من قاعدة بيانات DNS. ربما تتساءل، عزيزي الطالب، كيف يتم إدراج السجلات في قاعدة البيانات في المقام الأول؟ دعنا نجيب على التساؤل بمثال.

مثال:

افترض أنك أنشأت شركة جديدة أطلقت عليها اسم شبكة يوتوبيا (Network Utopia)، في البداية عليك تسجيل اسم النطاق networkutopia. com لدى أحد المسجلين أو مزودي الخدمة. المسجل هو كيان تجاري يتحقق من تفرد اسم النطاق، ويدخل اسم النطاق في قاعدة بيانات DNS مقابل رسوم رمزية (كما هو مبين أدناه)، وهناك العديد من المسجلين المعتمدين من مؤسسة الإنترنت للأسماء والأرقام المخصصة (the Internet Corporation for Assigned Names and Numbers(ICANN والقائمة الكاملة للمسجلين المعتمدين متوفرة على الموقع http : / / www . internic . net.

وعند تسجيل اسم النطاق networkutopia. com.

تحتاج أيضا إلى تزويد المسجل بأسماء وعناوين IP لخوادم DNS الموثوقة الأساسية والثانوية الخاصة بك، ولنفترض أن الأسماء والعناوين هي:

dns1.networkutopia.com, dns2.networkutopia.com, 212.212.212.1, 212.212.212.2

ولكل من هذين الخادمين الموثوقين يتأكد المسجل من إدخال سجل من نوع NS وآخر من نوع A إلى خوادم TLD com ، وبالتحديد لخادم networkutopia. com الموثوق الأساسي، فإن المسجل يدرج سجلي الموارد الآتيين إلى نظام DNS:

(networkutopia.com, dns1.networkutopia.com, NS)

21 - تطبيقات النظير للنظير (Peer - to - Peer P2P) | (Applications)

لا تعتمد بنية النظير للنظير (Peer - to - Peer : P2P) ، أو تعتمد بالحد الأدنى، على خوادم البنية التحتية تعمل دائما (always - on) ، بل يقوم ازواج من المضيفين المرتبطين بشكل متقطع، يطلق عليهم الله بالاتصال المباشر مع بعضهم البعض. والنظراء غير مملوكين لمزود الخدمة، بل هو عبارة عن أجهزة حاه مكتبية ومحمولة يديرها المستخدمون.

في هذا القسم سنقوم بدراسة أحد التطبيقات المناسبة تماما لتصاميم P2P ، وهو توزيع الملفات، حيث يوزع التطبيق ملفا من مصدر واحد إلى عدد كبير من النظراء، فتوزيع الملفات هو أفضل بداية لتحقيقنا في P2P ، إذ يعرض

بوضوح قابلية التوسع الذاتي في بنية P2P ، وسنأخذ نظام تورنت الشائع كمثال على توزيع الملفات.

٢ - 7 - ١ توزيع ملفات النظير للنظير (P2P File Distribution)

نبدأ P2P بالنظر في تطبيق طبيعي جدا، وهو توزيع ملف كبير (ملف موسيقى أو فيديو مثلا) من خادم واحد إلى عدد كبير من المضيفين، هم النظراء. في بنية العميل الخادم، يرسل الخادم نسخة من الملف إلى كل نظرائه فيضع عبئا هائلا على كاهل الخادم، ويستهلك كمية كبيرة من عرض النطاق الترددي. أما في بنية P2P ، يستطيع كل النظراء إعادة توزيع أي جزء تلقوه من الملف إلى أي من نظرائه، وبالتالي مساعدة الخادم في عملية التوزيع. اعتبارا من عام ٢٠١٢، أصبح تورنت أكثر بروتوكولات P2P شعبية لتوزيع الملفات، وهناك العديد من عملاء تورنت المستقلين تتوافق مع بروتوكول تورنت. في هذا القسم الفرعي، سندرس أولا قابلية التوسع الذاتي لبنية P2P في سياق توزيع الملفات، ثم نصف تورنت وأبرز خصائصه وميزاته.

قابلية التوسع في معمارية النظير للنظير Scalability of P2P Architectures

للمقارنة بين بنيتي العميل الخادم والنظير للنظير، وتوضيح قابلية التوسع الذاتي في P2P، سنختبر نموذجا كمية بسيطة لتوزيع ملف إلى مجموعة ثابتة من النظراء باستخدام المعماريتين. كما يبين الشكل (٢-٢٣)، يتصل الخادم والنظراء إلى الإنترنت من خلال روابط النفاذ.

تطبيق بت تورنت (سيل الثنائيات) BitTorrent بت

تورنت هو بروتوكول P2P شائع لتوزيع الملفات [٢٠١١ Chao]. وتسمى مجموعة النظراء المشاركين في توزيع ملف معين تورنت، وينزل نظراء التورنت قطعة (chunks) متساوية الحجم من الملف فيما بينهم، كل منها ٢٥٦ كيلوبايت، و عندما ينضم نظير لأول مرة، لا يكون لديه قطع، وتتراكم بمرور الوقت. فبينما يقوم بتنزيل قطع، يعمل على تحميل قطع لنظرائه الآخرين. وبعد حصوله على الملف بأكمله،
قد يترك التورنت (بانانية)، أو يستمر في تحميل أجزاء لنظرائه. كما يمكن مغادرة التورنت والانضمام مرة أخرى لاحق.

دعنا الأن نلقي نظرة فاحصة على كيفية عمل تورنت. كل تورنت لديه عقدة بنية تحتية تسمى متعقب tracker القدما ينضم نظير لتورنت، فإنه يسجل نفسه مع متعقب يبلغه بشكل دوري أنه لا يزال في تورنت. بهذه الطريقة، يتابع المتعقب النظراء المشاركين في تورنت، الذين قد يتراوح عددهم في اللحظة الواحدة من أقل من عشرة إلى أكثر من ألف مشارك.
كما يبين الشكل (٢-٢٥)، ص٩٨
عندما ينضم نظير جديد، أليس، إلى تورنت، يختار المتعقب عشوائيا مجموعة فرعية من النظراء المشاركين (ولنقل ٥٠)، ويرسل عناوين IP الخاصة بهم إلى أليس. تحاول أليس تأسيس ان TCP متزامن مع جميع النظراء على هذه القائمة، ولنطلق على جميع النظراء الذين نجحت أليس في الاتص بهم "نظراء مجاورون" (Neighboring peers)، وقد يزيد أو ينقص النظراء المجاورون بمرور الوقت كل نظير سيكون لديه قطع من ملفات متعددة، فتطلب أليس من كل نظير من جيرانها قائمة القطع التي لديهم عبر اتصال TCP)، فإذا كان لدى أليس L من الجيران، ستحصل على L من قوائم القطع، ثم تصدر أليس طلبات للحصول على قطع ليست بحوزتها حاليا. على أليس اتخاذ قرارين مهمين؛ الأول، أي من القطع تطاب من جيرانها أو لا؟ والثاني، لأي من جيرانها عليها أن ترسل القطع المطلوبة؟ لاتخاذ القرار الأول تستخدم أليس تقنية تسمى الأكثر ندرة أو rarest first، فتطلب أولا القطع التي لا تملكها والأكثر ندرة بين جيرانها (أي، أقل عدد من النسخ المتكررة

بين جيرانها). بهذه الطريقة، توزع القطع النادرة بسرعة أكبر، فيتساوى عدد نسخ كل قطعة في التورينت.

لتحديد أي طلب تستجيب له، يستخدم تورنت خوارزمية ذكية، فتعطي أليس الأولوية لجيرانها الذين يزودونها بالبيانات حاليا بمعدل أعلى، أي تقيس باستمرار المعدل الذي تحصل فيه على بنات من كل نظير، وتحدد أفضل أربعة نظراء (يطلق عليهم unchoked) وتتبادل إرسال القطع معهم. ثم تقوم باحتساب المعدلات كل ١٠ ثواني، وقد تستبدل النظراء الأربعة في ضوء ذلك.
وكل ٣٠ ثانية، تختار جار، إضافية عشوائيا (ولنقل "بوب") وترسل له القطع. ولأن أليس هي من أرسلت البيانات لبوب، فقد تصبح واحدة من أكثر أربعة محملين لبوب، فيبدأ بوب بإرسال البيانات إلى أليس. إذا كان المعدل الذي يرسل به بوب البيانات إلى أليس عالية بما فيه الكفاية، فقد يصبح بوب، بدوره، واحدة من أكثر أربعة محملين لأليس.

2 - 8 |برمجة المقابس: إنشاء تطبيقات الشبكة Socket Programming: Creating Network Applications)

بعد اطلاعك على عدد من تطبيقات الشبكة المهمة، حان دورك لإنشاء برامج تطبيقية للشركة على ارض الواقع. كما ذكرنا سابقا في القسم ٢-٢، يتكون تطبيق الشبكة النموذجي من زوج من البرامج العميل الخادم، وينفذان على نظامين مختلفين، فعندما يتم تنفيذ هذين البرنامجين، يتم إنشاء عمليتين تتواصد" بعضهما البعض من خلال القراءة من المقابس والكتابة عليها. فعند بناء تطبيق شبكة، تكمن المهمة الري المطور في كتابة التعليمات البرمجية لكل من العميل و الخادم.

وهناك نوعان من تطبيقات الشبكة

أ. تطبيق الشبكة المفتوح:

يتم تحديد العملية في معيار البروتوكول، مثل مراجع RFC أو أي معايير موثوقة أخرى، أي أن قواعد عملها معروفة للجميع.
لمثل هذا التنفيذ، فيجب أن تتوافق برامج العميل والخادم مع قواعد مرجع RFC. فإذا عمل مبرمجان الأول على برنامج العميل والآخر على برنامج الخادم، واتبعا قواعد RFC بدقة، سيتمكن البرنامجان من التعامل فيما بينهما.

ب. تطبيق الشبكة المملوك:

تستخدم برامج العميل والخادم بروتوكول طبقة التطبيقات التي قد لا يتم نشرها علنا في مراجع RFC ، وفي هذه الحالة يقوم مطور واحد (أو فريق تطوير) ببناء برنامجي العميل والخادم، ويكون لديهم سيطرة كاملة على محتوى التعليمات البرمجية، لذا لن يتمكن المطورون المستقلون من تطوير تعليمات برمجية تتوافق مع التطبيق.
عزيزي الطالب، في هذا القسم، سنقوم بدراسة القضايا الرئيسة اللازمة لتطوير تطبيقات العميل الخادم. خلال مرحلة التطوير، يجب على المطور اتخاذ القرار ما إذا كان التطبيق موجه للعمل على TCP أو UDP. تذكر أن TCP مهيأ للاتصال ويوفر قناة موثوقة تتدفق فيها البيانات بين نظامين نهائيين، أما UDP فهو بدون اتصال ويرسل حزم مستقلة من البيانات من نظام نهائي إلى آخر دون أي ضمانات بشأن التسليم. تذكر أيضا أنه عندما يطبق برنامج العميل أو الخادم بروتوكولا محددة في مرجع RFC ، ينبغي أن يستخدم رقم المنفذ المعروف والمرتبط بالبروتوكول، وعلى العكس، عند بناء تطبيق مملوك، يجب الحذر من استخدام هذه المنافذ المعروفة. سنستخدم لغة بايثون في برمجة المقابس لتطوير تطبيقين بسيطين، أحدهما على UDP والآخر على TCP ، وقد اخترنا هذه اللغة لأنها تكشف بوضوح المفاهيم الرئيسة المتعلقة بالمقبس باستخدام سطور أقل من التعليمات البرمجية، ويمكن لمبرمج مبتدي تفسير كل سطر بسهولة، ومن لديه تجربة في أي لغة أخرى كذلك يستطيع المتابعة بسهولة.

١ 2 - 8 - برمجة المقابس في بروتوكول المخطط البياني للمستخدم) Socket (Programming with UDP

في هذا القسم الفرعي، سنقوم بكتابة برامج عميل-خادم بسيطة تستخدم UDP، وفي القسم التالي، سلر باستخدام.TCP دعنا نلقي نظرة فاحصة على التفاعل بين اثنتين من العمليات التي تستخدم مقابسUDP ، قبل أن لا المرسلة من إرسال حزمة بيانات خارج المقبس باستخدامUDP ، يجب أولا إرفاق عنوان الوجهه به قابسUDP ، قبل أن تتمكن العملية وان الوجهة بهذه الحزمة

بعد مرور الحزمة من مقبس المرسل، يستخدم عنوان الوجهة لتوجيه الحزمة من خلال الإنترنت إلى مقبس العملية المستقبلة، التي تعمل على استرداد الحزمة من المقبس، وتفقد محتوياتها واتخاذ الإجراء المناسب ركن عنوان الوجهة المرفق بالحزمة من عنوان الإنترنت IP للمضيف الوجهة ورقم المنفذ، تستخدم أجهزة التله حبه عنوان الإنترنت لتتمكن من توجيه الحزمة إلى المضيف، ولكن قد تكون العديد من عمليات تطبيقات الشركة قيد التشغيل على المضيف عبر واحد أو أكثر من المقابس، لذا فمن الضروري أيضا تحديد رقم المنفذ، وهو رقم معرف يسند إلى المقبس عند إنشائه في المضيف الوجهة باختصار، يرفق المرسل بالحزمة المرسلة عنوان IP ورقم منفذ المقبس للمضيف الوجهة وكذلك المضيف المصدر، ولكن إرفاق عنوان المصدر لا يتم في التعليمات البرمجية لتطبيقUDP ، بل يقوم بذلك نظام التشغيل تلقائيا

مثال: سنستخدم تطبيق بسيطا للعميل - الخادم لشرح برمجة المقبس لكل من بروتوكولي UDP وTCP:

1. يقرأ العميل سطراً من الأحرف (البيانات من لوحة المفاتيح ويرسلها إلى الخادم

٢. يتلقى الخادم البيانات ويحول الأحرف إلى أحرف كبيرة.
٣. يرسل الخادم البيانات المعدلة إلى العميل.
٤ يتلقى العميل البيانات المعدلة ويعرض السطر على شاشته.

يبين الشكل (٢-٢٦)ص١٠٢

المهمة الرئيسة للعميل والخادم المتصلان عبر خدمة نقل بروتوكولUDP ، والمتعلقة بالمقبس. الآن، دعنا نلقي نظرة على زوج برنامج العميل الخادم لتنفيذ UDP لهذا التطبيق البسيط، حيث سنقدم تحليلا مفصلا سطرا بسطر بعد كل برنامج. سنبدأ بعميل UDP الذي سيرسل رسالة بسيطة على مستوى التطبيق إلى الخادم، وليتمكن الخادم من استقبال الرسائل والرد على العميل، يجب أن يكون الخادم جاهزاً وقيد التشغيل، أي يجب أن يتم تشغيل الخادم كعملية قبل أن يرسل العميل رسالته. النطق على برنامج العميل UDPClient. py ، وعلى برنامج الخادمUDPServer. py
، وللتأكيد على المسائل الأساسية، قدمنا عمدة الحد الأدنى من التعليمات البرمجية .(code) ونعلم بالتأكيد أن الكود الجيد لديه بضعة سطور مساعدة، وخصوصا لمعالجة حالات الخطأ، وفي هذا التطبيق، اخترنا ١٢٠٠٠ عشوائية كرقم منفذ للخادم

برمجة المقابس في بروتوكول التحكم بالنقلColet Programming with (TCP)

على عكس UDP بروتوكول TCP مهيأ للاتصال، أي أن العميل والخادم بحاجة إلى المصافحة وإنشاء اتصال Top قبل أن يبدأ إرسال البيانات فيما بينهما، حيث يرتبط أحد طرفي اتصال TCP بمقبس العميل ويرتبط الطرف الآخر بمقبس الخادم. عند إنشاء اتصالTCP ، يرتبط معه عنوان مقبس العميل)عنوان IP ورقم المنفذ (و عنوان مقبس الخادم) عنوان IP ورقم المنفذ(، فعندما يريد أحد الجانبين إرسال البيانات إلى الجانب الآخر، فما عليه سوى وضع البيانات لتنتقل عبر اتصال TCP عن طريق المقبس الخاص به، دون الحاجة إلى إرفاق عنوان الوجهة بالحزمة المرسلة كما كان الحال في .UDP

الآن دعنا نلقي نظرة فاحصة على التفاعل بين برنامجي العميل والخادم في TCP، العميل هو المسؤول عن بدء الاتصال بالخادم، وعلى الخادم أن يكون مستعدة للتفاعل مع العميل المتصل،

وهذا يعني أمرين:

١. يجب أن يكون خادم TCP قيد التشغيل كعملية (process) قبل محاولة العميل بدء الاتصال، كما فيحالة UDP..

2. يجب أن يكون لدى برنامج الخادم مقبس خاص، يرحب بأي اتصال يرد من عملية العميل قيد التشغيلعلى مضيف ما

بإمكان أي عملية في برنامج العميل بدء اتصال TCP مع عملية خادم قيد التشغيل عن طريق إنشاء مقبس (باب)TCP ، يحدد عنوان مقبس الترحيب في الخادم) أي عنوان IP ورقم منفذ المقبس(، عندئذ يبدأ العميل مصافحة ثلاثية) Three - Way handshake)في طبقة النقل، وينشئ اتصال TCP مع الخادم، لاحظ أن هذه المصافحة غير مرئية لبرنامجي العميل والخادم.

في مثالنا أدناه، سمينا مقبس الترحيبserverSocket ، وهو نقطة بدء الاتصال لجميع العملاء الراغبين في التواصل مع الخادم، وسمينا المقبس الذي أنشئ حديثا وخصص للعميل المتصل .ConnectionSocket من منظور التطبيق، فإن مقبس العميل ومقبس اتصال الخادم يتصلان مباشرة عن طريق ما يشبه الأنبوب.

وقد طلبة العميل البايتات عشوائية عبر المقبس، ويضمن TCP أن تستقبل عملية الخادم (عبر مقبس كل بابت حسب ترتيب إرسالها، كما هو مبين في الشكل (٢-٢٧). وبالتالي يقدم TCP خدمة موثوقة بين عمليتي العميل والخادم، علاوة على ذلك، فإن عملية العميل لا ترسل البايتات إلى مقبسها فحسب، ب، كما أن عملية الخادم لا تتلقى البايتات من مقبس اتصالها فحسب، بل ترسلها إليه ايضا.

