مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (30) العدد (2) 2008
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (30) No. (2) 2008

أمن الشبكات الحاسوبية في الاتصالات المرئية

الدكتور تاج الدين جركس *
الدكتور عدنان معترماوي**
رامي سلطان ***

(تاريخ الإيداع 13 / 1 / 2008. قُبِل للنشر في 2008/3/16)

□ الملخّص □

يتضمن هذا البحث دراسة أهمية التراسل المرئي عبر شبكات الـ IP ، حيث شهدت السنوات الأخيرة ثورة في عالم الاتصالات ، وبدأ جميع الناس باستخدام الحواسب الشخصية والإنترنت في أعمالهم ، وأصبحوا يمضون أوقات فراغهم في الاتصال مع بعضهم عبرها .

كما يتطرق البحث إلى أهم وأكثر البروتوكولات انتشاراً والمستخدمة في هذا المجال ، ويتناولها بدراسة تفصيلية وقد تم التركيز على بروتوكول الـ H323 ، كونه أكثر البروتوكولات انتشاراً والذي تبنته أعداد كثيرة من الشركات التي تؤمن خدمات التراسل المرئي.

تمت دراسة الوسائل والتجهيزات التقليدية المستعملة لحماية المستخدمين من الفيروسات والاختراقات التي تردهم عبر الإنترنت ، والتي من أهمها الجدران النارية و الـNATs و تم بيان عدم التوافق الحاصل بين هذه التجهيزات وبروتوكولات التواصل المرئي .

في النهاية تم تقديم الحل الأمثل لتأمين تواصل مرئي آمن عبر الإنترنت ، باستخدام نموذج الشبكات الخاصة الظاهرية المعدّل ، حيث تم تجميع القنوات المخصصة للتواصل المرئي من ديناميكية واستاتيكية في قناة واحدة لتخترق الجدار الناري والـ NAT ثم ليعاد تفكيكها في النهاية عند الطرفية المشتركة بالاتصال المرئي .

الكلمات المفتاحية : VOIP الفيديو عبر بروتوكول الانترنت .
NAT مترجم عنوان الشبكة .

* أستاذ – قسم هندسة الاتصالات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.
** مدرس – قسم هندسة الاتصالات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.
*** طالب دراسات عليا (ماجستير)– قسم هندسة الاتصالات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (30) العدد (2) 2008
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (30) No. (2) 2008

Security of Computer Networks in Video Communications

Dr. Tajaldeen jarkas*
Dr. Adnan matermawi**
Ramy Soultan***

(Received 13 / 1 / 2008. Accepted 16/3/2008)

□ ABSTRACT □

This research studies video over internet protocols, which are becoming more common. More networks and legacy systems are being connected to public networks, allowing organizations to reduce costs and improve their offerings while allowing users to enjoy a variety of new and advanced services.

The research also studies security as an important consideration when implementing VOIP because each element in the infrastructure is accessible on the network like any computer and can be attacked or used as a launching point for deeper internetwork and inside-the-organization attacks.

I presented a vpn solution which traverses existing infrastructures and can realize connectivity without requiring firewalls and/or NAT devices to be modified even for new protocols or revisions.

Key Words : VOIP, Video over IP protocol, NAT, Network Address Translator .

* **Professor, Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen university, Lattakia, Syria.**
** **Assistant Professor, Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen university, Lattakia, Syria.**
*** **Postgraduate Student, Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen university, Lattakia, Syria.**

مقدّمة:

لعل الضغط المتزايد لتخفيض النفقات التي تستنزف الشركات والمؤسسات يتطلب إيجاد بدائل أقل تكلفة. لنفرض أن شركة لديها عدة مواقع موزعة في أنحاء مختلفة من العالم وتريد إجراء اجتماع تفاعلي ، إن كلفة طيران شخصين من كل موقع من هذه المواقع وبالإضافة لأجور الإقامة ووجبات الطعام لهؤلاء الأشخاص ، تظهر لنا أن البدائل الأقل تكلفة هي الاتجاه العام لهذه الشركات .

مؤتمرات الفيديو والتي هي مجموع إرسالات الصوت والفيديو عبر خط مزدوج بشكل كامل(Full duplex) تمكن الأشخاص في مواقع مختلفة أن يروا ويسمعوا بعضهم كما لو أنهم يتشاركون في محادثات وجهاً لوجه . تُستخدم الكاميرا في كلا الطرفيتين لالتقاط وإرسال إشارات الفيديو ، ويستخدم الميكروفون أيضاً في كِلا الطرفيتين لالتقاط وإرسال الإشارات الصوتية والتي يتم إظهارها عبر مكبرات الصوت . تتم الاتصالات في هذا النمط في الزمن الحقيقي ولايتم تخزين شيء عموماً.

أهمية البحث وأهدافه:

دراسة الـVOIP وأهميته و دوره في تأسيس التواصل المرئي عبر شبكات الـ IP . والمقارنة بين الأنواع المختلفة من بروتوكولات الـ VOIP . كما تم دراسة البروتوكول H.323 وهو أهم النماذج المستخدمة في مجال التواصل المرئي عبر الإنترنت وأكثرها شيوعاً ، والإطلاع على آلية عمله ، و البروتوكولات العاملة تحت مظلته ، وتسلسل استخدامها . ثم دراسة وسائل الحماية التقليدية من جدران نارية و NATs ، وبيان عدم التوافق الحاصل بينها وبين بروتوكولات التواصل المرئي . وأخيراً تم استخدام نموذج الشبكات الخاصة الظاهرية في التقليل من المخاطر التي تتعرض لها الشبكات الداعمة لأساليب التواصل المرئي .

طرائق البحث ومواردة:

تم استخدام شبكة التعليم العالي والبحث العلمي السورية المسماة اختصاراً بـ :

Shern (Syrian High Education Research Network) كمنصة عمل من أجل اختبار وفحص بروتوكولات التواصل المرئي .

كما تم استخدام جدار ناري و NAT من أجل اختبار المظاهر الأمنية المتعلقة ببروتوكولات التواصل المرئي.

1- الفيديو عبر الـIP :

1- 1 - بروتوكولات الـVOIP :

يوجد عدد من البروتوكولات التي قد توَظف من أجل التزويد بخدمات اتصال الـVOIP . سنركز على البروتوكولات الأكثر استخداماً :

نظرياً كل جهاز في العالم يستخدم معياراً يدعى بروتوكول الزمن الحقيقي (RTP) لنقل حزم الصوت والفيديو بين الحواسب المتصلة .

أيضاً الـRTP يعالج مسائل مثل ترتيب الرزم ويزود بالميكانيكيات (عن طريق بروتوكول تحكم الزمن الحقيقي أو RTCP) لمعالجة مسألة التأخير و الـJitter .

قبل أن تستطيع وسائط الصوت والفيديو الجريان بين حاسبين ، يجب أن تطبق بروتوكولات متنوعة لإيجاد الجهاز البعيد وللتفاوض على الوسيلة التي ستجري بواسطتها الميديا (وسائط الصوت والصورة) بين الجهازين. البروتوكولات الأساسية في هذه العملية يشار إليها ببروتوكولات تأشير الاتصال ، والأكثر شهرةً هما H323 وبروتوكول إنشاء الجلسة SIP . وكلاهما يعتمد على بروتوكولات تموين محددة ومعروفة ، RAS (H225.0 مسجل لـITU-T) ،DNS ، TRIP موجود في 3219 RFC ، ENUM موجود في 3762 RFC ، وبروتوكولات أخرى لإيجاد مستخدمين آخرين . [1]

H323 و SIP كلاهما تأصَّلا في 1995 حيث كان الباحثون يبحثون لحل مشكلة كيف يستطيع حاسبين بدء اتصال من أجل تبادل وسائط الصوت والصورة . تمتع الـH323 بأول نجاح تجاري ، بسبب حقيقة أن هؤلاء الذين عملوا على البروتوكول في مؤسسة ITU (الاتحاد الدولي للاتصالات) قد عملوا بسرعة لإنشاء أول معيار في بداية 1996 . من الجهة الأخرى ، تقدم الـ SIP ببطء أكثر في مؤسسة IETF ، مع إنشاء أول مسودة في عام 1996 ، لكن أول معيار ملحوظ أنشء في نهاية 1999 . تمت مراجعة الـSIP عبر السنوات وأعيد إنشاؤه في عام 2002 في الوثيقة 3261 RFC ، وهي المعيار الملحوظ حالياً للـSIP . هذه التأخيرات في المعايير سببت تأخيرات في تبني السوق لبروتوكول الـ SIP . [2] .

عبر السنوات ، كُتبت أوراق كثيرة التي تناقش : SIP مقابل H323 . وما هو المهم حقيقةً : هل يقوم البروتوكول بعمله ؟ الحقيقة هي ، كلاهما يستطيع القيام بالعمل ، على الرغم من أن الـH323 متفوق في عدد من النواحي : أفضل بالتكامل مع شبكات الـPSTN ، دعم أفضل للفيديو ، تكامل ممتاز مع أنظمة الفيديو الكلاسيكية (مثلاً : H320) .

عرّف الذين اقترحوا الـSIP عدد من التعديلات غير المعيارية للـSIP (مثل: SIP-T و SIP-I) ، فضلاً عن عدد من الامتدادات غير المعيارية من أجل حمل المعلومات الضرورية أو للتزويد بالوظائف المطلوبة .

البعض قال إنه توجد تعديلات كثيرة على الـSIP بعدد استعمالاته الكثيرة .

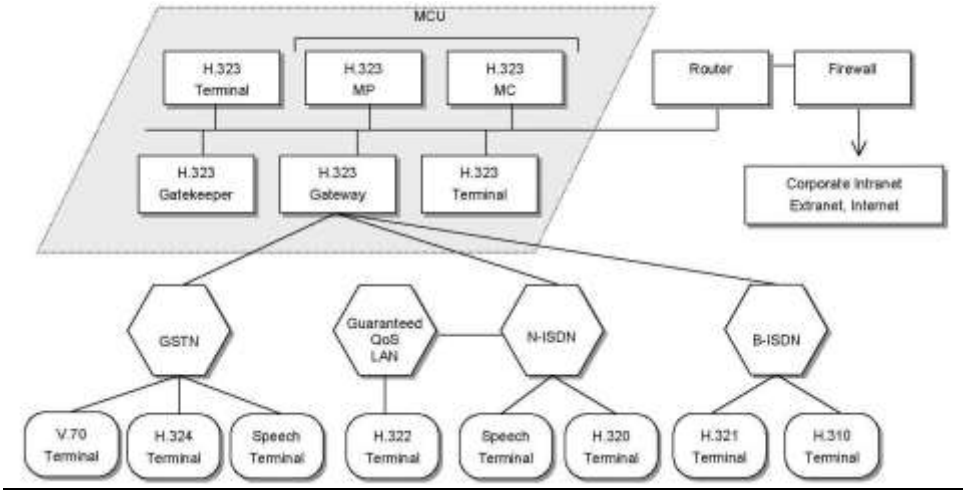
اليوم ، مازال الـH323 يسيطر على معظم تطبيقات الـVOIP في سوق مزودي خدمة نقل الصوت ، خاصةً في عمليات نقل الصوت الدولية . H323 يستخدم أيضاً على نطاق واسع في أنظمة غرف المؤتمرات الفيديوية وهو البروتوكول رقم واحد في أنظمة الفيديو المعتمدة على الـIP . أصبح الـSIP مؤخراً أكثر شيوعاً في أنظمة الـ Instant messaging (التراسل اللحظي) . يمكن أن يشار إلى كِلا الـH323 والـSIP على أنهما " بروتوكولات الطرفيات الذكية " ، مما يعني أن كل الذكاء المطلوب لإيجاد الطرفية البعيدة ولبدء مجاري الميديا بين الجهاز المحلي والبعيد هو جزء مكمل من البروتوكول . [3] .