مسرد المصطلحات

١. الاتصال الدائم أو الثابت(Persistent Connection)
٢. الاتصال غير الدائم أو المتقطع(Non - Persistent Connection)
٣. الأمن(Security)
٤. الإنتاجية(Throughput)
٥. التخزين المخبأ للويب(Web caching)
٦. الذاكرة المخبأة (التخزين المؤقت(DNS Caching)
٧. التسوق بنقرة واحدة(One - click shopping)
٨. التوقيت(Timing)
٩. الحركات أو المعاملات ((Transaction)
١٠. الخدمة الموجهة بالاتصال Connection - oriented Services
١١. الخوادم الموثوقة المخولة(Authoritative DNS servers)
١٢. الدالة الشرطية(GET (The Conditional GET ....)
١٣. الشبكة العنكبوتية العالمية(World Wide Web : WWW)
١٤. العميل الخادم(Client - Server)
١٥. الكوكيز(Cookies)
١٦. المأخذ أو المقبس(Socket)
١٧. المصادقة(Authentication)
١٨. المصادقة أو التفويض (Autherization)
١٩. المصافحة (handshaking)
٢٠. النظير للنظير(Peer - to - Peer : P2P)
٢١. النقل الموثوق للبيانات(Reliable Data Transfer)
٢٢. بت تورنت (سيل الثنائيات(BitTorrent)
٢٣. برتوكول التحكم بالنقل(Transport Control Protocol : TCP)
٢٤. بروتوكول الوصول إلى البريد عبر الإنترنت(Internet Mail Access Protocol : IMAP)

٢٥. بروتوكول مخطط بيانات المستخدم(User Datagram Protocol : UDP)
٢٦. بروتوكول مكتب البريد الإصدار3 (Post Office Protocol - Version 3 : POP3)
٢٧. بروتوكول نقل البريد البسيط(Simple Mail Transfer Protocol : SMTP)
٢٨. بروتوكول نقل الملفات(File Transfer Protocol FTP)
٢٩.)بروتوكول نقل النص التشعبي(HyperText Transfer Protocol : HTTP)
٣٠. .بنية النظير للنظير(Peer - to - Peer : P2P)
٣١. .تأخير الإنترنت(Internet delay)
٣٢. خادم معلومات الإنترنت(Internet Information Server : IIS)
٣٣. خدمة النقل الموثوق للبيانات(Reliable Data Transfer Services)
٣٤. خوادم الجذرRoot DNS servers
٣٥. خوادم النطاق عالي المستوى Top - Level Domain (TLD) serversus
٣٦. رسالة الاستجابتHTTP Response Message
٣٧. .رسالة الطلبHTTP Request Message
٣٨. رقم المنفذ(Port number)
٣٩. زمن التوزيع(Distribution time)
٤٠. زمن الذهاب والإياب(Round - Trip Time : RTT)
٤١. سلامة البيانات(Integrity)
٤٢. شبكات توزيع المحتوى (Content Distribution Networks : CDN)
٤٣. ضبط الازدحام(Congestion - control)
٤٤. طبقة المقابس الأمنة(Secure Socket Layer : SSL)
٤٥. عنوان الإنترنت(Internet Protocol : IP)
٤٦. عنوان الإنترنت(IP Address)
٤٧. عنوان الإنترنتIP Address
٤٨. قاعدة بيانات هرمية موزعةDistributed Hierarchical – Database
٤٩. مؤسسة الإنترنت للأسماء والأرقام المخصصة ICANN) the Internet Corporation for Assigned Names andNumbers)
٥٠. موقع المعلومات العالمي(Universal Resource Locator : URL)
٥١. نص الكيان(entity body)
٥٢. نطاق اسم الإنترنت من بيركلي (Berkley Internet Name Domain : BIND)

٥٣. نطاق اسم النطاق UL (DNS : Domain Name System

الوحدة الثالثة

تلخيص صفحة ١٢١

٢,٣ خدمات طبقة النقل: Transport layer services

يوفر بروتوكول طبقة النقل اتصالا بين عمليات التطبيق التي تعمل في مضيفات مختلفة .ونعني بالاتصال المنطقي .ان المضيفات التي تشغل العمليات ,من وجهة نظر التطبيق تبدو وكانها متصلة مباشرة مهما كانت متباعدة ومتصلة عبر العديد من اجهزة التوجيه وانواع مختلفة من خطوط الاتصال اما عمليات التطبيق فتستخدم الاتصال المنطقي لتبادل الرسائل بينها دون الاكتراث بتفاصيل البنية التحتية المستخدمة لنقلها .

تلخيص صفحة ١٢٢

تعمل بروتوكولات طبقة النقل على جانبي الارسال والاستقبال بدلا من موجهات الشبكة ففي جانب المرسل ,تحول رسائل طبقة التطبيقات التي تتلقها من عملية التطبيق المرسل الى حزم تسمى في مصطلحات الانترنت (شرائح طبقة النقل) وربما يتم ذلك من خلا تقطيع رسائل التطبيق الى قطع اصغر واضافة مقدمة طبقة النقل الى كل قطعة لانشاء شريحة طبقة النقل لتمررها الى طبقة الشبكة في الطرف المرسل حيث يتم تغليف الشريحة ضمن حزمة طبقة الشبكة وارسالها الى الوجه .

تلخيص صفحة ١٢٣

١,٢,٣ العلاقة بين طبقتي النقل والشبكة :

طبقة النقل تعلو طبقة الشبكة . فبينما يوفر بروتوكول طبقة النقل اتصالا منطقيا بين المعلومات التي تعمل على المضيفات المختلفة ,يوفر بروتوكول طبقة الشبكة اتصالا منطقيا بين المضيفات ورغم ان اختلاف بسيط الا انه مهم .

تعمل بروتوكولات طبقة النقل في النظم النهائية فتنقل الرسائل من عمليات التطبيق الى طبقة الشبكة والعكس بالعكس ولكن لا تدخل بكيفية نقل الرسائل داخل الشبكة الاساسية .لا تتصرف او تعترف الموجهات الوسيطة باي معلومات قد تكون اضافتها طبقة النقل الى رسائل التطبيق .

٢,٢,٣ نظرة عامة على طبقة النقل في الانترنت :

وهو بروتوكول غير موثوق او مهيأ للاتصال .UDB بروتوكولي نقل هما :بروتوكول مخطط بيانات المستخدم

وهو بروتوكول موثوق ومهيأ للاتصال بالتطبيق الذي يستدعيه .TCP بروتوكول التحكم بالنقل

وعند تصميم تطبيق الشبكة على مطور التطبيق تحديد اي منهما سيوظف التطبيق.

وتتمثل المسؤولية للبروتوكولين في التجميع وفك التجميع على مستوى طبقة النقل اي توسيع خدمة التوصيل التي يقدمها بين نظاميين نهائيين الى خدمة التوصيل بين عمليتين تعملان عليهما .

وكما يوفر هذان البروتوكولان فحصا لسلامة البيانات من خلال تضمين حقول كشف الاخطاء في مقدمات الشرائح .

تلخيص صفحة ١٢٤

٣,٣ التجميع وفك التجميع :

Multiplexing and demultiplexing

تهدف هذه العملية الى توسيع خدمة التسليم (مضيف الى مضيف) التي توفرها طبقة الشبكة لتصبح (عملية الى عملية) للتطبيقات قيد التشغيل على المضيفات .لدى المضيف الوجهة تتلقى طبقة النقل الشرائح من طبقة الشبكة التي تدنوها وطبقة النقل المسؤولة عن تسليم بيانات هذه الشرائح الى عملية التطبيق المناسب قيد التشغيل في المضيف .

تلخيص صفحة ١٢٥

كيف يوجه المضيف المستقبل شريحة واردة من طبقة النقل الى المقبس المناسب :
لكل شريحة حقول مخصصة لهذا الغرض فتقوم طبقة النقل لدى المستقبل بفحص هذه الحقول لتحديد المقبس الصحيح للمستقبل ثم توجيه الشريحة اليه ويطلق على هذه العملية فك التجميع . اما عملية التجميع فهي التقاط قطع البيانات لدى المضيف المصدر من مقابي مختلفة وتغليف كل قطعة من البيانات مع المعلومات المقدمة لانشاء الشرائح وتمريرها الى طبقة الشبكة .

صفحة ١٢٦ تقويم ذاتي (١,٣)

تدريب (١,٣) صفحة ١٢٧

تلخيص صفحة ١٢٧ و١٢٨

٤,٣ النقل بدون اتصال :وبروتوكول المخطط البياني للمستخدم :

Connectionless transport :UDP

هو بروتوكول غير مهيأ للاتصال (دون اتصال) .وهو لا يزيد عما يقوم به بروتوكول النقل فبعيدا عن وظيفته في التجميع وفك التجميع والتحقق من بعض الاخطاء فان لا يضيف شيئا الى عنوان الانترنت فاذا اختير لبناء التطبيق .فان التطبيق يتحدث فياخذ الرسائل من عملية التطبيق ويرفق بها حقلي رقم ويمرر الشريحة الناتجة الى طبقة الشبكة .
ip مباشرة مع

للاسباب التالية :UDP العديد من التطبيقات يلائمها

١ _ ضبط ادق على مستوى التطبيق (لما يتم ارساله من البيانات ومتى):
بمجرد ان تمرر عملية التطبيق البيانات الى
سوف يحزم البيانات داخل شريحة ويمررها مباشرة الى طبقة الشبكة .UDP
فلديه الية ضبط احتقان تخنق المرسل في طبقة النقل عندما يصبح خط الاتصال بين المضيفين .Tcp اما
٢Tcp _لا داعي لانشاء اتصال : مصافحة ثلاثية قبل البدء بنقل البيانات
يستخدم
اذ سيكون UDP على DNS فينطلق دون تمهيد ولا يحتمل التاخير وربما هو السبب وراء تشغيل UDP بينما
. Tcp ابطا بكثير لو استخدم

الذي يحافظ على حالة الاتصال في الانظمة النهائية وتشمل المخازن
٣Tcp _ لا تحتفظ بحالة الاتصال :على عكس المؤقتة
للاستقبال والارسال ومعامل ضبط الاحتقان .
٤Tcp _كلفة على ٢٠ بايت كلفة اضافية للمقدمة بينما تحتوي شريحة
مقدمة الحزمة قليلة :تحتوي كل شريحة
على ٨ بايت فقط .UDP
تلخيص صفحة ١٢٩
تقويم ذاتي (٢,٣) صفحة ١٢٩
١,٤,٣ بنية شريحة بروتوكول مخطط البيانات المستخدم ك
UDP

وتتكون المقدمة من ٤ حقول كل منها ٢ بايت :

١ _ حقل رقم المنفذ :

يسمح بمرور البيانات الى العملية الصحيحة قيد التشغيل لدى المضيف الوجهة (فك التجميع)

٢ _حقل الطول :

يبين المضيف عدد بايتات الشريحة بما في ذلك المقدمة والبيانات .

٣ _حقل مجموع الاختباري :

يتحقق المستقبل من ورود الاخطاء في الشريحة . في الواقه يتم حساب هذا المجموع على بعض حقول مقدمة .

تقويم ذاتي(٣,٣) صفحة ١٣٠

تدريب(٢,٣) صفحة ١٣٠

مثال صفحة

١٣٠

المجموع الاختباري لبروتوكول مخطط بيانات المستخدم (UDP Checksum):

يستخدم المجموع الاختباري للكشف عن الاخطاء أي لتحديد ما اذا تغير احد البتات في شريحة UDP اثنا انتقالها من المصدر الى الوجهة (بسبب التشويش في خط الاتصال او اثناء تخزينها في الموجة). ويقوم UDP في جانب المرسل بإيجاد المتمم (قلب البتات)
1 s complement لمجموع كل الكلمات ذات ال 16 بت في الشريحة ، واي فائض يصادف اثناء الجمع يضاف الى الناتج ويوضع الناتج في حقل المجموع الاختباري من الشريحة .

مثال :

اوجد المجموع الاختباري للكلمات الاتية في شريحة UDP : *(صفحة 130)*

C=1000111100001100 , B=0101010101010101 ,A=0110011001100000

الحل : مجمع الكلمتين الاولى والثانية كما يلي :

A 0110011001100000

B 0101010101010101

الناتج 1011101110110101

نجمع الناتج والكلمة الثالثة كما يلي:

1011101110110101

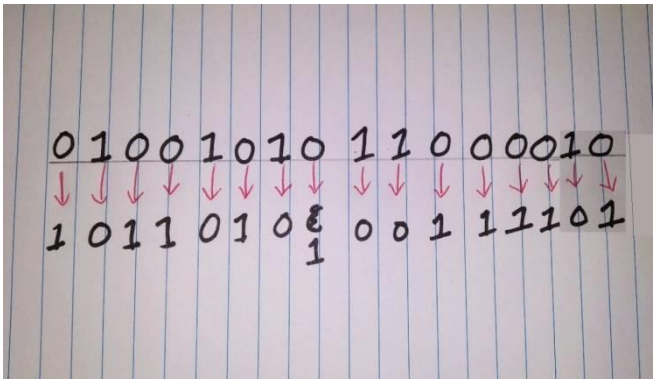
C 1000111100001100

الناتج 0100101011000001 الفائض يضاف الى الناتج كما يلي:

+ 0000000000000001 ليصبح الناتج

0100101011000010

نحسب المتمم **1 S Complement** بتغيير ١ الى ٠ وكذلك ٠ الى ١ كما في الصورة في الأسفل



فيصبح المجموع الاختباري :
1011010100111101

يرسل هذا المجموع ضمن الشريحة ، وفي جانب المستقبل ، نقوم بما يلي:

نجمع الكلمات الثلاث ثم نجمع الناتج مع المجموع الاختباري المرسل ، كما يلي :

A 0110011001100000

B 0101010101010101 **ناتج** A+B **1011101110110101**

C 1000111100001100

1011010100111101 *المجموع الاختباري المرسل*

[1] 0100010001001010

00101111111111110

1111111111111111

فإن لم يرد أي خطا في الحزمة ،سيكون الناتج بالتأكيد كما هو مبين أعلاه ،وإذا ظهر 0 في الناتج ، يكون هناك خطأ في هذه الحزمة .

اساسيات النقل الموثوق للبيانات .(صفحة 131)

(PRINCIPLES OF RELIABLE DATA TRANSFER)

رغم ان الـ UDPيوفر فحص الأخطاء إلا انه لا يعمل على تصحيحها فبعض تطبيقاتUDP

يتجاهل الشريحة التالفة; وبعضها الاخر يمررها الى التطبيق مع رسالة تحذير ، وبذلك يعتبر النقل الموثوق للبيانات قضية جوهرية في الشبكات; لانه يغطي العديد من اساسياتها وهي قضية لا تقتصر على طبقة النقل بل تطبق في طبقة الربط وطبقة التطبيقات . (الاطلاع علة الشكل 3-6 صفحة 132 لتتبع كيف يتم النقل الموثوق للبيانات : نموذج الخدمة المقدمة وتنفيذها)

في هذا القسم سنقوم تدريجيا بتطوير جانبي المرسل والمستقبل لبروتوكول نقل البيانات الموثوق ،مع مراعاة التدرج في نماذج اكثر تعقيدا للقناة الاساسية . فمثلا سنراعي الاليات التي تلزم عند تلف بعض البتات او فقدان حزم كاملة في القناة الاساسية وسنفرض هنا ان الحزم ستسلم حسب الترتيب الذي ارسلت به مع احتمال فقدان بعض الحزم ; أي لن تقوم القناة بإعادة الترتيب . (يبين الشكل 3-6 واجهات بروتوكول نقل البيانات)

- بناء بروتوكول موثوق لنقل البيانات :

ابسط حالة عندما تكون القناة موثوقة تماما فالبروتوكول الذي يمثل هذه الحالة بسيط وسنطلق عليه اسم rdt1.0(ويبنه الشكل 7-3 صفحة 133)

صفحة *134* يمكن ان يظهر خطأ في احدى بتات الحزمة فلابد من ايجاد بروتوكولات تعالج الخطا اطلقنا عليها . (rtd2.0,

rtd2.1,rtd2.2) وقد تكون القناة نفسها غير موثوقة، أي قد تضيع بعض البتات في القناة وقد اطلقنا على البروتوكول الذي يعالج هذه المسألة rtd3.0 في مثل هذه الحالة تظهر الحاجة الى اشعارات ايجابية من المستقبل الى المرسل ACK بالاستلام دون الخطأ او اشعارات سلبية NAK عند ورود الخطا وطلب اعادة الارسال وتعرف البروتوكولات التى تستند الى اعادة الارسال ببروتوكولات طلب الاعادة الالي (ARQ Automatic Repeat reQuest)

وفي هذه الحالة سنحتاج الى ثلاث وظائف اضافية لمعالجة اخطاء البت :

١. اكتشاف الخطأ ٢. اشعار من المستقبل ٣. اعادة الارسال

يوجد ثلاث احتمالات لمعالجة الاشعارات التالفة :

- **ACK/NAK الاشعارات الايجابية والسلبية فيقوم المستقبل بذلك**
- **اضافة بتات كافية للمجموع الاختباري بشكل يتيح للمرسل تصحيح الخطأ عند اكتشافه وهو حل مناسب للقنوات التي قد تتلف البتات ولكن لاتفقدها .**
- **ان يقوم المرسل ببساطة بإعادة ارسال حزمة البيانات الحالية عند استلامه إشعارات الـ ACK/NAK تالفة ولكن ينتج عن هذا حزم متكررة في قناة المرسل-الى-المستقبل وتكن الصعوبة في انا**

المستقبل لن يعرف اذا كان اشعار الـ ACK/NAK قد وصل المستقبل يرسل المرسل اشعارا يطلب فيه من المستقبل اعادة ارسال الـ

- **وبالتالي فيما اذا كانت الحزمة المرسلة هي حزمة بيانات جديدة ام اعادة إرسال**

وابسط حل لهذه المشكلة هو اضافة حقل جديد لحزمة البيانات يمثل الرقم التسلسلي لدى المرسل ، وعل المستقبل فحص هذا الرقم ليتبين انها حزمة جديدة ام معادة

يبين الشكل **3-9** و **3-8** صفحة **135** و **136** مثال لآله الحالات المنتهية **FSM**لجانبي المرسل والمستقبل من من بروتوكول **rdt2.2** على التوالي يرجى تتبعهما جيداً

ويبين الشكل **3-10** صفحة **137** آله الحالات المنتهية **FSM** للمرسل في بروتوكول **RTD3.0**).

خط انتاج بروتوكولات نقل البيانات الموثوقة

Pipelined Reliable Data Transfer Protocols

رغم ان بروتوكول نقل البيانات الموثوقة صحيح إلا ان اداءه ضعيف وخاصة في شبكات اليوم عالية السرعة ومن اهم مشاكله انه بروتوكول توقف وانتظر

(الاطلاع على مثال صفحة 138) لتعرف على كيف ان معدا استغلال المرسل في بروتوكول توقف وانتظ معادلة التالية:

$$U_{SENDER} = \frac{L\backslash R}{RTT+L/R}$$

لمعرفة كيفية عمل rtd3.0 بروتوكول ، البث المتناوب تتبع الشكل 3-11 صفحة 139

يوضح الشكل 3-13 صفحة 140عملية الارسال في بروتوكولي توقف – انتظر وخط الانتاج

يستطيع المرسل ارسال عدة حزم دون انتظار اشعار الوصول كما يوضح الشكل 3-13 صفحة 140 فإذا اتيح للمرسل ارسال ثلاث حزم دون انتظار سيزيد استغلال المرسل ثلاث مرات ويبدو ذلك كما يتم ملء خط انتاج وتسمى هذه التقنية بـ خط الإنتاج Pipelining

أما تبعات استخدامها في بروتوكولات نقل البيانات الموثوقة فهي :

- يجب زيادة عدد ارقام التسلسل ، لكل حزمة قيد الارسال (عدا عند الارسال) رقم متسلسل فريد وقد نكون هناك رزم متعددة بدون اشعار
- قد يتعين على طرفي المرسل والمستقبل التخزين المؤقت لاكثر من حزمة واحدة , بالحد الادنى على المرسل ان يخزن الحزم التي ارسلت ولم يتم اصدار أي اشعار لها حتى الان وقد يلزم التخزين المؤقت للحزم المستقبلة بشكل صحيح لدى المستقبل
- يتوقف مدى ارقام التسلسل اللازمة والتخزين المؤقت على الطريقة التي يستجيب بها البروتوكول نقل البيانات للحزم المفقودة والتالفة والمتأخرة ز وهناك نهجان اساسيان لتصحيح الخطأ في خط الانتاج :
- العودة ال ن (back to N)
- والتكرار الانتقالي (SELECTIVE REPEAT)

العودة -ن (back-n) صفحة ١٤١

يسمح للمرسل بارسال عدة حزم دون انتظار اشعار الوصول مع التقييد بحد اعلى لعدد الحزم التي لم يصل اشعارها N في خط الإنتاج

يبين الشكل (٣-١٤)

مدى الأرقام التسلسلية في بروتوكول GBNمن منظور المرسل حيث يمثل base الرقم التسلسلي لأقدم حزمه بدون اشعار
Nextseqnumاصغر رقم تسلسلي غير مستخدم (يستخدم لترقيم الحزمة اللاحقة)

يوجد ٤ فترات في مدى الأرقام التسلسلية

١. **الفترة [0,base-1]تشمل الحزم المرسلة التي وصل اشعارها**
٢. **الفتره [base,nextseqnum-1] تشمل الحزم المرسلة التي لم يصدر اشعارها**
٣. **الفترة [nextseqnum,base+n-1] تشمل الحزم قيد الارسال**
٤. **الرابعة لم تذكر في الكتاب**

حيث ان الأرقام التسلسلية اكبر او يساوي base+n لا يمكن استخدامها حتى تصل اشعارات الحزم الحالية في خط الإنتاج وخاصة الحزمه ذات الرقم التسلسلي base
مع النظر للشكل
يشار الى N على انها حجم النافذة windows size حيث تم تحديد الحجم ولم يترك مفتوحا لسببين
١. **السبب الأول لضبط التدفق flow control لفرض هذا الحد على المرسل**
٢. **والسبب الاخر لضبط الاحتقان في TCT**

يسمى بروتوكول GBN ببرتوكول النافذة المنزلقة

Note صفحة ١٤٢

يوضع الرقم التسلسلي في حقل ثابت الطول في مدقمة الحزمه

قانون :

اذا كان k يمثل عدد البتات في الحقل فان مدى الأرقام التسلسلية يساوي [0,2^k-1]

وتحسب باستخدام modulo 2^k أي ان الرقم الذي يلي الرقم 2^k-1 هو 0

يبين الشكل (٣-١٥) صفحة ١٤٣

الية عمل بروتوكول النافذة المنزلقة GBN بنافذة حجمها ٤ حزم فالمرسل يرسل الحزم 3-0 عليه انتظار وصول اشعار لحزمة او اكثر قبل استئناف العمل

وعند استلام كل اشعارين على التوالي مثلا (ACK0,ACK1) تنزلق النافذة قدما ويستطيع المرسل نقل حزمة جديدة (PKT3,PKT4) على التوالي

فاذا فقد المستقبل حزمة ٢ تعتبر الحزم ٣,٤,٥ خارج الخدمة وتهمل

اعادة الإرسال الانتقائية selective Reeat (SR)

يسمح برتوكول GBN للمرسل بتعبئة خط الإنتاج بالحزم ، وبالتالي تجنب مشاكل استخدام القناة التي ظهرت في بروتوكولات التوقف والانتظار مع ذلك هناك سيناريوهات يعاني فيها GBN نفسه من مشاكل في الأداء وخاصة عندما يكون حجم النافذة وتأخير عرض النطاق الترددي كلاهما كبير ، قد يكون العديد من الحزم في خط الإنتاج وبالتالي قد يؤدي خطأ في حزمة واحدة إلى إعادة إرسال عدد كبير من الحزم ،كثير منها غير ضروري ،وإذا

زاد احتمال الخطأ في القناة ،قد يصبح خط الإنتاج مليئاً بالحزم المعادة غير الضرورية .

وكما يوحي الاسم فإن بروتوكولات الإعادة الانتقائية تتجنب إعادة الإرسال غير الضرورية بل يعيد المرسل إرسال تلك الحزم التي يشتبه بورود خطأ فيها فقط (أي فقدت او تلفت) لدى المستقبل .وستتطلب إعادة الإرسال ، عند الحاجة أن يشعر المستقبل المرسل بالحزم السليمة المستلمة بشكل فردي (انتقائي) ويستخدم حجم النافذة N لحصر أرقام الحزم العالقة دون إشعار في خط الإنتاج

مع ذلك وعلى عكس GBN فإن المرسل قد تلقى بالفعل إشعارات ACKs لبعض الحزم في النافذة ، ويبين الشكل (٣_١٦) صفحة ١٤٥ فضاء الأرقام التسلسلية لبروتوكول SR
يصدر المستقبل إشعارات للحزم السليمة المستلمة سواء كانت بالترتيب أم لا ،فالحزم خارج الترتيب تخزن مؤقتاً حتى استلام أي حزم مفقودة (ذات رقم تسلسلي أصغر) عندها قد تسلم رزمة من الحزم بالترتيب للطبقة الأعلى . يبين الشكل (٣_١٧) صفحة ١٤٧مثالاً على آلية عمل بروتوكول SR بوجود حزم مفقودة ،حيث يعمل المستقبل مبدئياً على تخزين الحزم ٣,٤,٥ ويسلمها مجتمعة مع الحزمة ٢ عند استقبالها في نهاية المطاف إلى الطبقة الأعلى

إن غياب التزامن بين نافذتي المرسل والمستقبل قد تكون له تبعات مهمة في ظل المدى المحدود للأرقام التسلسلية . فماذا سيحدث مثلاً إذا كان المدى ٤ أرقام تسلسلية للحزم ٠,١,٢,٣ وحجم النافذة ٣؟ افرض أن الحزم ٠,١,٢ قد أرسلت واستلمت لدى المستقبل وأشعر المرسل بوصولها ، في هذه اللحظة تغطي نافذة المستقبل الحزم ٤,٥,٦ ذات الأرقام التسلسلة ٣,٠,١ على التوالي

السيناريو الأول :

كما يبين الشكل (a_18_3) صفحة ١٤٩ فقدت إشعارات ACK الحزم الثلاثة الأولى والمرسل يعيد إرسال هذه الحزم ، وعليه يستلم المستقبل الحزمة ذات الرقم التسلسلي ٠ أي نسخة من الحزمة الأولى المرسلة

السيناريو الثاني:

كما يبين الشكل(b_18_3) صفحة ١٤٩ إشعارات ACK الحزم الثلاثة الأولى وصلت سليمة فيحرك المرسل نافذته قدماً ويرسل الحزم ٦,٥,٤ ذات الأرقام التسلسلية ١,٠,٣ على التوالي . الحزمة ذات الرقم التسلسلي ٣ فقدت ،ولكن الحزمة ذات الرقم التسلسلي ٠ وصلت وهي حزمة تحتوي بيانات جديدة

من منظور المستقبل كونه لا يرى الإجراءات التي يتخذها المرسل ،كل ما يراه هو تسلسل الرسائل التي يستقبلها من القناة أو يرسلها ، فالسيناريو الأول والثاني متشابهان . وليس هناك طريقة للتمييز بين إعادة إرسال الحزمة الأولى وبين إرسال الحزمة الخامسة للمرة الأولى . من الواضح أن حجم النافذة الذي يقل بواحد عن مدى الأرقام التسلسلية لن يعمل .ولكن ما الحد الأدنى لحجم النافذة؟ أثبت أن حجم النافذة في بروتوكول SR يجب أن يكون أقل أو يساوي نصف مدى الأرقام التسلسلية . .

بروتوكول التحكم بالنقل بروتوكول طبقة النقل في الانترنت الموجه بالاتصال والموثوق

برتوكول TCP موجه بالاتصال

اي ان العمليتان تتصافحان(اي عليهما ارسال بعض الشرائح الاولية لإنشاء معاملات نقل البيانات لاحقا قبل بدء الارسال وعند انشاء اتصال كلا الجانبين يعدان متغيرات عدة حول حال TCP يعمل بالأجهزة الطرفي end systems لا الاجهزة البيئية كالموجهات والمقسمات التي لا تحفظ بحالة الاتصال TCP فهي تعني بمخططات البيانات لا بالاتصالات

يوفر الاتصال عبر TCP خدمة الارسال باتجاهين معا وهو دائما اتصال نقطة الى نقطة اي بين المرسل وحيد ومستقبل وحيد

يوجه TCP لبيانات نحو مخزن الارسال المؤقت وهو احد المخازن التي اعدت اثناء المصافحة الثلاثية وبين الوقت والاخر ينتزع TCP قطعا من البيانات من المخزن ليمرر شريحة الى طبقة الشبكة
ويحدد الحد الاعلى لحجم البيانات في الشريحة بقيمة حجم الشريحة الاقصى وتحسب بإيجاد طول اكبر اطار في طبقة الربط link-layar frame يستطيع المضيف المحلي المرسل ارساله ويطلق عليها وحدة الارسال القصوى من ثم ضبط MSS للتأكد ان الشريحة المغلقة في مخطط بيانات برتوكول الانترنت بالإضافة الى طول مقدمة TCP/IP البالغة ٤٠ بايت تناسب حجم اطار واحد لطبقة الربط والذي بلغ ١٥٠٠ بايت في كل من الإيثرنت وبرتوكول نقطة لنقطة لاحظ ان MSS هو الحد الاعلى لبيانات طبقة التطبيقات في الشريحة وليس الحد الاقصى لحجم شريحة TCP بما في ذلك المقدمة
يقوم TCP بمزج كل قعة من بيانات العميل بالمقدمة لتشكيل شريحة TCP مما تتكون بنية شريحة بروتوكول التحكم بالنقل TCP Segment Structure من حقول المقدمة وحقل البيانات فان MSS تحدد الحجم الاقصى لحقل البيانات عندما يرسل ملف كبير يقطع TCP الملف لقطع chunks حجمها MSS ما عدا القطعة الاخيرة التي تقل عن ذلك

تشمل المقدمة الحقول التالية ؟ص ١٥٢

حقل رقم التسلسل sequence number وحقل رقم الاشعار acknowlege number وكل منهما ٣٢ بت ويستخدمان لتوفير خدمة نقل موثوق للبيانات في المرسل والمستقبل

حقل نافذة الاستقبال receive window وطوله ١٦ بت ويستخدم في ضبط التدفق flow control اي عدد البايتات التي يقبل بها المستقبل

حقل طول المقدمة header length وطوله ٤ بت ويحدد طول مقدمة TCP في كلمات ٣٢ بت وقد يتغير طول المقدمة تبعا لحقل الخيارات TCP options فاذا كان هذا الحقل فارغ فان طول المقدمة القياسي ٢٠ بايت

حقل الخيارات options وهو اختياري متغير طول ويستخدم في التفاوض بين المرسل والمستقبل حول حجم الشريحة الاقصى MSS او كعامل تحديد حجم النافذة في شبكات عالية السرعة كما يتم خيار خاتم الوقت time stamping

حقل الراية flag وطوله ٦بت بت ACK يبين صلاحية حقل الاشعار اي ان في الشريحة اشعار بوصول شريحة اخرى بنجاح اما بتات RST,SYN,FIN فتستخدم في اعداد الاتصال وانهائه بت PSH يشير ان على المستقبل تمرير البيانات فورا الى الطبقة الاعلى واخيرا بت URG فيشير ان هناك بيانات في هذه الشريحة وسمت من جانب المرسل بانها طارئة

تخمين زمن الذهاب والاياب ونفاذ المهلة ؟

يستخدم بروتوكول TCPنفاذ المهلة timeout اعادة الارسال reteansmit لمعالجة فقدان الشرائح وعلى رغم انه مفهوم بسيط الا ان هناك بعض العقبات عند تطبيقه في بروتوكول حقيقي مثل TCP
سؤال مهم يتعلق بطول المهلة ومن الواضح انها اقل من زمن الذهاب والاياب وهو الزمن من لحظة ارسال الشريحة الى الاشعار بوصولها
كيفية تخمين زمن الذهاب والاياب بين المرسل والمستقبل وسنسمي العينة SampleRTT وهي الزمن بين ارسال الشريحة segment واستقبال الاشعار
بدل من قياس عينة لكل شريحة مرسلة تقاس عينة واحدة في المرة الوحدة
ان TCP لا يقيس باي حال عينة لشريحة اثناء اعادة الارسال تتباين قيم العينة من شريحة الى اخرى بسبب الاحتقان في الموجهات وتغيرالحمل في الانظمة النهائية لذا يتم احتساب متوسط العينات المخمنة EstimatedRTT لتخمين RTT القياس حسب المعادلة التالية EstimatedRTT=(1-a).EstimatedRTT+a.SampleRTT
فيعتمد على الوسط المرجح لقيمة EstimatedRTT السابقة والقيمة الجديدة للعينة SampleRTT
ولقياس التغير في RTTنحسب انحراف عينات زمن الذهاب والاياب عن تلك المخمنة DevRTT
فكلما زاد التذبذب في قيم العينات يكون الانحراف اكبر ويوصي بقيمة

ان خدمة بروتوكول IP service غير موثوقة أي لا تضمن استلام مخططات البيانات او ترتيبهاا او سلامتها
فقد تفيض عن سعة مخزن المؤقت للموجه فلا تصل ابدا وقد تصل غير مرتبة او تحتوي على بتات خاطئة و كون شريحة طبقة النقل تنقل عبر طبقة الشبكة من خلال مخططات بيانات فقد تعاني هذه شرائح من اشكاليات ذاتها

نفاذ مهلة اعادة الارسال :ضبطها وادارتها (setting and management the retransmission)

فترة نفاذ الكمية (time interval) في TCP يجب ان تكون اكبر بقليل او يساوي قيمة Estimated RTT وذلك لكي لا تظهر حالات ارسال غير ضرورية ويكون ليس اكبر منه بكثير بل اضافة هامش بسيط له. والا لن يقوم TCP بإعادة ارسال الشريحة المفقودة بسرعة
ويزيد الهامش بزيادة التذبذب في قيم sample RTT ويظهر دور الانحراف هنا وحسب هذه المعادلة

TimeoutInterval =Estmated RTT + 4.DevRTT

وتكون القيمة الابتدائية للمهلة Timeout Interval(١ ثانيه) حسب المرجع RFC ٦٢٩٨ ويتم مضاعفتها لتجنب انتهاء مهلة قبل اوانها لشريحة سيصدر اشعارها حالا

٣,٦,٤. النقل الموثوق للبيانات Reliable data transfer

خدمة بروتوكول الانترنت Ip service غير موثوقة اي لا تضمن استلام مخططات البيانات datagrams ولان طبقة النقل تنتقل عبر طبقة الشبكة من خلال مخططات البيانات فقد تعاني من نفس المشكلة

فيتم التحقق من النقل الموثوق من خلال بروتوكول التحكم بالنقل TCP ويتأكد بان البيانات خالية من الثغرات ومتسلسلة اي ان سلسلة byte stream التي تم استلامها هي نفسها المرسلة

النقل الموثوق يتطلب مؤقت منفصل يرتبط بكل شريحة ارسلت ولم يصل اشعار استلامها ولكن ذلك يتطلب كثير من الجهد ولهذا يتم استخدام مؤقت واحدة

عند ارسال ملف من A الى B فانه هناك ثلاث احداث رئيسية

١) استلام البيانات من التطبيق: يستقبلها TCP البيانات ويقوم بتغليفها ضمن شريحة ليمررها لبروتوكول الانترنت

٢)نفاذ مهلة المؤقت: يستجيب TCP لتفاد للمهلة بإعادة ارسال الشريحة المتسببة ويعيد تشغيل المؤقت

٣)اصدار اشعار الاستلام: عند استلام الاشعار يقارن قيمته بالرقم المتسلسل لآخر بايت بلا اشعار بسبب خاصية الاشعارات المتراكمة في ال TCP فلإشعار y يشير الى استلام جميع البايتات

السيناريوهات:

يرسل A الى B اشعار ويتلقاه B ويرسل اشعارا له لكنه يفقد فتنتهي مهلة الارسال دون استلام A الاشعار فيقوم بدوره بإعادة الارسال ولكن تهمل البيانات لان TCP يعلم بأنها قد وصلته سابقا

ارسال شريحتين من $_A$الى $_B$: يصلان الشريحتين الى $_B$ويرسل الاشعارات ولكن لم ترسل اشعار واحد منهم فيعيد $_A$ارسال الشريحة المفقودة ل $_B$

عند ارسال $_A$شرحتين وتلقيه اشعارهما من $_B$لا يعيد ارسالهم

السيناريو الأول شرح ص١٥٦ وشكل ص ١٥٧
السيناريو الثاني شرح ص١٥٧ وشكل ص ١٥٨
السيناريو الثالث شرح ص ١٥٨ وشكل ص ١٥٩

٣,٦,٥ضبط التدفق Flow control

المضيفين على طرفي اتصال $_{TCP}$يعد كلا منهما مخزن استقبال مؤقت $_{receive\ buffer}$اي انه لا يقوم بقراءة كل الرسائل دفعة وحده فيمكن ان يكون مشغولا بقراءة بيانات اخرى وإذا كان التطبيق بطيئا نسبيا فأنه إذا تم ارسال بيانات كثيرة فقد يفيض المخزن بسهولة كبيرة

يوفر $_{TCP}$خدمة ضبط التدفق لمنع المرسل من اغراق المخزن المؤقت للمستقبل ويكون ذلك بموائمة المعدل الذي يرسله المرسل مع المعدل الذي يقرأ به تطبيق المستقبل

وتسمى حالة ضبط اختناق المرسل بضبط الاحتقان

يوجد فرق بين ضبط التحكم وضبط الاحتقان

يوفر TCP ضبط التدفق من خلال احتفاظ المرسل بمتغير يسمى نافذة الاستقبال receive window ورمز لها rwnd وهي بدورها تعطي المرسل فكرة عن مساحة المخزن المؤقت ولان TCP يعمل باتجاهين (full_duplex) يحتفظ المرسل لي كلا جانبي الاتصال بنافذة استقبال مستقلة

عندما يتم ارسال ملف من A الى B فانه يمكن يتم تحديد المتغيرات كالتالي

١)البايت الاخير المقروء (last byte read)

٢) البايت الاخير المستقبل (last byte Rcvd)

ولكي لا يتم اغراق المخزن المؤقت فانه يتبع هذه المعادلة

RcvBuffer〉= LastByteRcvd_lastByteRead

نافذة الاستقبال rwnd تحدد كمية المساحة المتوفرة في المخزن المؤقت وتتغير مع الزمن

rwnd=RcvBuffer_[lastByteRcvd_lastByteRead]

بعد القدرة على ضبط التدفق باستخدام نافذة الاستقبال تبقى اشكالية بسيطة وهي انه اذا امتلئ مخزن استقبال المؤقت للمضيف المسقبل اي rwnd =0 فانه لن يستطيع ارسال شرائح جديدة لهذا الشيء لانه فقط يرسل اشعارات. ولمعالجة هذا الشيء فان من مواصفات ال TCP انه يسمع لانتقال بت واحد فقط من A ال B عندما تكون نافذة الاستقبال لدى B=0

بروتوكول UDP لا يوفر ضبط التدفق فعند ارسال الشرائح من A الى B فانه يضيفهم الى مخزن مؤقت محدود الحجم يسبق المقبس المقابل

وانه اذا لم تقرأ كافة السرائح وبسرعه وفاض المخزن فأنه سيتم اهمال الشرائح

٣-٦-٦ ادارة الاتصال في بروتوكول التحكم بالنقل TCP Connection Management

بشكل عام ينشأ اتصال TCP نتيجة رغبة عملية قيد التشغيل في العميل ببدء اتصال مع عملية اخرى في الخادم فتقوم عملية تطبيق العميل بإعلام TCP على العميل انه يرغب بإنشاء اتصال بعملية في الخادم

وتبدأ خطوات انشاء اتصال مع الخادم كالتالي: _

١)يرسل TCP العميل شريحة TCP الى TCP الخادم تحتوي الشريحة على احدى بتات الراية في مقدمه الشريحة فيمنح البت SYN القيمة ١ ولهذا سميت باسمها ويعطي العميل رقما تسلسليا عشوائيا لمنع لتجنب الهجمات الامنية client _isn ويتم تغليفها ضمن مخططات بيانات IP المرسل داخل الخادم