2-المعيار H323 :

2-1- مقدّمة : يشمل معيار الـH323 اتصالات الصوت ، الفيديو ، المعطيات . عبر شبكات التبديل بالرزم LAN ، الإنترانت الاكسترانت والإنترنت . طور الـH323 للسماح لمنتجات الوسائط المتعددة والتطبيقات من عدّة مصنّعين أن تتفاهم مع بعضها . التوافقية هي الاهتمام الأساسي للمصنّعين والمستخدمين للمنتجات المعتمدة في عملها على الـLAN في الأسواق الاستهلاكية وأسواق الأعمال والترفيه والاحترافية .

يعتبر المعيار H323 بروتوكول مهم لمجال واسع من التطبيقات التفاعلية ، المعتمدة على الـLAN من أجل اتصالات الوسائط المتعددة .

يعالج البروتوكول مسائل متعددة مثل التحكم بالاتصال والجلسة ، إدارة الوسائط المتعددة وعرض الحزمة لمؤتمرات النقطة إلى نقطة و المؤتمرات متعددة النقاط .



الشكل 1 : مجال استخدام المعيار H323

2-2- بنية الـ H323 :

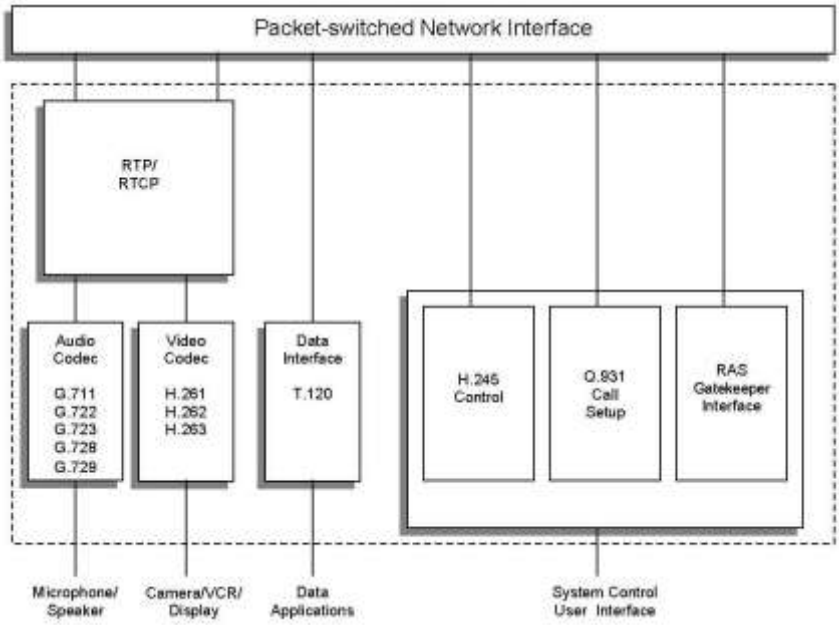
تغطي توصيات الـH323 المتطلبات التقنية لخدمات اتصالات الصوت والصورة عبر شبكات التبديل بالرزم، في حين يرجع الـH323 إلى محددات البروتوكول T.120 من أجل مؤتمرات المعطيات وتمكين المؤتمرات التي تتضمن نقل بيانات، فضلاً عن الصوت والصورة .

لايتضمن مجال اهتمام الـH323 الشبكة بحد ذاتها أو طبقة النقل التي قد تستخدم لربط عدة شبكات مختلفة مع بعضها .

يعرّف الـH323 أربعة مكونات أساسية لنظام الاتصال المعتمد على الشبكة : الطرفيات ، الـGateways ، الـGateKeepers ، وحدات التحكم متعددة النقاط (Mcu) .

الطرفيات: الطرفيات هي عبارة عن نقاط النهاية للزبائن التي تقدم اتصالات في الزمن الحقيقي في اتجاه واحد أو باتجاهين . يجب أن تدعم جميع الطرفيات الاتصالات الصوتية ، الاتصالات المرئية أو المعطيات اختيارية . يحدد الـH323 نماذج التشغيل المطلوبة لطرفيات الصوت ، الصورة ، و/أو المعطيات للعمل مع بعضها .

يجب أن تدعم جميع طرفيات الـH323 البروتوكول :H245 (الذي يستخدم للتفاوض في استخدام القناة وتبادل الإمكانيات) . هناك ثلاثة مكونات إضافية هي : النسخة المحدثة من الـQ931 لتأشير وتأسيس الاتصال ، التسجيل/القبول/الحالة (RAS) وهو بروتوكول يستخدم للاتصال مع الـGateKeeper ، والدعم لـ RTP/RTCP لترتيل رزم الصوت والصورة .

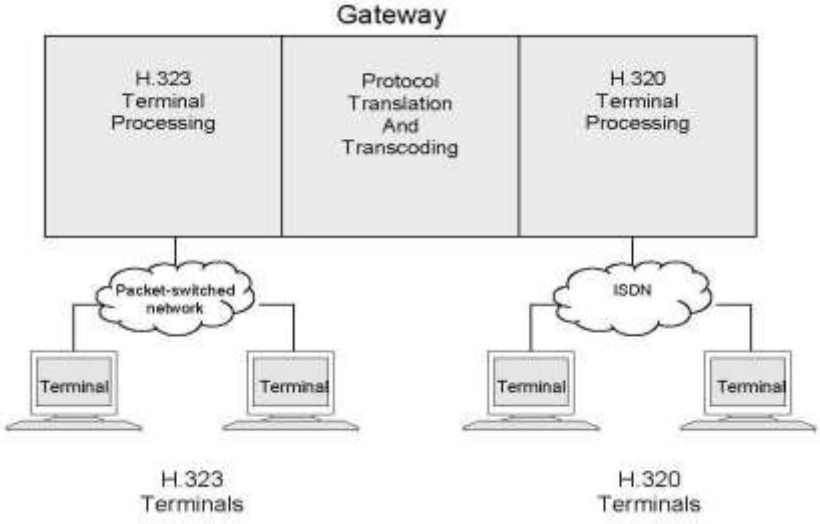


الشكل 2 : مكونات الطرفيات

الـ GateWays : إن الـGateWay هو اختياري في مؤتمر الـH323 . تقدم الـGateWays كثيراً من الخدمات ، تتضمن وظيفة الترجمة بين طرفيات مؤتمر الـH323 و الطرفيات الأخرى . تتضمن هذه الوظيفة الترجمة بين صيغ النقل (بمعنى :H225 إلىH221) وبين إجراءات الاتصال (بمعنى :H245 إلى H242) . بالإضافة ، يترجم الـGateWay أيضاً بين تشفيرات الصوت والصورة ويقوم بتأسيس الاتصال وإنهاءه على كلا جانبي الـLAN والـWAN ، يظهر الشكل 3 الـ GateWay بين H323/H320 .

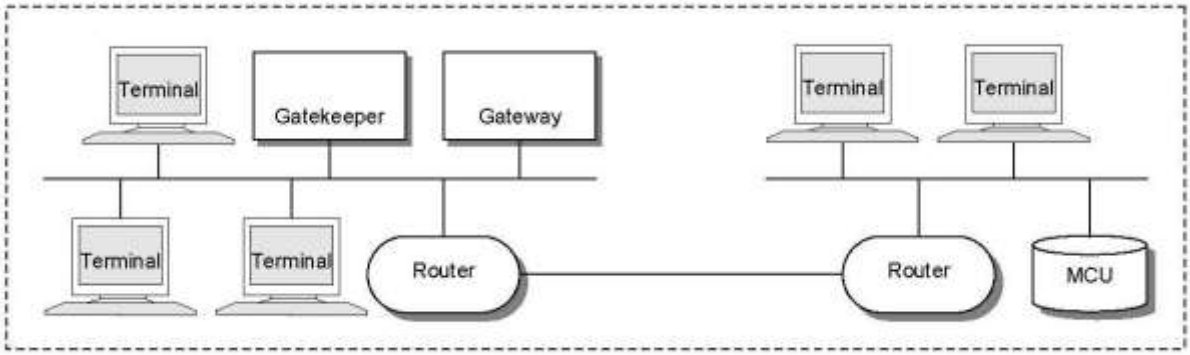
الهدف من الـGateWay هو ترجمة خصائص طرفيات الـH323 إلى طرفيات ليستH323 ، والعكس بالعكس .

تتصل الطرفيات مع الـGateWays باستخدام بروتوكولات الـH245 و Q931 .



الشكل 3 : بوابة عبور لـ H323/H320

الـ GatKeepers : تؤدي الـgateKeepers عدة وظائف مهمة تساعد في تحقيق التكاملية في شبكة معطيات الشركة .الوظيفة الأولى هي الترجمة من أسماء الـH323 للطرفيات و الـGateWays إلى عناوين شبكية ، كما هو معرّف في تحديد الـRAS . الوظيفة التالية هي التحكم بالوصول ، منع جلسات مؤتمرات الفيديو غير المرخّصة . الوظيفة الثالثة هي إدارة عرض الحزمة والذي هو مصمم أيضاً داخل الـRAS . كمثال : إذا حدد مدير الشبكة عتبة لعدد المؤتمرات المتزامنة على الـLAN ، يستطيع الـGateKeeper رفض أي اتصالات إضافية حالما يصل العدد إلى العتبة . الأثر هو تحديد عرض الحزمة الكلي للمؤتمرات إلى جزء محدد من الحجم الكلي المتوفر . السعة الباقية تترك للـEmail ، نقل الملفات ، ونشاطات الـLAN الأخرى . الوظيفة الرابعة هي إدارة عدد من الطرفيات ، GateWays ، MCUs كمجموعة منطقية واحدة تعرف كـ مجال H323 (H323 Zone) .



الشكل 4 : H.323 Zone (مجال الـ H323)

إن الـGateKeeper غير ضروري في نظام الـH323 . لكن إذا تواجد الـGateKeeper ، فإنه من الضروري أن تستخدم الطرفيات خدمات الـGateKeeper . [4] .

الـ Multipoint Control Units(MCU) : تدعم وحدة التحكم متعددة النقاط (MCU) المؤتمرات بين ثلاثة طرفيات أو أكثر . في نظام الـH323 تتكون الـMCU من متحكم متعدد النقاط (MC) ، والذي هو مطلوب، وصفر أو أكثر من معالجات متعددة النقاط (MP) .

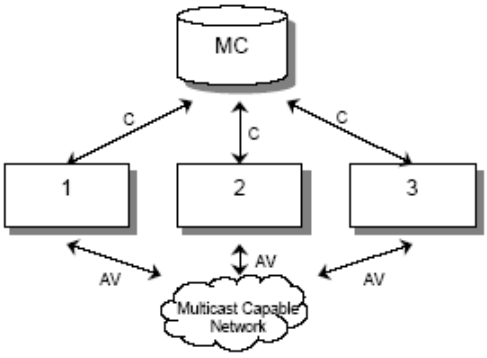
يتولى الـMC مفاوضات الـH245 بين جميع الطرفيات لتحديد الإمكانيات الشائعة لمعالجة الصوت والفيديو. تتحكم أيضاً الـMC بالموارد المخصصة للمؤتمر بتحديد مَن ، إذا وجِدت ، أي من سلاسل الصوت والفيديو من النوع Multicast .

لايتعامل الـMC مباشرةً مع سلاسل الميديا . هذا متروك للـ MP ، الذي يمزج ،يحوّل ، يعالج بيتات الفيديو ، الصوت ، البيانات إن وجدت .

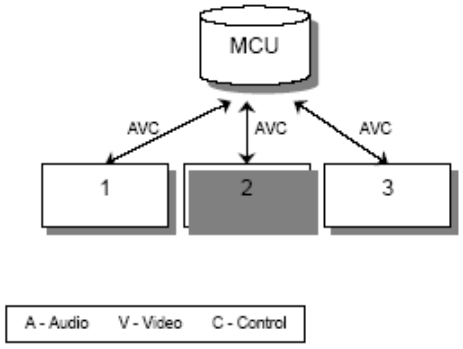
قد تتواجد إمكانيات الـMC والـMP في جهاز مستقل أو قد تكون جزءاً من مكونات الـH323 الأخرى .

المؤتمرات متعددة النقاط : إمكانيات المؤتمر متعدد النقاط يتم تحقيقها بطرق وإعدادات متنوعة تحت الـH323 . تستخدم التوصية مبادىء المؤتمرات المتمركزة وغير المتمركزة كما هي موصوفة في الشكلين 5و6 في الأسفل :

e



الشكل 5 : مؤتمر غير متمركز مع Multicast



الشكل 6 : مؤتمر متمركز مع Unicast

تتطلب المؤتمرات متعددة النقاط المتمركزة وجود MCU لتسهيل المؤتمر متعدد النقاط . جميع الطرفيات ترسل سلاسل الصوت،الفيديو ،المعطيات، التحكّم إلى الـMCU بشكل نقطة إلى نقطة . تدير الـMC المؤتمر بشكل مركزي باستخدام وظائف التحكم H245 والتي تعرّف أيضاً الإمكانيات لكل طرفية . تقوم الـMP بوظائف مزج الصوت ، توزيع المعطيات ، و تبديل/مزج الفيديو المؤداة نموذجياً في المؤتمرات متعددة النقاط وترسل السلاسل الناتجة عائدةً إلى الطرفيات المشاركة . قد تقدم الـMP التحويل بين الشيفرات المختلفة ومعدلات البيت وقد تستخدم الـMulticast لتوزيع الفيديو المعالَج . الـMCU النموذجي الذي يدعم المؤتمرات متعددة النقاط المتمركزة يحتوي على MC و MP خاص بالصوت والفيديو والمعطيات .

المؤتمرات متعددة النقاط غير المتمركزة تستخدم تقانة الـMulticast . طرفيات الـH323 المشاركة تقوم بـMulticast للصوت والفيديو للطرفيات الأخرى المشاركة بدون ارسال المعطيات إلى الـMCU . لاحظ أن معطيات التحكم متعددة النقاط مازالت تعالَج مركزياً من قبل الـMC ، ومعلومات قناة التحكم H245 مازالت ترسَل بنموذج نقطة إلى نقطة إلى الـMC . [5] .

2-4-الاتصالات تحت مظلّة الـH.323 :

يمكن اعتبار الاتصالات تحت الـH323 كمزيج من رزم الصوت والفيديو والمعطيات والتحكم . الإمكانيات الصوتية ، تنصيب اتصال الـQ931 ، التحكم RAS ، وتأشير الـH245 كلها مطلوبة . جميع الإمكانيات الأخرى ، بما فيها مؤتمرات الفيديو والمعطيات هي اختيارية .

عندما تكون هناك عدّة خوارزميات ممكنة ، الخوارزميات المستخدمة في المشفر تشتقّ من المعلومات العابرة عبر مفكك الترميز خلال عملية تبادل إمكانية الـH245 . طرفيات الـH323 أيضاً قادرة على العمل غير المتماثل (خوارزميات تشفير وفك تشفير مختلفة) وتستطيع أن ترسل/تستقبل قنوات صوت وفيديو متعددة .

التحكّم : وظائف التحكم بالاتصال هي قلب طرفية الـH323 . يتم تقديم التحكم بالنظام كاملاً عبر ثلاث قنوات تأشير منفصلة : قناة التحكم H245 ، قناة تأشير الاتصال Q931 ، وقناة الـRAS . وظائف التحكم تتضمن التأشير لتنصيب الاتصال ، تبادل الإمكانية ، تأشير الأوامر والدلائل والرسائل لفتح ووصف محتوى القنوات المنطقية . جميع

إشارات التحكم والصوت والصورة تمر عبر طبقة تحكم التي تصيغ سلاسل المعطيات في رسائل لإخراجها عبر منفذ الشبكة . تحدث العملية العكسية للسلاسل القادمة .

قناة التحكم H245 هي قناة موثوقة والتي تحمل رسائل التحكم والتي تقود تشغيل كيان الـH323 ، متضمنةُ تبادل الإمكانيات ، فتح وإغلاق القنوات المنطقية ، طلبات الأفضلية ، رسائل التحكم بالجريان ، والدلائل والأوامر العامة . تبادل الإمكانيات هو واحد من الإمكانيات الأساسية في توصية الـITU ، يقدم الـH245 إمكانيات إرسال وإستقبال منفصلة فضلاً عن طرائق لوصف هذه التفاصيل لطرفيات الـH323 الأخرى . يوجد قناة تحكم H245 واحدة فقط بين أي طرفيتين .

قناة تأشير الاتصال تستخدم Q931 لتأسيس اتصال بين طرفيتين . وظيفة تأشير الـRAS تؤدي عملية التسجيل ، القبول ، تغيرات عرض الحزمة ، الحالة ، وإجراءات الانفصال بين الطرفيات والـGateKeepers . لاتستخدم الـRAS إذا لم يكن الـGateKeeper موجوداً .

الصوت : تحتوي الإشارات الصوتية على الكلام الرقمي والمضغوط . خوارزميات الضغط المدعومة من قبل الـH323 جميعها معايير ITU قياسية . يجب أن تدعم طرفيات الـH323 معيار الصوت G711 لضغط الكلام . دعم معايير ITU صوتية أخرى اختياري .

توصيات الـITU المختلفة لترقيم وضغط الإشارات الصوتية تعكس مستويات مختلفة بين نوعية الكلام ، معدل البيت ، استطاعة الحاسب ، وتأخير الإشارة . ينقل الـG711 بشكل عام الصوت بمعدّل 56 أو64Kbps . يعمل الـG723 بمعدّلات بيت منخفضة جداً ، وهو مرمّز صوتي مشهور في تطبيقات الـH323 .

طرفيات الـ H323 الأكثر قوة تستطيع استعمال المرمّز عالي النوعية G728 16Kbps .

تدعم أيضاً أنظمة غرف الـH323 المرمّز- G722 لنوعية صوتية فائقة .

الفيديو : بينما الإمكانيات الفيديوية اختيارية ، أي طرفية H323 ممكَّنة الفيديو يجب أن تدعم مرمّز H261 (دعم الـH263 اختياري) .

يتم تبادل معلومات الفيديو بمعدّل لايزيد عن ذلك الذي تمّ اختياره خلال عملية تبادل الإمكانيات . الـH261، والذي يقدّم مقياس التوافقية عبر توصيات ITU مختلفة يستَخدم في قنوات الاتصال التي هي من مضاعفات الـ 64 Kbps .

تطبيقات الـH261 المرنة تعطي إمكانية توليد أي معدّل بيت ، حتى ولو كانت ليست من مضاعفات الـ 64 Kbps . يزيد هذا النوع من المرمّزات نوعية الفيديو في الكثير من الحالات . كمثال: تتواجد جلسة بـKbps 128 ويستخدم فيها الـG728 للصوت ، سيتوافر أكثر من 100 Kbps للفيديو (اعتماداً على معدّلات المعطيات) .

الـH263 هو تحديث للـH261 متوافق مع سابقيه. نوعية صورة الـH263 محسّنة بشكل كبير باستخدام تقنية توقّع الحركة ، وجدول تشفير هوفمان المحسّن من أجل معدّل نقل بيت منخفض . يعرّف الـH263 خمسة معايير لصيغ الصورة . الاتصالات بين أنظمة الـH261 وأنظمة الـH263 مسهّلة لأن كلاهما يجب أن يدعم الـQCIF .إذا كانت طرفية الـH323 تدعم كلا المرمزَين :H261 و الـ H263 ، فمن المستحسن استخدام الـH263 للمحادثات منخفضة معدّل البيت والـH261 للجلسات مرتفعة معدّل البيت . استخدام معدّل بيت معيّن يعتمد على المواصفات الخاصة بالمصنّع ومتطلبات التطبيقات . ميزة المرمزات المعتمدة على الـHardware هي إمكانيتها لدعم معدّل بيت ومعدّل إطار عاليين في صيغ صورة كبيرة : CIF, 4CIF, 16CIF ، كما في الجدول 1.

(الجدول 1) صيغ صور الـITU لمؤتمرات الفيديو

ITU Image Formats for Videoconferencing

Videoconferencing Picture Format	Image Size in Pixels	H.261	H.263
Sub-QCIF	128 x 96	Optional	Required
QCIF	176 x 144	Required	Required
CIF	352 x 288	Optional	Optional
4CIF	702 x 576	N/A	Optional
16CIF	1408 x 1152	N/A	Optional

المعطيات : مؤتمرات المعطيات هي إمكانية اختيارية . عندما يتم دعمها ، تمكّن مؤتمرات المعطيات عملية التعاون عبر التطبيقات مثل الألواح البيضاء المشتركة ، مشاركة التطبيقات ، نقل الملفات .

تدعم الـH323 مؤتمرات المعطيات عبر بروتوكول الـT.120 ، وهو معيار ITU ، يحلّ الـT.120 مسألة مؤتمرات المعطيات من نقطة إلى نقطة والمؤتمرات متعددة النقاط . وهو يقدّم التعاونية بين التطبيق والشبكة وطبقة النقل . [6] .