٢)عندما يصل مخطط بيانات IP يتم استخراج الشريحة ويحدد المخازن المؤقتة والمتغيرات الخاصة بالاتصال

تحتوي الشريحة على ثلاث معلومات مهمة في مقدمة الشريحة يمنح البت الاول SYN القيمة واحد ثانيا يمنح حقل اشعار المقدمة الشريحة قيمة Client_isn+1 ثالثا يختار رقم تسلسل مبدئيا server_isn ويطلق على شريحة موافقة الاتصال شريحة SYNACK

٣)عندما يتم استقبال SYNACK ويخصص العميل ايضا المخازن المؤقتة ومتغيرات الاتصال

بعد ذلك يتم اعطاء شريحى بت SYN القيمة 0 وتسمى عملية الاتصال ب المصافحة الثلاثية three -way handshakes وعند انهاء الاتصال يقوم TCP العميل بارسال شريحة خاصه للخادم تشمل بث راية في مقدمتها FIN ويعطي القيمة رقم ١

*عندما لا تطابق عنوان IP مع منافذ المصدر فأنه يرسل شريحة Reset الى المصدر تحتوي على بت راية RST ويعطي القيمة ١ وهكذا يخبر مصدر الرسالة بانه يرجى عدم اعادة ارسال هذه الشريحة لعدم وجود مقبس لها

وفي حاله حزمة UDP فأنه يرسل مخطط بيانات من نوع ICMP

٣-٧ مبادئ ضبط الاحتقان (الازدحام) Principles of congestion control ص١٦٣

٣-٧-١ اسباب الاحتقان وكلفته and the costs of the causes congestion ص١٦٣

يتم ضبط الاحتقان من خلال ثلاث سيناريوهات

السيناريو الاول :

مرسلان وموجه بمخازن مؤقتة لامحدودة and a router with two senders Infinite buffers

لنفرض وجود المرسل A يرسل بيانات عبر الاتصال

فتكون هذه البيانات اصلية وترسل عبر المقبس مرة واحدة حيث يتم تغليف البيانات دون تصحيح الاخطاء ولذلك تكون معدل الحركة التي يوفرها المضيف A الى الموجه هي in بايت في الثانية ويعمل المضيف B في نفس الطريقة وتمر الحزم عبر المضيفات من خلال موجه وخط اتصال خارج مشترك سعته R

الانتاجية لكل اتصال تكون عدد الايتات لكل ثانية لدى المستقبل مقابل معدل الارسال فعندما يكون معدل الارسال بين R/2-0 فان الانتاجية لدى المستقبل تساوي معكل ارسال المرسل اي ان كل ما يرسله المرسل يتلقاه المستقبل بعد زمن تأخير محدود finite delay

عندما يكون معدل الارسال اكبر من R/2 تكون الانتاجية على اي حال فقط ويكون هنا الحد الاعلى

ولو ارتفع معدل الارسال لن تزيد الانتاجية نهائيا عن R/2

السناريو الثاني :

مرسلان وموجه ذو مخزن مؤقت محدود a router with TWO sender and finite buffers : لنعدل السيناريو الاول بشكل طفيف بطريقتين

1. اولا سنفترض ان كمية التخزين المؤقت للموجه محدودة وبالنتيجة سيتم اهمال الحزم عند امتلاء المخزن المؤقت
2. ثانيا سنفترض ان كل الاتصالات موثوقة فاذا اهملت حزمة تحتوي على شريحة من مستوى النقل في الموجه فان المرسل سيعيد ارسالها

يعتمد هذا السيناريو بقوة على اعادة الارسال فاذا كان المضيف قادرةا على تحديد ما اذا كان المخزن المؤقت متاح فانه لن يحدث فقدان للحزم وستكون λ_{in} **تساوي** λ'_{in}

وسيكون هذا الاداء المثالي للإنتاجية في حالة نفاذ المهلة قبل اوانها فان المرسل سيرسل نسخة من نفس الحزمة ولأنها قد وصلت الحزمة الأصلية للمستقبل فان المستقبل سيتجاهلها

تقترب قيمة الانتاجية من R/4 عندما تقترب الحمولة المقدمة من R/2

يوجد ثمن كلفة لاحتقان الشبكة تتمثل في ان إعادة الارسال غير الضرورية قد تؤدي الى تأخيرات كبيرة واستنفاد عرض النطاق الترددلخط الاتصال link bandwidth الذي يستخدمه الموجه في تحويل نسخ غير ضرورية من الحزمة

السيناريو الثالث:

اربعة مرسلين وموجه ذو مخزن مؤقت محدود ومسارات متعددة القفزات

Four senders, routers with finite buffers,and multhiop path

في السيناريو الاخير يقوم اربعة مضيفين بإرسال الحزم كل منها عبر موجات متراكبة تنائيه القفز

عند حالة المرورية الكبيرة اي λ_{in} وبالتالي فان λ'_{in} كبيرة للغاية

بهذه الحالة يكون معدل وصول حركه المرور من B_D عند $R2$ اكبر بكثير من حركه المرور A_C

يعزى انخفاض الانتاجية مع زيادة الحمولة المقدمة الى مقدار الهدر في عمل الشبكة ففي الشبكة ذات الحركة المرورية المرتفعة كما في السيناريو الرابع كلما اهملت حزمة في موجه القفزة الثانية فان العمل الذي ينجزه موجه القفزة الاولى في تحويل الحزمة الي موته القفزة الثانية يعتبر هدرا

عند اهمال حزمة في المسار فان سعة (قدرة) الارسال التي استخدمت في كل من وصلات المنبع لإحالة تلك الحزم الي النقطة اتي اهملت عندها تعتبر هدرا.

مصطلحات :

فترة نفاذ المهلة .. Time interval

القيمة الابتدائية للمهلة .. TimeoutInterval

مخططات البيانات .. datagrams

مخزن استقبال مؤقت receive buffer

نافذة الاستقبال ... receive window (rwnd)

TCPيعمل باتجاهين .. full-duplex

البايت الاخير المقروء ... LastByteRead

البايت الاخير المستقبل .. LastByteRcvd

رقم تسلسلي مبدئي للهجمات الامنية ... CLIENT_ isn

رقم تسلسلي مبدئي للخادم server_isn

شريحة الموافقة ... SYNACK

خدمة معدل الارسال المتاح ... Available bit-rate ABR

وضع النقل غير المتزامن Asynchronous transfer mode ATM

قفزة واحدة single hop

الانتاجية throughout

تاخير محدود ... Finite delay

خط الاتصال ... Link bandwidth

ضبط الازدحام(الاحتقان)في بروتوكول التحكم بالنقل

يعتبر ضبط الاحتقان من المكونات الاساسية لبروتوكول TCP كما اشرنا في الاقسام السابقة ،ويجب ان يستخدم TCP ضبط الاحتقان نهاية إلى نهاية (end-to-end congestion control) لان طبقة بروتوكول الانترنت لا توفر تغذية راجعة صريحة للأنظمة النهائية(end system) حول احتقان الشبكة. فكل مرسل يحدد معدل الارسال في خط الاتصال الخاص به بدلالة ضبط الاحتقان .فاذا احس المرسل بان الاحتقان قليل في مساره نحو الوجهة، عندها يزيد معدل الارسال ،واذا ادرك ان هناك احتقان على طول المسار يقلل معدل الارسال. وهذه الطريقة تثير ثلاثة اسئلة؛

كيف يحدد مرسلTCP معدل الارسال؟ وكيف يدرك المرسل ان هناك احتقان بينه وبين الوجهة؟ وما الخوارزمية التي يستخدمها لتغيير معدل الارسال بدلالة الاحتقان؟

****للإجابة على السؤال الاول وكما اشرنا في القسم ٣_٦ يتكون كل جانب من اتصال TCP من مخزن مؤقت للاستقبال وآخر للإرسال، وعدة متغيرات (rwnd , lastByteRead) وغيرها، تتبع الية ضبط الاحتقان لدى المرسل المتغير الاضافي نافذة الاحتقان(congestion window: cwnd) والتي تضع قيدا على معدل الارسال (حركة المرور)عبر الشبكة، وبالتحديد الا تتجاوز البيانات بلا اشعار الحد الادنى للمتغيرين rwnd ,cwnd أي:**

{LastByteSent-LastByteAcked<=mincwnd,rwnd}

ولكي نركز على ضبط الاحتقان لا التدفق .دعنا نفترض ان مخزن الاستقبال المؤقت كبير يسمح بإهمال القيود على نافذة الاستقبال. وعليه فان كمية البيانات بلا اشعار تحدد بالمتغير cwnd وسنفترض ايضا ان لدى المرسل دائما بيانات ليرسلها .اي ان جميع الشرائح في نافذة الاحتقان قد ارسلت. وبذلك يستطيع المرسل تحديد معدل الارسال . وللتوضيح اعتبر ان هناك خط اتصال زمن تأخير الفقدان ونقل الحزم لديه مهمل. في بداية كل RTT تقريبا يسمح للمرسل بإرسال بيانات cwnd بايت. وفي نهايتها يستقبل اشعارات الاستلام. اي ان معدل الارسال تقريبا cwnd/ RTT بايت/ثانية ويضبط cwnd يتمكن المرسل من تعديل معدل الارسال على هذا الخط

للإجابة على هذا السؤال دعنا نعرف فقدان الحزم لدى مرسل TCP بالحدث عند نفاذ المهلة او استلام ٣اشعارات متكررة من المستقبل. عندما يكوم هناك احتقان كبير. يفيض مخزن واحد(او اكثر) من مخازن الموجه على طول المسار. مسببا اهمال مخطط بيانات يحتوي على شريحة TCP ويؤدي ذلك بدوره الى حدوث فقدان لدى المرسل فيتخذ المرسل هذا الحدث مؤشر احتقان على مساره إلى المستقبل. ولكن ماذا إذا لم يظهر هذا الحدث؟ في

هذه الحالة تصل إشعارات الشرائح التي لم تصل سابقا الى المرسل.
فيستخدم TCP هذه الاشعارات كمؤشر ان الامور على ما يرام اي ان جميع الشرائح المرسلة استلمت بنجاح. فيزيد حجم نافذة الاحتقان .وبالتالي يزيد معدل الارسال

ننتقل الى السؤال الثالث. فكيف يستطيع المرسل تحديد معدل الارسال؟ اذا كان اكثر من مرسل يرسلون بسرعة فانهم يسببون احتقان الشبكة اما اذا كانوا يرسلون ببطء فانهم يقللون استغلال النطاق الترددي للشبكة. اي كان بإمكانهم الارسال بمعدلات اعلى دون التسبب في الاحتقان يجيب TCP على هذا السؤال بالاستعانة بالإرشادات الاساسية الآتية

الارشادات الازمة لتحديد معدل الارسال:

- **يشير فقدان شريحة الى وجود احتقان .وبالتالي على المرسل تقليل معدل الارسال**
- **يشير وصول اشعار الاستلام لشريحة ان الشبكة تسلم الشرائح للمستقبل وبالتالي يستطيع المرسل زيادة معدل الارسال**
- **التحقق من النطاق الترددي بالنظر الى الاشعارات ACKs التي تشير الى خلو المسار من المصدر الى الوجهة من الاحتقان وحدوث فقدان الشرائح الذي يشير الى احتقان المسار .**

فان استراتيجية TCP لتعديل معدل الارسال بزيادته استجابة لوصول الاشعارات حتى حدوث فقدان شريحة عندها يقلل معدل الارسال وبالتالي فان مرسل TCP يزيد معدل الارسال للتحقق من المعدل الذي يبدأ عنده الاحتقان. فيتراجع عن هذا المعدل. ثم يبدأ التحقق مرة أخرى لفحص ما اذا كان معدل بداية الاحتقان قد تغير

تتكون خوارزمية ضبط الاحتقان من ثلاثة مكونات رئيسية :

(١) البداية البطيئة (slow start)
(٢) تجنب الاحتقان (congestion avoidance)
(٣) الاسترداد السريع (fast recovery)

*****المكونان الاول والثاني الزاميان بينما الثالث يوصى به ولكن ليس إلزاميا لمرسلي TCP**

البداية البطيئة

عندما يبدا الاتصال يتم تهيئة المتغير cwnd بقيمة ابتدائية صغيرة(1 MSS) وتزداد قيمة (1MSS) كلما وصل اشعار استلام لأول مرة .والقيمة الابتدائية الناتجة لمعدل الارسال حوالي MSS/RTT فاذا كان MSS=500بايت وكان RTT=200 ميلي ثانية فان معدل الارسال الابتدائي حوالي 20 kbps ولان النطاق الترددي المتوفر بسرعة . في المثال المبين صفحة ١٧١ يرسل TCP الشريحة الاولى وينتظر اشعار الاستلام. وعندما يصل يزيد المرسل نافذة الاحتقان بقيمة (١ MSS) ويرسل شريحتين بحجمهما الاقصى. وعندما يصل اشعارهما يزيد المرسل نافذة الاحتقان بقيمة (1 MSS) لكل منهما فتصبح النافذة (4 MSS)وهكذا...

ينتهي نمو معدل الارسال خلال المرحلة البطيئة في حالات عدة منها:

١_عند حدوث فقدان(loss event)بعد نفاذ المهلة. يحدد مرسل TCP قيمة cwnd=1 وتبدا عملية البداية البطيئة مجددا.. كما انه يحدد متغير حالة آخر يسمى العتبة(ssthresh)بقيمة(cwnd /2).اي نصف قيمة نافذة الاحتقان عند اكتشافه

٢_يرتبط انتهاء وضع البداية البطيئة مباشرة بقيمة المتغير ssthresh وهي نصف قيمة cwnd عند كشف الاحتقان مؤخرا قد يكون من التهور الحفاظ على مضاعفة cwnd عندما يضل او يتجاوز قيمة ssthresh وبالتالي عندما يصبح (cwnd = ssthresh) تنتهي البداية البطيئة ويتنقل TCP الى وضع "تجنب الاحتقان"

٣_اكتشاف وصول ثلاثة اشعارات استلام)ACKs متكررة. عندها ينفذ TCP اعادة ارسال سريعة وينتقل الى وضع الاسترداد السريع

تجنب الاحتقان

عند دخول وضع تجنب الاحتقان تكون قيمة المتغير cwnd تقريبا نص قيمته عند مواجهة آخر احتقان وهكذا .. بدلا من مضاعفة cwnd كل RTT يتبنى TCP نهجا تكثر تحفظا ويزيد قيمة cwnd بمقدار MSS واحدا فقط كل RTT . بطرق عدة..

هنالك طريقة شائعة بان يزيد المرسل cwnd بمقدارMSS بايت cwnd/MSS عندما يصل اشعار جديد على سبيل للمثال اذا كان 14,600MSS بايت وكان 14,600cwnd بايت يتم ارسال 10 شرائح خلال فترةRTT وكل اشعار ACK يصل (بافتراض اشعار واحد لكل شريحة) يزيد حجم نافذة الاحتقان بمقدار 1/10 MSS وبالتالي فان قيمة نافذة الاحتقان ستزداد بمقدار MSS واحد بعد وصول اشعارات

ACKs عند استلام الشرائح العشر

انتهاء الزيادة لخطية في تجنب الاحتقان

تتصرف بنفس طريقة نفاذ المهلة وكما هو الحال في البداية البطيئة :تحدد قيمة cwnd بمقدار 1 MSS ويتم تحديث قيمة ssthresh الى نصف قيمة cwnd عندما حصل حدث الفقدان .الذي قد يسببه ايضا حدث تكرار الاشعار الثلاثي .

وفي هذه الحالة، تواصل الشبكة تسليم الشرائح من المرسل الى المستقبل لذا ينبغي ان يتصرف TCP مع هذا النوع من الفقدان بشكل اقل حدة من الفقدان الناجم عن نفاذ المهلة: ينصف TCP قيمةcwnd (اضافة 3 MSS كمقياس جيد لحساب الاشعارات الثلاث المتكررة المستلمة) ويسجل قيمة ssthresh بمقدار نصف قيمة cwnd عند استلام اشعارات ACKs الثلاث المتكررة ثم يدخل في وضع "الاسترداد السريع"

الاسترداد السريع

في الاسترداد السريع تزداد قيمة cwnd بمقدار 1 MSS لكل اشعار ACK مكرر للشريحة المفقودة التي سببت دخول TCP وفي وضع تجنب الاحتقان بعد تضاؤل cwnd اذا حصل حدث نفاذ المهلة ينتقل الاسترداد االسريع الى وضع البداية البطيئة بعد تنفيذ نفس الاجراءات كما هو الحال في البداية البطيئة وتجنب الاحتقان ؛ تحدد قيمة cwnd بمقدار 1 MSS وتحدد قيمة ssthresh بنصف قيمةcwnd عند حصول حدث الفقدان ..لاحظ انه مكون يوصى به وليس الزامي

سمي الاصدار القديم TCP Tahoe وهو يقطع نافذة الاحتقان دون شرط الى MSS 1 ويدخل مرحلة البداية البطيئة بعد فقدان حزمة اما لنفاذ المهلة او نتيجة اشعار مكرر ثلاثي اما الاصدار الاحدث فيطلق عليه TCP Reno

ويستخدم الاسترداد السريع, ويبين الشكل صفحة ١٧٣

تطور نافذة الاحتقان لكليهما العتبة الابتدائية 8 MSSS في اول ثماني جولات للنقل يتصرفان بنفس الطريقة .تزداد نافذة الاحتقان اسيا بسرعة اثناء البداية البطيئة لتصل الى العتبة في الجولة 4 ثم تزداد خطيا حتى حدوث فقدان واشعار مكرر ثلاثي بعد الجولة 8 فورا لتصبح 12 MSS وتعطى قيمة ssthresh حينها 6.MSS=0.5 .cwnd في حالة TCP Renoتعطى نافذة الاحتقان القيمة 6.MSS=cwnd ثم تزداد بشكل خطي, اما في حالة TCP Tahoe تعطى نافذة الاحتقان القيمة 1 MSSوتكبر بشكل اسي حتى تصل قيمة ssthresh وعندها تزداد بشكل خطي

وصف دقيق للإنتاجية في بروتوكول التحكم بالنقل (TCP)

ما متوسط الانتاجية لاتصال TCP طويل الاجل ؟ بإهمال مراحل البداية البطيئة بعد حدث نفاذ المهلة كونها قصيرة جدا وخلال فترة ذهاب واياب معينة يكون المعدل الذي يرسل فيه TCP البيانات كدالة الاحتقان وقيمة RTT الحالية اذا كان حجم النافذة w بايت وزمن الذهاب والاياب الحالي RTT ثانية يكون معدل الارسال W\RTT تقريبا ثم يتحقق TCPمن النطاق الترددي الاضافي بزيادة w بمقدار 1MSS كل RTT الى ان يحصل حدث الفقدان عندها سنعبر عن حجم النافذة بالرمز w وبافتراض ان RTT وw ثابتان تقريبا خلال مدة الاتصال

يتراوح معدل الارسال من w\2*RTT الى W\RTT وهذا يقودنا الى نموذج مبسط جدا لسلوك TCP في الحالة الثابتة تهمل الشبكة حزمة اذا زاد المعدل الى W\RTT ثم يهبط المعدل الى النصف ويزداد بمقدار MSS\RTT كلRTT حتى يصل الى W\RTT مره اخرى وتتكرر العملية ولان الانتاجية تزداد خطيا بين قيمتين متطرفتين يصبح متوسط الانتاجية 0.75*W\RTT