3- Internet Firewalls و الـ NATs :

3-1- ما هو الجدار الناري في الشبكة : الجدار الناري هو نظام أو مجموعة من الأنظمة التي تفرض سياسة تحكم بالوصول بين شبكتين أو مجموعة من الشبكات . الوسائل الفعلية التي يتم إنجاز ما سبق بوساطتها تختلف فيما بينها كثيراً ، لكن بشكل أساسي ، يمكن التفكير بالجدار الناري كزوج من الميكانيكيات : واحد موجود من أجل إيقاف النقل ، والآخر موجود من أجل السماح بالنقل . تضع بعض الجدران النارية تركيزاً أكبر على إيقاف النقل ، بينما تركِّز الأخرى على السماح بالنقل . ربما الشيء الأكثر أهمية الذي يجب تمييزه حول الجدران النارية هو أنها تطبق سياسة تحكّم بالوصول . إذا لم يكن لديك فكرة جيدة عن نوع الوصول الذي تريد أن تسمح به أو تتجاهله ، فإن الجدار الناري لن يساعدك بالفعل . من المهم أيضاً أن تميِّز أن إعدادات الجدار الناري ، تفرض سياستها على كل ماهو خلفها . [7] .

3- 2 - منافذ الـTCP والـUDP :

3-2-1- المنافذ : المنفذ هو "حيز وهمي Virtual Slot " في هيكلية الـTCP و الـUDP خاصتك والتي تستخدم لترتيب الربط بين مضيفين ، وأيضاً بين طبقة الـTCP/UDP والتطبيقات الفعلية التي تعمل على هذه المضيفات .

إنها مرقَّمة من 0 إلى 65535 ، حيث يشار إلى المجال 0 إلى 1023 بالمحفوظ أو المميَّز ، والبقيَّة (1024-65535) بالديناميكية أو غير المميزة .

يوجد بالأساس استخدامين أساسيين للمنافذ :

- " الاستماع" على المنفذ . ويستخدم هذا من قبل تطبيقات المخدِّم التي تنتظر المستخدمين للاتصال بها ، للحصول على خدمة معروفة جيداً ، كمثال HTTP (TCPمنفذ80) ، Telnet (TCPمنفذ23) ، DNS (UDP وأحياناًTCP على منفذ53) .

- فتح منفذ " ديناميكي" : كِلا طرفي اتصال الـTCP يحتاج لأن يتم تعريفه بعناوين IP وأرقام منفذ . لهذا السبب ، عندما تريد " الاتصال " بعملية على المخدِّم ، فإن طرفك من قناة الاتصالات يحتاج أيضاً إلى " منفذ " . يتم ذلك باختيار منفذ أعلى من 1024 على آلتك وليس موضوع حالياً في الاستخدام من قبل قناة اتصالات أخرى ، وتستخدمها كـ" مرسل " في الاتصال الجديد

يمكن أيضاً استخدام المنافذ الديناميكية كـ منافذ " مستمعة " في بعض التطبيقات ، والأكثر ملاحظةً هو الـFTP .

المنافذ في المجال 0–1023 هي تقريباً دائماً منافذ للمخدِّم . المنافذ في المجال 1024–65535 هي عادةً المنافذ ديناميكية (بمعنى: تُفتَح ديناميكياً عندما تتصل مع منفذ مخدِّم) . لكن ، يمكن استخدام أي منفذ كـ منفذ مخدِّم ، ويمكن استخدام أي منفذ كمنفذ خروج . لذلك ، لكي نوجز ، هذا مايحدث في عملية اتصال أساسي :

- في لحظة ما من الزمن ، تطبيق مخدِّم على المضيف 1.2.3.4 يقرر " الاستماع " على المنفذ 80 (HTTP) لاتصالات جديدة
- أنت (5.6.7.8) تريد أن تتواصل مع 1.2.3.4 منفذ 80 ، ويقوم المستعرض الخاص بك بطلب إنشاء اتصال إليه .
- طلب الاتصال ، يدرك أنه لايملك بَعد رقم منفذ محلِّي ، ويذهب ليصطاد واحداً . إن رقم المنفذ المحلِّي ضروري حيث إنه عندما تأتي الردود في وقت ما مستقبَلاً ، على هيكلية الـ TCP/IP الخاصة بك يجب أن تعرف إلى أي تطبيق يجب أن تمرر الرد إنها تفعل ذلك بتذكُّر أي تطبيق يستخدم أي رقم منفذ محلِّي .
- هيكلية الـTCP خاصَّتك تجد منفذ ديناميكي غير مستخدم ، عادةً في مكان ما فوق 1024 . لنفرض أنها وجدته وكان 1029 .
- ثم سيتم إرسال أول رزمة لك ، من الـIP المحلِّي 5.6.7.8 على المنفذ 1029 ، إلى 1.2.3.4 على المنفذ 80 .
- يستجيب المخدِّم برزمة من 1.2.3.4 منفذ 80 ، إليك 5.6.7.8 منفذ 1029 .

3–2–2–كيف أعرف أي تطبيق يستخدم أي منفذ : هناك العديد من القوائم التي تبيِّن الـ المنافذ " المحفوظة " و" المعروفة جيداً " .

بالإضافة إلى المنافذ " المستخدمة بشكل شائع " ، وأفضل قائمة موجودة في الموقع [10] .

هذه اللوائح لاتضع أي نوع من الدساتير لتحديد رقم المنفذ والوظيفة الموافقة له .

نعبِّر عن ذلك بقولنا : لا توجد طريقة للتحديد الفعلي لرقم المنفذ ووظيفته الموافقة بالنظر إلى اللائحة ببساطة.

3–2–3– المنافذ الآمن عبورها للجدار الناري :

في الواقع . لاتستطيع أن تتأكد أي المنافذ آمنة بالنظر ببساطة إلى رقمها ، لأن الرقم هو كل ما يحتاجه المهاجم ليبني هجومه ، حيث يكفي حصوله على الرقم ذو الـ 16 Bit ليهجم من خلاله .

يعتمد أمن المنفذ على التطبيق الذي ستصل إليه عبر ذلك المنفذ . اعتقاد خاطىء هو أن المنفذ 25 (SMTP) و 80 (HTTP) آمنَين للعبور عبر الجدار الناري . فقط لأن الجميع يستخدمه لايعني أنه آمن .

إذا كنت تستخدم مخدِّم ويب مكتوب جيداً ، وقد تمَّ تصميمه من البداية ليكون آمناً ، فإنك قد تستطيع أن تشعر بمسؤولية وتتأكد أنه من الآمن السماح للناس في الخارج بالوصول إليه عبر المنفذ 80. و إلا فإنك لا تستطيع .

المشكلة هنا ليست في طبقة الشبكة ، إنما في كيفية معالجة التطبيق للمعطيات التي يستقبلها . قد يتم استقبال هذه المعطيات عبر المنفذ 80 أو المنفذ 666 ، خط تسلسلي ، القرص المرن أو أي طريق آخر . إذا كان التطبيق غير آمن ، فليس المهم كيف تصل المعطيات إليه . إن الخطر الحقيقي يتوضع في معطيات التطبيق .

إنها مسألة أمن التطبيق أكثر من مسألة أمن الجدار الناري . قد يجادل أحد ما أنه على الجدار الناري إيقاف كل الهجمات المحتملة ، لكن مع عدد بروتوكولات الشبكات الجديدة ، الغير مصممة مع اعتبار الأمن في الحسبان ، مثل الـH323 يصبح من المستحيل على الجدار الناري الحماية ضد الهجمات المرتكزة على المعطيات. [8] .

3-3 - تجهيزات ترجمة عنوان الانترنت (NATs) :

إن الـNAT هو بروتوكول ، والذي بوساطته تستخدم الـLAN حزمة واحدة من عناوين الـIP للاتصالات الداخلية (داخل LAN الشركة) وعنوان مختلف للاتصال مع الشبكة الخارجية ، مثل الانترنت . إنها توفر حلاً من أجل مسألتين أساسيتين :

- أمان الشبكة : إن عناوين الـIP الداخلية مخفية عن المستخدمين الخارجيين . هذا يساعد في حماية حواسب الشبكة من المهاجمين .
- العدد المحدود من عناوين الـIP المتوفرة : إن عدد عناوين الـIP العمومية محدود . بتعريف عناوين من أجل الاستخدام الداخلي فقط ، تستطيع الشركة أن تستخدم عدد كبير من العناوين المختلفة بدون أن تتضارب مع العناوين المستخدمة في مكان آخر .

داخل الـNAT ، تمتلك العقد عناوين داخلية والتي لايمكن الوصول إليها أصلاً من العقد التي في الخارج . بدون وسيلة اختراق ، العقد الداخلية لاتستطيع استقبال النداءات والاتصالات من العقد الخارجية . حتى ولو بدأت العقدة داخل الـNAT بإنشاء الاتصال ، فإنها لاتستطيع أن تستقبل الجواب – إن الجواب بهذه الحالة يتم إرساله إلى عنوان IP غير قابل للتدوير (Nonroutable) .

جهاز الـNAT يربط عناوين الـIP العمومية مع عناوين الـIP الخاصة و المنافذ . إنها أيضاً تخصص المنافذ للعقد داخل شبكتها ، لكن عناوين الـIP الخاصة تبقى غير معروفة من قبل المستخدمين الخارجيين .

لتمكين الاتصال الخارجي ، فإن جهاز الـNAT يفتح قناة إلى الشبكة العمومية . يُلحِق الـNAT عنوان الـIP العمومي بجميع رزم المعطيات المرسلة إلى خارج الشبكة . وبالمثل ، للمعطيات القادمة ، يبدل جهاز الـNAT عنوانه العمومي بالعنوان الداخلي المربوط معه .

عادةً ، تخصيصات الـNATs تستمر لفترة قصيرة من الزمن ثم يتم تحريرها . من المهم أن تبقى تخصيصات الـNAT شرعية خلال فترة فتح الارتباط . لإنجاز هذا ، أي عقدة تتصل عبر جهاز NAT يجب أن ترسل رزمة " Keep-alive " على فترات لمنع إعادة الربط خلال جلسة اتصال مفتوحة . [9] .

4- تطبيق مؤتمر فيديو باستخدام البروتوكول H.323 :

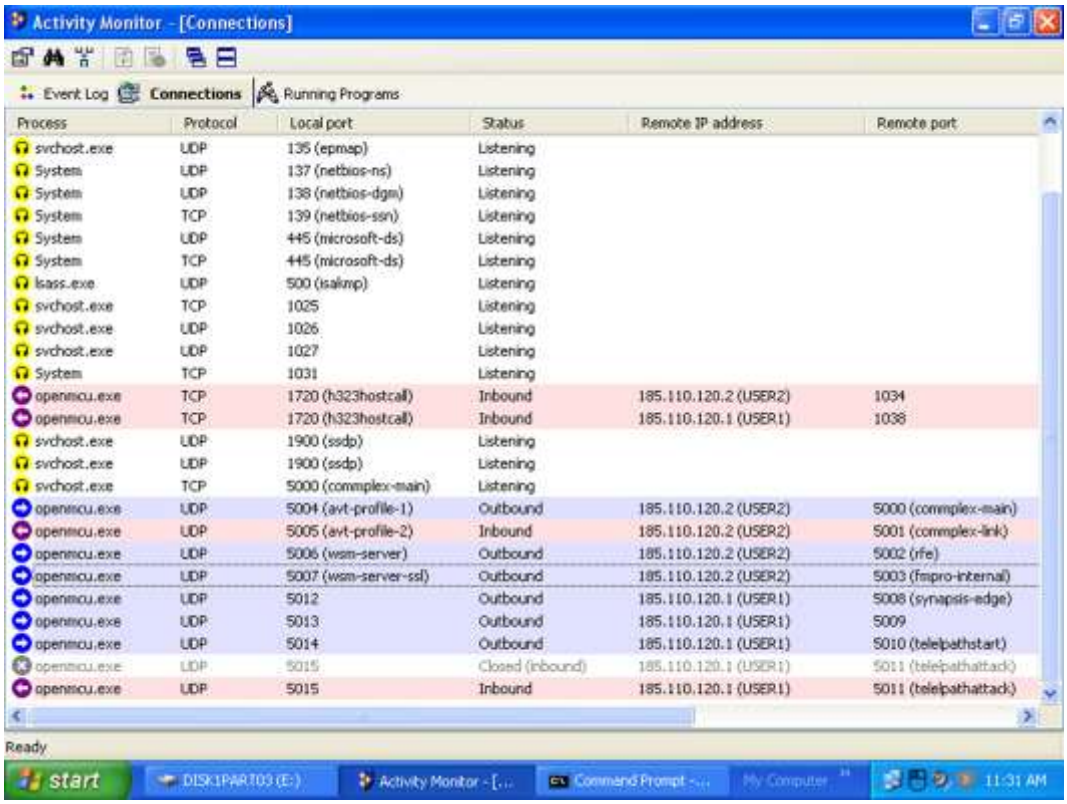
لدينا ثلاثة حواسب ، تمَّ تنصيب برنامج المخدِّم على واحد ، و تنصيب برنامج الزبون على الاثنين الباقيين . وتمَّ تشكيل مؤتمر صوتي فيديوي بين الزبونين ، حيث تمَّ تجهيز كل منهما بسماعات و مايكروفون للصوت ، و كاميرا للصورة .

تمَّ تشغيل وربط الحواسب مرَّ تين ، و أُخذَت نتائج برنامج مراقبة المنافذ الذي تمَّ تنصيبه على كل جهاز من الأجهزة الثلاثة user1 ، user2 ، user3 ، من أجل تحديد المنافذ المنشأة والمفتوحة في كل مؤتمر .

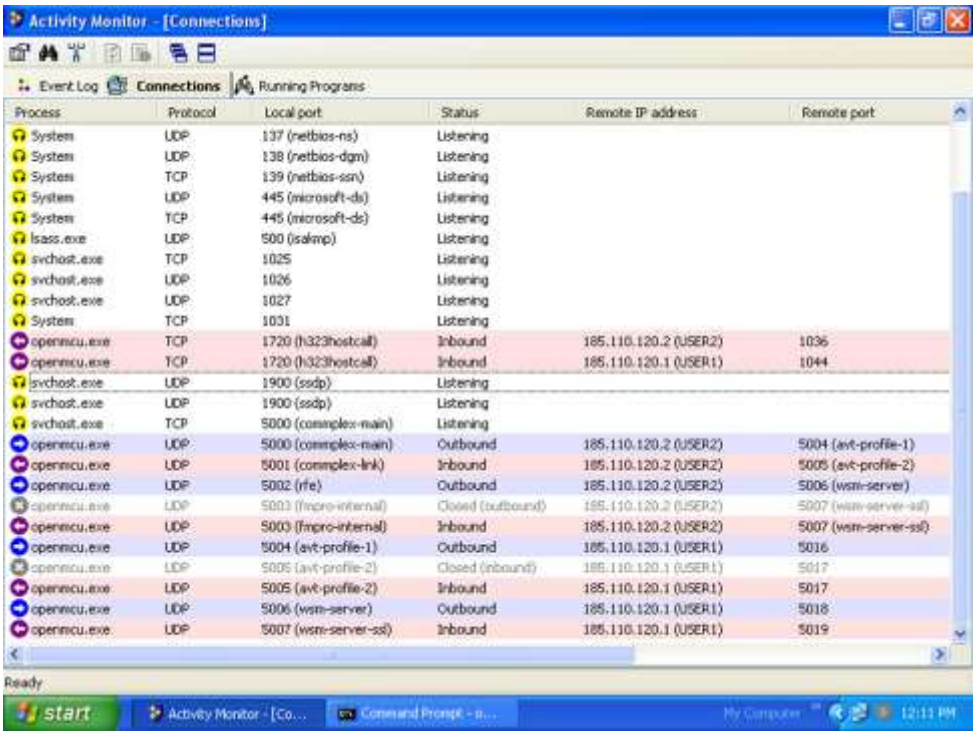
إن user3 هو المخدِّم ، بينما user1, user2 فهي حواسب الزبائن . خصص المخدم خمسة قنوات لكل من user1 و user2 ، قناة واحدة استاتيكية على المنفذ 1720 والقنوات الأربعة الباقية ديناميكية .

عدد المنافذ المفتوحة على المخدم user3 أصبحت عشر قنوات لتأمين اتصال صوتي فيديوي بين user1 و user2 .

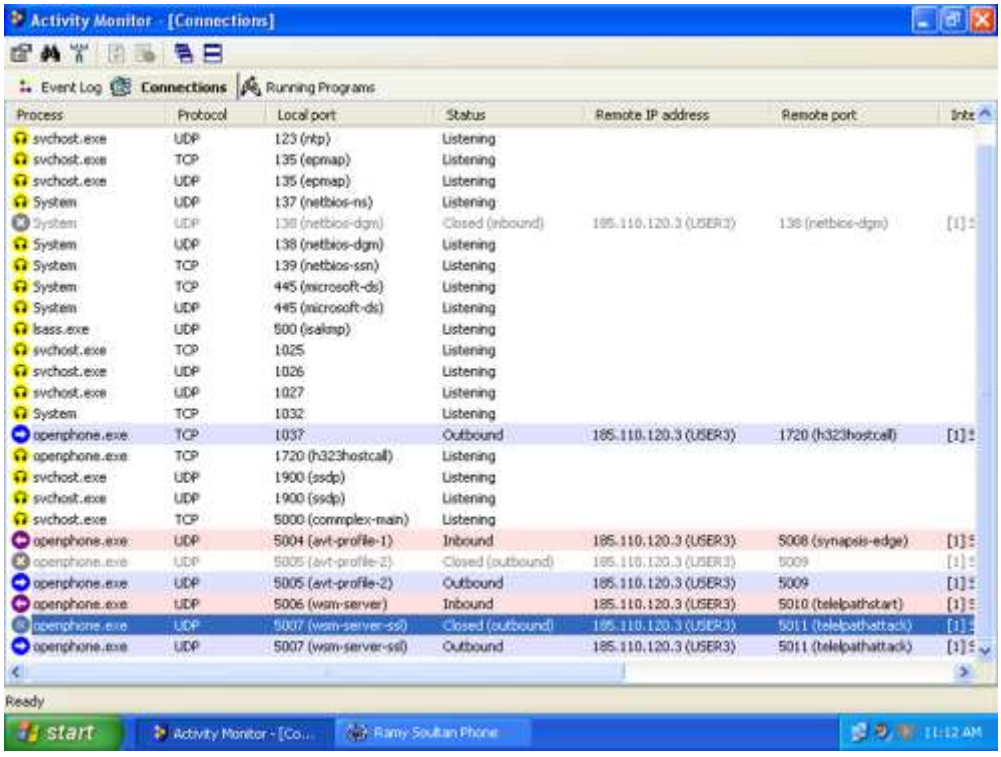
فيما يلي النتائج : كما أخذت من على شاشة الحواسب الثلاثة والتي تمثل المخدم و المستخدمَين .



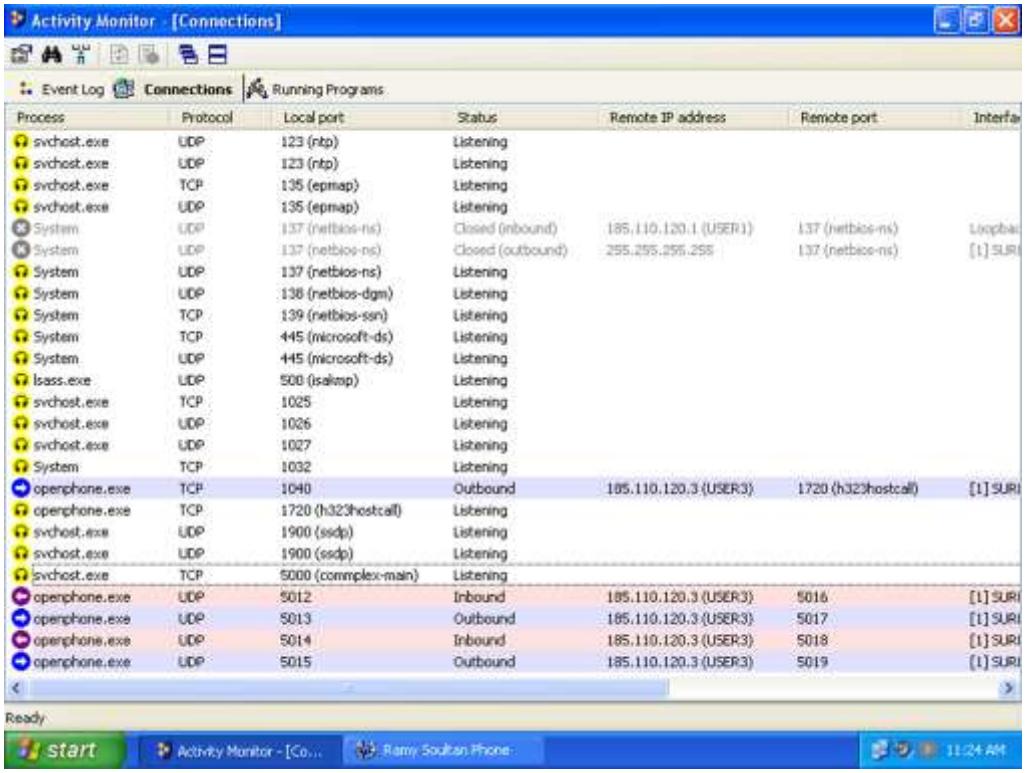
الشكل 7 : الاختبار الأول على الـ user3 (المخدِّم) ، برنامج المخدِّم هو OpenMCU.exe ، عنوان المخدِّم هو 185.110.120.3