بروتوكول التحكم في النقل عبر مسارات ذات نطاق ترددي عالي

ما زالت الحاجة الى تطوير بروتوكول التحكم في النقل مستمرة في توفير الاتصالات عالية السرعة الازمة لتطبيقات الشبكة والحوسبة السحابية على سبيل المثال اعتبر ان حجم شريحة اتصال TCP 1500 بايت وان RTT=100 ms ولنفترض اننا نريد ارسال البيانات عبر هذا الاتصال بمعدل 10GBPS فان متوسط حجم نافذة الاحتقان 83333 شريحه وهي كثيره قد تفقد واحده منها فكم من الشرائح تسمح خوارزمية ضبط الاحتقان بفقدانها مع تحقيق المعدل المطلوب 10GBPS? يمكن كتابة الانتاجية كدالة لمعدل الفقدان (L) وزمن الذهاب والاياب RTT والحد الاقصى لحجم الشريحة MSS بالصيغة الاتية

متوسط الانتاجية =1.22.MSS\RTT L

باستخدام هذه الصيغة ولتحقيق الانتاجية المطلوبة نجد ان الخوارزمية قد تسمح بفقدان 2*10^-10 فقط أي فقدان شريحه واحده كل 5000000000 شريحه وهو معدل منخفض جدا

العدل والمساواة

لنعتبر ان لدينا عدد K من خطوط اتصال TCP لكل منها مسار مختلف ولكنها جميعا تمر عبر وصلة تشكل عنق الزجاجة BOTTELNECK معدل ارسالها R bps أي ان لكل خط اتصال جميع الوصلات على مسار خط الاتصال لا تعاني من الاحتقان ولديها قدرة ارسال وفيرة مقارنه بقدرة وصلة عنق الزجاجة ولنفرض ان كل خط اتصال ينقل ملفا كبيرا دون حركة مرور من نوع UDP عبر وصلة عنق الزجاجة يمكن تحقيق العدل في الية ضبط الاحتقان اذا كان

متوسط معدل الارسال لكل خط اتصال R\K تقريبا أي ان لكل خط حصة متساوية من عرض النطاق الترددي للوصلة
فهل خوارزمية الزيادة المضافة . النقصان المضاعف عادله؟ اذا علمت ان خطوط الاتصال المختلفة قد تبدا في اوقات مختلفة وعليه لها احجام نوافذ مختلفة في نقطه زمنية محدده؟ لنعتبر ان لدينا حالة مبسطة تتكون من خطي اتصال TCPيشتركان في وصلة واحد ذات معدل إرسال R كما في الشكل (٣-٣٧) صفحة١٧٦
اعتبر ان خطي الاتصال لهما نفس قيمة MSS ونفس قيمةRTT (أي إذا كان لهما نفس حجم نافذة الاحتقان فإن لهما نفس الإنتاجية)، ولديهما كمية كبيرة من البايتات لإرسالها، وليس هناك خطوط اتصال TCP أو مخططات بيانات UDP تجتاز هذه الوصلة المشتركة.
لنتجاهل أيضاً مرحلة البداية البطيئة ولنفرض أن خطوط الاتصال تعمل في وضع (collision avoidance :CA) تجنب التصادم (AIMD) طوال الوقت.

يبين الرسم البياني في الشكل (٣-٣٨)
إنتاجية خطي الاتصال . ولتقسين عرض النطاق الترددي بينهما بالتساوي يجب أن تقع الإنتاجية على السهم بزاوية 45 درجة (أي حصة متساوية من عرض النطاق). في الحالة المثالية يكون مجموع الإنتاجية لهما يساوي R . والهدف هو الوصول إلى إنتاجية تقترب من تقاطع خط الحصة المتساوية من عرض النطاق الترددي وخط استغلال النطاق الكامل

لنفترض أن أحجام نافذة TCP في نقطة زمنية معينة يحقق خطأ الاتصال 1 و2 الإنتاجية المشار إليها في النقطة A في الشكل(٣-٣٨) ولأن كمية عرض النطاق الذي يشترك فيه الخطان أقل من R فلن يحدث أي فقدان . وسيزيدان نافذتيهما بمقدار MSS 1 لكل RTT تبعاً لخوارزمية تجنب الاحتقان .وهكذا . فإن الإنتاجية المشتركة تقع على خط 45 درجة بدءاً من النقطة A . في نهاية المطاف .سيكون عرض النطاق الذي يستهلكه الخطان أكبر من R ويحدث فقدان الحزم. لنفترض أن خطي الاتصال 1و2 يعانيان من فقدان الحزم عند تحقيق الإنتاجية المشار إليها في النقطة B عندها يخفضان حجم نافذتيهما بمعامل2, فيحققان الإنتاجية عند النقطة C (منتصف المسافة على متجه يبدأ في B وينتهي في نقطة الأصل. ولأن عرض النطاق المشترك المستخدم أقل منR عند النقطة C يزيد الخطان إنتاجيتهما مرة أخرى على خط 45 درجة بدءاً من C . في النهاية . سيتكرر فقدان الحزم مثلاً عند النقطة D فيخفضان حجم نافذتيهما بمعامل 2 وهكذا

• عزيزي الطالب، عليك أن تقتنع بأن عرض النطاق الذي يحققه الخطان يتأرجح في نهاية المطاف على خط الحصة المتساوية، وأنهما سيتقاربان نحو هذا التصرف. على الرغم من الافتراضات المثالية في هذا السيناريو، فإنه يولد شعوراً لديك لماذا يقسم TCP عرض النطاق بالتساوي بين خطوط الاتصال. من الناحية العملية، لا تتوفر هذه المثالية وبالتالي قد تحصل تطبيقات العميل-الخادم على حصص غير متساوية من عرض النطاق، وخاصة، عندما تشترك اتصالات متعددة في عنق الزجاجة. فإن الجلسات ذات RTT الأصغر قد تستحوذ على عرض النطاق الترددي المتاح بسرعة أكبر ، وبالتالي سوف تتمتع بإنتاجية أعلى من غيرها

العدالة في UDP واتصالات TCP المتوازية

عادةً ، لا تستخدم تطبيقات الوسائط المتعددة TCP لأنها لا تريد أن يقل معدل الإرسال نتيجة لضبط الاحتقان ، لذا تلجأ إلى UDP لتتمكن من نقل الصوت والفيديو بمعدل ثابت ، مع التساهل في أمر الحزم المفقودة .
ولمعالجة الأمر ، يلجأ TCP إلى الاتصالات المتوازية ، إذ تستطيع التطبيقات فتح اتصالات متعدد على التوازي بين مضيفين ، وهذا ما تقوم به متصفحات الإنترنت . مثلاً إذا كان معدل الإرسال لوصلة R وتدعم ٩ تطبيقات عميل-خادم كل منها يستخدم اتصال TCP واحد فإذا طلب تطبيق جديد اتصال TCP واحد ، سيحصل كل تطبيق على معدل إرسال متساوٍ تقريبا R/10 وإذا كان التطبيق الجديد يستخدم 11 اتصال TCP معاً على التوازي سيخصص له بشكل غير منصف أكثر من R/2 أي R.(11/20

مسرد المصطلحات

١. اعاده الارسال (retransmit)
٢. الوسط الأسي المرجح المتنقل (Ewma: Exponential Weighted Moving Average)
٣. انحراف عينات زمن الذهاب والإياب عن تلك المخمنة (Devrtt)
٤. برتوكول نقطة لنقطة (Ethernet and ppp)
٥. حجم شريحة الأقصى (Mss: maximum segment siz)
٦. رقم الاشعار (acknowledge number)
٧. رقم التسلسل (sequence number)
٨. رقم منفذ المصدر: (source port number)

٩. رقم منفذ الوجهة (destination port number)
١٠. زمن الذهاب والإياب (Rtt: Round - Trip Time)
١١. شريحة بروتوكول التحكم بالنقل (TCP Segment Structure)
١٢. فك التجميع (demultiplexing)
١٣. قطع البيانات (data chunks)
١٤. متوسط العينات المخمنة (EstimatedRTT)
١٥. مجموع الاختبار (checksum)
١٦. معدل الإرسال المتاح (ABR: Available bit- rate)
١٧. نفاد المهلة (timeout)
١٨. وحدة الإرسال القصوى (MTU: Maximum transmission unit)
١٩. وضع النقل غير المتزامن (ATM: Asynchronous transfer mode)

انتهت الوحدة الثالثة

الوحدة الرابعة :

طبقة الشبكات The network layer :

تقوم طبقة الشبكات بتنفيذ خدمة الاتصال بين المضيفات hosts وعلى عكس طبق النقل يوجد جزء من طبقة الشبكة في كل مضيف وموجه router في شبكة الاتصال ولهذا السبب فان بروتوكولات طبقة الشبكة هي من بين البروتوكولات الاكثر تحديا
الدور الاساسي للموجهات هو اعادة توجيه رزم البيانات من وصلات الادخال input links الى وصلات الاخراج output links
١ _ اعادة التوجيه (التمرير) والتوجيه :

دور طبقة الشبكة هو نقل رزم packets البيانات من جهاز مستقبل الى جهاز مستقبل وذلك باستخدام عمليتين هما:

- **التمرير او اعادة التوجيه : ان تصل الرسالة الى احد مداخل الموجه وينقلها الموجه الى مخرج مناسب**
- **التوجيه : يجب ان تحدد طبقة الشبكة المسار الذي تتخذه الرزم اثناء تبادلها بين المرسل الى جهاز الاستقبال الخوارزميات التي تحدد هذه المسارات يشار اليها باسم خوارزميات التوجيه routing algorithms حيث تعمل على تحديد المسار الذي تتدفق عليه الرزم من h1الى h2 .**

لكل موجه جدول تمرير forwarding table في شكل فهرس يحتوي على مجموعة من القيم ولكل قيمة رقم مخرج مرافق ولكل رزمة ترويسة تحتوي على قيمة معينة تقوم خوارزميات التوجيه routing algorithms في الموجه بالاطلاع على محتوى هذه الترويسة لمعرفة المخرج الذي سيتم تمرير الرزمة اليهبعد مقارنة القيمة مع الفهرس الموجود في جدول التمرير .

2_نماذج خدمة الشبكة network service models:

يعرف نموذج خدمة الشبكة خصائص نقل الرزم من جهاز مرسل الى آخر مستقبل
بعد ان ترسل طبقة النقل رزمة البيانات الى طبقة الشبكة تقدم طبقة الشبكة الخدمات الاتية لبتي تتضمن وصول المعلومات .

- **ضمان التوصيل guaranteed delivery: تضمن هذه الخدمة ان الرزمة ستصل الى الجهاز المستقبل .**
- **ضمان التوصيل معع التأخير المحدود guaranteed delivery with bounded delay : لا تضمن هذه الخدمة وصول الرزمة الى الجهاز المستقبل فقط وانما تحدد الزمن اللازم لوصول الرزمة لذلك**

وايضا فان طبقة الشبكة توفر الخدمات التالية اللازمة لتدفق الرزم بين المرسل والمستقبل :

الخدمات التي تقدمها طبقة الشبكة لتدفق الرزم بين المرسل والمستقبل

- **توصيل الرزم بنفس الترتيب** in- order packet delivery **تضمن هذه الخدمة وصول الرزم الى المستقبل حسب ترتيب ارسالها.**
- **ضمان الحد الادنىمن سعة الرزمة** guaranteed minimal bandwidth **: تحاكي خدمة طبقة الشبكة هذا السلوك لمعدل بتات محدد بين المرسل والمستقبل وطالما يرسل المرسل بتات (كجزء من الرزم) بمعدل يقل عن معدل البتات المحدد فانه لا تفقد اي رزمة وكل رزمة تصل في غضون زمن تاخير معرف مسبقا .**
- **ضمان اقصى تباعد زمني للتاخير** guaranteed maximum jitter**: هذه الخدمة تضمنان مقدار الوقت بين انتقال رزمتين متتاليتين في المرسل يساوي مقدار الوقت بين استلامها في الوجهة**
- **خدمات الامن** security services **: باستخدام مفتاح تشفير معلوم فقطللمرسل و المستقبل تعمل طبقة الشبكة في جهاز المرسل على تشفير جميع الرزم قبل ارسالها وتتم عملية فك التشفير في الجهاز المستقبل فقط باستخدام المفتاح المعطى مع مثل هذه الخدمة سيتم توفير السرية لجميع شرائح طبقة النقل**(TCP and UDP) **بين المضيفين المرسل والمستقبل وبالاضافة الى السرية يمكن ان توفر طبقة الشبكة خدمات سلامة البيانات** (data integrity)**ومصادقة المصدر** (source authentication) **توفر طبقة الشبكة في الانترنت خدمة واحدة تعرف بخدمة افضل جهد** best effort **هي تعبير تلطيفي لا خدمة على الاطلاق .**

الدارات الافتراضية وشبكات رزم البيانات

Virtual circuits and datagram networks

تقدم طبقة الشبكة خدمات مشابهة لخدمات طبقة النقل من حيث الاتصال الموجه وعدم الاتصال فالخدمة الموجهة بالاتصال connection oriented services **تتطلب اجراء عملية تعرف باسم المصافحة** handshake **بينما الخدمات عديمة الاتصال** connection-less services **لا تتطلب اجراء مصافحة اولية بين المرسل والمستقبل .**

رغم تشابه طبقة النقل مع طبقة الشبكة بتوفيرها طرق الاتصال الموجه او غير الموجه الا انه يوجد فروقات في توفير الطبقتين لهذه الخدمات

تتلخص فروقات توفير الطبقتين فيما يلي :

- **تعمل الخدمات في طبقة الشبكة بين الاجهزة** host-to-host **بينما في طبقة النقل فان الخدمات تعمل بين معالجات** process-to-process
- **في جميع معماريات شبكات الحواسيب الحديثة اليوم يمكن لطبقة الشبكة ان تقدم اما خدمات موجهة اتصال غير موجهة** connectionless-oriented **او خدمات اتصال غير موجهة** connectionless **ولكن لا يمكنها ان تقدم كلا منهما في آن واحد**
- **تختلف طريقة تنفيذ خدمة الاتصال الموجهة في طبقة النقل اختلافا جوهريا عن طبقة الشبكة**
- **تعتبر شبكات الدارة الافتراضية** virtual circuit **وشبكة رزم البيانات فئتان اساسيتان من شبكات الكمبيوتر وهي تستخدم معلومات مختلفة جدا في قرارات اعادة توجيهها.**

شبكات الدارات الافتراضية virtual circuit network

تتكون الدارة الافتراضية virtual circuit من :

*مسار path :

مجموعة من الروابط والموجهات بين المصدر و الوجهة .

***عدد الدوائر الافتراضية VC number :عدد يزيد مع كل رابط موجود في المسار بين المصدر و الوجهة.**

*مدخلات entries:

وهي سجلات مسجلة على جدول التمرير في جميع الموجهات الموجودة على المسار .

تحمل الرزمة في ترويستها رقم الدارة الافتراضية التي تنتمي اليها ويتم تخصيص رقم مميز لكل دارة افتراضية في جدول التمرير forwarding table عند كل موجة ولان الرزمة الواحدة قد تمر باكثر من دارة افتراضية vc فلا بد ان تقوم الموجهات بتغيير رقم الدارة الافتراضية في ترويسة الرزمة عند مرورها بالموجه يتم تعيينه من جدول التمرير.

أسباب عدم احتفاظ الرزمة بنفس رقم ال vc

لا تحتفظ الرزمة بنفس رقم vc على كل وصلة من الوصلات على طول المسار لسببين هما :

١- هو ان تغيير الرقم من وصلة الى وصلة يقلل طول حقل VC في ترويسة الرزمة .

٢-السبب الاهم ان عملية اعداد VC تكون ابسط بكثير عند السماح لرقم VC بالتغير لكل وصلة على طول مسار VC وبالتحديد باستعمال ارقام VC متعددة يمكن ان تختار كل وصلة على المسار قم VC بشكل مستقل عن ارقام VC التي يتم اختيارها على الوصلات الاخرى على طول المسار

اما اذا تطلب ان يكون رقم VC ثابتا لكل الوصلات على طول المسار فان الموجهات يجب ان تتبادل وتعالج عددا كبيرا من الرسائل للموافقة على رقم المشترك لكي يستعمل لهذه التوصيلة الجديدة .

يجب ان تحتفظ موجهات الشبكة في شبكة vc بمعلومات حالة عن التوصيلات الموجودة حاليا بالتحديد في كل مرة يتم تأسيس توصيلة يجب ان يضاف مدخل جديد عن التوصيلة الى جدول التمرير وفي كل مرة انهاء توصيلة يجب ان يحذف المدخل المتعلق بها من الجدول.

حتى في حالة عدم وجود ترجمة لارقام الدارات الافتراضية ما زال من الضروري الاحتفاظ بمعلومات حالة عن التوصيلات تربط ارقام vc بارقام واجهات المخرج تعتبر قضية احتفاظ الموجه او عدم احتفاظه بمعلومات حالة لكل توصيلة موجودة حاليا من القضايا الهامة والتي سنعود اليها مرارا .

يوجد ثلاث مراحل اساسية تمر بها الدارات الافتراضية VC وهي:

١ـ مرحلة الاعداد VC Setup :

في هذه المرحلة تقوم طبقة النقل في الجهاز المرسل بمخاطبة طبقة الشبكة وتحديد عنوانالجهة التي ستستقبل الرسالة وتنتظر عندما يتم اعداد الدارة الافتراضية ثم تقوم طبقة الشبكة بتحديد المسار الذي ستسلكه الرزمة في طريقها من المرسل الى المستقبل يشمل هذا المسار جميع الموجهات و الروابط التي ستمر بها الرزمة كما تقوم طبقة الشبكات بتحديد الدارات الافتراضية الموجودة على المسار واخيرا يتم اضافة سجل جديد في جدول التمرير لكل موجه موجود على المسار بين المرسل والمستقبل

٢ـ مرحلة نقل البيانات data transfer :

بعد انشاء وتهيئة الدارة الافتراضية يمكن نقل البيانات عليها مباشرة بين المرسل والمستقبل

٣ـ تدمير(انهاء) الدارة الافتراضية VC teardown:

تحدث هذه المرحلة عندما يقوم المرسل او المستقبل باخطار طبقة الشبكة انه انتهى من اتصاله او انه يريد الغاء التعامل مع هذه الدارة الافتراضية ستقوم طبقة الشبكة باعلام الاجهزة المشاركة اولا ثم اعادة تحديث جداول

التمرير على كل موجه في المسار لحذف سجل الدارة الافتراضية التي تم ايقافها .

تعرف الرسائل التي ترسلها الانظمة الطرفية الى الشبكة لبدء او انهاء vcوالرسائل التي تعبر بين الموجهات لبدءvc (اي لتعديل حالة الاتصال في جداول الموجه) باسم "رسائل التحكم " (رسائل التأشير signaling messages) وغالبا ما تسمى البروتوكولات المستخدمة لتبادل تلك الرسائل بروتوكولات التحكم (بروتوكولات التأشير signaling protocols) .

٢- شبكات رزم البيانات datagram networks

عندما يريد جهاز ارسال رسالة في هذا النوع من الشبكات يقوم المرسل بتعليم الرسالة stamp the packet بعنوان الجهاز المستقبل ثم ارسال هذه الرسالة الى الشبكة عامة لا يوجد اعدادات دارة افتراضية والموجهات لا تحتوي معلومات عن حالة الدارة الافتراضية (ذلك لانه لا يوجد دارات افتراضية) تمر الرسالة بعدد من الموجهات في مسارها من المرسل الى المستقبل يقوم كل موجه بالاستفادة من عنوان الوجهة destination address لتمرير الرسالة فلكل موجه جدول توجيه forwarding table يحتوي على رقم مخرج مناسب لكل عنوان وجهة موجود في الشبكة تتم عملية البحث عن العنوات بصورة عمياء brute-force implementation ولوجود عدد ضخم جدا من عناوين شبكة الانترنت (اكثر من ٤ مليون عنوان) فهذا الاحتمال غير ممكن يستخدم الموجه ما يعرف بال prefix الذي يمثل اول عدد من الخانات في عنوان الشبكة (بعد تحويله الى عدد ثنائي binary) يطابق لعنوان الوجهة وتسمى هذه القاعدة longest prefix matching rule وتقوم خوارزمية التوجيه بتحديث
جدول التمرير في الموجه كل فترة زمنية محددة.

مصطلحات

نموذج ارسال رزم البيانات : datagram model

نموذج الدارات الافتراضية : virtual circuit model

العنونة : addressing

اعادة التوجيه (التمرير) : forwarding

التوجيه : routing

بروتوكول الانترنت ip التمرير و العنونة forwarding & addressing
من الكتاب صفحة ٢٠١

هناك نسختان من برتوكول الانترنت ip قيد الاستخدام اليوم

- برتوكول الانترنت الإصدار ٤ و الذي عادة ما يشار اليها ببساطة باسم ipv4

- برتوكول الانترنت الإصدار ٦ و الذي كان قد اقترح لاستبدال ipv4

*** ان طبقة شبكة الانترنت لديها ثلاثة مكونات رئيسية**

- المكون الأول هو برتوكول الانترنت ip

- المكون الثاني هو التوجيه الذي يحدد المسار الذي يتبعه رزمة البيانات من المصدر الى الوجهة

- المكون الثالث للشبكة هو وسيلة للإبلاغ عن الأخطاء في رزم البيانات و هو الرد على طلبات معلومات معينة عن طبقة الشبكة

صيغة رزمة البيانات datagram format صفحة ٢٠٢

_ ان رزمة طبقة الشبكة تسمى رزمة البيانات datagram

_ ان رزمة البيانات تعلب دورا محوريا في الانترنت

الحقول الرئيسية في مخطط بيانات ipv4 كما يلي

- رقم الإصدار: و تحدد هذه البتات الأربع نسخة البروتوكول ipمن رزمة البيانات من خلال النظر في رقم الإصدار يمكن للموجه تحديد كيفية تفسير ما تبقى من حقول مخطط البيانات ip . الإصدارات المختلفة من ip تستخدم صيغ رزم بيانات مختلفة الاشكال
- طول الترويسة : لانه يمكن ان يحتوي مخطط بيانات ipv4 عل عدد متغير من (التي يتم تضمينها في رزم الترويسة ipv4) هناك حاجة الى هذه البيانات في مخطط البيانات ip . معظم وحدات بيانات ip لا تحتوي على خيارات . و بالتالي فان رزم بيانات ip العادية يحتوي على ترويسة مكونة من ٢٠ بايتا .
- نوع الخدمة : تحتوي ترويسة ipv4 على بتات نوع الخدمة (TOS) للسماح لانواع مختلفة من رزم بيانات ip لتمييز كل منها عن الاخر . و يعتبر مستوى الخدمة المحدد الذي يتعين تقديمه هو مسالة تتعلق بالسياسة التي يحددها مسؤول الموجه .
- طول رزمة البيانات : و هو يمثل الطول الإجمالي لرزمة بيانات ip (الترويسة بالإضافة الى البيانات) و تقاس بالبايت . و و بما ان هذا الحقل طوله ١٦ بتا فان الحد الأقصى النظري لحجم رزمة بيانات ip هو ٦٥٥٣٥ بايت . و مع ذلك فان من النادر ما تكون وحدات البيانات اكبر من ١٥٠٠ بايت
- المعرف identifier و الاعلام flags و عنوان التجزئة fragmentation offset : هذه

الحقول الثلاثة لها علاقة بما يسمى تجزئة ip

- ان اللاصدار الجديد لبروتوكول الانترنت ipv6 لا يسمح بالتجزئة في الموجهات

وقت العمر (الزمن المتبقي) Time-to-live :

يضمن حقل الوقت ان رزمة البيانات لا تدور الى الابد في شبكة الاتصال . يتم تقليل هذا الحقل بقدر واحد في كل مرة يتم فيها معالجة رزم البيانات بواسطة الموجه . و اذا أصبحت قيمة الحقل تساوي صفرا , فانه يجب اسقاط رزم البيانات

البروتوكول :

يتم استخدام هذا الحقل فقط عندما يصل مخطط بيانات ip الى وجهته النهائية . حيث تشير قيمة هذا الحقل الى بروتوكول طبقة النقل المحدد و التي يجب ان يتم تمرير هذا الجزء من رزم بيانات ip على سبيل المثال

تشير القيمة ٦ الى ان جزء البيانات يتم تمريره الى TCP . بينما القيمة ١٧ تشير الى انه يتم تمرير البيانات الى UDP .
ان رقم البروتوكول في رزمة بيانات ip له دور مماثل لدور حقل رقم المنفذ في رزمة بيانات طبقة النقل . و ان رقم البروتوكول هو الغراء الذي يربط الشبكة و طبقة النقل معا . في حين ان رزمة المنفذ هو الغراء الذي يربط النقل و طبقات التطبيقات معا

المجموع الاختباري للترويسة header checksum:

هذا الحقل يساعد الموجه في الكشف عن وجود أخطاء البتات في رزمة بيانات ip و يتم حساب المجموع الاختباري للترويسة بمعالجة كل ٢ بايت في الترويسة كعدد و تلخيص هذه الأرقام (١ 's complement arithmetic) يحسب الموجه المجموع الاختباري للترويسة لكل رزمة بيانات تم استلامها , و يكشف حالة خطأ اذا كان المجموع الاختباري المحسوب لا يساوي القيمة المتضمنة في رزمة البيانات . و عادة م تتجاهل الموجهات وحدات البيانات التي تم اكتشاف خطا بها . لاحظ ان المجمع الاختباري يجب إعادة حسابه و تخزينه مرة أخرى في كل موجه , لأنه قد يتغير حقل ttl و ربما حقل الخيارات أيضا
لماذا يقوم TCP/IP بالتحقق من الخطأ في كل من طبقة النقل و طبقة الشبكة ؟ لعدة أسباب أولا لاحظ انه في طبقة ip يتم حساب المجموع الاختباري للترويسة فقط , بينما يتم حساب المجموع الاختباري في TCP/UDP على كامل جزء TCP/UDP . ثانيا ليس بالضرورة ان تنتمي كل من ip و TCP/UDP الى نفس كومة البروتوكولات . أي انه يمكن تشغيل بروتوكول TCP على بروتوكول مختلف عن ip

عناوين ip المصدر و الوجهة :

عندما يقوم مصدر بانشاء رزمة بيانات , فانه يدرج عنوان ip الخاص به في حقل عنوان ip المصدر و يدرج عنوان الوجهة النهائية في حقل عنوان ip الوجهة في كثير من الحيان يحدد المضيف المصدر عنوان الوجهة من خلال بحث DNS

خيارات Options :

تسمح حقول الخيارات بتمديد ترويسة ip نادرا ما تستخدم خيارات الترويسة و بالتالي فانه تقرر عدم تصمين البيانات في حث=قول الخيارات في الترويسة رزم البيانات من اجل تقليل العبء الإضافي overload مع ذلك فان مجرد وجود حقول خيارات يعقد الأمور ذلك ان تغيير طول ترويسة رم البيانات يعوق إمكانية تحديد مكان بداية حقل البيانات مسبقا . ايضا لان بعض وحدات البيانات قد تتطلب معالجة الخيارات بينما لا يحتاج بعضها الاخر لذلك و عليه فان مقدار الوقت اللازم لمعالجة رزم بيانات ip في الموجه router يمكن ان يختلف الى حد كبير , و تصبح هذه الاعتبارات ذات أهمية خاصة لمعالجة بروتوكول الانترنت في

الموجهات المضيفات عالية الأداء . و لهذه الأسباب و غيرها , لم تستخد خيارات في ترويسة ipv6

البيانات (الحمولة النافعة) (payload) data :

تعتبر المبرر الأساسي لرزمة البيانات , يحتوي حقل رزم بيانات ip على مقطع (segment) طبقة النقل (على بروتوكول TCP او IP) الى ان يتم تسليمها الى الوجهة , و مع ذلك فان حقل البيانات يمكن ان تحمل أنواعا أخرى من البيانات مثل رسائل ICMP
ان رزم بيانات ip يحتوي على ٢٠ بتا في الترويسة (على افتراض عدم وجود خيارات) ازا كانت رزمة البيانات تحمل قطعة segment من TCP فان كل رزمة بيانات (غير مجزأة) تحمل ما يعال ٤٠ بايتا للترويسة (٢٠ بايت لترويسة ip و ٢٠ بايت لترويسة TCP) بالإضافة الى رسالة طبقة التطبيقات .

تجزئة رزم بيانات بروتوكول الشبكة IP Datagram Fragmentation

لا يمكن لجميع بروتوكولات طبقة ربط البيانات ان تحمل رزم طبقة الشبكة من نفس الحجم . بعض البروتوكولات يمكن ان تحمل رزم بيانات كبيرة , في حين يمكن لبروتوكولات أخرى ان تجمل رزم بيانات قليلة الحجم فقط . على سبيل المثال يمكن ان تحمل إطارات ايثرنت ما يصل الى ١٥٠٠بايت من البيانات , في حين ان بعض الإطارات الواسعة النطاق (wide-area links) لا يمكن ان تحمل اكثر من ٥٧٦ بايت , و يسمى الحد الاقصى من البيانات التي يمكن ان يحملها اطار طبقة ربط البيانات بوحدة الارسال القصوى (MUT) maximum transmission unit و لأنه يتم تغليف كل رزم البيانات ip ضمن اطار طبقة ربط البيانات من اجل نقلها من الموجه واحد الى الموجه التالي فان كمية MTU من بروتوكول طبقة ربط البيانات تتمثل بالحد الأعلى على طول رزم البيانات ip وجود الحد الأعلى على حجم رزم بيانات ip لا تعتبر مشكلة كبيرة بل تكمن المشكلة في ان كل الروابط على طول الطريق بين المرسل و المقصد تستخدم بروتوكولات طبقة ربط البيانات المختلفة , و يمكن ان يكون لكل هذه البروتوكولات وحدات MTU مختلفة
و لفهم مسالة إعادة التوجيه (التمرير) بشكل افضل , تخيل انك موجه يربط عدة روابط , كل وصلة تستخدم بروتوكول مختلف لطبقة ربط البيانات و لها حجم اعلى مختلف لوحدة النقل MTU لنفترض انك تتلقى رزم بيانات IP من رابط واحد يقوم بالتحقق من إعادة التوجيه من جدول التمرير لتحديد الارتباط الصادر، وهذا الارتباط الصادر لديه MTU أصغر من طول رزمة بيانات IP. كيف لك أن تضغط رزمة بيانات IP الكبيرة جدا في حقل الحمولة النافعة (payload) في إطار طبقة ربط البيانات؟ الحل يكمن في تجزئة البيانات في رزمة البيانات IP إلى رزمتين او اكثر تكون أصغر حجما، ثم بتغليف كل من رزم بيانات IP الأصغر حجما في اطار منفصل و ارسال هذه الأطر عبر رابط المخرج كل من هذه البيانات الصغيرة يشار إليها على أنها جزء segment

يجب إعادة تجميع الأجزاء قبل أن تصل الى طبقة النقل في الوجهة , في الواقع يتوقع كل من TCP و UDP أن يستلما قطعا كاملة و غير مجزأة من طبقة الشبكة . و رأى مصممو بروتوكول ذو الإصدار IPv4 ان إعادة تجميع الوحدات الجزئية سيتسبب في إدخال تعقيدات كبيرة في البروتوكول مما سيؤدي إلى تقليل كفاءته من أجل التمسك بمبدأ الحفاظ على الشبكة الأساسية البسيطة قرر مصممو IPv4 اسناد هذه المهمة من إعادة تجميع الرزم الجزئية إلى الأنظمة الطرفية end systems بدلا من موجهات الشبكة .

يتلقى مضيف الوجهة سلسلة من رزم البيانات من المصدر نفسه، فإنه يحتاج الى تحديد ما إذا كانت أي **من هذه** الرزم هي أجزاء من رزمة اصلية أكبر. إذا كانت بعض رزم البيانات المستلمة أجزاء، يجب أن يحدد كذلك متى تلقى الجزء الأخير وكيف يجب أن تكون الأجزاء التي تلقاها لتجميعها معا لتشكيل رزمة البيانات الأصلية من أجل السماح لمضيف الوجهة أداء مهمة إعادة التجميع هذه , وضع مصممو بروتوكول الانترنت IP (الإصدار ٤) حقول: المعرف identifier، والعلم flag، و عنوان تجزئة fragment offset في ترويسة رزمة بيانات IP عند انشاء رزمة البيانات، فإن مضيف الإرسال يحدد رقم تعريفي (المعرف) بالإضافة إلى عناوين المصدر والوجهة. عادة، المضيف يزيد العدد التعريفي لكل رزمة بيانات يرسلها بعد ذلك عندما يحتاج موجهة إلى تجزئة رزمة البيانات، يتم اضافة كل الرزمة الجزئية الناتجة بنفس عنوان المصدر و عنوان الوجهة والعدد التعريفي لرزمة البيانات الأصلية. عندما تتلقى الوجهة سلسلة من رزم البيانات من المضيف نفسه، فإنه يفحص العدد التعريفي لكل رزمة بيانات لتحديد أي منها تعتبر في الواقع جزءا من نفس رزمة البيانات الأكبر. ولأن IP يوفر خدمة غير موثوق فيها لنقل البيانات، واحد أو أكثر من الأجزاء قد لا تصل أبدا إلى الوجهة. ولهذا السبب، من أجل أن يتأكد مضيف الوجهة أنه قد تلقى الجزء الأخير من رزمة البيانات الأصلية، يتم وضع قيمة حقل العلم flag إلى 0 بهذا الجزء، في حين أن جميع الأجزاء الأخرى قد تعيين هذا العلم flag إلى ١. أيضا، من أجل أن يتمكن مضيف الوجهة من تحديد ما إذا كان جزء مفقود (و أيضا لتكون قادرة على إعادة تجميع الأجزاء في ترتيبها الصحيح)، يتم استخدام حقل العنوان لتحديد أين يقع هذا الجزء داخل رزمة بيانات IP الأصلية ويوضح الشكل ١٤٤ صفحة ٢٠٦ مثالا على ذلك رزمة بيانات حجمها ٤٠٠٠ بايت (٢٠ بايت من ip الترويسة بالإضافة إلى ٣٩٨٠ بايت حمولة نافعة payload) يصل الى الموجه , و يجب ان يتم توجيهها الى وصلة مع وحدة MTU تساوي ١٥٠٠ بايت. وهذا يعني أنه يجب تقسيم بايتات البيانات ال ٣٩٨٠ في الرزمة الاصلية لثلاث أجزاء منفصلة (كل منها يعتبر أيضا رزمة بياناتIP) لنفترض ان رزمة البيانات الأصلي مختوم مع عند تعريفي قيمته ٧٧٧. يتم عرض خصائص الأجزاء الثلاث الجدول المطلب و تعكس البيانات في الجدول بان كمية بيانات الحمولة النافعة payload الاصلية كل جزء باستثناء الجزء الأخير يجب أن يكون مضاعفات ل ٨ بايتات، وأن تحدد القيمة في العنوان بوحدات من بايتات

في الوجهة، يتم تمرير الحمولة النافعة payload لرزمة البيانات إلى طبقة النقل فقط بعد أن تعمل طبقة الشبكة على إعادة بناء رزمة البيانات الاصلية بالكامل اذا لم يصل جزء او اكثر من الأجزاء إلى الوجهة فسوف يتم التخلص بالكامل من رزمة البيانات الناقصة ولا يتم تمريرها

الى طبقة النقل . ولكن اذا تم استخدام بروتوكول TCP في طبقة النقل فانه سيعوض هذا الفقد من خلال الطلب من المصدر إعادة ارسال البيانات المفقودة من جديد
لقد علمنا توا أن التجزئة في بروتوكول الانترنت IP يلعب دورا هاما في توصيل العديد من التقنيات المختلفة لطبقة ربط البيانات. ولكن التجزئة لها أيضا تكلفتها أولا، أنها تعقد الأنظمة الطرفية والموجهات، والتي تحتاج إلى أن تصمم لاستيعاب تجزئة رزم البيانات واعادة تجميعها ثانيا، يمكن أن تستخدم التجزته لتتر هجمات حجب الخدمة (DoS)، حيث يمكن للمهاجم أن يرسل سلسلة من الأجزاء الغريبة وغير المرغير المتوقعة ومثال تقليدي هو هجوم Jolt2، حيث يرسل المهاجم فيضا من الأجزاء الصغيرة التي ليس فيها فيها قيمة صفر في حقل العنوان إلى المضيف الهدف يمكن أن ينهار الهدف لأنه يحاول إعادة بناء رزم بيانات من تلك الرزم الجزئية التالفة. حيلة أخرى يمكن أن تحث بأن يرسل المهاجم أجزاء IP متداخلة، يتم تعيين قيم عناوين نسبية لا تسمح بإعادة وضع الرزم الجزئية بشكل صحيح. ويمكن الانظمة التشغيل الضعيفة أن تنهار تلك التي لا تعرف ماذا تفعل مع تلك الرزم الجزئية المتداخلة , ان النسخة الجديدة من بروتوكول الانترنت IPv6 تلغي التجزئة تماما، وبالتالى تحسن معالجة رزم بيانات بروتوكول الانترنت و جعل ip اقل عرضة للهجوم

العنونة في بروتوكول IPv4 Addressing IPv4

قبل مناقشة عنوان **ip** سنحتاج ان نعرف عن كيفية توصيل المضيقين و الموجهات بالشبكة عادة ما يكون للمضيف فقط وصلة واحدة في الشبكة والتي من خلالها يقوم بروتوكول **ip** بارسال المادي بالواجهة رزمة بيانات للشبكة. وتسمى نقطة تلاقي المضيف والرابط المادي بالواجهة **interface**. لننظر ان الموجه وواجهاته لأن وظيفة الموجه هي تلقي رزم بيانات على وصلة واحدة وإعادة ارسالها على وصلة أخرى، فإن الموجه يوصل عن طريق وصلتين أو أكثر بين موجه وأي واحد من روابطه يطلق ايضا واجهة. وبالتالي فإن الموجه يحتوي على واجهات متعددة، واحدة لكل وصلة من روابطه لأن كل مضيف وموجه قادر على إرسال واستقبال رزم بيانات **IP**، يتطلب بروتوكول **IP** أن يحتوي كل واجهة اضف أو وموجه عنوان **IP** الخاص بها، وبالتالي، فإن عنوان **IP** مرتبط تقنيا مع واجهة، وليس مع المضيف أو بالموجه الذي يحتوي على تلك الواجهة

كل عنوان **IP** يتكون من ٣٢ بت طويلة (بما يعادل ٤ بايت)، وبالتالي يكون المجموع العناوين **IP** المحتملة = ٢٣٢ من خلال تقريب ٢١٠ إلى ١٠٣، فمن السهل أن نرى أن هناك حوالي ٤ بلايين عنوان **IP** محتمل. تتم
كتابة هذه العناوين عادة ما تكتب في صيغة التدوين العشري المنقط، والتي يتم كتابة كل بايت من العنوان في شكل عشري ويتم فصله بنقطة من وحدات البايت الأخرى في العنوان
على سبيل المثال، عنوان **IP** التالي .١٩٣,٣٢,٢١٦,٩ يتكون من أربعة بايتات: القيمة ١٩٣ هو المعادل العشري من ٨ بت الأولى من العنوان و ٣٢ هو المعادل العشري من ٨ بت الثانية من العنوان، وهكذا فإن الصيغة الثنائية المكافئة للعنوان ١٩٣,٣٢,٢١٦,٩
هي:
١١000001 00 100000 11011000 00001001
يجب أن يكون لكل واجهة على كل مضيف وموجه في شبكة الإنترنت العالمية عنوان **IP** فريد من نوعه عالميا، باستثناء الواجهات وراء أنظمة **NAT**. لا يمكن اختيار هذه العناوين بطريقة عشوائية، حيث أن جزءا من عنوان **IP** للواجهة يحدد الشبكة الفرعية المتصلة بتلك الواجهة ويقدم الشكل ٤-١٥ صفحة ٢٠٨ مثالا على عناوين بروتوكول الإنترنت (**IP**) والواجهات. في هذا الشكل ، يستخدم موجه واحد (مع ثلاث واجهات) لربط سبعة مضيفين. سنلقي نظرة فاحصة على عناوين **IP** المعينة إلى واجهات المضيفات والموجهات، كما أن هناك عدة أمور يجب ملاحظتها عناوين لكل من واجهات المضيفات الثلاثة في الجزء العلوي الأيسر من الشكل، وواجهة الموجه التي يرتبط بها كل منهم له الصيغة **xxx** . ١. ١. ٢٢٣ أي ان لديهم جميعا نفس ال ٢٤ بت في أقصى اليسار في عنوان **IP** الخاصة بهم. الواجهات الأربعة هي مترابطة ايضا ببعضها البعض بواسطة شبكة لا تحتوي على موجهات ايضا يمكن ربط هذه الشبكة بشبكة إيثرنيت مثلا، وفي هذه الحالة يمكن هذه الحالة يمكن ربط الوصلات البينية بواسطة (**Ethernet switch**) أو بنقطة وصول لاسلكية (**Wireless access point**).
في مصطلحات بروتوكول الإنترنت، تشكل هذه الشبكة التي تربط بين ثلاث واجهات مضيفة وواجهة راوتر واحدة شبكة فرعية [**RFC950**]. (وتسمى الشبكة الفرعية ايضا شبكة **IP** او مجرد شبكة في **IP** الإنترنت) يعين عنوان **IP** عنوانا لهذه الشبكة الفرعية هو **223. 1.1.0/24**

حيث يشير الرمز ٢٤، الذي يعرف أحيانا باسم قناع الشبكة الفرعية (**subnet mask**)، إلى أن ال ٢٤ بت في أقصى اليسار من كمية ٣٢ بت تمثل عنوان الشبكة الفرعية وتتكون الشبكة الفرعية من واجهات المضيف الثلاثة
(**223.1.1.1** و **223.1.1.2** و **223.1.1.3**) و واجهة موجه واحدة (**223.1.1.4**) وستكون هناك حاجة إلى أي مضيفات إضافية مرتبطة بالشبكة الفرعية **223.1.1.0/24** للحصول على عنوان الصيغة **xxx.223.1.1**
لا يقتصر تعريف بروتوكول **IP** لشبكة فرعية على قطاعات إيثرنت التي تربط مضيفات متعددةبواجهة الموجه لتوضيح ذلك. عزيزي الطالب. انظر الشكل ٤١٧ صفحة ٢٠٨، الذي يظهر ثلاثة موجهات مترابطة مع بعضها البعض من خلال وصلات من نوع "نقطة إلى نقطة **point-to – point** . يحتوي كل موجه على ثلاث واجهات , واحدة لكل وصلة من نوع "نقطة إلى نقطة وواحدة لوصلة البث التي تربط الموجه مباشرة مع زوج من المضيفات, ما هي الشبكات الفرعية الموجودة هنا؟ هناك ثلاث شبكات فرعية, **223.1.1.0/24** , **223.1.2.0/24** , **223.1.3.0/24** و وهي مشابهة للشبكات الفرعية التي واجهناها في الشكل ٤ ولكن لاحظ ان هناك ثلاث شبكات فرعية إضافية في هذا المثال أيضا شبكة فرعية **223.1.9.0/24** للواجهات التي تربط الموجهات **RT** و **R2** شبكة فرعية اخري **223.1.8.0/24** للواجهات التي تربط الموجهات **R2** و **R3** شركة فرعية ثالثة **223.1.7.0/24** للواجهات التي تربط الموجهات **R3** و **R1** بالنسبة لشبكة عامة وموجهات ومضيفات، يمكننا استخدام الوصفة التالية لتحديد الشبكات الفرعية في تلك الشبكة :
لتحديد الشبكات الفرعية، تفصل كل واجهة من المضيف أو الموجه، وخلق جزر من شبكات معزولة، مع واجهات انهاه نقاط نهاية الشبكات المعزولة. وتسمى كل من هذه الشبكات المعزولة شبكة فرعية .

تعرف استراتيجية تخصيص عناوين الإنترنت باسم "التوجيه غير المتقطع" **Classless Interdomain [RFC 4632] Routing (CIDR)**

وهو تعميم لمفهوم عنونة الشبكة الفرعية. كما هو الحال مع عنونة الشبكة الفرعية، ينقسم عنوان **IP** المكون من ٣٢ بت إلى جزأين، ويشتمل مرة أخرى على الشكل العشري المنقط **a. b . c . d / x** حيث يشير **x** إلى عند البنات في الجزء الأول من العنوان
تشكل **X** البتات الأكثر أهمية لعنوان **a. b . c . d / x** جزء الشبكة من عنوان **IP**، وغالبا ما يشار إليها بالبادئة **prefix** (او بادئة الشبكة) للعنوان , عادة ما يتم تعيينه لعدد من العناوين المتجاورة، أي مجموعة من العناوين ذات البادئة المشتركة في هذه

الحالة، ستشارك عناوين **IP** الخاصة بالأجهزة داخل شبكة المؤسسة في البادئة الشائعة

يمكن اعتبار بقية البتات في العنوان على أنها تميز بين الأجهزة ضمن المنظمة التي لها نفس بادئة الشبكة هذه البتات هي التي ستفحص عند توجيه الرزم داخل المنظمة . وقد يكون (أو لا يكون) لهذه البتات ذات الرتبة الأدني تركيب لفريغ شبكي إضافي او كالذي ناقشناه من قبل، على سبيل المثال افترض ان البتات ال٢١ الأولى من العنوان **A .b . c . d . /21** تحدد بادئة الشبكة المنظمة و هي ثابتة في عناوين الاجهزة في تلك المنظمة . أما البتات الباقية الإحدى عشرة الأخرى في اقصى اليمين لعناوين الشبكات الفرعية ضمن المنظمة كما ذكرنا سابقا على سبيل المثال قد يشير العنوان **A .b . c . d . /24** الى شبكة فرعية معينة ضمن المنظمة

قبل استخدام أسلوب **CIDR** للعنونة، كان جزء من العنوان الذي يدل على الشبكة مقيدا بواحد من الاطوال ٨ أو ١٦ أو ٢٤ بتأ، وهو ما عرف بالعنونة النوعية (**classful addressing**) و تعرف الشبكات التي تنتمي لكل نوع من هذه العناوين بالفئة **A** و **B** و **C** على الترتيب. لكن المطلوب أن أن يكون طول الجزء الدال على الشبكة لعنوان محصورا في تلك القيم (أي ١ او ٢ او ٣ بايتات) سبب مشكلة لدعم العدد ال الشبكة العنوان محصورا في د المنظمات التي تمتلك شبكات فرعية صغيرة ومتوسطة الحجم. كما أن تخصيص عناوين من الفئة **C (14/)** يدعم فقط **2^8-2=254** مضيف كحد اقصى (حيث ان اثنين من تلك العناوين محجوزان للاستعمال الخاص) و الذي قد يكون صغيرا جدا بالنسبة للعديد من المنظمات في حين أن أقصى عدد تدعمه الفئة **B (6/١)** من المضيفات يساوي **65,534** مضيفا والذي قد يعتبر كبيرا جدا لتلك المنظمات. بالتالي اذا استخدمنا هذا الأسلوب للعنونة فإن منظمة لديها فقط **2,000** مضيف ستحتاج إلى عنوان من الفئة **B** الامر الذي يؤدي لاستنزاف سريع لفضاء عناوين الفئة **B** واستخدام سيء للعناوين المخصصة على سبيل المثال المنظمة السابقة التي لديها **2,000** مضيف فقط **2,000** عنوان من عناوين الفئة **B** التي خصصت لها تاركة بذلك اكثر من **63,000** عنوان لا يمكن استخدامها من قبل منظمات أخرى سنكون مقصرين إذا لم نذكر نوعا آخر من عناوين بروتوكول الإنترنت وهو عنوان الإذاعة

255.255.255.255 فعندما يرسل مضيف وحدة بيانات لهذا العنوان كعنوان الوجهة تسلم الرسالة إلى كل المضيفات على نفس الشبكة الفرعية، ويمكن أن ترسل الموجهات الرسالة إلى الشبكات الفرعية المجاورة أيضا (غير أن هذا الاختيار لا يستخدم عادة).

بعد أن درسنا عنونة بروتوكول الإنترنت بالتفصيل، نحتاج لمعرفة كيفية حصول المضيفات والشبكات الفرعية على عناوينها في البداية دعنا نبدأ بالنظر إلى كيفية حصول منظمة ما على كتلة عناوين غوين لأجهزتها، ثم إلى كيفية حصول جهاز (كمضيف مثلا) على عنوان من بين كتله عناوين المنظمة .

وفي ما يلي سنعرض مثالين على الفئة **B** و الفئة **C** باستخدام أسلوب إلى **CIDR** للعنونة.

ولكن قبل ان نبدا لا بد من توضيح كيفية تحديد فئة عنوان الانترنت **C**، **B**، **A** ، ويتم معرفة ذلك من خلال النظر في المجموعة الأولى في أرقام عنوان الانترنت **IP** (ال **octet** الأول من اليسار) وبناء على وبناء على قيمة هذا الرقم يتم تحديد فيما إذا كان من الفئة **A** أو **B** أو**C**.

حيث تكون الفتات على النحو التالي :

الفئة **A** : القيمة من **1** إلى **126** (مثال: الرقم **10** في العنوان **10.50.70.1**) و يكون عدد بتات قناع الشبكة هو **8** و عدد بتات عنوان ال **IP** للمضيف هو **24** (و يكون مجموع البتات = **32**)

الفئة **B** : القيمة من **128** إلى **191** (مثال : الرقم **170** في العنوان **170.75.20.2**) و يكون عدد بتات قناع الشبكة هو **16** وعد بتات عنوان ال **IP** للمضيف هو **170** (و يكون مجموع البتات = **32**)

الفئة **C**: القيمة من من **192** إلى **223** (مثال : الرقم **200** في العنوان **200.75.20.2**) و يكون عدد بتات قناع الشبكة هو **24** وعد بتات عنوان ال **IP** للمضيف هو **8** (و يكون مجموع البتات = **32**)

مثال (١):

ما هي الشبكة الفرعية التي ينتمي إليها عنوان **IP** التالي **255.255.224.0** **131.107.32.1** ؟

وكم عنوان انترنت يوجد في كل شبكة فرعية؟ وما هي الشبكات الفرعية ؟

الإجابة

أولا ننظر الى قناع الشبكة **255.255.224.0** ونقوم بتحويل قناع الشبكة إلى النظام الثنائي

11111111111111.11100000.00000000

التمثيل قناع الشبكة بالشكل الأخر(/) نقوم بعد الواحدات في العدد الثنائي والذي يمثل مدى **range** قناع الشبكة و هو **19**.

ثانيا ننظر إلى المجموعة الأولى **octet** من عنوان **IP** (المجموعة الأولى من اليسار وهي **131**) ونحدد من أي فئة كان، وبما أن العدد **131** يقع بين **128 191** فهذا يعني أن عنوان الانترنت من الفئة **B** التي تمثل ب **16** بت لتحديد قناع الشبكة و**16** بت لتحديد عند خانات عنوان **IP** للمضيف **host**
ولكن في هذا المثال قمنا باستعارة **3** بتات من عنوان الانترنت المضيف إلى قناع الشبكة. وهذا يعني أن عدد الشبكات الفرعية يساوي **23** (حيث أن العدد **3** هي عدد البتات المستعارة) وبالتالي فإنه يتبقى (**16-3=13** بت) لعنوان الانترنت للمضيف ويكون عنوان الانترنت للمضيف في كل شبكة فرعية يساوي **213** عنوان **IP**
وأما الشبكات الفرعية فإنها تكون على النحو التالي:

1st Subnet 131.107.0.0

2nd Subnet 131.107.32.0*

3rd Subnet 131.107.64.0

4th Subnet 131.107.96.0

5th Subnet 131.107.128.0

6th Subnet 131,107.160.0

7th Subnet 137,107,192,0

8th Subnet 131.107.224,0

و عليه فان عنوان الانترنت **ip** التالي **131.107.32.1** بقع في الشبكة الفرعية الثانية **131.107.32.0**

مثال (**2**)
ما هي الشبكة التي ينتمي اليها عنوان **ip** التالي **192.168.100.203/27** ؟ و كم عنوان انترنت يوجد في كل شبكة فرعية ؟ و ما هي الشبكة الفرعية ؟
من عنوان تنظر إلى **27** الذي يحدد قناع الشبكة، وننظر أيضا إلى المجموعة الأولى **octet** من عنوان الانترنت **IP** وهو **192** والذي يقع بين **192** و**232** وهذا يعني أن عنوان **IP** من الفئة **C** وكما نعلم أن الفئة **C** لديها **24** بت لتحديد قناع الشبكة و**8** بتات للتحديد عنوان **IP** للمضيف.
ولكن في هذا السؤال لدينا **27** بت لتحديد عنوان الشبكة وهذا يعني أنه تم استعارة **3** بتات من عنوان الانترنت **IP** للمضيف لصالح عنوان الشبكة . و هذا يعني ان عدد الشبكات الفرعية يساوي **23** (حيث أن العدد **3** هي عدد البتات المستعارة) وبالتالي فإنه يتبقى (**8-3=5** بتات) لعنوان الانترنت للمضيف ويكون عنوان الانترنت للمضيف في كل شبكة فرعية يساوي **25** عنوان **IP** لكل شبكة فرعية .
و اما الشبكات الفرعية فانها تكون على النحو التالي :

Subnet I 192.168.100.0 hosts 1-30 (broadcast = 31)

Subnet 2 192.168.100.32 hosts 33-62 (broadcast = 63)
Subnet 3 192.168.100.64 hosts 65-94 (broadcast = 95)
Subnet 4 192.168.100.96 hosts 97-126 (broadcast = 127)
Subnet 5 192.168.100.128 hosts 129-158 (broadcast = 159)
Subnet 6 192.168.100.160 hosts 161-190 (broadcast = 191)
Subnet 7 192.168.100. 192 hosts 193-222 (broadcast = 223)*
Subnet 8 192.168.100,224 hosts 225-254 (broadcast = 255)

و عليه فان عنوان الانترنت **ip** التالي **192.168.100.203** بقع في الشبكة الفرعية السابعة **192.168.100.192**

● الحصول على كتلة العناوين Obtaining a Block of Address

• يتصل المشرف على الشبكة اولا بموفر خدمة ISP لتخصيص عناوين من كتلة اكبر من العناوين التي تم تخصيصها لموفر الخدمة من قبل

*انظر الى الصورة صفحة ٢١٣ في الكتاب المقرر

• هناك سلطة عالمية لها مسؤولية نهائية لإدارة عناوين الانترنت و تخصيص كتل منها لموفري خدمة الانترنت والمنظمات الأخرى

• عناوين الانترنت مدارة تحت سلطة شركة الانترنت للأسماء والأعداد المخصصة ICANN ،المرجع ICANN 2007 بناء على الارشادات الموجودة ب RFC 2050 ودور هذه المنظمة اللاربحية ليس فقط تخصيص عناوين بروتوكول الانترنت ،ولكن

أيضا ادارة خدمات اسماء النطاقات الجذرية DNS root server ،كذلك تعمل على تخصيص اسماء النطاقات وحل النزاعات المتعلقة بها

• تخصص ICANN عناوين مكاتب تسجيل الانترنت الاقليمية (مثل: ARIN، RIPE، APNIC، LACNINC) والتي تشكل سوية المنظمة المساندة للعناوين ل (ICANN ASO-ICANN، 2007) وتعالج تخصيص وادارة العناوين ضمن نطاقها .

• الحصول على عنوان مضيف: بروتوكول تهيئة المضيف الديناميكي (DHCP)

• بعد ان تحصل المنظمة على كتلة عناوين يمكنها تخصيص عناوين لواجهات الموجهات والمضيفات لديها

• يقوم المسؤول عن الشبكة بتهيئة عناوين IP للموجهات يدويا (غالبا ما يتم ذلك عن بعد باستخدام اداة ادارة الشبكة)

• يمكن تهيئة عناوين المضيفات بطريقة يدوية الا أنه في اغلب الأحيان تستخدم هذه العملية بروتوكول DHCP لتهيئة المضيفات ديناميكيا [RFC 2131]

• يستخدم بروتوكول DHCP لمضيف بالحصول على عنوان IP آليا

• يمكن ان يهيئ المشرف على الشبكة بروتوكول DHCP أيضا لمضيف بالحصول على معلومات اضافية مثل قناع شبكته الفرعية subnet mask وعنوان الموجه الأول first hop router (والذي يطلق عليه في أغلب الأحيان البوابة الاعتمادية default getaway) وعنوان خادم اسماء النطاقات المحلي DNS server

• بسبب قدرة بروتوكول DHCP على أتمتة الشبكة فيما يتعلق بتوصيل مضيف لها ،فإنه دائما ما يطلق عليه بروتوكول "وصّل و شغّل " plug and play .

• يتمتع بروتوكول DHCP بالاستعمال الواسع الانتشار في شبكات الاتصال بالانترنت السكني و في الشبكات المحلية اللاسلكية .

• في بروتوكول DHCP تتصل المضيفات بالشبكة وتغادرها كثيرا

،مثل شخص ينتقل بهاتفه المحمول من غرفته الى المكتبة الى قاعة الدروس ،في كل موقع سيوصل بشبكة فرعية ولذلك سيحتاج عنوان IP جديد في كل موقع ويب وهذا يناسب مع DHCP بطريقة مثالية

حيي العديد من المستخدمين يأتون ويغادرون

▪حيث العناوين مطلوبة لفترة محدودة فقط

•يفيد DHCP بنفس الطريقة شبكات الوصول السكني لموفر خدمة انترنت

• يستخدم خادم بروتوكول DHCP بنية خادم/زبون

اذا لم يوجد خادم DHCP فسنحتاج الى وجود وكيل ترحيل realy agent يعرّف عنوان خادم يعرّف

▪انظر الشكل ٤ـ٢٠ صفحة ٢١٤

• يعتبر بروتوكول DHCP عملية مكونة من ٤ خطوات

▪انظر الشكل ٤ـ٢٠ صفحة ٢١٥

● اكتشاف خادم DHCP :

• ان المهمة الأولى للمضيف القادم حديثا للشبكة هي ان يجد خادم DHCP الذي سيتفاعل معه ،ويتم ذلك بارسال رسالة اكتشاف DHCP والتي يرسلها المضيف ضمن رزمة UDP الى المنفذ المخصص

• تغلف رزمة UDP في رزمة بيانات IP

• ان المضيف لا يعرف على الاطلاق حتى عنوان IP للشبكة التي يتصل بها وبالأحرى لا يعرف عنوان خادم DHCP لهذه الشبكة

● عروض خادمات DHCP

• يستلم خادم DHCP رسالة استكشاف DHCP ويرد على الزبون برسالة عرض DHCP تذاع الى كل العقد على الشبكة الفرعية ،ونظرا لاحتمال وجود عدة خادمات DHCP على الشبكة الفرعية حيث يستطيع الزبون الاختيار من بين عدة عروض ،تحتوي كل رسالة عرض من الخادم على لبرقم التعريفي لرسالة الاكتشاف التي تلقاها و عنوان بروتوكول الانترنت المقترح للزبون وقناع الشبكة network mask ومدة ايجار عنوان (IP address lease time) أي المدة التي سيكون فيها العنوان صحيحا -محجوزا ولا يمكن استخدامه لمضيف آخر-

● طلب DHCP

• بعد ان يختار المضيف الواصل حديثا للشبكة واحدا من عروض DHCP المقدمة له سيرد عليها برسالة طلب DHCP ويضع بها نفس قيم بارامترات التهيئة الموجودة في العرض المختار

● اشعار استلام (DHCP ACK) DHCP

• يرد الخادم على رسالة طلب DHCP برسالة اشعار استلام DHCP مؤكدا قيم البارامترات المطلوبة

▪ بمجرد استلام الزبون اشعار استلام DHCP يكون التفاعل بين الزبون والخادم قد اكتمل

▪يمكن ان يستعمل الزبون عنوان IP المخصص له من خادم DHCP حتى تنتهي مدة الايجار

▪يوفر DHCP آلية تسمح للزبون تحديد عنوان IP اذا كان الزبون يرغب في استعمال عنوانه بعد انتهاء مدة الايجار

▪ الفائدة في خاصية "وصّل و شغّل " plug and play في بروتوكول DHCP ان البديل هو تهيئة المضيف يدويا

▪ يعاني بروتوكول DHCP من بعض أوجه القصور من منظور قابلية الحركة ،فمثلا لا يمكن الاحتفاظ بتوصيلة TCP لعقدة تتحرك بين شبكات فرعية لأنها تحصل على عنوان IP جديد من DHCP في كل مرة توصل بشبكة فرعية جديدة

▪ يوجد برنامج مصدر مفتوح (open source code)لتحقيق بروتوكول DHCP من اتحاد نظم الانترنت (Internet System Consortium)

● ترجمة عناوين الشبكة (NAT)

SOHO : Small Office Home Office (المكتب الصغير و المكتب المنزلي)

• ترجمة عناوين الشبكة (NAT) هي طريقة بسيطة لتخصيص العناوين

▪انظر الشكل ٤-٢٢ صفحة ٢١٧ الذي يوضح كيفية عمل موجه مزود بNAT

• المقصود ب منطقة عناوين خاصة realm with private address بأنها شبكة يكون لعناوينها معنى فقط لدى الأجهزة الموجودة ضمن تلك الشبكة

• يحجب موجه الNAT تفاصيل الشبكة عن العالم الخارجي

• يحصل الموجه على عنوانه من خادم DHCP لمزود خدمة الانترنت

• يشغل الموجه خادم DHCP لتزويد العناوين الى اجهزة الحاسوب ضمن فضاء عناوين الشبكة المنزلية التي تقع في نطاق تحكم موجه DHCP

• اذا كانت كل وحدات البيانات التي تصل الى موجه NAT من الشبكة الواسعة النطاق WAN لها نفس عنوان IP للموجه فيعرف الموجه المضيف الداخلي الذي يجب أن يرسل له رزمة البيانات من خلال استعمال جدول ترجمة NAT في الموجه ويتضمن في مدخلاته أرقام المنافذ بالاضافة الى عناوين IP

• عندما يولد موجه NAT رقما جديدا لمنفذ المصدر يمكن أن يختار اي رقم غير موجود حاليا في جدول ترجمة NAT

• يضيف NAT الموجود في الموجه ايضا مدخلا الى جدول ترجمة NAT

• لا يدرك خادم الويب أن رزمة البيانات الواصلة والتي تحتوي على طلب HTTP قد عولجت بموجه NAT ويرد بارسال رزمة بيانات تحتوي على IP لموجه NAT لعنوان الوجهة ورقم منفذ الوجهة ، عندما تصل رزمة البيانات هذه إلى موجه يقوم الموجه بالبحث في جدول ترجمة ال NAT مستخدما عنوان IP للوجهة ورقم منفذ الوجهة

للحصول على رقم IP المناسب ورقم منفذ الوجهة ويرسل رزمة البيانات الى الشبكة المنزلية

- هناك العديد من الأصوليين في محيط فريق عمل هندسة الانترنت IETE يعترضون على NAT بشدة ،لأنه من المفترض ان تستخدم ارقام المنافذ لعنونة العمليات و ليس لعنونة المضيفات ،ويعترضون ثانيا لأنه من المفروض أن الموجهات تعالج الرزم حتى الطبقة ٣ فقط والسبب الثالث لاعتراضهم أن بروتوكول NAT ينتهك ما يسمى بقضية من طرف الى طرف ؛أي أن المضيفات يجب أن تتكلم مباشرة مع بعضها البعض بدون تدخل عقد لتعديل عناوين IP وأرقام المنافذ

ويعترضون رابعا لأنه يجب استخدام Ipv6 للتغلب على مشكلة النقص في عناوين IP ،بدلا من تلك الحلول الترقيعية المؤقتة للمشكلة كحلول NAT

● من المشكلات الرئيسية الأخرى التي تواجه NAT

• تداخلها مع تطبيقات النظائر P2P ،كمشاركة النظائر للملفات P2P File وتطبيقات النظائر لنقل الصوت عبر الانترنت P2P Voice

• في تطبيقات النظاير يستطيع أي نظير مشارك A أن يبدا توصيلة TCP مع اي نظير مشارك آخر B

• تكمن المشكلة في أنه لو كان النظير B وراء ال NAT فإنه لا يستطيع العمل كخادم و بالتالي لا يستطيع ان يقبل توصيلات TCP

• يمكن التخلص من مشكلة NAT اذا لم يكن النظير A وراء ال NAT و يجري معه النظير B حاليا اتصال TCP

• يمكن أن يسأل النظير A النظير B عن النظير C ان يبدأ اتصال TCP خلفي مع النظير A

• بمجرد انشاء الاتصال المباشر بين النظيرين A و B يمكن أن يتبادلا الرسائل او الملفات وتسمى هذه العملية "الاتصال الخلفي" connection reversal وتستخدم في الواقع من قبل الكثير من تطبيقات النظائر لتجاوز NAT

• اذا كان كل من النظيرين A و B وراء ال NAT الخاص به تكون هذه الحالة الأصعب نوعا ما ،ولكن يمكن أن تعالج باستعمال تطبيقات الترحيل application relays .

● بروتوكول رسائل التحكم في الانترنت (ICMP)

Internet Control Message Protocol

• يتم استخدام بروتوكول ICMP في المرجع [RFC 792] من قبل المضيفات و الموجهات لتبادل معلومات طبقة بين بعضها البعض

• الاستخدام الأكثر شيوعا من ICMP هو للإبلاغ عن الخطأ

• كثيرا ما يعتبر بروتوكول ICMP جزءا من بروتوكول IP ،لكن من الناحية المعمارية يقع فوق بروتوكول الانترنت

• يتم نقل رسائل ICMP داخل رزم بيانات IP -يعني أن رسائل ICMP يتم حملها كمحمولة IP

• عندما يستلم المضيف رزم بيانات IP تحمل رسالة ICMP فإنه يعمل على انتزاع محتويات رسالة ICMP

• تحتوي رسائل ICMP على حقل من نوع type وحقل رمز code لكل نوع وتحتوي على أول ٨ بايتات من ترويسة رزمة IP الذي تسبب في انشاء رسالة ICMP في المقام الأول (بحيث يمكن للمرسل تحديد رزمة البيانات التي تسببت بالخطأ)

▪ انظر الشكل ٤-٢٣ صفحة ٢٢٠

حيث تظهر أنواع رسائل ICMP ،ومن الملحوظ أن رسائل ICMP لا تستخدم فقط للإبلاغ عن حالات الأخطاء

• يقوم برنامج ping المعروف بإرسال رسالة ICMP من النوع ٨ بالرمز ٠ الى المضيف المحدد

• تدعم معظم تطبيقات TCP/IP خادم ping مباشرة في نظام التشغيل

• برنامج الزبون يحتاج إلى أن يكون قادرا على توليد نظام التشغيل لإنشاء رسالة ICMP من نوع ٨ رمز ٠

• رسالة ICMP اخرى هي رسالة اخماد مصدر source quench ،الغرض منها هو اجراء التحكم في الازدحام

• برنامج Traceroute هو برنامج تتبع المسار ،يستخدم رسائل ICMP لقرير أسماء وعناوين الموجهات بين المصدر والوجهة، حيث يقوم البرنامج بإرسال سلسلة من وحدات بيانات IP العادية إلى الوجه ،تحمل كل وحدة قطعة UDP برقم منفذ UDP غير محتمل الوجود

يكون زمن TTL في اول هذه الوحدات له القيمة ١ وفي ثانية له القيمة ٢ وهكذا
يبدأ المصدر ايضا موقتات لكل وحدة من وحدات البيانات

عندما تصل رزمة البيانات n الى الموجة n يلاحظ الموجه n ان مدة TTL لرزمة البيانات انتهت
بنسبة او وفق لقواعد برتوكول ip يتلخص الموجه من رزمة البيانات ويرسل رسالة ICMP تحذيرية الى المصدر من نوع ١١بكود ٠ تتضمن اسم الموجه وعنوان IP
عندما تصل تلك الرسالة الى المصدر يحصل على زمن رحلة الذهاب والاياب من المؤقت واسم وعنوان ip للموجه n من رسالة ICMP
برتوكول IPv6بدأ فريق عمل هندسة الانترنت IETF في اوائل التسعينات ومحاولة تطوير برتوكول يخلف بروتوكول IPV4
كان احد الحوافز الاساسية لهذا الجهد هو ادراك ان فضاء العناوين المكونة ن ٣٢ بتا يشرف على النفاذ بمعدل سريع
توصيل الشبكات الفرعية وعقد برتوكول IP جديد بالانترنت وتخصيص عناوين IP فريدة بمعدلات عالية للغاية
كانت توقعات عمر العناوين في فريق العمل هندسة الانترنت هو انها ستنفذ بين عامي ٢٠٠٨و٢٠١٨
لا يزال هناك متسع من الوقت حتى تستنزف عناوين IPv6
لقد بدا العمل في برتوكول الانترنت القادم IPng

من اهم المتغيرات في برتوكول IPv6 والتي تتضح من صيغة رزمة البيانات ؟

١.التوسع في العناوين :

زاد برتوكول IPv6 حجم عنوان برتوكول الانترنت من ٣٢ بتا الى ٢٨ بت وهذا يتضمن بان العالم لن يستنفذ عناوين برتوكول الانترنت

٢. انسيابية الترويسة المكونة من ٤٠ بايتا:

تم اسقاط عدد من حقوق IOv4 او جعلها اختيارية واستخدام ترويسة جديدة بطول ثابت قدره ٤٠ بايتا تسريع معالجتها ويسمح استخدام نظام تكويد جديد للخيارات بمرونة اكثر في معالجة تلك الخيارات

٣.وسم التدفق والاولوية

يستخدم IPv6 تعريفا مبهما بعض الشيء للتدفق

الحقول المعرفة في بروتوكول IPv6 ؟

أ. رقم النسخة او الاصدار يميز هذا الحقل المؤلف من ٤ بتات رقم النسخة برتوكول الانترنت وليس مستغربا ان يحتوي هذا الحقل على القيمة ٦ لبروتوكول IPv6

ب. نوع حركة مرور البيانات يمثل هذا الحقل المكون من ٨بتات من حيث مبدا حقل TOS الموجود في IPv4
ت. وسمة التدفق flow labelيستعمل هذا الحقل المكون من ٢٠ بت لتمييز تدفق وحدات البيانات

ث. طول الحمل الاجر payload lenght تعامل هذه القيمة المكونة من ١٦ بت كعدد صحيح بدون إشارة الترويسة التالية next header يميز هذا الحقل بروتوكول الذي ستسلم اليه محتويات رزم البيانات يستخدم هذا الحقل قيما مماثلة لتلك المستخدمة في IPv4

ج. الحد الاعلى لعدد القفزات hop limit تخفض محتويات هذا الحقل بمقدار واحد عند كل موجه يقوم بإرسال رزمة بيانات تلك واذا اصبحت قيمته صفرا سيهمل الموجه رزمة البيانات

و. عناوين المصدر والوجهة يوجد وصف للصيغ المختلفة لعناوين IPv6 والمكونة من ١٢٨ بت
ي. البيانات يمثل هذا الجزء الحمل الاجر payload لرزمة البيانات IPv6 عندما تصل رزمة البيانات الى وجهتها يتم استخلاص هذا الجزء من رزمة البيانات ونقلها الى بروتوكول المحدد في حقل الترويسة التالية

•التجزئة وإعادة التجميع لوحدات البيانات

Fragmentation /Reassembly :

.لا يسمح IPv6 بتجزئة وإعادة تجميع وحدات البيانات في الموجهات المتوسطة ،وانما يمكن أن تؤدي هذه العمليات فقط بواسطة المصدر والوجهة

.اذا استلم موجه رزمة بيانات IPv6 كبيرة جدا لكي ترسل على الوصلة الخارجية فإن الموجه ببساطة يسقط رزمة البيانات ويرسل رسالة خطأ ICMP بمعنى "رزمة كبيرة جدا" الى المرسل ،يمكن حينئذ ان يعيد المرسل إرسال البيانات مستخدما حجما أصغر لرزمة بيانات IP

.إن التجزئة Fragmentation و إعادة التجميع Reassembly عملية مضيّعة للوقت لذا ستؤدي ازالة هذه الوظيفة من الموجهات ووضعها مباشرة في الأنظمة الطرفية إلى تسريع بروتوكول الانترنت إلى حدٍّ كبير

.المجموع التدفقي للترويسة :header checksum

.يلزم حساب المجموع التدقيقي للترويسة بعد كل قفزة نظرا لوجود حقل TTL والذي تتغير قيمته مع كل قفزة

.الخيارات :

.لم يعد حل الخيارات جزءا من ترويسة IP المعيارية ،مع ذلك فإنه لم يلغ

تماما و انما أصبح حقل الخيارات أحد الترويسات التالية المحتملة والمشار إليها من ترويسة IPv6
.يؤدي إزالة حقل الخيارات إلى جعل ترويسة بروتوكول الإنترنت ثابتة الطول ومؤلفة من ٤٠ بايت

- بروتوكولICPM

يُستخدم من قِبل عُقد بروتوكول الانترنت للابلاغ عن حالات الخطأ وتزويد النظام الطرفي بمعلومات محدودة من بروتوكول ICPM لبروتوكولIPv6
،المرجع [RFC 443] ،بالاضافة الى اعادة تنظيم تعريفات الأنواع والأكواد الموجودة

- أضافت ICPMPv6 انواع وأكواد جديدة تطلبها وظائف IPv6 الجديدة ،يشمل ذلك "رزمة كبيرة جدا" و "خيارات IPv6 غير معروفة "
- يتضمن بروتوكول ICPMPv6 وظائف بروتوكول IGMP
- في السابق كان- IGMP والذي يستعمل لإدارة انضمام مضيف ومغادرته لمجموعات الارسال الجماعي- بروتوكولا منفصلا عن ICPM في IPv6

.الانتقال من IPV4 إلى IPv6

- كيف ستتحول الانترنت العامة والتي تعمل طبقا لبروتوكول IPV4 الى بروتوكول IPv6 ؟

هناك عدة خيارات

1- الاعلان عن موعد محدد يتم فيه توقف تام للإنترنت وترقية كل أجهزتها من IPV4 الىIPv6

2- تقديم عقد IP بحزمة بروتوكولات مزدوجة

.يمكن أن يُرجع DNS عنوان IPv6 اذا كانت العقدة المعطى اسمها قادرة على التعامل ببروتوكول IPv6

.يُرجع DNS عنوان IPV4 فقط اذا كانت العقدة التي تصدر تطلب DNS قادرة فقط على استعمال IPV4

في طريقة حزمة البيانات المزدوجة

- اذا كان المرسل اذا كان المرسل او المستقبل قادر على التعامل ببروتوكول IPV4 فقط فإنه يجب استخدام وحدات بيانات IPV4
- ترسل وحدات بيانات IPV4 الى بعضها البعض في الحالة الموضحة في الشكل ٤-٢٥ صفحة ٢٢٦
- يمكن أن ينسخ حقل البيانات من رزمة بيانات IPv6 الى حقل البيانات من رزمة IPV4 مع عمل تحويل للعناوين
- ومع ذلك فعند رباط التحويل من IPv6 إلى IPV4 سيكون هناك حقول معينة في رزمة بيانات IPv6 ليس لها نظير في IPV4 وبالتالي ستفقد المعلومات الموجودة في تلك الحقول

.هناك طريقة بديلة لحزمة البروتوكولات المزدوجة تعرف باستخدام الأنفاق (tunnles)

- انظر الشكل ٤-٢٦ صفحة ٢٢٧

.تقوم موجهات IPV4 الفاصلة على طول النفق بتوجيه رزمة بيانات IPV4 هذه بيانات تماما مثلما تفعل مع أي رزمة بيانات أخرى دون أن تدرك أن رزمة بيانات IPV4 تلك تحتوي على رزمة بيانات IPv6

.في النهاية تستلم عقدة IPv6 على جنب الاستقبال للنفق رزمة بيانات IPV4 وتدرك أن رزمة بيانات IPV4 تحتوي على رزمة بيانات IPv6 فتنتزع رزمة بيانات IPv6 من أحد جيرانها الذين يتعاملون ببروتوكول IPv6 مباشرة

.يعطي انتشار الأجهزة كهواتف الانترنت والأجهزة النقالة الأخرى دفعا اضافيا لانتشار أوسع ل IPv6

.لقد حدد برنامج شراكة جيل أوروبا الثالث ان يتم اعتماد IPv6 كأسلوب معياري للعنونة للوسائل المتعددة النقالة

.من الدروس التي يمكن أن نتعلمها من IPv6 أنه من الصعب جدا تغيير بروتوكولات طبقة الشبكة

.يشبه تغيير بروتوكولات طبقة الشبكة استبدال أساسات البيت

.الاستخدامات السريعة لبروتوكولات طبقة التطبيقات : الويب والرسائل الفورية ومشاركة النظائر P2P للملفات ،تتضمن أيضا التسجيل الصوتي ،والألعاب الموزعة ،وعرض الفيديو
.يشبه تقديم بروتوكولات جديدة في طبقة التطبيقات إضافة طبقة جديدة من الطلاء الى البيت والتي من السهل نسبيا عملها

خوارزميات التوجيه Routing Algorithms:

.الغرض من خوارزميات التوجيه هو إيجاد مسار جيد بين المصدر الى الوجهة
.أنظر الشكل ٤-٢٧ صفحة ٢٢٩
.للحافة قيمة تمثل تكلفتها ،وقد تعكس تكلفة الحافة الكول الفيزيائي للروابط المقابلة أو سرعة الوصلة او التكلفة النقدية المرتبطة بالرابط