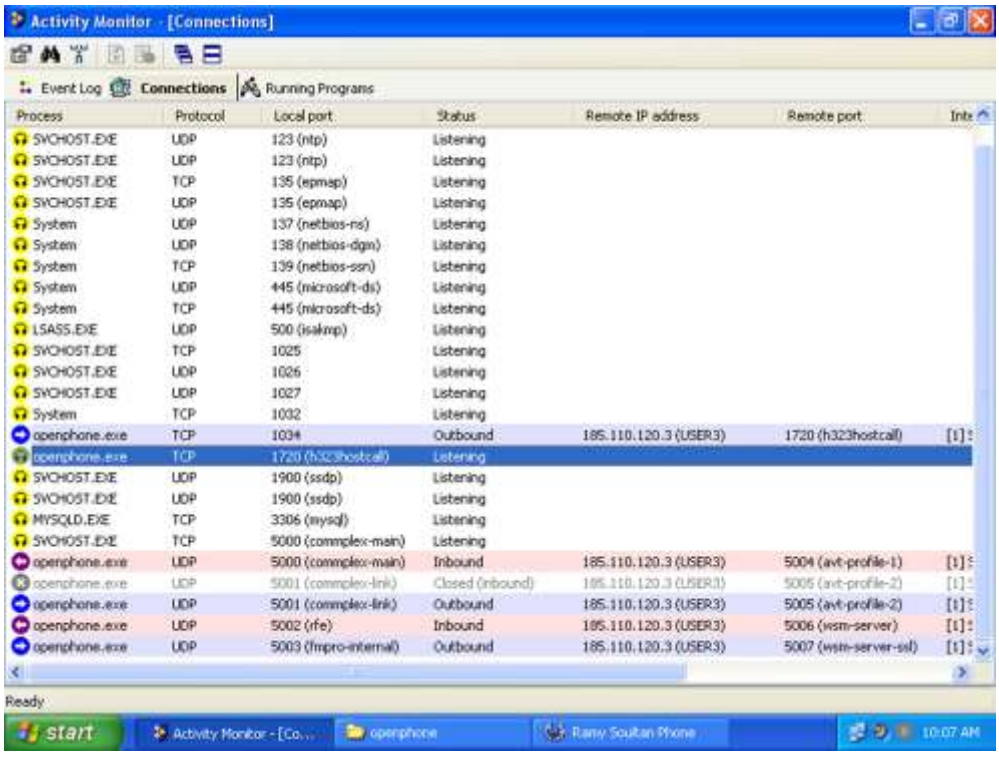
الشكل 8 : الاختبار الثاني على الـ user3 (المخدِّم)



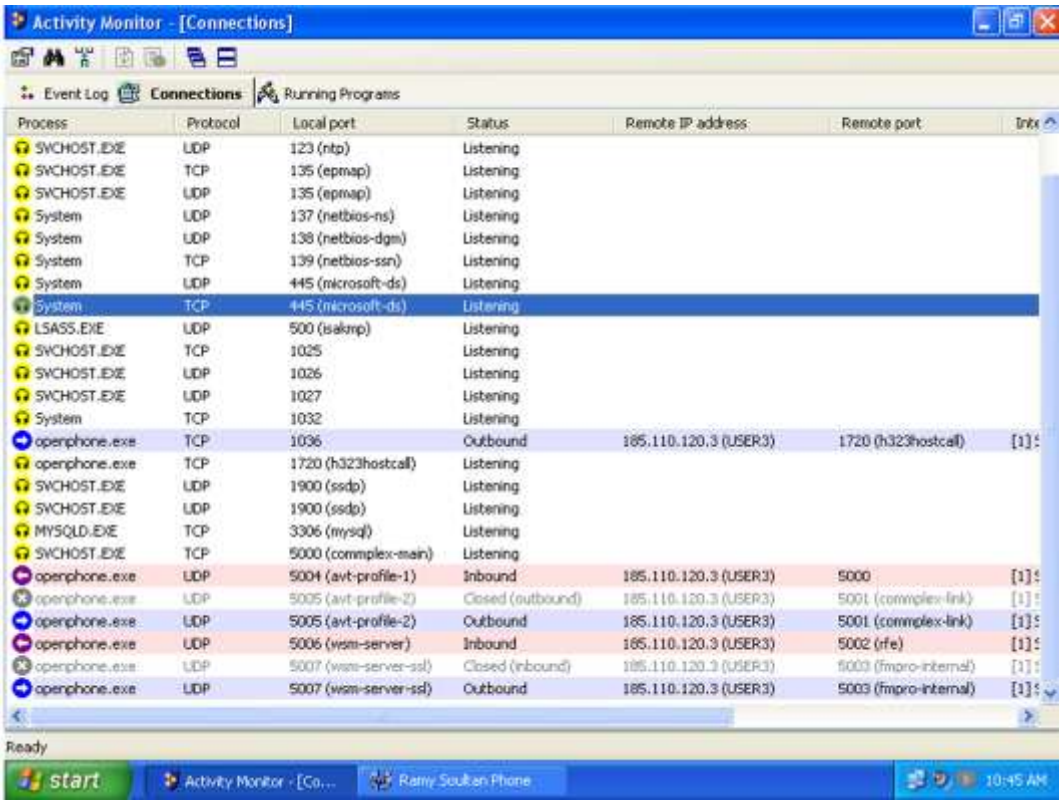
الشكل 9 : الاختبار الأول على الـ user1 (الزبون) ، برنامج الزبون هو Openphone.exe ، عنوان الحاسب هو 185.110.120.1



الشكل 10 : الاختبار الثاني على الـ user1 (الزبون)



الشكل 11 : الاختبار الأول على الـ user2 (الزبون) ، برنامج الزبون هو Openphone.exe ، عنوان الحاسب هو 185.110.120.2



الشكل 12 : الاختبار الثاني على الـ user2 (الزبون)

يمكن تلخيص خطوات إنشاء اتصال فيديوي باستخدام البروتوكول H.323 بالجدول2 ، والذي يقسم إلى قسمين الأول إجباري في الأعلى من أجل الاتصال ونجد فيه :

- اتصال UDP استاتيكي على المنفذ 1719 لاستكشاف الـ GateKeeper باستخدام بروتوكول RAS .
- اتصال TCP استاتيكي على المنفذ 1720 لتأسيس الاتصال باستخدام Q931 .
- اتصال TCP ديناميكي على المنفذ (1024–65535) من أجل تبادل بارامترات الاتصال باستخدام البروتوكول H.245
- اتصال UDP ديناميكي على المنفذ (1024–65535) من أجل تراسل معطيات الفيديو باستخدام الـRTP
- اتصال UDP ديناميكي على المنفذ (1024–65535) من أجل تراسل معطيات الصوت باستخدام الـRTP
- اتصال UDP ديناميكي على المنفذ (1024–65535) من أجل نقل معلومات التحكُّم باستخدام الـ RTCP

والثاني اختياري يمكن إضافته إلى حزمة البروتوكول H.323 من أجل ميزات إضافية .

الجدول 2 – المنافذ والبروتوكولات المستخدمة في المؤتمر المرئي

Port	Type	Protocol	Description
Common/Required			
1719	Static	UDP	Gatekeeper RAS
1720	Static	TCP	Q.931 (Call Setup)
1024-65535	Dynamic	TCP	H.245 (Call Parameters)
1024-65535	Dynamic	UDP (RTP)	Video Data Streams
1024-65535	Dynamic	UDP (RTP)	Audio Data Streams
1024-65535	Dynamic	UDP (RTCP)	Control Information
Optional			
389	Static	TCP	ILS Registration (LDAP)
1002	Static	TCP	Site Server Registration (Windows 2000 Built-in LDAP)
1503	Static	TCP	T.120 (Data Channel)
1718	Static	UDP	Gatekeeper Discovery (requires multicast address 224.0.1.41)
22136	Static	TCP	VCON MXM - Remote VCON Endpoint Admin
26505	Static	TCP	VCON MXM - Remote Console Login

5- تأثير الجدران النارية و الـ NATs في مؤتمرات الفيديو عبر H.323 :

بالمقارنة مع بروتوكولات اتصالات المعطيات الأخرى مثل HTTP و FTP فإن للـH.323 خصائص فريدة و التي تسبب صعوبات في بيئات الشركات المحمية بالجدران النارية و بالـ NATs .

1. النقل في H.323 يتضمَّن طمر عنوان الـIP للمرسل داخل رزم البيانات . مستقبل النداء يرسل الصوت والفيديو عائدةً إلى المستخدم البادئ على عنوان الـIP المطمور بالإرسالات الأصلية . إذا كان عنوان الـIP خاصاً ، فإن الـRouters الخاصة بالانترنت ستستبعد نموذجياً رزم الصوت والفيديو المرسلة من الطرفية الخارجية لأنه تمَّ إرسالها إلى عنوان IP خاص ليس Routable .
2. خلال اتصالات الـH.323 ، بارامترات عديدة للبروتوكول ، متضمنةً قيم المنفذ للـIP ، يتم تحديدها ديناميكياً خلال مفاوضات إنشاء الاتصال بدلاً من أن تكون محددة مسبقاً . هذا يشكل مشكلة في التجهيزات الأمنية مثل الجدران النارية ، والتي عادةً تتطلب مخططاً أمنياً يعتمد على فتح منافذ معروفة ومحددة .
3. يتطلَّب استخدام اتصال الصوت والفيديو للـH.323 من الجدار الناري أن يفتح مجالاً عريضاً من المنافذ بحيث يستطيع النقل أن يمر دون إعاقة . بروتوكولات اتصالات الصوت والفيديو عبر الـIP تتطلَّب عدَّة منافذ مفتوحة لتستقبل رسائل التحكُّم بالاتصال ولتؤسس قنوات معطيات الصوت والفيديو . أرقام المنافذ الإضافية هذه يتم تحديدها ديناميكياً ، وليس مسبقاً . لذلك ، فإنه يجب على مديري الشبكة أن يفتحوا جميع المنافذ للجدار الناري للسماح لنقل الـH.323 بالمرور . وهذا يشكِّل خرقاً للغاية من الجدران النارية ، والتي تفضِّل إغلاق قدر ما تستطيع من المنافذ .

في أغلب الشركات ، الجدران النارية معدَّة لتحدَّد بصرامة أنواع نقل المعطيات المتجهة إلى الداخل و التي سوف تصل إلى حواسب المستخدمين الداخليين ، ومخدِّماتهم ، ومعداتهم المحيطية .

تدعم الجدران النارية العديد من البروتوكولات المختلفة ، ولكنها غير متخصصة في اتصالات الـH.323 . وهذا قد يسبب اختلافات في مستوى الدعم للـH.323 بين الجدران النارية لمصنِّعين مختلفين . وهذا يسبب فشل اتصال عرضي .

تفرض أيضاً الـNATs عوائق على اتصالات الصوت والفيديو عبر الـIP . تخصص الـNATs عناوين IP خاصة للحواسب والمخدِّمات المتواجدة ضمن حدود LAN خاصة . لكن معظم تجهيزات الـRouting التي تتحكم بجريان المعلومات عبر الإنترنت تستطيع أن ترسل المعطيات فقط إلى التجهيزات التي تمتلك عناوين IP عمومية وقابلة للتدوير Routable . عناوين المستخدمين في الشبكات المحمية بالـNAT غير معروفة للتجهيزات على الجانب العمومي من الـNAT .

تعيق الـNATs أيضاً اتصالات الـH.323 والتي يتم تأسيسها من قبل مستخدمي الـLAN الخاصين إلى الجانب العمومي . كما أشير سابقاً ، عنوان الـIP للمرسل موجود داخل إرسالات الصوت والفيديو . إذا كان هذا العنوان ليس Routable ، فإن أي إرسال عائد سوف لن يخترق الشبكة المحمية بالـNAT . المستخدم الذي يقع خلف الـNAT سوف لن يستقبل أبداً الصوت والفيديو من المستخدم على الجانب العمومي .

6- تطبيق مؤتمر فيديو آمن عبر الـ SSL-VPN باستخدام البروتوكول H.323 :

تم في هذا الجزء من الجانب العملي إعداد وتنصيب برنامج الـSSL-VPN بقسميه(المخدِّم والزبون) ، والذي يقوم بتطبيق الأمن الشبكي في الطبقتين الثانية والثالثة من نموذج OSI ذو الطبقات السبعة . باستخدام المعيار الشائع لبروتوكول SSL/TLS . والذي يدعم وسائل ترخيص بسيطة للزبائن اعتماداً على اسم المستخدم وكلمة المرور ، ويسمح لمستخدم واحد أو لمجموعة بسياسات تحكم وصول محددة باستخدام قوانين الجدار الناري مطبقةً على المنفذ الوهمي للـVPN .

استخدمنا الـVPN باعدادات مفتاح تشفير ثابت Static Key والتي تجعل تنصيب البرنامج من أبسط مايمكن . إن هذه الاعدادات مثالية من أجل الـVPNs من نقطة إلى نقطة ، وطبعاً أسهل في الاختبار .

<u>ميزات الـStatic Key :</u> – تنصيب أسهل

- لانحتاج لاستخدام بنية تحتية بمفتاح تشفير عمومي PKI

<u>عيوب الـStatic Key :</u> – استخدام محدود ، زبون واحد ومخدِّم واحد

- فقدان الأمن المطلَق ، حيث تؤدي معرفة المفتاح إلى كشف جميع الجلسات السابقة .
- يجب أن يتواجد المفتاح السري – التشفير بصيغة نص كتابي مقروء PlainText على كل طرفية VPN .
- يجب وضع نفس المفتاح ، أي نقله إلى كل طرفية VPN (زبون أو مخدِّم) مشاركة بالاتصال.

إذاً كما تم التنويه سابقاً : تم القيام بإعداد اتصال VPN من نقطة إلى نقطة ، وفي أبسط أشكاله . سيتم إنشاء نفق VPN بين طرفية مخدِّم واحدة ذات عنوان 10.8.0.1 و طرفية زبون واحدة ذات عنوان 10.8.0.2 ليتم عبرها اتصال مشفَّر باستخدام مفتاح ثابت مابين الزبون والمخدَِم ، والذي سوف يحدث عبر البروتوكول UDP ذو المنفذ 1194 .

تم القيام بتوليد مفتاح التشفير الثابت باستخدام الأمر :

openvpn --genkey --secret static.key

ثم تم نسخه وحفظه في كل من المخدَِم والزبون .

<u>إعدادات الجدار الناري :</u> – السماح للبروتوكول UDP ذو المنفذ 1194 بالعبور فقط .

- منفذ TUN الوهمي المستخدم من قِبل الـVPN غير مقفل على كل من المخدِّم والزبون . في نظام Windows فإن منفذ TUN سوف يظهر لنا بالشكل **Local Area Connection *n*** إلا إذا قمنا بتسميته باسم مختلف من خلال لوحة التحكم .

تم القيام أخيراً بكتابة ملَفي الإعداد لكل من الزبون والمخدِّم وتخزينه على كل منهما على التتالي .

للتحقق من أن الـ VPN يعمل يمكن كتابة :

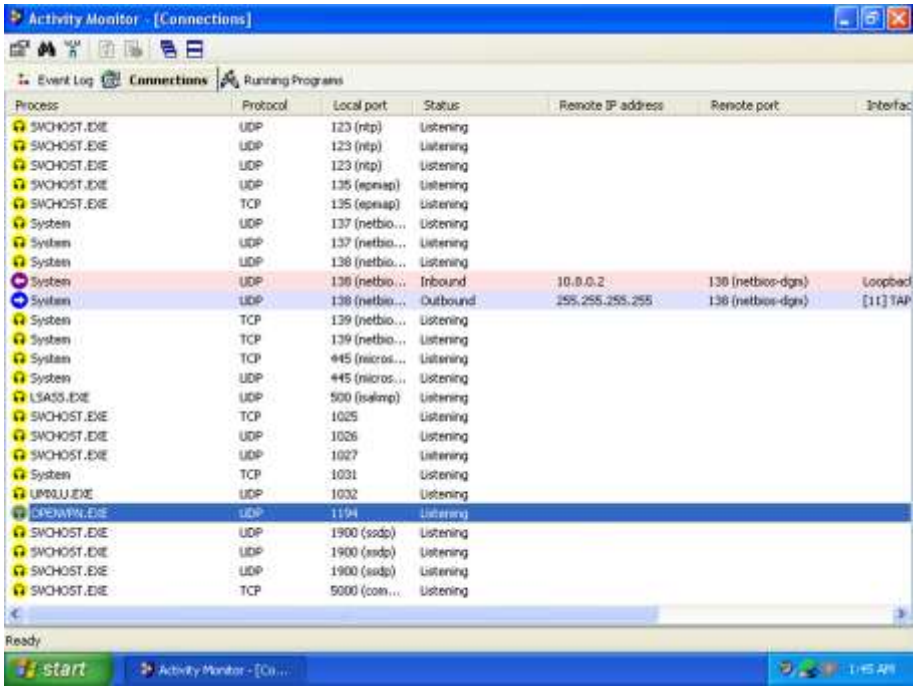
من المخدِّم : Ping 10.8.0.2

من الزبون : Ping 10.8.0.1

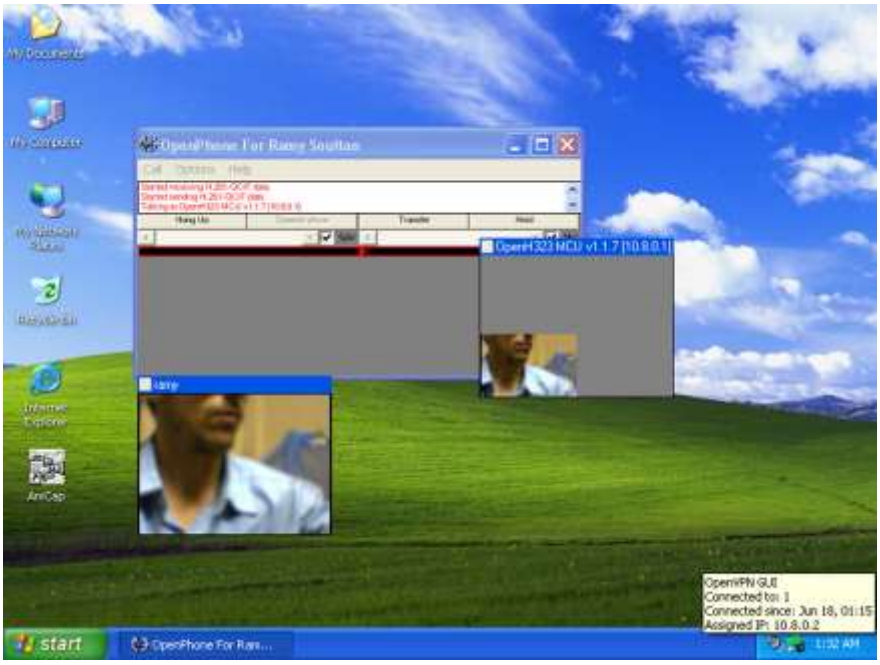
تم التوصل إلى النتائج الآتية:

أ- النتائج على الزبون والذي يتضمَّن برنامج SSL-VPN Client و H.323 Endpoint :

عنوان الـIP الحقيقي للزبون هو 185.110.120.1 بينما عنوان الـIP الوهمي المنسوب له من قبل الـVPN فهو 10.8.0.2 :



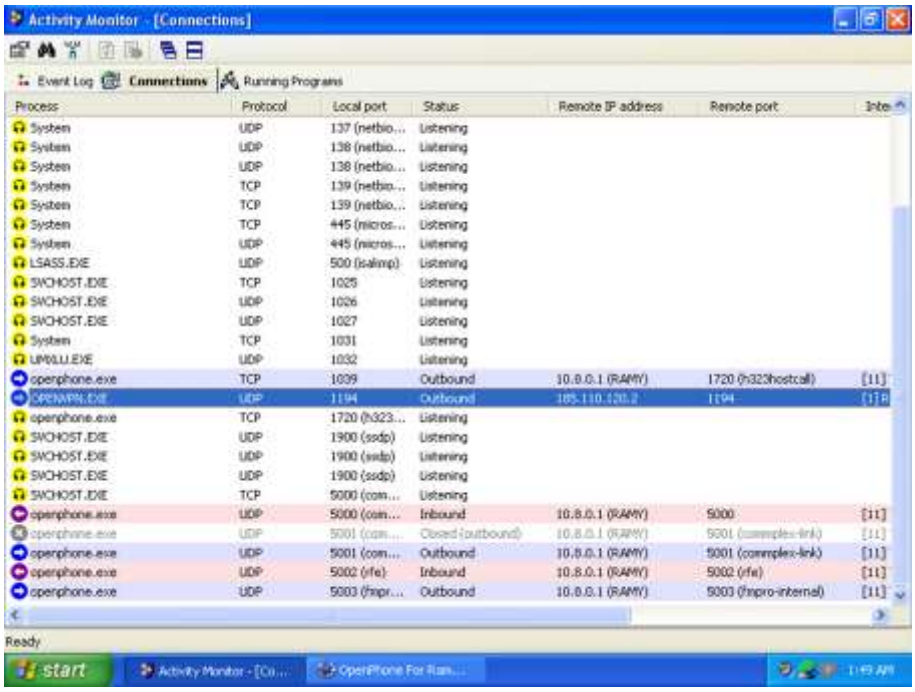
الشكل 13 : نتأكد أن نفق VPN قد تم إنشاؤه بين الزبون والمخدِّم عبر البروتوكول UDP ذو المنفذ 1194



الشكل 14 : نقوم الآن بالاتصال بالمخدِّم على عنوان الـIP الوهمي المنسوب له وهو 10.8.0.1 علماً أن عنوان الـIP الحقيقي له هو 185.110.120.2

نتحقق الآن من البوابات الأربعة الديناميكية التي يقوم برنامج زبون الـH.323 بفتحها عادةً كما رأينا في الجزء العملي الأول ولكن هذه المرّة متجهة إلى العنوان الوهمي لمخدِّم الـMCU وهو هنا 10.8.0.1 .

لنتذكر أن هذه المنافذ الأربعة مخصصة لقنوات الصوت والفيديو (اثنان لكل منهما عبر البروتوكول RTP):

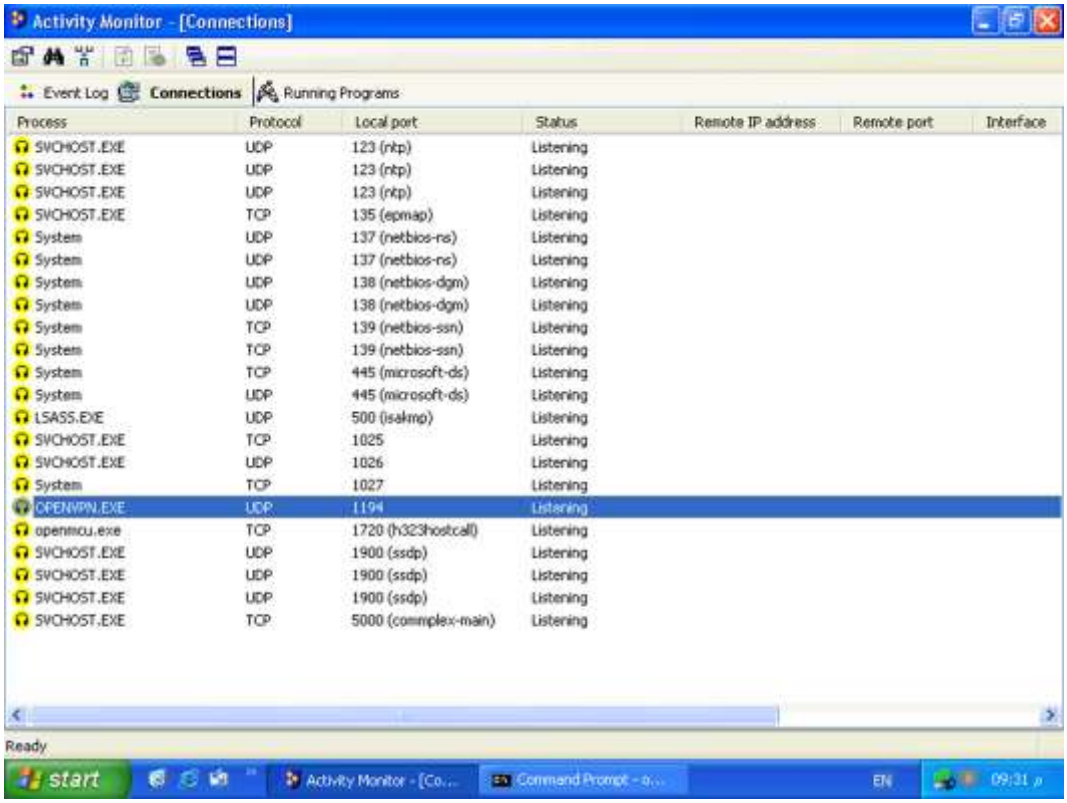


الشكل 15 : البوابات الأربعة الديناميكية التي يقوم برنامج زبون الـH.323 بفتحها

ب- النتائج على المخدِّم والذي يتضمَّن برنامجي SSL-VPN Server و H.323 MCU Server :

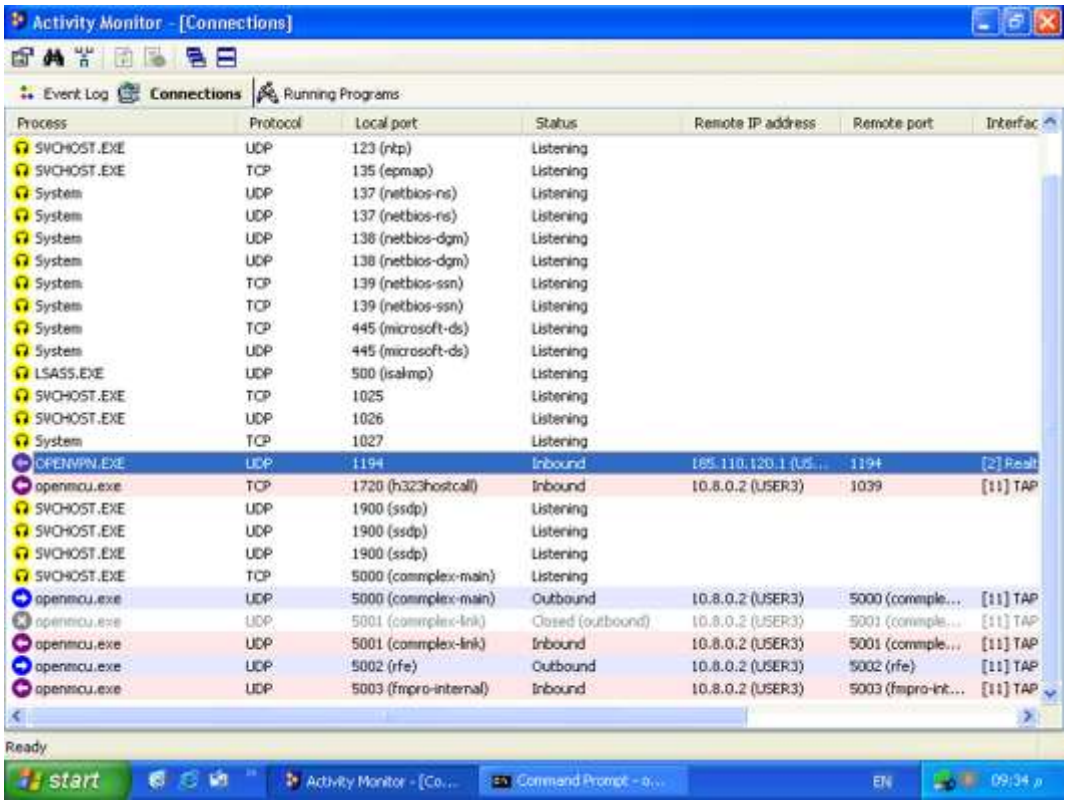
عنوان الـIP الحقيقي للمخدِّم هو 185.110.120.2 بينما عنوان الـIP الوهمي المنسوب له من قبل الـVPN فهو : 10.8.0.1 :

إن معنى Connected to:1 في الأعلى هو أن مخدِّم الـVPN يتصل مع زبون واحد فقط (حاسب واحد فقط).



الشكل 16 : نتأكد الآن من أن نفق VPN قد تم إنشاؤه بين الزبون والمخدِّم عبر البروتوكول UDP ذو المنفذ 1194

بعد إنشاء الاتصال الأول مع المخدِّم على عنوان الـIP الوهمي المنسوب له وهو 10.8.0.1 ، نستطيع أن نرى المنافذ المفتوحة فيه ، وهي عبارة عن منفذ واحد 1194 على العنوان الحقيقي ، بينما البقية فهي على عنوان الـIP الوهمي ، وبالتالي لايوجد فعلياً إلا منفذ واحد مفتوح على الحاسب 185.110.120.2 : الشكل 17 .



الشكل 17 : منفذ واحد مفتوح على الحاسب 185.110.120.2

الاستنتاجات والتوصيات:

– أصبحت تطبيقات الفيديو عبر الإنترنت أكثر شيوعاً واستخداماً . كنتيجة ، فإن المزيد من الشبكات المحلية والأنظمة التقليدية أصبحت مرتبطة مع الشبكات العالمية . سامحةً بذلك للشركات والمؤسسات بتخفيض التكاليف وزيادة الإنتاجية في أثناء السماح للمستخدمين بالاستمتاع بأنواع جديدة من الخدمات المتطورة .

– إن الأمن هو اعتبار مهم أثناء تطبيق الـVOIP لأن كل عنصر في البنية التحتية يمكن الوصول إليه عن طريق الشبكة ، فأي حاسب يمكن مهاجمته أو استخدامه كنقطة انطلاق لهجوم أعمق .

– لقد أثبت الـVOIP أنه يملك عوامل خطورة عالية ، فنداءات الـVOIP عرضةَ لـ:هجمات غياب الخدمة DOS ، الـGateways المهاجَمة تقود إلى اتصالات مجانية غير مرخصة ، الإنصات على الاتصال وإعادة توجيهه .....

– إن أكثر بروتوكولين مستخدمين في مؤتمرات الفيديو عبر الـIP هما H.323 و SIP .

– إن الـH.323 هو معيار مظلي وضعته الـITU ، يصف عائلة من البروتوكولات المستخدمة لإنجاز التحكم باتصالات الوسائط المتعددة عبر شبكات التبديل بالرزم . إن أكثر البروتوكولات أهمية والمستخدمة لـ: إنشاء ، إدارة ، إنهاء الاتصالات هي H.245 و H.225 .

– يستخدم الـH.225 لتنفيذ التحكم بالاتصال ، ويستخدم الـH.245 لتنفيذ إدارة الاتصال .

إن نوعية مقبولة من اتصال فيديو عبر الـIP بين طرفيتين تستخدمان الـH.323 تحتاج نموذجياً لأن تتجاوز معدل نقل معطيات 380Kbps .

– معظم الشركات تطبق في شبكاتها الجدران النارية ومترجمات عنوان الشبكة NAT في محاولة لمنع المهاجمين والأشخاص غير المرخصين من الوصول إلى داخل الشبكة . إن الـVOIP غير متوافق مع الجدران النارية والـNAT . سوف تحتاج هذه المؤسسات أن تضع في اعتبارها كيف ستخترق بشكل **آمن** جدارها الناري و الـ NAT وإعادة إعدادهما للسماح لمؤتمر الفيديو عبر الـIP .

– ما تزال الحلول المتوافرة مرتفعة الثمن جداً ، كما أنها تمتلك نسبة عالية من العيوب ، وتحتاج لكمية كبيرة من التعديلات على الشبكة وتستهلك وقت وجهد كبيرين .

تم تقديم أحد أرخص الحلول المتوافرة و أكثرها سهولةً وبساطةً وفعالية ، وهو تأسيس اتصال نفقي عبر الـVPN وتجميع جميع قنوات الـH.323 داخل قناة VPN واحدة ثابتة .

المراجع:

[1] O'Reilly Media; 1 edition (June 30, 2005) *ISBN: 0596008686 Switching to VoIP"Paperback: 477 pages* "

[2] Cisco Press (February 23, 2004) *ISBN: 1587200929 "Taking Charge of Your VoIP Project" Paperback: 312 pages*

[3] O'Reilly Media; 1 edition (December 1, 2005) *ISBN: 0596101333 "VoIP Hacks : Tips & Tools for Internet Telephony" Paperback: 306 pages*

[4] John Wiley & Sons, Inc. (April 2001) *Format: Adobe Reader "IP Telephony with H.323: Architectures for Unified Networks and Integrated Services" File Size: 7348 KB*

[5] VON Publishing LLC (October 2005) *ISBN: 0974813001 "SIP Beyond VoIP: The Next Step in the IP Communications Revolution" Paperback: 334 pages*

[6] Cisco Press; 1st edition (September 25, 2002) *ISBN: 1587050145 "Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security" : Hardcover: 224 pages*

[7] O'Reilly Media; 2nd edition (January 15, 2000) *ISBN: 1565928717 "Building Internet Firewalls (2nd Edition)" Paperback: 869 pages*

[8] Addison-Wesley Professional; 1st edition (2003) *ISBN: 0672322498 "RTP: Audio and Video for the Internet" Hardcover: 432 pages*

[9] Addison-Wesley Professional; 1st edition (October 13, 2000) *ISBN: 0201615983 Paperback: 499 pages "SSL and TLS: Designing and Building Secure Systems"*

[10] ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers