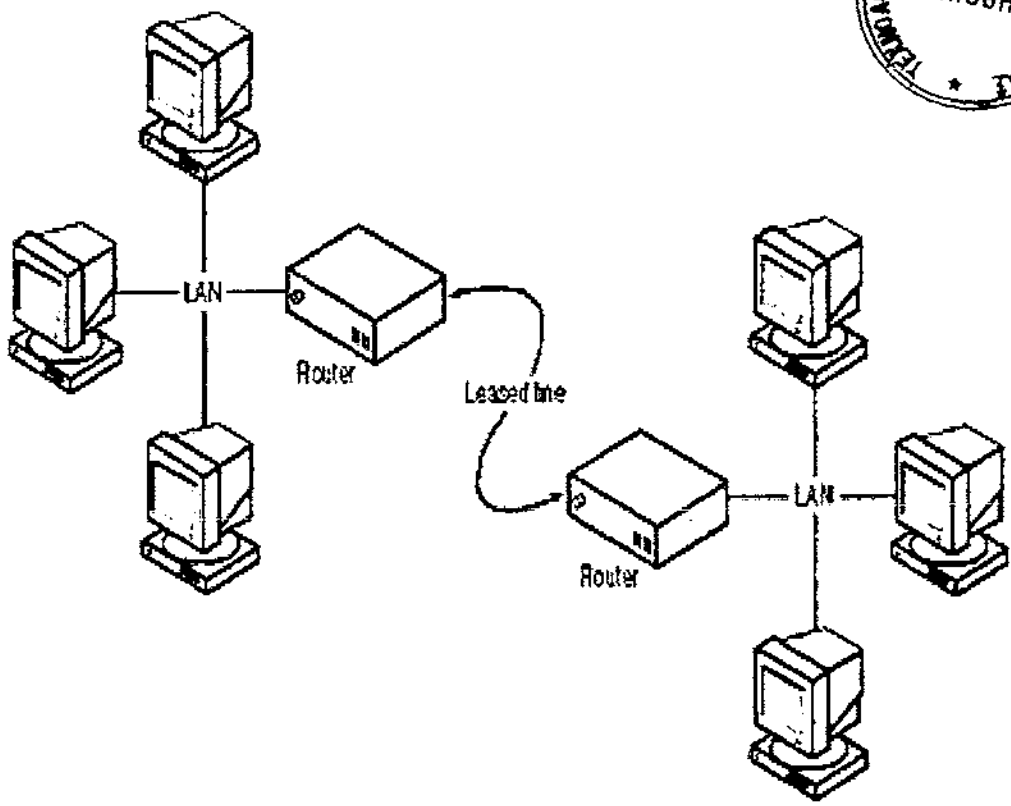
Σύγχρονα δίκτυα IP. Εφαρμογή τους στο Επιχειρηματικό Περιβάλλον



Σπουδαστής : Κακαλιάγκος Ιωάννης-Στυλιανός
Επιβλέπων : Δαρσινός Βασίλης

Χρονική διάρκεια : 10-1-04 ως 25-6- 2004

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή

Ένα δίκτυο είναι ένα σύνολο αυτόνομων συνδεδεμένων υπολογιστών το οποίο εξυπηρετεί την ανάγκη για ανταλλαγή πληροφοριών.

*Ορισμός του όρου **δίκτυο***:

Ένα σύστημα επικοινωνίας το οποίο αποτελείτε από μία ομάδα υπολογιστών που λειτουργούν με το ίδιο σύστημα και μοιράζονται τους ίδιους πόρους.

Η είσοδος των Η/Υ στις επιχειρήσεις τα τελευταία είκοσι χρόνια έχει επιφέρει δραστικές αλλαγές στην οργάνωση και λειτουργία τους. Έτσι σήμερα η χρήση του Η/Υ και των δικτύων στις σύγχρονες ευρωπαϊκές μικρομεσαίες επιχειρήσεις είναι πια αρκετά διαδεδομένη και καλύπτει ένα μεγάλο εύρος δραστηριοτήτων και αναγκών. Η ολοκληρωμένη πληροφοριακή υποδομή προσφέρει στις επιχειρήσεις την δυνατότητα να επικεντρωθούν σε παραγωγικές δραστηριότητες, στην βελτίωση και προώθηση των προϊόντων και υπηρεσιών τους και όχι σε γραφειοκρατικά θέματα που αφορούν την υποστήριξη αυτών των δραστηριοτήτων. Έτσι τα δίκτυα των υπολογιστών θα γίνουν τα βασικά εργαλεία οργάνωσης και λειτουργίας της σύγχρονης επιχείρησης. Έτσι η επιχείρηση που χρησιμοποιεί Η/Υ συνδεδεμένους σε δίκτυο μπορεί να αναπτυχθεί στους τομείς :

- ⇨ *Διατήρηση των αρχείων της επιχείρησης.*
- ⇨ *Μηχανοργάνωσης*
- ⇨ *Αυτοματισμού Γραφείου*
- ⇨ Επιτραπέζιων εκδόσεων
- ⇨ Επικοινωνίας, Πληροφόρησης και Αλληλεπίδρασης (μέσω του Internet)
- ⇨ Αποστολή και λήψη ψηφιακών πληροφοριών
- ⇨ Ψηφιακής διαφήμισης και άμεσης συνεργασίας με πελάτες και συνεργάτες
- ⇨ Ηλεκτρονικού εμπορίου
- ⇨ Συναλλαγής με δημόσιους οργανισμούς και τράπεζες

Η ελληνική κυβέρνηση έχοντας κατανοήσει τα οφέλη που προσφέρει η χρήση υπολογιστών σε δίκτυο σε μία επιχείρηση δημιούργησε και προωθεί τα τελευταία χρόνια ένα πρόγραμμα το οποίο ονομάστηκε «Δικτυωθείτε». Αυτό το πρόγραμμα αποτελεί πρωτοβουλία του Υπουργείου Ανάπτυξης και έχει σκοπό την προώθηση των τεχνολογιών του Διαδικτύου και των εφαρμογών τους στις ελληνικές επιχειρήσεις καθώς και την διαμόρφωση και ανταλλαγή ιδεών και προτάσεων για το e-επιχειρήν με έμφαση στις μικρομεσαίες επιχειρήσεις. Το πρόγραμμα ΔΙΚΤΥΩΘΕΙΤΕ χρηματοδοτείται από το μέτρο 3.2 του επιχειρησιακού προγράμματος Κοινωνία της Πληροφορίας του Υπουργείου Εθνικής Οικονομίας και Οικονομικών καθώς και από το μέτρο 8.2 του Επιχειρησιακού Προγράμματος Ανταγωνιστικότητα , του Υπουργείου Ανάπτυξης.

1.1 Ιστορική Αναδρομή

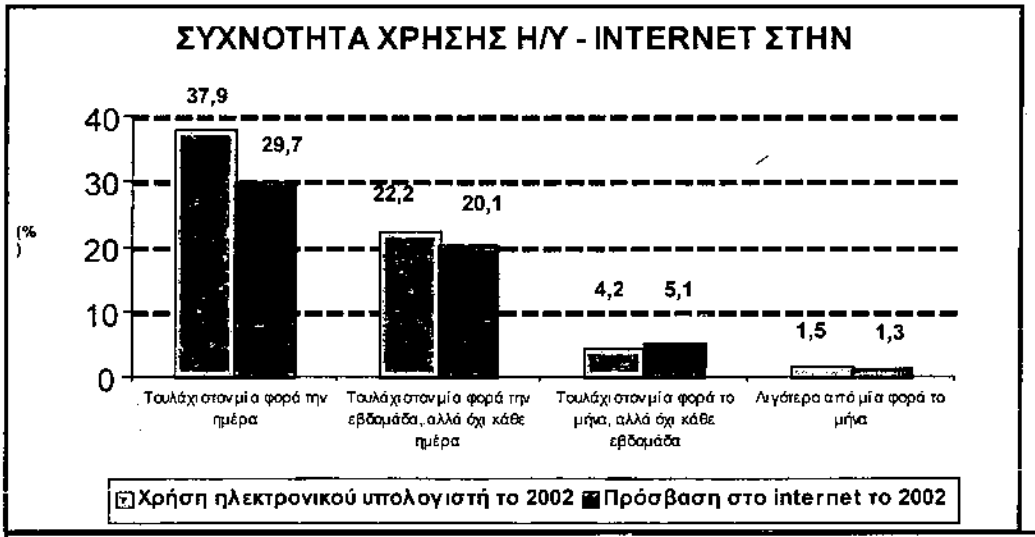
Παρακάτω θα αναφέρουμε τους βασικότερους ιστορικούς σταθμούς στην πορεία του παγκόσμιου δικτύου.

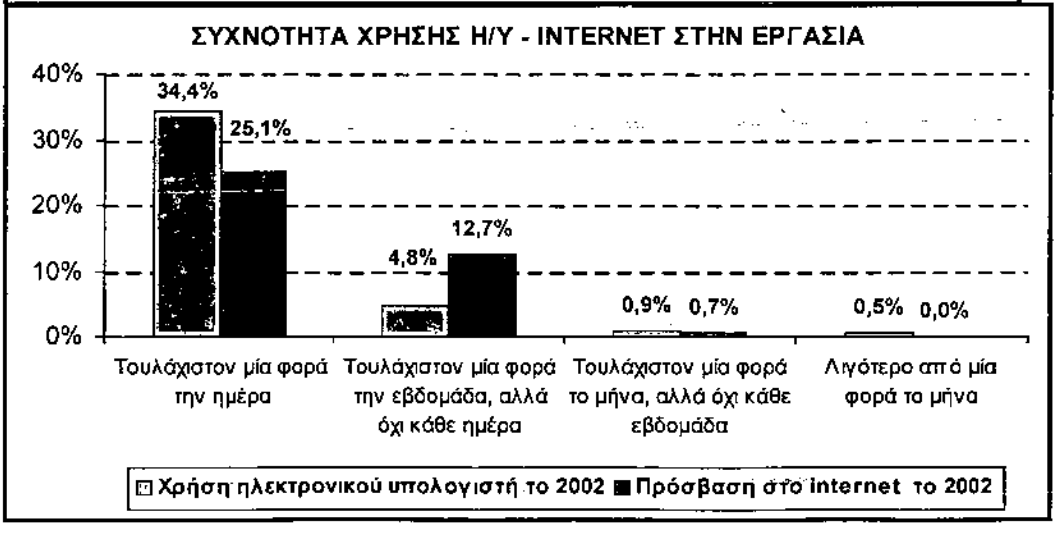
1. Το 1962 ο Paul Barab της εταιρίας RAND αναπτύσσει την ιδέα της διανομής πακέτων μέσα από το δίκτυο.
2.

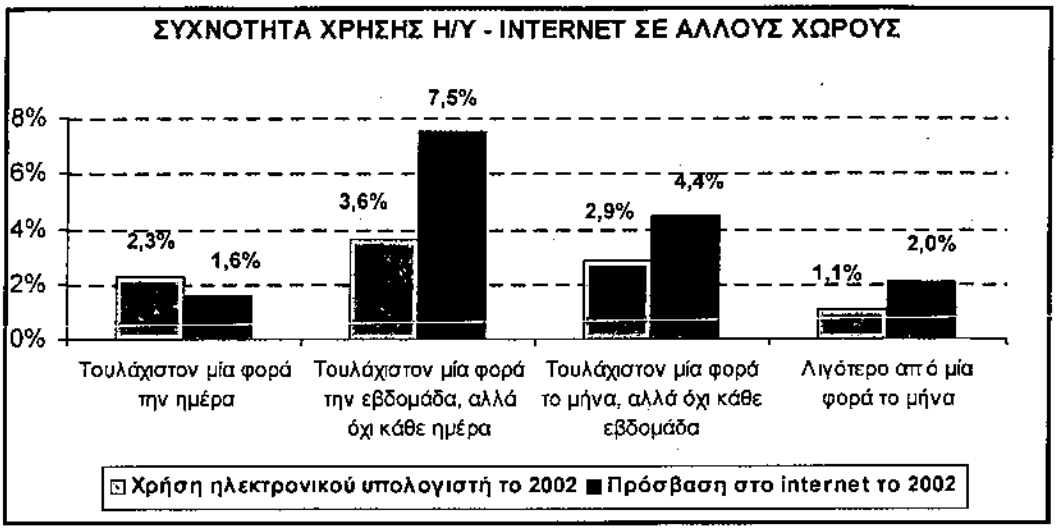
3. Το 1969 δημιουργείται το ARPANET
4. Οι βασικές ιδέες του Internet αναπτύσσονται από τους Kahn και Vint Cerf το 1973
5. Το 1974 η BBN θέτει σε λειτουργία το πρώτο δίκτυο μεταφοράς πακέτων και το ονομάζει Telnet
6. Ένας σύνδεσμος της μορφής UUCP δημιουργείται μεταξύ του πανεπιστήμιου της Νότιας Καρολίνας και του πανεπιστημίου Duke και δημιουργείται το USENET το 1979.
7. Στις αρχές του 1982 δημιουργείτε το πρωτόκολλο TCP/IP και γίνεται πρότυπο χρήσης στο ARPANET
8. 1989 Ο αριθμός των δρομολογητών φτάνει τις 100.000 και την ίδια χρονιά οι Tim Berners – Lee δημιουργούν τον παγκόσμιο ιστό WWW (World Wide Web)
9. Το 1993 ο WWW έχει σημειώσει αύξηση της τάξης του 341,634%

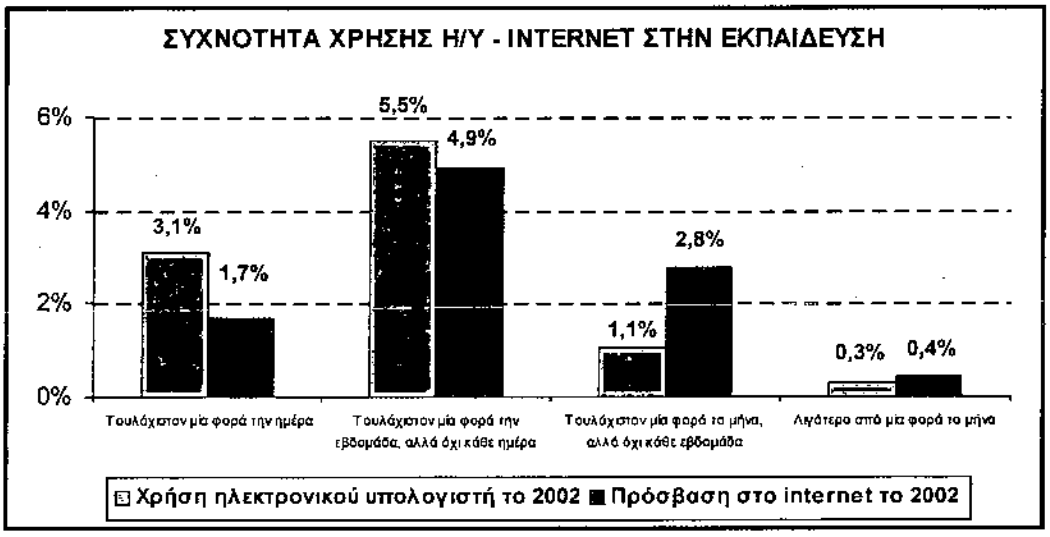
1.2 Πώς είναι η κατάσταση σήμερα;

Σύμφωνα με τα επίσημα στοιχεία της Εθνικής Στατιστικής Υπηρεσίας το ποσοστό χρηστών του διαδικτύου στην Ελλάδα κατά το τελευταίο τρίμηνο του 2002 ανέρχεται στο 24,1% των ερωτηθέντων (σε δείγμα 5216 ατόμων σε τυχαία νοικοκυριά). Η μεγαλύτερη συχνότητα χρήσης, όπως απεικονίζεται στα διαγράμματα που ακολουθούν, ήταν τουλάχιστον μία φορά την ημέρα στο χώρο κατοικίας ή εργασίας και τουλάχιστον μία φορά την εβδομάδα στην εκπαίδευση ή σε άλλους χώρους.









1.3 Προς τα πού πάμε;

Η τεχνολογική ανάπτυξη που ξεκίνησε την δεκαετία του 60 συνεχίζεται και σήμερα με ταχύτατους ρυθμούς. Οι αλλαγές είναι σε επίπεδο ηλεκτρονικών υπολογιστών και σε επίπεδο δικτύου.

Σε επίπεδο Η/Υ έχουμε ταχύτερους επεξεργαστές καθώς και μεγαλύτερες μνήμες. Επίσης οι μεγάλες απαιτήσεις στον επιχειρησιακό κόσμο έχουν οδηγήσει του κατασκευαστές λογισμικού να δημιουργούν συνεχώς ποιο εξειδικευμένα προγράμματα.

Σε επίπεδο δικτύου τα μέσα επικοινωνίας έχουν αλλάξει. Από το απλό ομοαξονικό καλώδιο προοδεύσαμε στις οπτικές ίνες και στα δίκτυα υψηλών ταχυτήτων, ενώ τα τελευταία χρόνια γίνάνε πράξη τα ασύρματα δίκτυα.

Η τεχνολογική ανάπτυξη των τελευταίων δεκαετιών είναι σίγουρο ότι θα συνεχιστεί και τις επόμενες, έχοντας σαν αποτέλεσμα την μείωση του όγκου των μηχανημάτων καθώς και την αύξηση της απόδοσης τους. Η χρήση του

διαδικτύου μέσω του κινητού τηλεφώνου είναι μία υπηρεσία που τώρα εμφανίζεται στην αγορά και αναμένεται να έχει θεαματικά αποτελέσματα.

1.4 Αναγκαία η χρήση του δικτύου στην επιχείρηση ;

Είναι όμως αναγκαία η χρήση του δικτύου μέσα στην επιχείρηση; Για να αντιληφθούμε την αναγκαιότητα ενός δικτύου σε μία επιχείρηση θα δώσουμε το παρακάτω παράδειγμα : *Έστω μια μικρομεσαία επιχείρηση που ασχολείται με την δημιουργία ερωτηματολογίων και στεγάζεται σε ένα διώροφο κτίσμα κάπου στην αττική. Στον πρώτο όροφο βρίσκετε το τμήμα μάρκετινγκ και η παραγωγική μονάδα της εταιρίας και στο δεύτερο όροφο στεγάζεται το διοικητικό συμβούλιο. Έστω ότι ο διευθυντής χρειάζεται για την δημιουργία ενός στρατηγικού σχεδίου τα αποτελέσματα μιας έρευνας του διευθυντή μάρκετινγκ της εταιρίας. Ο διευθυντής δίνει εντολή στον κλητήρα, ο οποίος με την σειρά του πάει στον διευθυντή μάρκετινγκ παραλαμβάνει τα έγγραφα και επιστρέφει στον διευθυντή. Αυτόματος δημιουργούνται κόστη για την πληρωμή του κλητήρα καθώς και για τον χρόνο που χάνεται. Η ύπαρξη ενός δικτύου θα επέτρεπε την εκμηδένιση του κόστους αυτού αφού με την αποστολή ενός e-mail στον διευθυντή μάρκετινγκ ο διευθυντής της επιχείρησης θα μπορούσε να έχει την έρευνα στον Η/Υ σε μηδενικό χρόνο και με μηδενικό κόστος.*
Ποίο γενικά , το θέμα είναι καταμερισμός πόρων και στόχος είναι να καταστούν διαθέσιμα όλα τα προγράμματα και ο εξοπλισμός και προ πάντως τα δεδομένα.
Ένας δεύτερος στόχος είναι η παροχή υψηλής αξιοπιστίας μέσω εναλλακτικών πηγών τροφοδοσίας. Για παράδειγμα όλα τα αρχεία θα μπορούσαν να αντιγραφούν σε δύο ή τρεις μηχανές έτσι ώστε να είναι διαθέσιμα σε περίπτωση βλάβης κάποιας.
Τέλος ένας άλλος στόχος είναι η εξοικονόμηση χρημάτων. Οι μικροί Η/Υ έχουν καλύτερο λόγο κόστους προς επίδοση από τους μεγάλους. Αυτή η ανισορροπία έχει αναγκάσει τους σχεδιαστές να χτίσουν συστήματα που απαρτίζονται από προσωπικούς Η/Υ, ένα ανά χρήστη, με τα δεδομένα να σε έναν ή περισσότερους εξυπηρετητές αρχείων. Επίσης το δίκτυο είναι ένα πολύ δυνατό επικοινωνιακό μέσο για τούς εργαζόμενους που είναι απομακρυσμένοι μεταξύ τους και δεν έχουν διαθέσιμο χρόνο για προσωπική επαφή.

1.5 Τι υπηρεσίες προσφέρουν;

Οι υπηρεσίες τις οποίες προσφέρουν τα σύγχρονα δίκτυα είναι :

FTP	*Μεταφορά αρχείων*
TELNET	*Απομακρυσμένη Πρόσβαση*
SMTP	*Ηλεκτρονικό Ταχυδρομείο*
WEB	*Παγκόσμιος Ιστός*
DNS	*Υπηρεσία Ονοματολογίας*
IMAP	*Απομακρυσμένη ανάγνωση e-mail*

2. Δίκτυα Ηλεκτρονικών Υπολογιστών

2.1.1 Ορισμός

Με τον όρο «δίκτυο υπολογιστών» εννοούμε μια διασυνδεδεμένη συλλογή από αυτόνομους υπολογιστές. Δύο Η/Υ αποκαλούνται διασυνδεδεμένοι αν είναι σε θέση να ανταλλάξουν πληροφορίες. Σύμφωνα με τον ορισμό που δίνει το US Department of Homental Security[1] ως δίκτυο υπολογιστών ορίζεται ένα σύνολο υπολογιστών συνδεδεμένων μεταξύ τους έτσι ώστε να μπορούν να ανταλλάζουν δεδομένα.

2.1.2 Είδη δικτύων

Ταξινομώντας τα δίκτυα βάσει απόστασης

Τα δίκτυα υπολογιστών κατηγοριοποιούνται σύμφωνα με την περιοχή στην οποία επεκτείνονται. Οι βασικές κατηγορίες δικτύων είναι οι ακόλουθες :

- ✓ LAN (Local Area Networks).

Τοπικά δίκτυα. Τα LAN είναι ένα δίκτυο Η/Υ το οποίο καλύπτει μια μικρή περιοχή. Τα περισσότερα LAN εντοπίζονται σε ένα κτίριο ή ένα σύνολο κτιρίων. Παρόλα αυτά ένα LAN μπορεί να συνδεθεί με άλλα LAN μέσω τηλεφωνικής γραμμής ή ραδιοκυμάτων. Ένα σύστημα από LAN συνδεδεμένα με αυτόν τον τρόπο καλείται δίκτυο ευρείας περιοχής η WAN (Wide Area Network).
Τα περισσότερα LAN συνδέουν σταθμούς εργασίας και προσωπικούς υπολογιστές. Κάθε ανεξάρτητος Η/Υ σε ένα δίκτυο LAN έχει τον δικό του επεξεργαστή και τα δικά του προγράμματα αλλά έχει πρόσβαση σε δεδομένα και συσκευές οπουδήποτε εντός δικτύου. Αυτό σημαίνει ότι πολλοί χρήστες μπορούν να μοιραστούν πολλές ακριβές συσκευές, όπως εκτυπωτές laser, όπως και δεδομένα. Οι χρήστες μπορούν να επικοινωνήσουν μεταξύ τους με e-mail.
Υπάρχουν διαφορετικά είδη δικτύων LAN, Ethernet είναι το ποιο κοινό για τους συμβατούς υπολογιστές.

Τα παρακάτω χαρακτηριστικά διαφοροποιούν το ένα δίκτυο LAN από ένα άλλο :

- ✓ *Τοπολογία :* Η γεωμετρική κατανομή των συσκευών στο δίκτυο. Για παράδειγμα, οι συσκευές μπορεί να είναι διαταγμένες σε δακτύλιο ή σε ευθεία γραμμή.
- ✓ *Πρωτόκολλα :* Οι κανόνες και η κωδικοποίηση κανόνων για τα απεσταλμένα δεδομένα. Τα πρωτόκολλα καθορίζουν εάν το δίκτυο χρησιμοποιεί αρχιτεκτονική peer-to-peer ή client/server.
- ✓ *Μέσα :* Οι συσκευές μπορεί να είναι συνδεμένες με ανεστραμμένο καλώδιο, ομοαξονικό καλώδιο ή οπτική ίνα. Ορισμένα δίκτυα δεν συνδέουν τις συσκευές τους με κάποιον από τους παραπάνω τρόπους, αλλά επικοινωνούν με ραδιοκύματα.

Τα δίκτυα LAN είναι ικανά να μεταδίδουν δεδομένα με πολύ υψηλές ταχύτητες, υψηλότερες από αυτές που μπορεί να προσφέρει μια τηλεφωνική γραμμή, αλλά

---

[1] http://www.ciao.gov/ciao_document_library/glossary/C.htm

υπόκεινται σε περιορισμό από την απόσταση και επιπρόσθετα δεν μπορούν να συνδεθούν σε ένα δίκτυο LAN περισσότεροι Η/Υ από έναν συγκεκριμένο αριθμό.

- ✓ *WAN (Wide Area Networks)*

Ένα δίκτυο υπολογιστών το οποίο καλύπτει μία μεγάλη γεωγραφικά περιοχή. Τυπικά ένα δίκτυο WAN αποτελείται από δύο η περισσότερα δίκτυα LAN.
Οι υπολογιστές που συνδέονται σε ένα τέτοιο δίκτυο είναι συνδεδεμένοι σε δημόσια δίκτυα , όπως τα τηλεφωνικά. Μπορεί επίσης να είναι συνδεδεμένοι με *μισθωμένες γραμμές*, ή δορυφόρους. Αυτή την στιγμή το μεγαλύτερο δίκτυο WAN εν ενεργεία είναι το Internet. Το δίκτυο MAN (Metropolitan Area Network) είναι ουσιαστικά ένα WAN το οποίο καλύπτει μια μητροπολιτική περιοχή.

- ✓ *CAN (Campus Area Network)*

Όπως αναφέρει και το όνομα ένα CAN είναι ένα δίκτυο το οποίο επεκτείνετε σε μια περιορισμένη γεωγραφική περιοχή όπως ένα πανεπιστήμιο ή ένα στρατόπεδο. Ουσιαστικά αυτό το δίκτυο είναι LAN δίκτυο το οποίο χρησιμοποιείται για συγκεκριμένο σκοπό.

Ταξινομώντας τα δίκτυα βάση συνδεσμολογίας

Ο τρόπος με το οποίο συνδέονται οι συσκευές που συμετέχουν σε ένα δίκτυο υπολογιστών, καθορίζεται από την τοπολογία του δικτύου. Οι πιο συχνά χρησιμοποιούμενες τοπολογίες παρουσιάζονται στην συνέχεια:
Τοπολογία αστέρα Μια σειρά από συνδέσεις σημείου προς σημείο (point-topoint connections) σε μορφή αστέρα.
Τοπολογία κοινού αγωγού Οι συσκευές συνδέονται σε έναν κοινό αγωγό π.χ. καλώδιο και ανταλλάσσουν πληροφορία μέσω αυτού.
Τοπολογία δακτυλίου Οι συσκευές συνδέονται στη σειρά σε σχήμα δακτυλίου. Τα δεδομένα ανταλλάσσονται είτε προς τη μμια είτε προς την άλλη κατεύθυνση.
Τοπολογία αστέρα δακτυλίου Η συγκεκριμένη τοπολογία είναι υβριδική, και αποτελεί έναν συνδυασμό των τοπολογιών αστέρα και δακτυλίου.
Πλήρης τοπολογία (mesh topology) Είναι η τοπολογία στην οποία κάθε συσκευή συνδέεται με όλες τις υπόλοιπες που συμμετέχουν στο δίκτυο.

2.2 Τρόποι υλοποίησης τους στο επιχειρηματικό περιβάλλον.

Σε αυτό το κεφάλαιο θα εξετάσουμε πώς στήνετε ένα LAN στο σπίτι ή στο γραφείο. Παρακάτω θα δούμε:

- ✓ *Το (υλικό) μηχανήματα που χρειάζονται.*

2.2.1 Βασικές δικτυακές συσκευές

Οι βασικές συσκευές που συμμετέχουν σε ένα δίκτυο είναι οι ακόλουθες :

- Σταθμοί εργασίας
- Κινητά τερματικά
- Εκτυπωτές δικτύου

Για την διασύνδεση σ' ένα δίκτυο υπολογιστών των συσκευών που προαναφέραμε χρησιμοποιούμε ειδικό υλικό (Hardware) και συγκεκριμένα τα ακόλουθα :

- Διαμορφωτές/Αποδιαμορφωτές (Modems)
- Κάρτες δικτύου
- Hubs

Τέλος για να συνδέσουμε επιμέρους δίκτυα Η/Υ σε ευρύτερα δίκτυα χρησιμοποιούνται συσκευές όπως :

- Γέφυρες (Bridges)
- Πύλες (Gateways)
- Δρομολογητές (Routers)

Παρακάτω θα δώσουμε μια μικρή περιγραφή των παραπάνω συσκευών ώστε ο αναγνώστης να έχει γνώση της βασικής τεχνολογίας των δικτύων υπολογιστών.
Θα παρακάμψουμε τις πρώτες συσκευές των οποίων ο καταμερισμός είναι ένας βασικός σκοπός των δικτύων και θα ασχοληθούμε με το υλικό που είναι απαραίτητο για την σύνδεση των συσκευών αυτών στο δίκτυο, καθώς και των επιμέρους δικτύων σε ευρύτερα δίκτυα.

1.Διαμορφωτές/Αποδιαμορφωτές (Modems). Η λέξη modem είναι το ακρωνύμιο των λέξεων modulator (διαμορφωτής)/ demodulator (αποδιαμορφωτής). Σε γενικές γραμμές μπορούμε να πούμε ότι το modem είναι μια συσκευή η οποία διαμορφώνει και αποδιαμορφώνει κάποια σήματα.
Στην ασύρματη επικοινωνία, το modem είναι μια συσκευή η οποία παρέχει μία διεπαφή για την μετάδοση δεδομένων σ ένα ασύρματο δίκτυο.
Το μόντεμ που αποστέλλουν δεδομένα, διαμορφώνουν τα δεδομένα σε σήμα που είναι συμβατό με την τηλεφωνική γραμμή, και το μόντεμ που λαμβάνει τα δεδομένα τα αποδιαμορφώνει σε ψηφιακό σήμα. Τα ασύρματα μόντεμ μετατρέπουν το ψηφιακό σήμα σε σήμα ραδιοφώνου και ξανά σε ψηφιακό.

2.Κάρτες δικτύου. Οι κάρτες δικτύου συχνά αναφέρονται και με το ακρωνύμιο NIC (network interface card), και είναι μία πλακέτα που εισάγεται στην μητρική πλακέτα του υπολογιστή ώστε να μπορεί να συνδεθεί σε ένα δίκτυο. Οι περισσότερες κάρτες δικτύου είναι σχεδιασμένες για συγκεκριμένους τύπους δικτύων, πρωτοκόλλων και πολυμέσων, αν και υπάρχουν κάποιες που είναι συμβατές με πολλά δίκτυα.

3.Hubs. Τα hubs είναι συσκευές σύνδεσης για δίκτυα. Επιτρέπει σε πολλά τμήματα ή Η/Υ να συνδέονται μεταξύ τους και να μοιράζονται πακέτα με πληροφορίες.

4.Γέφυρες (Bridges). Οι γέφυρες είναι hardware που χρησιμοποιείται για την διασύνδεση επιμέρους τοπικών δικτύων. Έτσι μια γέφυρα μπορεί να ενώσει δύο ή περισσότερα LAN δίκτυα. Αυτό που την κάνει διαφορετική από έναν αναμεταδότη είναι το γεγονός ότι η γέφυρα δεν θα προχωρήσει στην αναμετάδοση των δεδομένων ,από το ένα τοπικό δίκτυο στο άλλο εάν δεν έχει λάβει όλο το πακέτο των δεδομένων.

5.Πύλες (Gateways). Οι πύλες λειτουργούν για τα δεδομένα σαν είσοδος σε ένα άλλο δίκτυο. Μία πύλη πρόσβασης είναι μία πύλη μεταξύ το δίκτυο της τηλεφωνίας και άλλων δικτύων, όπως το Internet.

6.Δρομολογητές (Routers). Ο δρομολογητής είναι ένα μηχάνημα που η βασική του λειτουργία είναι να τεμαχίζει το δίκτυο, με σκοπό την μείωση της κυκλοφορίας και παρέχει ασφάλεια, έλεγχο και διασφαλισμένες διαδρομές. Είναι μια συσκευή που συνδέει διαφορετικά τοπικά δίκτυα στο στρώμα του δικτύου και έχει πρόσβαση σε διευθύνσεις του δικτύου, με σεβασμό στα πρωτοκολλά τα οποία τις διέπουν.

2.2.2 Δημιουργία ενός peer-to-peer δικτύου

Όπως όλες οι επιχειρηματικές κινήσεις , έτσι και η δημιουργία ενός δικτύου πρέπει να γίνει μεθοδικά και προσεκτικά, μεγιστοποιώντας τα πλεονεκτήματα για την επιχείρηση και παρέχοντας όλες τις απαιτούμενες υπηρεσίες.
Η δημιουργία ενός τοπικού δικτύου είναι μία σημαντική λειτουργία και δεν πρέπει να αντιμετωπίζεται αποσπασματικά. Από την στιγμή που θα δημιουργηθεί θα αποτελέσει τον συνδετικό ιστό των στελεχών της επιχείρησης.
Στο πλαίσιο αυτό οι βασικές παράμετροι που αποκτούν ιδιαίτερη σημασία για την ανάπτυξη ενός δικτύου είναι οι εξής:

- Η εξασφάλιση της αποδοτικής και αδιάλειπτης λειτουργίας του δικτύου.
- Η προστασία του δικτύου από πιθανή πρόσβαση χρηστών που δεν έχουν την αρμόδια εξουσιοδότηση.
- Η διατήρηση των πληροφοριών σε έγκυρη και ενημερωμένη μορφή, ακόμη και στο δικτυακό περιβάλλον, που πολλοί χρήστες έχουν δικαίωμα πρόσβασης.
- Η τμηματοποίηση του τοπικού δικτύου, έτσι ώστε να καλύπτονται οι ανάγκες των επιμέρους τμημάτων, από πλευράς ταχύτητας, όγκου διακινούμενων δεδομένων, πρόσβασης σε συγκεκριμένους πόρους και υπηρεσίες.

Η δυνατότητα επέκτασης του δικτύου, ώστε να μπορεί να ανταποκρίνεται στις συνεχώς αυξανόμενες απαιτήσεις της επιχείρησης.

3. Πρωτόκολλο IP

3.1 Τι είναι ένα πρωτόκολλο;

Ένα πρωτόκολλο, είναι κανόνες ή οδηγίες για την μετάδοση δεδομένων και υλοποιείται με το κατάλληλο λογισμικό. Όταν τα δεδομένα είναι έτοιμα προς μετάδοση, εκτελείται αυτό το λογισμικό. Το πρωτόκολλο ετοιμάζει τα δεδομένα για μετάδοση και αρχίζει την μετάδοση. Ο δέκτης των δεδομένων κάνει χρήση του λογισμικού αυτού για να καθαρίσει τα δεδομένα από πληροφορίες που προστέθηκαν σε αυτά κατά την μετάδοση.

3.2 Πόσα είδη πρωτοκόλλων υπάρχουν;

3.2.1 Πρωτόκολλα σημείου προς σημείου

SLIP

Το πρωτόκολλο IP σειριακής γραμμής (Serial Line Ip) είναι το παλιότερο από τα πρωτόκολλα αυτού του είδους. Επινοήθηκε από τον *Rick Adams* το 1984 για να συνδεθούν οι σταθμοί εργασίας της Sun στο Internet μέσω μιας τηλεφωνικής γραμμής με την χρήση μόντεμ.
Το SLIP είναι πολύ απλό. Ο σταθμός εργασίας στέλνει απλώς τα ακατέργαστα πακέτα IP μέσω της γραμμής με ειδικό σήμα byte σημαία Αν η σημαία εμφανισθεί μέσα στο πακέτο IP χρησιμοποιείται μια μορφή παραγεμίσματος με χαρακτήρες και στέλνεται άντ' αυτής η ακολουθία από δύο byte.

PPP

Το πρωτόκολλο PPP ήρθε σαν μία βελτίωση του προκατόχου του και του δόθηκε αυτή η ονομασία από τα αρχικά (Point-to-point Protocol) δηλαδή πρωτόκολλο σημείου προς σημείο. Το PPP υποστηρίζει την ανίχνευση λαθών, πολλαπλά πρωτόκολλα, επιτρέπει την διαπραγμάτευση διευθύνσεων IP κατά την διάρκεια της σύνδεσης, επιτρέπει την πιστοποίηση της αυθεντικότητας και παρουσιάζει πολλές ακόμα βελτιώσεις σε σχέση με το SLIP.

3.2.2 Πρωτόκολλα πολλαπλής προσπέλασης

Καθαρό ALOHA

Η βασική ιδέα ενός τέτοιου πρωτοκόλλου είναι απλή: αφήστε τους χρήστες ελεύθερους να μεταδίδουν οποτεδήποτε έχουν δεδομένα για μετάδοση. Θα υπάρξουν συγκρούσεις, και τα συγκρουόμενα πλαίσια θα καταστραφούν. Επειδή όμως η εκπομπή παρουσιάζει την δυνατότητα της ανάδρασης, ο πομπός μπορεί να διαπιστώνει εάν το πλαίσιο καταστράφηκε ακούγοντας τον δίαυλο, ακριβώς όπως και οι άλλοι χρήστες. Εάν το πλαίσιο καταστράφηκε ο πομπός το στέλνει ξανά.

ALOHA με σχισμές

Σύμφωνα με αυτήν την μέθοδο (Roberts 172), δεν επιτρέπεται σε έναν H/Y να μεταδίδει κάθε φορά που πληκτρολογείται ο χαρακτήρας carriage-return. Αντίθετα πρέπει να περιμένει την έναρξη της επόμενης σχισμής.

3.2.3 Πρωτόκολλα Πολλαπλής Προσπέλασης με Ανίχνευση Φέροντος

Επίμονο και Μη Επίμονο CSMA

Πρώτα θα αναφερθούμε στο επίμονο CSMA. Όταν ένας σταθμός έχει να στείλει δεδομένα αρχικά αφουγκράζεται τον δίαυλο για να δει μήπως μεταδίδει κάποιος άλλος εκείνη την στιγμή. Εάν ο δίαυλος είναι απασχολημένος, ο σταθμός περιμένει έως ότου ο δίαυλος ελευθερωθεί και τότε μεταδίδει ένα πλαίσιο. Εάν συμβεί σύγκρουση, ο σταθμός περιμένει για κάποιο τυχαίο χρονικό διάστημα και μετά αρχίζει πάλι από την αρχή.
Στο μη επίμονο CSMA καταβλήθηκε μια προσπάθεια να είναι λιγότερο άπληστο από το πρώτο. Πρώτου στείλει ένας σταθμός αφουγκράζεται τον δίαυλο. Εάν κανείς άλλος δεν στέλνει τότε ο σταθμός αρχίζει. Ωστόσο, αν ο δίαυλος είναι ήδη σε χρήση, ο σταθμός δεν τον ανιχνεύει συνέχεια με σκοπό να τον καταλάβει αμέσως μόλις εντοπίσει το τέλος της προηγούμενης μετάδοσης. Αντίθετα περιμένει μια τυχαία χρονική περίοδο και κατόπιν επαναλαμβάνει τον αλγόριθμο.

CSMA με Ανίχνευση Σύγκρουσης

Σε αυτό το πρωτόκολλο εάν οι δύο σταθμοί αντιληφθούν ότι ο δίαυλος είναι ελεύθερος και αρχίσουν να μεταδίδουν συγχρόνως τότε και οι δύο θα ανιχνεύσουν την σύγκρουση σχεδόν αμέσως. Αντί να ολοκληρώσουν την μετάδοση των πλαισίων τους, τα οποία έτσι και αλλιώς έχουν παραμορφωθεί ανεπανόρθωτα, πρέπει να διακόψουν αυτόματα την μετάδοση μόλις ανιχνεύσουν την σύγκρουση. Ο γρήγορος τερματισμός των κατεστραμμένων πλαισίων εξοικονομεί χρόνο και εύρος ζώνης.

3.2.4 Πρωτόκολλα με αντιστοιχίες bit

Πρωτόκολλο με αντιστοιχίες bit

Σε αυτό το πρωτόκολλο κάθε περίοδος ανταγωνισμού περιέχει N ακριβώς σχισμές. Εάν ο σταθμός 0 έχει ένα πλαίσιο να στείλει, μεταδίδει το bit 1 κατά την διάρκεια της μηδενικής σχισμής. Κανένας άλλος σταθμός δεν επιτρέπεται να μεταδώσει κατά την διάρκεια αυτής της στιγμής. Έτσι μετά την πάροδο N σχισμών, κάθε σταθμός έχει πλήρη γνώση των σταθμών που επιθυμούν να μεταδώσουν. Στο σημείο αυτό οι σταθμοί αρχίζουν να μεταδίδουν αριθμητικά.

3.2.5 Πρωτόκολλα Ελέγχου στο Internet

Πρωτόκολλο ICMP

Η λειτουργία του Internet παρακολουθείται στενά από τους δρομολογητές. Όταν συμβεί κάτι αναπάντεχο, το γεγονός αναφέρεται από το πρωτόκολλο μηνυμάτων ελέγχου του Internet το ICMP, που χρησιμοποιείται επίσης για την διεξαγωγή δοκιμών στο Internet.

Πρωτόκολλο ARP

Παρόλο που το κάθε μηχάνημα στο Internet έχει μία ή περισσότερες διευθύνσεις IP, αυτές δεν μπορούν να χρησιμοποιηθούν για αποστολή πακέτων, επειδή το υλικό του στρώματος ζεύξης δεδομένων δεν μπορεί να καταλάβει τις διευθύνσεις στο Internet.
Στο σημείο αυτό δημιουργείται η ερώτηση: ' Σε ποιόν ανήκει η η διεύθυνση IP 192.31.65.2;'. Το πακέτο θα φτάσει σε κάθε μηχανή του δικτύου που έχει διευθύνσεις της μορφής 192.31.65.0 και κάθε μία από αυτές θα ελέγξει για τις δικές τη δική της διεύθυνση IP. Με αυτόν τον τρόπο μόνο ο host 2 θα ανταποκριθεί με την δική του διεύθυνση. Το πρωτόκολλο που διατυπώνει αυτήν την ερώτηση και λαμβάνει την απάντηση είναι το πρωτόκολλο επίλυση διευθύνσεων ARP.

Πρωτόκολλο RARP

Κάποιες φορές δημιουργείται το εξής πρόβλημα: Δεδομένου μιας διευθύνσεως στο δίκτυο ποία είναι η IP διεύθυνση του μηχανήματος; Συγκεκριμένα με την εκκίνηση ενός σταθμού εργασίας χωρίς δίσκο δημιουργείται αυτό το πρόβλημα. Ένα τέτοιο μηχάνημα κανονικά θα λειτουργήσει σε περιβάλλον του λειτουργικού συστήματος του κεντρικού υπολογιστή. Πως όμως να μάθει την IP διεύθυνση του; Η λύση είναι να χρησιμοποιήσει το πρωτόκολλο αντίστροφης επίλυσης διευθύνσεων.

3.2.6 Πρωτόκολλα Δικτύου

Πρωτόκολλο IP

Τα πρωτόκολλα Internet είναι τα ποίο δημοφιλή πρωτόκολλα τεχνολογίας ανοιχτής αρχιτεκτονικής, επειδή μπορούν να χρησιμοποιηθούν για την διασύνδεση οποιονδήποτε υποδικτύων και είναι εφαρμόσιμα για την επικοινωνία LAN και WAN δικτύων. Τα ποίο γνωστά πρωτόκολλα της κατηγορίας αυτής είναι τα TCP/IP. Επίσης πρέπει να αναφέρουμε ότι τα πρωτόκολλα αυτής της κατηγορίας δεν περιλαμβάνουν μόνο πρωτόκολλα της χαμηλής κατηγόριας του μοντέλου OSI, αλλά περιλαμβάνουν λειτουργίες όπως το ηλεκτρονικό ταχυδρομείο και μεταφορές αρχείων
Τα πρωτόκολλα αυτής της κατηγορίας αναπτύχθηκαν στα μέσα της δεκαετίας του 1970, όταν η DAPRA έδειξε ενδιαφέρον για την δημιουργία ενός δικτύου πακέτων, που θα έκανε δυνατή την επικοινωνία μεταξύ δικτύων που χρησιμοποιούσαν διαφορετικά πρωτόκολλα.. Έχοντας αυτό κατά νου, η DAPRA άρχισε τις έρευνες σε συνεργασία με το πανεπιστήμιο του Stanford, έρευνες των οποίων το αποτέλεσμα ήταν τα πρώτα πρωτόκολλα δικτύου τα οποία ολοκληρώθηκαν στα τέλη της δεκαετίας του 1970.

Το πρωτόκολλο TCP/IP περιλαμβανόταν στην πλατφόρμα UNIX και από τότε έγινε ο ακρογωνιαίος λίθος του Internet και του παγκόσμιου ιστού.

Πρωτόκολλο UPD

Αυτό το πρωτόκολλο είναι ποίο απλό από το TCP, και παρέχει την πλειοψηφία των λειτουργιών του IP, αριθμούς θυρών, και προσθετό έλεγχο συνόλου για να διαπιστώσει εάν τα δεδομένα που έλαβε είναι σωστά. Το UPD δεν παρέχει μέσα για να λέει την αλφαβητική σειρά της εκπομπής πολλών πακέτων μετάδοσης, και έτσι περιορίζεται σε εκπομπές δεδομένων μεγέθους αρκετά μικρού, ώστε να χωράει σε ένα πακέτο IP.

Πρωτόκολλο X.25

Η τεχνολογία X 25 εφευρέθηκε στις αρχές του 1970 και είναι προσαρμοσμένη στις απαιτήσεις της εποχής εκείνης. Τα σημαντικότερα χαρακτηριστικά του πρωτοκόλλου είναι :

1. Από τεχνολογικής πλευράς, το X 25 έπρεπε να αντιμετωπίζει τους υψηλούς ρυθμούς λαθών των μέσων μετάδοσης εκείνης της εποχής. Γι' αυτό τον σκοπό, ενσωματώνει ισχυρούς μηχανισμούς ανίχνευσης και διόρθωσης λαθών, οι οποίοι όμως καθυστερούν την επικοινωνία. Εκείνη την εποχή οι πιο γρήγορες γραμμές στην Ευρώπη λειτουργούσαν στα 72kbps
2. Ένα μάλλον ασυνήθιστο χαρακτηριστικό του X 25 είναι ο έλεγχος ροής που επιβάλλεται από το δίκτυο. Αυτό σημαίνει ότι μπορεί να ρυθμίζει την ταχύτητα ροής των πακέτων σε ένα κύκλωμα, χωρίς να μεσολαβούν οι χρήστες. Στόχος αυτού του μηχανισμού είναι η επικοινωνία συστημάτων διαφορετικής ταχύτητας

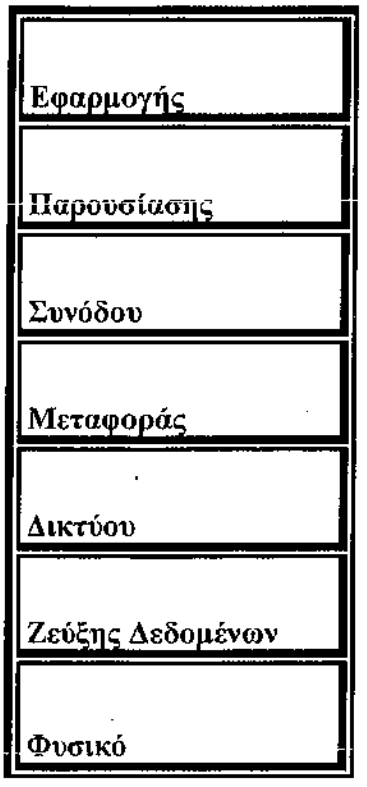
3.3 Παρουσίαση του πρωτοκόλλου IP και συσχέτιση του με το μοντέλο OSI

Το ARPANET ήταν το πρώτο δίκτυο που δημιουργήθηκε υπό την εποπτεία του Υπουργείου Άμυνας των Η.Π.Α, και συνέδεε εκατοντάδες πανεπιστήμια και κυβερνητικές εγκαταστάσεις χρησιμοποιώντας μισθωμένες γραμμές. Όταν αργότερα προστέθηκαν δορυφορικά και ασύρματα δίκτυα, τα τότε υπάρχοντα πρωτόκολλα είχαν προβλήματα διαλειτουργίας με τα νέα και έτσι χρειάστηκε μια καινούργια αρχιτεκτονική αναφοράς. Κατά συνέπεια, η δυνατότητα να συνδέονται μαζί πολλαπλά δίκτυα με διαφανή τρόπο ήταν κύριος στόχος από την αρχή. Η αρχιτεκτονική αυτή έγινε γνωστή ως μοντέλο αναφοράς TCP/IP από τα ονόματα των δύο πρωτοκόλλων της.
Επειδή όμως το Υπουργείο Άμυνας ανησυχούσε μήπως κάποιοι από τους πολύτιμους host ή τους δρομολογητές ή τις πύλες των διαδικτύων καταστραφούν μέσα σε μία στιγμή, ένας άλλος στόχος ήταν να μπορεί το δίκτυο να επιζήσει σε περίπτωση που υλικό του υποδικτύου υποστεί βλάβη, χωρίς να διακόπτονται οι υπό εξέλιξη επικοινωνίες.
Όλες αυτές οι απαιτήσεις οδήγησαν στην επιλογή ενός δικτύου μεταγωγής πακέτου, βασισμένου σε ένα στρώμα διαδικτύου που παρέχει υπηρεσίες χωρίς σύνδεση. Αυτό το στρώμα, που αποκαλείται στρώμα διαδικτύου είναι ο ακρογωνιαίος λίθος που συγκρατεί

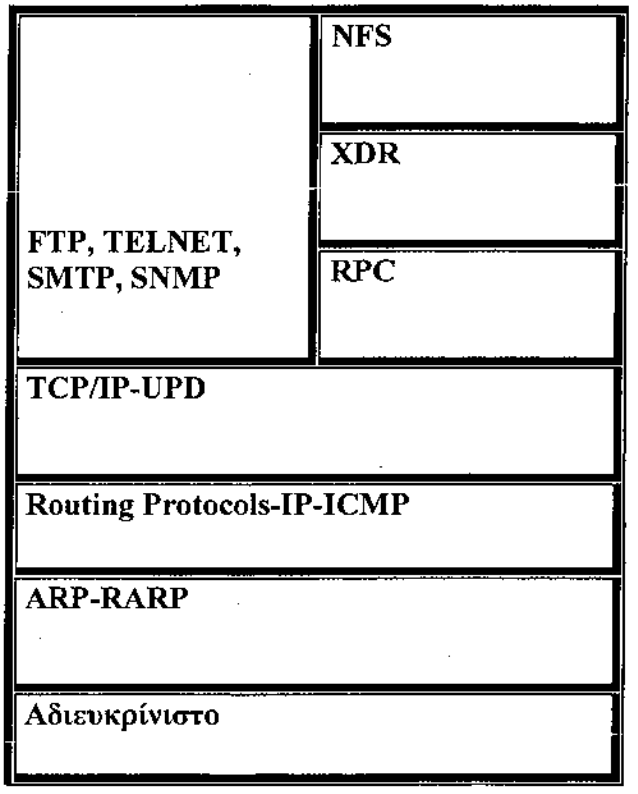
όλη την αρχιτεκτονική. Η δουλεία του είναι να επιτρέπει στους host να εισάγουν πακέτα σ' οποιοδήποτε δίκτυο και να δρομολογεί τα πακέτα ανεξάρτητα από τον προορισμό τους. Μπορεί να φθάσουν με διαφορετική σειρά από την οποία στάλθηκαν, οπότε είναι δουλεία των ανωτέρων στρωμάτων να τα επαναδιατάξουν, εφόσον είναι επιθυμητή η παραλαβή με την ορθή σειρά.
Το στρώμα διαδικτύου καθορίζει μία επίσημη μορφή πακέτου και πρωτοκόλλου που ονομάζεται πρωτόκολλο διαδικτύου IP. Η δουλεία του στρώματος διαδικτύου είναι να παραδίδει τα πακέτα IP στον προορισμό τους. Το βασικό θέμα εδώ είναι η δρομολόγηση πακέτων καθώς και η αποφυγή συμφόρησης. Για τους λόγους αυτούς είναι εύλογο να ειπωθεί ότι η λειτουργικότητα του στρώματος διαδικτύου του TCP/IP είναι παρόμοια μ' εκείνη του στρώματος δικτύου του OSI. Στον πίνακα 1 βλέπουμε την αντιστοίχηση του πρωτοκόλλου IP στα επίπεδα της OSI Στον πίνακα 2 βλέπουμε τις υπηρεσίες και τα πρωτόκολλα που υπάρχουν σε κάθε επίπεδο του μοντέλου αναφοράς της OSI.

OSI	**TCP/IP**
Εφαρμογής	Εφαρμογής
Παρουσίασης	Απόντα από μοντέλο
Συνόδου	Απόντα από μοντέλο
Μεταφοράς	Μεταφοράς
Δικτύου	Διαδικτύου
Ζεύξης Δεδομένων	Host προς δίκτυο
Φυσικό	

Πίνακας 1



Πίνακας 2.1



Πίνακας 2.2

3.4 Πλεονεκτήματα μειονεκτήματα σε σχέση με άλλα πρωτόκολλα

Το πρωτόκολλο Internet χρησιμοποιεί τις διευθύνσεις IP, για να στείλει πληροφορίες σπασμένες σε κομμάτια, τα οποία ονομάζονται πακέτα, σε όλο το Internet. Μερικές φορές τα πακέτα που μεταδίδονται έχουν υποστεί ζημία, δεν μπορούν να βρουν την διεύθυνση της μηχανής που είναι ο παραλήπτης τους ή έχουν κολλήσει σε ένα κύκλο αναμετάδοσης από πολλές μηχανές. Ένα νούμερο, το οποίο είναι αποθηκευμένο στο πρώτο κομμάτι ενός πακέτου IP (γνωστό και σαν *επικεφαλίδα IP),* μειώνεται κάθε φορά που ένα πακέτο δεν μπορεί να βρει μια διαδρομή προς τον δέκτη. Όταν το νούμερο αυτό φτάσει 0, το πακέτο θεωρείται «χαμένο». Εφόσον κάθε πακέτο μεταδίδεται μόνο του, δεν υπάρχει εγγύηση ότι δύο συνεχόμενα πακέτα θα επιλέξουν την ίδια διαδρομή προς τον προορισμό, ή ότι κατά την άφιξη τους στον δέκτη αυτά τα πακέτα θα τοποθετηθούν με την σειρά με την οποία μεταδόθηκαν. Αυτές τις δυσλειτουργίες λύνει το πρωτόκολλο Internet. Επιπλέον τα δεδομένα δεν έχουν αρίθμηση κατά την αποστολή για να είναι σίγουρη η σωστή επανασύνταξη τους από τον δέκτη. Από την στιγμή που μια πληροφορία ξεκινάει από τον δέκτη ο πομπός δεν μπορεί να κάνει τίποτα για να εγγυηθεί την πληρότητα και ασφάλεια της. Παρόλο που τα πακέτα IP δεν χρειάζεται να ανησυχούν για την σειρά των αποσταλμένων δεδομένων, η για το αν θα πάρει τα-

δεδομένα ο δέκτης, η ταχύτητα του πρωτοκόλλου για μεταδώσεις δεδομένων μέσα από το δίκτυο η ταχύτητα είναι ανυπερέαστη.
Η ανάγκη για μέτρηση των δεδομένων και κατάταξη της πληροφορίας οδήγησε στην ανάπτυξη του πρωτοκόλλου TCP. Αυτό χρησιμοποιεί αριθμούς που μεγαλώνουν για να εντοπίσει ποίο κομμάτι της συγκεκριμένης μετάδοσης περιέχεται σ' ένα πακέτο, και με ποία σειρά θα πρέπει να ταξινομηθούν τα πακέτα.. Αν μια συγκεκριμένη μετάδοση που χρησιμοποιεί το πρωτόκολλο φτάσει στην μηχανή δέκτη με τέσσερα από τα έξι πακέτα, με την σειρά **1, 3, 5, 2** , η μηχανή δέκτης θα ταξινομήσει αυτά τα πακέτα, και θα αποθηκεύσει αυτά τα πακέτα, καθώς θα στείλει και ένα μήνυμα στην μηχανή πομπό ότι τα πακέτα **4, 6** πρέπει να ξανασταλθούν. Όταν όλα τα πακέτα μετάδοσης ληφθούν κανονικά από την μηχανή δέκτη, τα πακέτα τοποθετούνται σωστά και η μετάδοση ολοκληρώνεται. Με το πρωτόκολλο αυτό οι Η/Υ μπορούν να προσομοιώσουν, μέσα από μία μη-ευθύ και ασυνεχές σύνδεση, μια ευθεία σύνδεση μεταξύ δύο Η/Υ. Μια εκπομπή με TCP χρησιμοποιεί ένα καλό κομμάτι της αρχικής επικοινωνίας μεταξύ μηχανών, και επιπλέον πληροφορίες που μεταδίδονται για να διατηρήσουν συνεχή την επικοινωνία μεταξύ των μηχανών κατά την διάρκεια της μετάδοσης.
Το πρωτόκολλο TCP εισάγει στο πρωτόκολλο IP την έννοια των *αριθμών θυρών*. Αυτή είναι μια σημαντική τεχνική σ' αυτόν τον κόσμο της πληροφορίας. Με την χρήση τους το TCP αναγνωρίζει ποία υπηρεσία ζητείται από την μηχανή δέκτη. Χωρίς τους αριθμούς θυρών, η μηχανή δέκτης δεν θα γνώριζε εάν η εισερχόμενη πληροφορία πρέπει να διαχειριστεί από το σύστημα ηλεκτρονικού ταχυδρομείου στο συγκεκριμένο μηχάνημα ή εάν είναι αίτηση για μία από τις σελίδες του δικτυακού τόπου που τρέχει σ' αυτή την μηχανή και πρέπει να πρέπει να επεξεργαστεί από λογισμικό του web server. Οι αριθμοί θυρών είναι νούμερα μεταξύ 0 και 65.000, που επιτρέπει στις μεταδόσεις να κατευθύνονται στο συγκεκριμένο κομμάτι λογισμικού που 'ακούει' την συγκεκριμένη θύρα. Μια θύρα σε έναν Η/Υ ορίζεται από την διευθυνσιωδότηση του πρωτοκόλλου IP της μηχανής στην οποία η θύρα είναι ενεργή, Οι αριθμοί θυρών κάτω του 1024 θεωρούνται προνομιούχοι αριθμοί και τους έχουν μόνο οι διαχειριστές συστήματος, οι οποίοι είναι υπεύθυνοι για την λειτουργία λογισμικού στις θύρες αυτές. Αυτό γίνεται για λόγους ασφάλειας. Εάν κάποιο άτομο μπορούσε να βάλει στην θύρα που είναι αρμόδια για το ηλεκτρονικό ταχυδρομείο, ένα λογισμικό που να ακούει τα εισερχόμενα μηνύματα, τότε θα μπορούσε να έχει πρόσβαση στην ηλεκτρονική αλληλογραφία.
Το πρωτόκολλο UPD είναι απλούστερο από το TCP. Παρέχει σαν επιπρόσθετη εφαρμογή αυτών του IP, αριθμούς θυρών, και έχει μια προαιρετική εφαρμογή ακεραιότητας δεδομένων που ονομάζεται "check summing". Το check summing επιτρέπει σε μία μηχανή δέκτη να πει εάν τα δεδομένα που έλαβε σε πακέτο UPD είναι σωστά, ή εάν προέκυψαν κάποια λάθη κατά την διάρκεια της επικοινωνίας. Από την στιγμή που το UPD δεν παρέχει κάποια μέσα για να γίνεται γνωστή η αριθμητική κατάταξη των πακέτων μεγάλων εκπομπών, είναι ώριμο να χρησιμοποιείται σε εκπομπές μικρού μήκους. Εφόσον υπάρχει μόνο ένα πακέτο σε τέτοιες εκπομπές κάθε αρίθμηση πακέτων θα καταλάμβανε άχρηστο χώρο. Έτσι η χρήση του πρωτοκόλλου αυτού γίνεται εξαιρετικά σπάνια.

3.5 Πεδία που περιέχονται σε ένα πακέτο IP

Έκδοση	IHL	Τύπος υπηρεσίας	Συνολικό μήκος		
Ταυτότητα			DF	MF	Θέση τεμαχίου
Χρόνος ζωής		Πρωτόκολλο	Άθροισμα ελέγχου Επικεφαλίδας		
Διεύθυνση πηγής					
Διεύθυνση προορισμού					
Προαιρετικές επιλογές					

Πίνακας 3

Το πεδίο **Τύπος υπηρεσίας** επιτρέπει στον host να πει στο υποδίκτυο το είδος της υπηρεσίας που επιθυμεί.
Το πεδίο **Συνολικό μήκος** περιλαμβάνει τα πάντα που βρίσκονται μέσα στο πακέτο, τόσο στην επικεφαλίδα όσο και στα δεδομένα.
Το πεδίο **Ταυτότητα** χρειάζεται για να επιτρέπει στον host προορισμού να καθορίσει σε ποίο πακέτο ανήκει το καινούργιο τεμάχιο.
Το **DF** σημαίνει (don't fragments) μην τεμαχίζεις, ενώ το **MF** (more fragments) σημαίνει περισσότερα τεμάχια.
Το πεδίο **Θέση τεμαχίου** πληροφορεί για το σε ποίο σημείο του τρέχοντος πακέτου ανήκει το τεμάχιο αυτό.
Το πεδίο **Χρόνος ζωής** είναι ένας μετρητής που χρημοποιείται για να περιορίσει την διάρκεια ζωής των πακέτων.
Το πεδίο **Πρωτόκολλο** λέει σε ποία διαδικασία μεταφοράς να δώσει ένα πακέτο που μόλις έχει ολοκληρωθεί.
Το πεδίο **Άθροισμα ελέγχου επικεφαλίδας** ελέγχει μόνο την επικεφαλίδα. Ένα τέτοιο άθροισμα είναι χρήσιμο για την ανίχνευση λαθών που δημιουργούνται από χαλασμένες λέξεις μνήμης μέσα σ ένα δρομολογητή.
Τα πεδία **Διεύθυνση πηγής** και **Διεύθυνση προορισμού** δείχνουν τον αριθμό του δικτύου και τον αριθμό host
Τέλος το πεδίο **Προαιρετικές επιλογές** σχεδιάστηκε για να προσφέρει μια διέξοδο, ώστε οι επόμενες εκδόσεις του πρωτοκόλλου να περιλαμβάνουν πληροφορίες που δεν ήταν παρούσες στην αρχική σχεδίαση, να επιτρέπει την δοκιμή νέων ιδεών και για να αποφευχθεί η εκχώρηση bit της επικεφαλίδας σε πληροφορίες που σπάνια είναι αναγκαίες.

4. Νέες τεχνολογίες

4.1 IPv6

Η ανάγκη για περισσότερη και ποίο έγκυρη πληροφόρηση οδηγούν στην βελτίωση και την αναβάθμιση των διαδικτύων, καθώς και των πρωτοκόλλων που τα διέπουν. Έτσι και το πρωτόκολλο IP αναβαθμίστηκε από την IETF, σε μία νεότερη έκδοση, που δεν θα ξέμενε από διευθύνσεις, θα έλυνε μια ποικιλία από άλλα προβλήματα και θα ήταν περισσότερο ευέλικτη και αποδοτική. Οι κύριοι στόχοι του ήταν:

- Να υποστηρίξει δισεκατομμύρια host, ακόμη και με αναποτελεσματικό καταμερισμό του χώρου των διευθύνσεων.
- Να μειώσει το μέγεθος των πινάκων δρομολόγησης.
- Να απλοποιήσει το πρωτόκολλο για να επιτρέψει στους δρομολογητές να επεξεργάζονται τα πακέτα ταχύτερα.
- Να παρέχει καλύτερη ασφάλεια από το παρόν πρωτόκολλο.
- Να επιδείξει περισσότερη προσοχή στον τύπο της υπηρεσίας, ειδικά στα δεδομένα πραγματικού χρόνου.
- Να βοηθήσει την πολλαπλή διανομή με το να επιτρέπει τον καθορισμό ακτινών δράσης.
- Να επιτρέψει την περιπλάνηση χωρίς αλλαγή της διεύθυνσης του host.
- Να επιτρέψει στο πρωτόκολλο να μετεξελιχθεί αργότερα.
- Να επιτρέψει την συνύπαρξη παλιών και νέων πρωτοκόλλων για χρόνια.

Για να βρει ένα πρωτόκολλο που να ικανοποιεί όλες τις παραπάνω απαιτήσεις , η IETF εξέδωσε μια πρόσκληση για τις προτάσεις και συζήτηση στο RFC 1550. Παρέλαβε 21 απαντήσεις, όχι όλες τους ολοκληρωμένες προτάσεις. Μέχρι τον Δεκέμβριο του 1992, στο τραπέζι βρίσκονταν εφτά σοβαρές προτάσεις. Εκτείνονταν από μικρές επιδιορθώσεις του IP, μέχρι την ολική απόρριψη τού και την αντικατάσταση του με ένα εντελώς διαφορετικό πρωτόκολλο.

Μια πρόταση ήταν να τρέχει το TCP πάνω από το CLNP, που με διευθύνσεις των 160bit θα παρείχε αρκετό χώρο διευθύνσεων για πάντα και θα ενοποιούσε δύο κύρια πρωτόκολλα στρώματος δικτύου. Ωστόσο, πολλοί είπαν ότι αυτό θα ήταν μια παραδοχή ότι θα υπήρχε κάτι στον κόσμο του OSI που δεν είχε γίνει σωστά, μία δήλωση που θεωρείται πολιτικά λανθασμένη στους κύκλους του Internet. Το CLNP καθορίσθηκε να μοιάζει με το IP, έτσι ώστε τα δύο να μην διαφέρουν τόσο πολύ μεταξύ τους. Στην πραγματικότητα, το πρωτόκολλο που τελικά επιλέχθηκε διαφέρει από το IP πολύ περισσότερο από το CLNP. Ένα άλλο πλήγμα κατά του CLNP ήταν η αδυναμία του για υποστήριξη τύπων υπηρεσιών, κάτι που είναι απαραίτητο για την αποδοτική μετάδοση των πολυμέσων.

Μετά από αρκετές συζητήσεις, αναθεωρήσεις και διαγκονισμούς, επιλέχθηκε μια τροποποιημένη έκδοση του συνδυασμού των προτάσεων του Deering και Francis που τώρα καλείται SIPP (simple internet protocol plus) και της δόθηκε ο χαρακτηρισμός IPv6 (Το IPv5 βρισκόταν ήδη σε χρήση για ένα πειραματικό πρωτόκολλο ροής πραγματικού χρόνου).

Το IPv6 εκπληρώνει τους στόχους που προαναφέραμε αρκετά καλά. Διατηρεί τα καλά χαρακτηριστικά του IP, απορρίπτει ή υποβιβάζει τα κακά και προσθέτει καινούργια εκεί

που χρειάζεται. Γενικά, το IPv6 δεν είναι συμβατό με το IPv4, αλλά είναι συμβατό μ' όλα τα άλλα πρωτόκολλα του Internet, συμπεριλαμβανομένων των TCP,UPD,ICMP,IGMP,OSPF,BPS,DNS μερικές φορές μετά από αναγκαίες μικρές μετατροπές. Παρακάτω θα δούμε τα κύρια χαρακτηριστικά του IPv6.
Πρώτα απ' όλα, το IPv6 έχει μακρύτερες διευθύνσεις άπο το IPv4. Έχουν μήκος 16bit, που λύνει το πρόβλημα λύση του οποίου ήταν το IPv6:να προμηθεύσει μια πρακτικά απεριόριστη δεξαμενή από διευθύνσεις Internet.
Η δεύτερη μεγάλη βελτίωση του IPv6 είναι η απλοποίηση της επικεφαλίδας. Περιέχει μόνο εφτά πεδία (έναντι δεκατεσσάρων του IPv4). Αυτή η αλλαγή επιτρέπει στους δρομολογητές να επεξεργαστούν τα πακέτα ταχύτερα και έτσι να βελτιώσουν την διέλευση.
Η Τρίτη μεγάλη βελτίωση ήταν η καλύτερη υποστήριξη για επιλογές. Αυτή η αλλαγή ήταν απαραίτητη λόγω της καινούργιας επικεφαλίδας, διότι πεδία τα οποία προηγουμένως ήταν αναγκαία τώρα είναι προαιρετικά. Επιπλέον, είναι διαφορετικός ο τρόπος που παρουσιάζονται τα προαιρετικά, κάτι που διευκολύνει τους δρομολογητές να παραλείψουν όσα δεν προορίζονται για αυτούς. Αυτό επιταχύνει την επεξεργασία των πακέτων.
Μία τέταρτη περιοχή στην οποία το IPv6 παρουσιάζει βελτίωση είναι η ασφάλεια.. Η πιστοποίηση αυθεντικότητας (authentication) και η μυστικότητα (privacy) είναι καίρια χαρακτηριστικά του νέου IP.
Τελικά, έχει δοθεί περισσότερη προσοχή στον τύπο της υπηρεσίας απ' ότι στο παρελθόν. Το IPv4 έχει πράγματι ένα πεδίο 8bit αφιερωμένο στον σκοπό αυτό, αλλά με την αναμενόμενη ανάπτυξη της κίνησης πολυμέσων στο μέλλον, χρειάζεται πολύ περισσότερο.

Η σταθερή επικεφαλίδα του IPv6

Η επικεφαλίδα του πρωτοκόλλου φαίνεται στο παρακάτω σχήμα.

----------**32 Bit**----------

Έκδοση	Προτεραιότητα	Ετικέτα Ροής
Μήκος ωφέλιμου φορτίου	Επόμενη επικεφαλίδα	Όριο βημάτων
Διεύθυνση πηγής (16 byte)		
Διεύθυνση προορισμού (16 byte)		

Πίνακας 4

Το πεδίο **έκδοση** είναι πάντα 6 στο IPv6 και 4 στο IPv4. Κατά την περίοδο μετάβασης από το ένα στο άλλο, οι δρομολογητές θα είναι σε θέση να εξετάζουν αυτό το πεδίο για να δουν τι είδους πακέτο έχουν. Η εκτέλεση αυτού του ελέγχου σπαταλά μερικές εντολές επανειλημμένα, έτσι πολλές εφαρμογές είναι πιθανόν να προσπαθήσουν να τον αποφύγουν χρησιμοποιώντας κάποιο πεδίο στην επικεφαλίδα ζεύξης δεδομένων ώστε να ξεχωρίζουν τα πακέτα IPv4 από τα IPv6. Κατ' αυτόν τον τρόπο, τα πακέτα μπορούν να περάσουν απ' ευθείας στον σωστό χειριστή στρώματος δικτύου.
Το πεδίο **προτεραιότητα** χρησιμοποιείται για την διάκριση μεταξύ των πακέτων, των οποίων η ροή των πηγών τους μπορεί να ελεγχθεί και αυτών που δεν μπορεί να γίνει κάτι τέτοιο.

Το πεδίο **Ετικέτα ροής** είναι ακόμη πειραματικό, αλλά θα χρησιμοποιηθεί για να επιτρέψει στην πηγή και στον προορισμό να εγκαταστήσουν μια ψευδό-σύνδεση με ιδιαίτερες ιδιότητες και απαιτήσεις.
Το πεδίο **Μήκος ωφέλιμου φορτίου** πληροφορεί για το πόσα byte ακολουθούν την επικεφαλίδα 40 byte. Το όνομα άλλαξε από **Συνολικό μήκος** που ήταν στο IPv4 επειδή άλλαξε ελαφρώς και το νόημα: τα 40 byte της επικεφαλίδας δεν μετριούνται πια ως μέρος του μήκους όπως γινόταν πριν.
Το πεδίο **Επόμενη επικεφαλίδα** είναι αυτό που απελευθερώνει. Ο λόγος που η επικεφαλίδα απλοποιήθηκε είναι ότι μπορούν να υπάρξουν πρόσθετες επικεφαλίδες επέκτασης. Αυτό το πεδίο καθορίζει το ποία, αν υπάρχει καμία , από τις έξι επικεφαλίδες επέκτασης ακολουθεί.
Το πεδίο **Όριο βημάτων** χρησιμοποιείται για να μην αφήνει τα πακέτα να ζουν για πάντα. Πρακτικά είναι το ίδιο με το **χρόνος ζωής** του IPv4, δηλαδή ένα πεδίο που μειώνεται σε κάθε βήμα.
Τέλος τα πεδία **Διεύθυνση πηγής** και **Διεύθυνση προορισμού.** Η αρχική πρόταση του Deering, το SIP, χρησιμοποιούσε διευθύνσεις των 8 byte, άλλα κατά την διάρκεια της αναθεώρησης πολλοί αισθάνθηκαν ότι με διευθύνσεις των 8 byte το IPv6 σε λίγες δεκαετίες θα ξέμενε από διευθύνσεις, ενώ με διευθύνσεις των 16 byte δεν θα ξέμενε ποτέ. Άλλοι διαφώνησαν και είπαν ότι τα 16 byte ήταν πολύ περισσότερα απ' όσα απαιτούνταν, άνω άλλοι προτιμούσαν διευθύνσεις των 20 byte για να είναι συμβατές με το πρωτόκολλο των δεδομενογραφημάτων του OSI. Μετά από πολύ συζήτηση αποφασίσθηκε ότι η καλύτερη συμβιβαστική λύση ήταν οι διευθύνσεις σταθερού μήκους των 16 byte.

4.2 Ασύρματα δίκτυα

Η δικτύωση των υπολογιστών στις επιχειρήσεις αποτελεί πλέον υπόθεση ρουτίνας, τα δε οφέλη της είναι πολύπλευρα και αναγνωρισμένα, ακόμη και για πολύ μικρές εταιρίες.
Η εγκατάσταση ενός επιχειρησιακού δικτύου είναι μία απλή υπόθεση, η οποία ωστόσο απαιτεί σεβασμό και πρέπει να γίνει με προσεκτικά βήματα κατά την επιλογή εξοπλισμού καθώς και κατά την σχεδίαση της τοπολογίας του δικτύου. Ενώ τα παραπάνω αποτελούν κανόνα σε κτιριακή εγκατάσταση ενός κτιρίου, οι λύσεις για την δικτύωση μεταξύ διαφορετικών κτιρίων απαιτούν μία εντελώς διαφορετική αντιμετώπιση, για την οποία προτείνονται διάφορες λύσεις.
Για απομακρυσμένες κτιριακές εγκαταστάσεις μία λύση είναι οι ασύρματες συνδέσεις. Ένα παράδειγμα είναι η επικοινωνία μεταξύ διαφορετικών κτιρίων μιας εταιρίας, χωρίς καλωδιακή σύνδεση. Τα προϊόντα που υπάρχουν αυτή την στιγμή στην αγορά, επιτρέπουν την δημιουργία ενός πλήρους ασύρματου δικτύου. Υπάρχουν όμως δύο περιορισμοί: αφ ενός το περιοριστικό κόστος και αφετέρου οι σχετικά χαμηλές ταχύτητες σε σχέση με το παραδοσιακό παραδοσιακό Ethernet των 10Mbps και το fast Ethernet με ταχύτητες 100Mbps.

Εφαρμογές ασυρμάτων δικτύων

Ανεξάρτητα από το γνωστό πλαίσιο ενός υπολογιστικού δικτύου, οι ασύρματες επικοινωνίες μπορούν να καλύψουν επικοινωνιακές ανάγκες σε ειδικές περιπτώσεις. Για

παράδειγμα, σε ιστορικούς χώρους που ακόμα και εάν η καλωδίωση είναι τεχνολογικά εφικτή, είναι τελικά μη αποδεκτή. Τότε, η ασύρματη επικοινωνία αποτελεί τον πλέον κομψό τρόπο. Μία άλλη εφαρμογή είναι η εγκατάσταση σε σημεία που τα καλώδια αποτελούν εμπόδιο ή απαιτείται συχνή μετακίνηση εξοπλισμού.
Τα ασύρματα τερματικά σε αποθήκες είναι μία άλλη γνωστή εφαρμογή των ασύρματων δικτύων που εξασφαλίζει άμεση ενημέρωση των κεντρικών συστημάτων.
Η σύνδεση μίας εταιρίας στο Internet αποτελεί επίσης μία δυνατή εφαρμογή της ασύρματης επικοινωνίας (υπό την προϋπόθεση να παρέχεται από τον provider). Η τελευταία περίπτωση είναι άκρως ενδιαφέρουσα, με δεδομένο το γεγονός ότι μία ασύρματη σύνδεση στα 2Mbps εξασφαλίζει μεγαλύτερη ταχύτητα από μία γραμμή T1.

Κατηγορίες Ασύρματων δικτύων φωνής

AMPS (Advanced Mobile Phone System). Το AMPS είναι ένα υπάρχον σύστημα κινητής τηλεφωνίας που χρησιμοποιείται στην Αμερική. Η επικοινωνία των χρηστών του κυτταρικού συστήματος με τους χρήστες της PSTN, γίνετε μέσω σημείων πρόσβασης, τα οποία λειτουργούν σαν πύλες. Υπάρχει ένας κεντρικός σταθμός οποίος επικοινωνεί μέσω ασύρματων και ενσύρματων δεσμευμένων γραμμών με τα σημεία πρόσβασης, για να ελέγχει την εγκατάσταση, λειτουργία και αποδέσμευση της γραμμής. Στο AMPS οι κυψέλες έχουν μέγεθος 100(km)2 για την ύπαιθρο. Καθώς ένα κινητό τηλέφωνο κινείται μεταξύ γειτονικών κυψελών, γίνετε αυτόματη αναπροσαρμογή έτσι ώστε να βρεθεί ένα ανταποκρινόμενο σημείο πρόσβασης.
Το να στείλεις δεδομένα με το υπάρχον κυτταρικό-αναλογικό δίκτυο είναι μία διαδικασία όχι και τόσο αποδοτική. Πρώτα ο χρήστης πρέπει να συνδεθεί στο δίκτυο , το οποίο παίρνει συνήθως 20 με 30 δευτερόλεπτα. Αφού εγκατασταθεί η σύνδεση , οι συνθήκες διάδοσης που επικρατούν μπορεί να προκαλέσουν handoff μεταξύ των πλευρών της κυψέλης. Ο ρυθμός των λαμβανόμενων δεδομένων είναι συνήθως γύρω στα 4,8 Kbps.

GSM. Το GSM είναι το Ευρωπαϊκό κυτταρικό σύστημα. Παρουσιάστηκε πρώτη φορά το 1992, και σήμερα είναι ευρέως διαδεδομένο στην Ευρώπη και σταδιακά αρχίζει να κατακτά την Ασία και την Αυστραλία. Πριν την εισαγωγή του GSM οι ευρωπαϊκές χώρες είχαν μη συμβατά εθνικά στάνταρ για τα κυτταρικά συστήματα.. Το GSM σήμερα επεκτείνετε για να μεταφέρει δεδομένα στα 9,6Kbps. Η υπηρεσία του GSM για την αποστολή μηνυμάτων προς το παρόν επιτρέπει την αποστολή μηνυμάτων μέχρι 420 χαρακτήρες. Στο GSM ένα τηλέφωνο μπορεί να συνδεθεί με έναν υπολογιστή και να πραγματοποιήσει έτσι μέσω του GSM επικοινωνία Η/Υ. Αυτό μπορεί να γίνει με την σύνδεση μίας κάρτας Η/Υ με τον Η/Υ η οποία με την βοήθεια ενός καλωδίου προσαρμόζεται στο τηλέφωνο.

Ψηφιακά Κυτταρικά Συστήματα 2ης Γενιάς στις ΗΠΑ. Η ανάπτυξη του ψηφιακού κυτταρικού συστήματος άρχισε στις ΗΠΑ το 1995. Υπάρχουν δύο τεχνολογίες στο σύστημα αυτό, που σκοπό έχουν την παροχή υψηλής χωρητικότητας: η TDMA (Time Multiple Access) και η CDMA (Code Division Multiple Access). Η TIA (Telecommunications Industries Association) υιοθέτησε πρότυπα και από τις δύο τεχνολογίες το 1993.

Στο CDMA η βασική ιδέα είναι ότι σε κάθε κλήση παραχωρείται ένας ψηφιακός κωδικός που την ξεχωρίζει από τις άλλες κλήσεις, που μοιράζονται το ίδιο φάσμα. Η TDMA τεχνική χωρίζει το φάσμα σε κανάλια στην διάσταση του χρόνου και παραχωρεί σε κάθε συνομιλία ένα συγκεκριμένο κανάλι. Συμπιέζει τρεις κλήσεις σ' ένα μόνο κανάλι μετάδοσης με εύρος 30KHz.

PCS. Το PCS είναι ένα αμερικάνικο ψηφιακό κυτταρικό σύστημα που προσφέρει υπηρεσίες όπως paging και ηλεκτρονικό ταχυδρομείο με ήχο. Η διαφορά του με τα παραδοσιακά ψηφιακά κυτταρικά συστήματα είναι το μικρό μέγεθος της κάλυψης των κυψελών. Στο PCS οι κυψέλες τυπικά είναι σε διάταξη του ενός τετάρτου του χιλιομέτρου, κάτι που επιτρέπει στα σημεία πρόσβασης να είναι μικρά και φτηνά. Το μικρό μέγεθος των κυψελών επιτρέπει επίσης στα σημεία πρόσβασης να μεταδίδουν και να λαμβάνουν με μικρότερη ισχύ, επιτρέποντας στους μεταφερόμενους αποδέκτες να είναι ελαφροί και οι μπαταρίες τους να διαρκούν πολύ. Το μεγάλο μέγεθος κυψέλης στα παραδοσιακά κυτταρικά συστήματα συγκριτικά με το PCS έχει σαν αποτέλεσμα να μπορούν να υποστηρίξουν μεγαλύτερο αριθμό χρηστών ανά κυψέλη. Μείωση του μεγέθους της κυψέλης αυξάνει την συνολική χωρητικότητα του συστήματος , με το να επιτρέπει μεγαλύτερη επαναχρησιμοποίηση συχνότητας σε συγκεκριμένη περιοχή. Σε σχέση με το αναλογικό κυτταρικό σύστημα το PCS έχει καλύτερη ποιότητα ήχου, φθηνότερες τιμές και παρέχει περισσότερες υπηρεσίες.

PCN. Το PCN στηρίζεται στην ιδέα της χρησιμοποίησης ενός μοναδικού αναγνωριστικού αριθμού από ένα συγκεκριμένο άτομο. Όλη η κίνηση που αφορά το συγκεκριμένο άτομο φθάνει στο άτομο αυτό οπουδήποτε και αν βρίσκεται. Για να μπορεί να εφαρμοσθεί μια ιδέα το άτομο θα πρέπει να είναι διατεθειμένο να μεταφέρει μια ασύρματη συσκευή επικοινωνίας, όπου και εάν πηγαίνει.

DECT. Το σύστημα DECT είναι μία Ευρωπαϊκή ασύρματη τηλεφωνική υπηρεσία κυρίως για το σπίτι ή για επιχειρήσεις. Παρόλο που περιλαμβάνει υπηρεσία για μετάδοση δεδομένων , είναι ανεπαρκές γιατί είναι ένα σύστημα προσανατολισμένο σε σύνδεση με πολύ μεγάλο χρόνο εγκατάστασης της σύνδεσης και τερματισμό της σύνδεσης ανά κλήση. Τα συστήματα που είναι προσανατολισμένα σε σύνδεση επιβάλουν μεγάλη καθυστέρηση ακόμα και αν πρόκειται για μικρή μετάδοση δεδομένων. Γίνεται προσπάθεια από αρκετές εταιρίες τηλεπικοινωνιών για βελτίωση της διεπαφής του DECT με τα LAN.

PHS. Στην Ιαπωνία μία νέα ψηφιακή ασύρματη τηλεφωνική υπηρεσία ονομάζεται PHS (Personal Handyphones System). Το σύστημα κοστίζει σχεδόν όσο και η συμβατή κινητή τηλεφωνία και το ασύρματο τηλέφωνο είναι μικρότερο και ελαφρύτερο από τα άλλα κυτταρικά τηλέφωνα.]
Όλα αυτά τα υπάρχοντα ασύρματα δίκτυα ευρείας περιοχής (WANs) εξυπηρετούν μια συγκεκριμένη ανάγκη: αυτή της σύνδεσης τω κινούμενων χρηστών έτσι ώστε να μπορούν να κάνουν και να λαμβάνουν τα τηλεφωνήματα τους τα e-mail κ.α. Ήδη κάποια συστήματα μπορούν να υποστηρίξουν μετάδοση ήχου, δεδομένων και βίντεο προς και από φορητό υπολογιστή.

5. IPsec

5.1 Ασφάλεια δικτύων

Το πεδίο της πληροφορικής συνθέτει έναν ιδιόρρυθμο κόσμο. Πέρα από τις ιδιαιτερότητες και τα αρνητικά σημεία που κάθε επιστημονικό πεδίο έχει και προσπαθεί να τις μειώσει, το πληροφορικό πεδίο παρουσιάζει πρόσθετα προβλήματα εξαιτίας της αυτονομίας των χρηστών. Η γνώση του είναι επιφανειακή και ο έλεγχος ανύπαρκτος, περιορισμένος σε μερικές τυπικές λειτουργίες.
Η νομοθεσία διαφόρων χωρών επιχειρεί εδώ και περισσότερο από δύο δεκαετίες να ορίσει και να θέσει τα όρια που άπτονται του πληροφορικού εγκλήματος, διαχωρίζοντας το νομικά επιτρεπτό με το νομικά ανεπίτρεπτο. Οι αρχικές νομοθεσίες, που αναπτύχθηκαν πρόσφεραν ένα γενικό πλαίσιο του πληροφοριακού εγκλήματος και επέκρουσε να το αντιμετωπίσει κυρίως με ποινικές μεθόδους ασύμβατες με την φύση και την σχέση της πληροφορικής.
Στο κεφάλαιο αυτό θα ασχοληθούμε με τα 'κακά ' της Πληροφορικής, με τους ιούς (virus) και τις διάφορες παραλλαγές τους, όπως τα σκουλήκια (worms) και οι δούρειοι ίπποι (Trojan horses). Θα ασχοληθούμε επίσης με την παραβίαση προσωπικών δεδομένων στο διαδίκτυο και θα γνωρίσουμε τις έννοιες hacker,cracker. Τέλος θα αναφερθούμε στους τρόπους αντιμετώπισης των παραπάνω.

5.1.1 Ιός

Ο ιός αποτελεί τον πιο διαδεδομένο και συχνό τρόπο μόλυνσης των Η/Υ. Όταν αναφερόμαστε σε ιούς, εννοούμε προγράμματα τα οποία έχουν δημιουργηθεί για να διεισδύουν στο Η/Υ χωρίς την έγκριση μας και να μολύνουν άλλα αρχεία, προκαλώντας σημαντικές ζημιές.

Τα βασικά χαρακτηριστικά ενός ιού είναι:

- Μπορεί να αναπαράγει τον εαυτό του σε δισκέτες, σκληρούς δίσκους, αρχεία και μηνύματα ηλεκτρονικού ταχυδρομείου.
- Συνήθως, εκτελείται στον υπολογιστή χωρίς την έγκριση του κατόχου του και, τις περισσότερες φορές, χωρίς καν να γίνει αντιληπτή η δραστηριότητα αυτή.

Ανάλογα με τον ιό, οι συνέπειες από την μόλυνση μπορεί να είναι από μηδαμινές έως καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές στο τοπικό δίκτυο ή στο διαδίκτυο. Υπάρχουν αρκετά ήδη ιών:

1. *Ιοί τομέα εκκίνησης,* που προσβάλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου και είναι εξαιρετικά σπάνια σήμερα.
2. *Ιοί προγραμμάτων,* που προσβάλουν εκτελέσιμα αρχεία.
3. *Ιοί μακροεντολών,* που κρύβονται σε μακροεντολές, όπως του Word και του Excel.
4. *Πολυμορφικοί,* οι οποίοι μπορεί να ανήκουν σε μερικές ή σε όλες τις παραπάνω κατηγορίες.

5.1.2 Σκουλήκια

Τα σκουλήκια είναι παρασιτικά προγράμματα που μπορούν να αναπαράγουν τον εαυτό τους αλλά δεν μολύνουν άλλα αρχεία στον υπολογιστή που προσβάλουν. Κάνουν χρήση του ηλεκτρονικού ταχυδρομείου, για να πολλαπλασιάζονται και να εξαπλώνονται πιο εύκολα και με μεγαλύτερη ταχύτητα λόγω της εύκολης επικοινωνίας των χρηστών.
Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα μηνύματα ηλεκτρονικού ταχυδρομείου σε όλη την λίστα επαφών του χρήστη. Η μαζική αποστολή ηλεκτρονικού ταχυδρομείου, εκτός από την σπατάλη του ήδη μικρού εύρους ζώνης του modem σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Διαδικτύου, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας.

5.1.3 Δούρειοι Ίπποι

Πρόκειται για προγράμματα που, ενώ εμφανίζονται σαν κανονικά προγράμματα για την εκτέλεση μιας εργασίας στον υπολογιστή, κρυφά εκτελούν κάποια διαφορετική, συνήθως κακόβουλη. Αποτελούνται από δύο μέρη, τον πελάτη και τον διακομιστή. Ο διακομιστής κρύβεται με κάποιο τρόπο στον υπολογιστή του θύματος και ο πελάτης εκτελείται στο μηχάνημα του θύτη. Από την στιγμή που ο χρήσης του υπό επίθεση υπολογιστή συνδεθεί με το Διαδίκτυο, ο διακομιστής του δουρείου ίππου, που εκτελείται σιωπηρά στο παρασκήνιο, στέλνει ένα σήμα το οποίο λαμβάνει ο πελάτης. Στην συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο κακόβουλος χρήστης (cracker) αποκτά πρόσβαση στον υπολογιστή στόχο.
Από την στιγμή που εγκαθιδρύεται μεταξύ τους η συνεδρία, ο κακόβουλος χρήστης μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη – π.χ ανοιγοκλείνοντας το συρταράκι του CD-ROM. Μπορεί όμως και να του διαγράψει αρχεία ή ακόμη και να προκαλέσει ζημίες στο υλικό του υπολογιστή, όπως να διαγράψει το BIOS ή να καταστρέψει τον σκληρό δίσκο. Μία άλλη λειτουργία των προγραμμάτων αυτών είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πατάει το θύμα. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στον θύτη.

5.1.4 Η παραβίαση του προσωπικού απορρήτου

Είναι γεγονός ότι κάθε Διαδικτυακή επίσκεψη καταγράφεται, καθώς επίσης και ότι το ηλεκτρονικό σας ταχυδρομείο δεν είναι καθόλου ιδιωτικό.
Το ηλεκτρονικό ταχυδρομείο, αλλά και γενικότερα η ηλεκτρονική τεχνολογία, διευκόλυνε την ζωής μας, ταυτόχρονα όμως δημιούργησε δυνατότητες παραβίασης του προσωπικού απορρήτου και υποκλοπών που πριν από μερικά χρόνια ακόμη και η πιο νοσηρή φαντασία θα είχε προβλέψει. Σήμερα, δεν χρειάζεται κάποιος να παραβιάσει αλληλογραφία ή να τοποθετήσει κοριούς. Η ηλεκτρονική τεχνολογία δίνει την δυνατότητα παρακολούθησης όλων των δεδομένων που διακινούνται στον σύγχρονο κόσμο και, ταυτόχρονα, την επιλεκτική συλλογή και αποθήκευση αυτών.

5.1.5 Προβλήματα στο Διαδίκτυο

Τρύπα πρώτη η αρχιτεκτονική του: Σχεδιασμένο πριν από 30 χρόνια για να το χρησιμοποιούν μόνο μερικοί επιλεγμένοι χρήστες, το διαδίκτυο στηρίζεται σε μερικούς βασικούς διακομιστές ονομάτων. Είναι μηχανές που έχουν τις βασικές διευθύνσεις του Διαδικτύου και κατευθύνουν την κυκλοφορία των δεδομένων. Είναι 13 όλες και όλες στον κόσμο και έχουν ήδη δείξει τις αδυναμίες τους , γι' αυτό αποτελούν εύκολο στόχο.
Τρύπα δεύτερη, το λογισμικό. Από την φύση τους, ιοί είναι και αυτοί προγράμματα. Εκατομμύρια γραμμές οδηγιών , που δεν είναι πρακτικά δυνατόν να ελεγχθούν όλες πριν βγουν στην αγορά. Οι κυβερνο-πειρατές χρησιμοποιούν πολύ συχνά ιούς για να σπάσουν τους κωδικούς προσωπικών υπολογιστών ή ιστοσελίδων του δικτύου.
Τρύπα τρίτη , η ιδιωτική ζωή των χρηστών. Έχουν τόσα γραφτεί για την παραβίαση της, που τώρα απλώς συνειδητοποιούμε ότι πλέον γίνεται ενσυνείδητα. Γιατί εάν δεν γνωρίζεις τον χρήστη, δεν θα τον κάνεις πελάτη. Άρα δεν συμφέρει να τον προστατεύσεις κρύβοντας τα ίχνη του , γιατί δεν θα μάθεις ποτέ τι θέλει για να του πουλήσεις.
Τρύπα τέταρτη, η έλλειψη ικανών στελεχών που θα επαγρυπνούν για την ασφάλεια του διαδικτύου.

5.1.6 Hacker-Cracker

Ορισμός Hacker

Hacker είναι αυτός που του αρέσει να εξερευνά τις λεπτομέρειες συστημάτων και προγραμμάτων και αναπτύσσει τις ικανότητες του σε αυτά τα συστήματα, σε αντίθεση με τους περισσότερους χρήστες που απλώς προτιμούν να γνωρίζουν όσα χρειάζεται για να κάνουν την δουλεία τους. Κάποιος που προγραμματίζει γρήγορα, κάποιος που γνωρίζει καλά ένα συγκεκριμένο πρόγραμμα, κ.λ.π. Οι χάκερ δεν προσπαθούν να προκαλέσουν βλάβες στα συστήματα ή στα προγράμματα που ερευνούν. Αυτοί που έχουν σκοπό τις υποκλοπές και την πρόκληση βλάβης στα συστήματα ονομάζονται cracker.

Ορισμός Cracker

Συχνά διαβάζουμε για επιθέσεις σε εταιρικά δίκτυα και γνωστές τοποθεσίες του ιστού, για εξιστορήσεις περιστατικών όπου ο υπολογιστής συμπεριφερόταν περίεργα κ.α. Όπως αναφέραμε και πιο πάνω οι cracker είναι αυτοί που δημιουργούνε τα προβλήματα στο διαδίκτυο. Είναι αυτοί που αρέσκονται να σπάζουν κωδικούς πρόσβασης, να κλέβουν και να παραποιούν στοιχεία. Χρησιμοποιώντας διάφορες τεχνικές, καταφέρνουν να αποκτούν πρόσβαση σε υπολογιστικά συστήματα και να προκαλούν ζημίες προσποριζόμενοι οφέλη μέσω σωρείας εγκληματικών ενεργειών.

5.2 Ασφαλής μετάδοση δεδομένων σε δίκτυα που υποστηρίζουν το πρωτόκολλο IP

Οι ανάγκες των εταιριών ολοένα και μικρότερου μεγέθους για γεωγραφικά κατανεμημένα ιδιόκτητα δίκτυα επικοινωνιών, μεγαλώνουν μαζί με την πρόοδο της

τεχνολογίας που ενσωματώνουν τα δίκτυα αυτά. Η σημερινή πρακτικά μοναδική επιλογή για την υλοποίηση τέτοιων δικτύων είναι μέσω μισθωμένων γραμμών, οι οποίες όμως, για ανεκτές για τα σημερινά δεδομένα ταχύτητες, έχουν κάθε άλλο παρά αμελητέο κόστος.
Μια τακτική καλύτερης αξιοποίησης της επένδυσης αυτής είναι μέρος της κίνησης υπηρεσιών τηλεφωνίας να περνά μέσα από τις μισθωμένες γραμμές που χρησιμοποιούνται για δεδομένα. Το πρόβλημα θα μπορούσε να είναι τεχνικά απλό, όμως ότι η ασύγχρονη φύση των δικτυακών πρωτοκόλλων που χρησιμοποιούνται ευρέως, το καθιστά σημαντικά πιο σύνθετο και κάνει τη λύση να εμφανίζεται λιγότερο ελκυστική. Η χρήση ανοιχτών δικτύων και κυρίως του Internet απορρίπτεται από την αρχή, διότι δεν εξασφαλίζει την ασφάλεια των διακινούμενων πληροφοριών και η δελεαστικότερη των διαφαινόμενων επιλογών φαίνεται να είναι τα VPNs (Virtual Private Networks) τα οποία εμφανίζονται ελκυστικά για εταιρίες κάθε μεγέθους, με την προϋπόθεση ασφαλώς ότι εξασφαλίζεται η ασφάλεια στη μετάδοση δεδομένων.
Η υλοποίηση του όποιου σχήματος ασφάλειας μπορεί να γίνει σε οποιοδήποτε από τα επίπεδα με αναφορά στο πρότυπο OSI. Μια συνηθισμένη περίπτωση είναι αυτή κατά την οποία η κρυπτογράφηση των δεδομένων γίνεται στο επίπεδο εφαρμογής (το κοντινότερο στο χρήστη) με τη βοήθεια μηχανισμών κρυπτογράφησης έτοιμων δεδομένων. Ωστόσο, η έλλειψη προτύπων για ασφαλή μετάδοση δεδομένων σε χαμηλότερα επίπεδα στο πρότυπο OSI (επίπεδα 2 και 3) δημιουργεί σημαντικά προβλήματα και οδηγεί τις εταιρίες σε χρήση μη πρότυποποιημένων πρωτοκόλλων και στην εξ' αυτής συνεπαγόμενη εξάρτηση από τα προϊόντα ενός και μόνο συγκεκριμένου προμηθευτή.

5.3 Το πρωτόκολλο IPsec

Για την αντιμετώπιση του προβλήματος, η IETF (Internet Engineering Task Force) επεξεργάζεται την περιγραφή ενός νέου συνόλου προτύπων που ακούει στο όνομα IPsec (rfcs 1825-1829). Το IPsec θα περιγράφει τόσο την πιστοποίηση κόμβων του Internet στα χαμηλά επίπεδα του OSI, όσο και την κρυπτογράφηση και τη μετάδοση κλειδιών στα επίπεδα αυτά. Παράλληλα θα υποστηρίζονται όλα τα πρότυπα ασφαλείας που ήδη χρησιμοποιούνται στα υψηλότερα επίπεδα του OSI (SSL κλπ).
Ένα εύλογο ερώτημα είναι πως μπορεί κανείς να επέμβει σήμερα σε οποιοδήποτε επίπεδο του TCP/IP χωρίς να δημιουργήσει αναστατώσεις, εδώ όμως βρίσκεται και ένα σημαντικό μέρος της ευελιξίας του TCP/IP το οποίο επιτρέπει την εύκολη πρόσθεση νέων υπηρεσιών και πρωτοκόλλων. Μέρος του IP header κάθε πακέτου είναι το πεδίο "next protocol", το οποίο καθορίζει το είδος του πακέτου που θα ακολουθήσει και συνήθως σήμερα είναι TCP ή UDP και ακριβώς στο σημείο αυτό είναι που βρίσκεται η ευελιξία του. Το IPsec προσθέτει νέες πληροφορίες στα header των πακέτων με χρήση των οποίων γίνεται δυνατή η κρυπτογράφηση και πιστοποίηση της προέλευσης αυτών.
Λέγοντας πιστοποίηση εννοούμε την επαλήθευση ότι η αναγραφόμενη στο header διεύθυνση προέλευσης είναι και η πραγματική διεύθυνση προέλευσης του πακέτου. Δεδομένου ότι οι περισσότερες επικοινωνίες περιλαμβάνουν ανταλλαγή πακέτων μεταξύ των μερών, τότε όλα τα μέρη πιστοποιούνται μεταξύ τους και ελαχιστοποιείται η πιθανότητα παρεμβολής παρείσακτων δια της δικτυακής παραποίησης ταυτότητας. Επιπλέον της διαδικασίας πιστοποίησης και παράλληλα με αυτή, έρχεται η

κρυπτογράφηση των περιεχομένων του πακέτου ώστε τελικά αυτά να μεταδίδονται ασφαλή και μεταξύ του πραγματικού αποστολέα και παραλήπτη.
Στο IPsec διακρίνουμε τρία επίπεδα υλοποίησης του παραπάνω σχήματος: την ασφαλή ενσωμάτωση περιεχομένου (**ESP: Encapsulation of Security Payload**), την επικεφαλίδα πιστοποίησης (**AH: Authentication Header**) και το πρωτόκολλο διαχείρισης κλειδιών ασφαλείας (**ISAKMP: IP Security Association Key Management Protocol**). Τα δύο πρώτα ορίζουν νέα πακέτα για την κρυπτογραφημένη μετάδοση δεδομένων και για τη μετάδοση πληροφοριών πιστοποίησης διεύθυνσης αντίστοιχα, ενώ το τρίτο διαχειρίζεται την ανταλλαγή κλειδιών μεταξύ αποστολέων και αποδεκτών των πακέτων ESP και AH.
Το ESP καθορίζει τα περιεχόμενα ενός πακέτου IP. Κάθε πακέτο ESP αποτελείται από μια επικεφαλίδα ελέγχου, το κύριο μέρος δεδομένων και προαιρετικά από ένα δεύτερο τμήμα ελέγχου πιστοποίησης. Η επικεφαλίδα μπορεί να περιέχει πληροφορίες ελέγχου που απαιτούνται από τους χρησιμοποιούμενους αλγόριθμους κρυπτογραφίας όπως ο DES, οι οποίες ονομάζονται διάνυσμα αρχικοποίησης (initialization vector), ενώ το τμήμα ελέγχου που ακολουθεί (authentication trailer) περιέχει κάποιο κλειδί πιστοποίησης της κρυπτογράφησης του κυρίως πακέτου, κάτι ανάλογο του γνωστού και απλού checksum. Ο αλγόριθμος που συνήθως χρησιμοποιείται για την κρυπτογράφηση του κυρίως πακέτου είναι ο DES, ο οποίος είναι διαθέσιμος και σε hardware, καθώς και ο ασφαλέστερος triple-DES, για την εξαγωγή αμφοτέρων των οποίων υπάρχει αυστηρός έλεγχος από την κυβέρνηση των ΗΠΑ.
Αντίστοιχα με το ESP, τα πακέτα AH επίσης αναφέρονται στο κύριο μέρος των δεδομένων που μεταφέρει το πακέτο, χωρίς να κρυπτογραφούν αυτά καθεαυτό, αλλά παρέχοντας ένα είδος πιο σύνθετου checksum πιστοποιώντας παράλληλα και την ταυτότητα των μερών που επικοινωνούν. Για το σκοπό αυτό χρησιμοποιείται είτε ο αλγόριθμος MD5 (Message Digest 5) της RSA, είτε ο SHA-1 (Security Hash Algorithm 1) που αναπτύχθηκε για λογαριασμό της κυβέρνησης των ΗΠΑ, ενώ δεν αποκλείεται η χρήση πιο σύνθετων αλγορίθμων κρυπτογράφησης οι οποίοι υπάρχουν ή θα αναπτυχθούν στο μέλλον. Με το σχήμα αυτό, κρυπτογραφούνται τόσο τα περιεχόμενα του πακέτου, όσο και τα χαρακτηριστικά κλειδιά επαλήθευσης αυτών και μάλιστα με διαφορετικούς αλγόριθμους, ώστε να καθίσταται πολύ δύσκολη η αποκρυπτογράφησή τους.
Το τρίτο από τα προαναφερθέντα επίπεδα είναι το ISAKMP (επαναλαμβάνουμε τον ορισμό ISAKMP: Internet Security Association and Key Management Protocol και εντοπίζουμε την ανάγκη δημιουργίας ενός νέου πρωτοκόλλου αποκρυπτογράφησης των συντμήσεων). Το ISAKMP βασίζεται στο πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman το οποίο θεωρεί γνωστές τις ταυτότητες των δύο μερών είτε με χρήση κλειδιών ασφαλείας εκ των προτέρων γνωστών σε αμφότερα, είτε με τη βοήθεια πιστοποιητικών ασφαλείας (digital certificates) και ανταλλάσσει πληροφορίες με τη βοήθεια πακέτων UDP προκειμένου να πιστοποιηθούν από κοινού τα κοινά κλειδιά ασφάλειας μεταξύ αμφοτέρων των μερών. Μια εναλλακτική μέθοδος υλοποίησης της ασφάλειας στο επίπεδο αυτό είναι το SKIP (Simple Key Management for Internet Protocols) το οποίο όμως δεν υποστηρίζει επικοινωνία μεταξύ αλγορίθμων κρυπτογράφησης με αποτέλεσμα να υπάρχει ο κίνδυνος απώλειας πακέτων. Το ISAKMP φαίνεται ότι τελικά θα επικρατήσει, έχοντας επιλεγεί και για την υλοποίηση του IPv6.
Η απόφαση του αν θα χρησιμοποιηθούν πακέτα ESP ή AH εξαρτάται από τις εκάστοτε συνθήκες: η χρήση και των δύο εξασφαλίζει πιστοποίηση και κρυπτογράφηση

ταυτόχρονα, έχει όμως χειρότερες επιδόσεις από την χρήση μόνο του ESP (η οποία είναι και η συνηθισμένη περίπτωση), εκτός και αν το μόνο που απαιτείται είναι η πιστοποίηση της ταυτότητας των μερών, οπότε τα πακέτα AH είναι αυτό που χρειάζεται.
Η περίπτωση στην οποία το πακέτο που πρόκειται να μεταφερθεί μέσα από το δίκτυο (και περιλαμβάνει το αρχικό πακέτο ως πακέτο δεδομένων μέσα στο κέλυφος ασφάλειας του IPsec) είναι μεγαλύτερο από το μέγιστο υποστηριζόμενο μέγεθος στο μέσο μετάδοσης (λ.χ. 1518 bytes για το Ethernet) τότε αυτό είτε απορρίπτεται από το PCP/IP stack πριν μεταδοθεί (με τη βοήθεια παραβολής με την παράμετρο MTU : Maximum Transmission Unit) είτε κόβεται σε δύο μικρότερα τμήματα, αυτό όμως είναι θέμα που αφορά τα συγκεκριμένα προϊόντα που υλοποιούν το IPsec. Αυτό που σε κάθε περίπτωση παραμένει, είναι ότι το πακέτο-κέλυφος για τα προστατευμένα δεδομένα μας κλπ, είναι σε κάθε περίπτωση και πάλι ένα πακέτο IP το οποίο μεταδίδεται χρησιμοποιώντας την ήδη υπάρχουσα υποδομή του Internet, απλά περιέχει ως κέλυφος το κωδικοποιημένο "απροστάτευτο" πακέτο που θα μεταδίδονταν αν δεν μας απασχολούσε η κρυπτογράφηση και η πιστοποίηση.

5.4 Στόχοι και τομείς εφαρμογής

Η πρώτη χρήση του IPsec αναμένεται να είναι αυτή της υλοποίησης ασφαλών VPNs (Virtual Private Networks) μέσω του Internet και σε επόμενη φάση συνολικά της ανάπτυξης του δικτύου ενδέχεται να γενικευτεί η χρήση του, τουλάχιστον εκεί που απαιτείται είτε πιστοποίηση ταυτότητας, είτε κρυπτογράφηση, είτε και τα δύο (e-mail, εμπορικές συναλλαγές, κ.ά.). Οι ενδιαφερόμενοι για την υλοποίηση ενός τέτοιου ασφαλούς VPN με το θεωρητικό σχήμα που περιγράψαμε, μέσω του Internet, έχουν τρία βασικά ερωτήματα: πώς υλοποιείται, τι είδους ασφάλεια παρέχει και πόσο κοστίζει.
Το πρώτο και σημαντικότερο βήμα, όπως σε όλες τις περιπτώσεις χρήσης τέτοιων τεχνολογιών, είναι να ξεκαθαριστούν οι απαιτήσεις του υποψήφιου χρήστη από την αρχή. Το IPsec είναι κατάλληλο για τις περιπτώσεις εκείνες που η μέσω του δικτύου μεταδιδόμενη πληροφορία είναι εμπιστευτικής φύσης, όπως για παράδειγμα τα ιατρικά δεδομένα ή τα στοιχεία μισθοδοσίας ενός μεγάλου οργανισμού. Επίσης, προσφέρεται για τον έλεγχο πρόσβασης σε εταιρικούς πόρους πιστοποιώντας τη δικτυακή ταυτότητα όποιου επιχειρεί να τους χρησιμοποιήσει, ενώ ασφαλώς, σε υποστηρίζονται και τα δύο ταυτόχρονα, όπου είναι επιθυμητό.
Προσφέρεται όμως μόνο για εκείνες τις περιπτώσεις που δεν υπάρχει άλλος μηχανισμός ασφάλειας σε κάποιο άλλο επίπεδο του OSI. Το IPsec δεν προσθέτει ασφάλεια εκεί που για το σκοπό αυτό χρησιμοποιούνται άλλοι μηχανισμοί, όπως για παράδειγμα σε ένα web session μέσω SSL, στην ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου μέσω PGP ή S/MIME, ή στις ηλεκτρονικές εμπορικές συναλλαγές μέσω SET. Σε όλες τις περιπτώσεις αυτές, η ασφάλεια προσφέρεται στο επίπεδο της εφαρμογής και με αποκλειστικά δική της ευθύνη. Στην περίπτωση του IPsec, είναι το δίκτυο και όχι η συγκεκριμένη εφαρμογή που παρέχει την ασφάλεια, οπότε τίθεται ζήτημα επαναπροσδιορισμού των ευθυνών στον τομέα της ασφάλειας (τι ακριβώς και με ποιον τρόπο θα φυλάσσεται) μέσα σε έναν οργανισμό.
Τα πακέτα κρυπτογραφούνται και ελέγχονται ο αποστολέας και ο παραλήπτης μόνο όταν βγουν από το ελεγχόμενο εσωτερικό δίκτυο του οργανισμού. Η εφαρμογή της ιδέας στην πράξη μπορεί να γίνει με δύο τρόπους: είτε μεταξύ gateways, είτε μεταξύ συγκεκριμένων

hosts. Το ενδιαφέρον εστιάζεται στην πρώτη περίπτωση που αντιστοιχεί στην υλοποίηση δικτύου VPN, μέσω του Internet . Στο σενάριο αυτό, εσωτερικά στον οργανισμό τα πακέτα μεταδίδονται χωρίς ασφάλεια στο επίπεδο του δικτύου, μόνο με αυτή που ενδεχομένως οφείλεται στην εφαρμογή που τα δημιουργεί. Όταν ένα πακέτο προορίζεται για το άλλο τμήμα του VPN δικτύου οπότε πρέπει να περάσει μέσα από το gateway, τότε το τελευταίο είναι υπεύθυνο για την κωδικοποιημένη και πιστοποιημένη μετάδοσή του, προς το gateway του δικτύου προορισμού. Μέσα στο δίκτυο προορισμού το πακέτο ταξιδεύει και πάλι χωρίς ασφάλεια στο φυσικό επίπεδο. Το όλο σχήμα φαίνεται να παρέχει την ασφάλεια της μισθωμένης γραμμής, χωρίς όμως το κόστος της αλλά διάμεσο του Internet.
Η περίπτωση της υλοποίησης IPsec σε επίπεδο hosts προσφέρεται για τις περιπτώσεις εκείνες που υπάρχουν ανομοιογενή εταιρικά δίκτυα, με διαφορετικό Λογισμικό και hardware με μοναδική απαίτηση η επικοινωνία να γίνεται μέσω TCP/IP. Παράδειγμα (μάλλον όχι χαρακτηριστικό για τα ελληνικά δεδομένα) ένας υπολογιστής mainframe ο οποίος εξυπηρετεί πελάτες άλλοι εκ των οποίων τρέχουν προγράμματα προσομοίωσης τερματικών 3270 και άλλοι Java applets σε web browsers. Τότε, χρησιμοποιώντας IPsec μπορούμε να παρακάμψουμε τη χρήση μισθωμένων γραμμών. Τότε, ακόμα και όταν δε διαθέτουμε υλοποίηση του IPsec για μια συγκεκριμένη μηχανή, μπορούμε να χρησιμοποιήσουμε gateway σύμφωνα με το προηγούμενο σχήμα. Τέλος, οι επιλογές για την κρυπτογράφηση των δεδομένων είναι πολλές και αφήνονται στις απαιτήσεις της εκάστοτε περίπτωσης, με παραμέτρους το κόστος, την πολυπλοκότητα και τις επιδόσεις, αλλά και την άδεια της κυβέρνησης των ΗΠΑ και τις επιδόσεις των απανταχού μαχητών της κρυπτογράφησης.

5.5 Αλγόριθμοι κρυπτογράφησης και πιστοποίησης

Ορισμός κρυπτογράφησης: Η κρυπτογράφηση ενός κειμένου, αλλάζει την δομή του αρχικού κειμένου (καθαρό κείμενο), κάνοντας την ανάγνωση του δυνατή μόνο με την βοήθεια κάποιας επιπρόσθετης πληροφορίας (κλειδί), η οποία είναι γνωστή μόνο στον αποστολέα και στον δέκτη του κειμένου.

Ορισμός Αλγόριθμου κρυπτογράφησης: Αλγόριθμος κρυπτογράφησης, είναι μία λεπτομερής σειρά μαθηματικών πράξεων, με την χρήση των οποίων συνδυάζονται το καθαρό κείμενο και το κλειδί, για να παράγουν το κρυπτογραφημένο κείμενο.

*Ορισμός Αλγόριθμου πιστοποίησης:*Αλγόριθμος πιστοποίησης είναι μία διαδικασία ή ένα εργαλείο του οποίου τα αποτελέσματα του κρυπτογραφημένου κειμένου, εξαρτώνται από όλα τα σχετικά στοιχεία πιστοποίησης.

Αλγόριθμος του Καίσαρα

Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται

από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερα του στο αλφάβητο. Θα μπορούσε φυσικά το κλειδί να ήταν 6, οπότε το κρυπτογραφημένο κείμενο θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο και αλλάζοντας κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.
Έστω η λέξη **αβγό**. Με τον αλγόριθμο του Καίσαρα θα προέκυπτε η λέξη **δεζς**. Για να το αποκρυπτογραφήσει αυτό κάποιος θα πρέπει να αντιστρέψει την διαδικασία της κρυπτογράφησης, δηλαδή να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερά του στην αλφάβητο.

Αλγόριθμος με κλειδί πίνακα

Σε αυτόν τον αλγόριθμο δημιουργούμε και χρησιμοποιούμε, έναν πίνακα που ορίζει την αλλαγή που πρέπει να γίνει. Ο πίνακας λέει ποιο γράμμα να βάλουμε στο κρυπτογραφημένο κείμενο.
Αυτή είναι μία πολύ πιο ισχυρή μέθοδος από την μέθοδο του Καίσαρα, καθώς ο κρυπταναλυτής θα πρέπει να δοκιμάσει πολλούς περισσότερους πίνακες για να είναι σίγουρος ότι θα διαβάσει το μήνυμα. Πάντως οι αλγόριθμοι απλής αντικατάστασης, όπως αυτός, είναι εύκολο να σπάσουν λόγω της συχνότητας εμφάνισης γραμμάτων της γλώσσας.

DES - Data Encryption Standard

Είναι ένα σώμα κρυπτογραφικών εντολών που δημιουργήθηκε από την IBM και πήρε έγκριση από την Αμερικάνικη κυβέρνηση το 1977. Χρησιμοποιεί ένα 56-bit κλειδί και χρησιμοποιεί μια ομάδα από 64 bits. Είναι σχετικά γρήγορος αλγόριθμος και χρησιμοποιείται για την κρυπτογράφηση μεγάλου όγκου δεδομένων, ταυτόχρονα

Triple DES

Βασίζεται στον DES αλγόριθμο. Κρυπτογραφεί μια ομάδα δεδομένων τρεις φορές, με τρία. διαφορετικά κλειδιά. Έχει προταθεί σαν εναλλακτική λύση αντί του DES, γιατί υποστηρίζεται ότι τον τελευταίο καιρό έχει γίνει πιο εύκολο και πιο γρήγορο το "σπάσιμο" του DES αλγόριθμου.

RC2 και RC4.

Σχεδιάστηκαν από τον Ron Rivets (από εκεί προέρχεται το R στην RSA Data Security Inc.) . Παρέχουν ποικιλία ως προς το μέγεθος του κλειδιού αποκρυπτογράφησης για πολύ γρήγορη και μεγάλου όγκου κρυπτογράφηση. Οι δυο αυτοί αλγόριθμοι θεωρούνται λίγο πιο γρήγοροι από τον DES και μπορούν να γίνουν ακόμα πιο ασφαλείς αν επιλέξουμε μεγαλύτερο μήκος κλειδιού. Ο αλγόριθμος RC2 αποτελείται από μια ομάδα (block) κρυπτογράφησης και μπορεί να χρησιμοποιηθεί στην θέση τον DES. Ο RC4 είναι ένα "ρεύμα" (stream) ψηφίων κρυπτογράφησης και θεωρείται περίπου 10 φορές πιο γρήγορος από τον DES.

IDEA

Ο **International Data Encryption Algorithm** δημιουργήθηκε το 1941 και σχεδιάστηκε για να είναι ικανός για πραγματοποίηση υπολογισμών στο λογισμικό. Προσφέρει πολύ δυνατή κρυπτογράφηση, χρησιμοποιώντας ένα **128-bit** κλειδί.

RSA

Ονομάστηκε έτσι από τους σχεδιαστές του, Rivest, Shamir και Adelman. Είναι ένας αλγόριθμος "δημόσιου κλειδιού" (public-key) ο οποίος υποστηρίζει μια ποικιλία μήκους κλειδιών, καθώς επίσης ποικιλία όσον αφορά το μέγεθος τον σώματος του κειμένου προς κρυπτογράφηση. Το απλό block κειμένου πρέπει να είναι μικρότερο από το μήκος τον κλειδιού. Το συνηθισμένο μήκος κλειδιού είναι 512 bits.

Diffie-Hellman

Αποτελεί το παλιότερο "δημόσιου κλειδιού" σύστημα κρυπτογραφίας, που ακόμα χρησιμοποιείται. Δεν υποστηρίζει κρυπτογράφηση ή ψηφιακές υπογραφές. Το σύστημα έχει σχεδιαστεί για να επιτρέπει στις δυο πλευρές να συμφωνούν με την χρήση ενός κατανεμημένου κλειδιού (shared key) , ακόμα και αν το μόνο που κάνουν είναι να ανταλλάσσουν μηνύματα δημοσίως.

DSA

Ο Digital Signature Algorithm σχεδιάστηκε από την NIST και στηρίχθηκε πάνω σε αυτό που αποκαλείται EI Gamal αλγόριθμος. Το σχήμα των υπογραφών χρησιμοποιεί το ίδιο είδος κλειδιού που χρησιμοποιεί και ο Diffie - Hellman αλγόριθμος και μπορεί να δημιουργήσει υπογραφές πιο γρήγορα από τον RSA. 'Εχοντας προωθηθεί από την NIST ως ένα DSS σύστημα, το Digital Signature Standard, παρόλη την αποδοχή του, απέχει ακόμα πολύ από το να παρέχει σιγουριά

Αλγόριθμος MD5

Ο αλγόριθμος αυτός ανήκει στην κατηγορία των αλγορίθμων περίπλεξης. Δίνεις μία είσοδο στον αλγόριθμο και σου βγάζει έναν αριθμό που να μοιάζει τυχαίος. Ο αλγόριθμος MD5 επεξεργάζεται ένα κείμενο σε block των 512 bit τα οποία σπάει σε 16 block των 32 bit. Η έξοδος του αλγορίθμου είναι ένα σετ από 4 block των 32-bit τα οποία συνδέονται αλυσιδωτά σε μία φόρμα των 128 bit.

5.6 Πλεονεκτήματα της χρήσης του IPsec σε εμπορικές συναλλαγές και επιχειρηματικά δίκτυα

Είναι γεγονός ότι το Internet προβάλλεται μεταξύ άλλων και σαν ένας χώρος στον οποίο μπορούν να διακινούνται εμπορικά προϊόντα και να γίνονται συναλλαγές γενικότερα. Ωστόσο πρώτα πρέπει να αντιμετωπιστεί η πρόκληση της ασφαλούς διακίνησης δεδομένων μέσα από ένα από τη φύση του δημόσιο και ανοιχτό σε όλους δίκτυο, στη σχεδίαση των δομικών συστατικών του οποίου καθόλου δεν ελήφθη υπόψη ο παράγοντας "ασφάλεια".
Οι τράπεζες έχουν αρκετή τεχνογνωσία ασφαλούς ηλεκτρονικής διακίνησης πληροφοριών σχετικά με συναλλαγές, μέσα από ιδιωτικά όμως δίκτυα, τα οποία πάραυτα έχει πολλάκις αποδειχτεί ότι δεν είναι απαραβίαστα. Πρέπει, λοιπόν, να επιτευχθεί ένα υψηλό επίπεδο ασφάλειας για τις πληρωμές μέσω πιστωτικών καρτών μέσα από το Internet, αντίστοιχο με αυτό που υπάρχει κατά την "παραδοσιακή" χρήση τους (όταν ασφαλώς η πιστοποίηση της ταυτότητας του αγοραστή γίνεται σωστά).
Το πρότυπο SET (Secure Electronic Transactions) που αναπτύχθηκε από τις MasterCard, VISA, και RSA σε συνεργασία με μικρότερους φορείς, φιλοδοξεί να αντιμετωπίσει με επιτυχία το πρόβλημα της ασφαλούς μετάδοσης "ευαίσθητων" προσωπικών και οικονομικών πληροφοριών μέσα από δημόσια δίκτυα

IPSec

Το IPSec λειτουργεί κλείνοντας το πακέτο των πληροφοριών το οποίο στέλνεται, σε ένα άλλο πακέτο, πριν σταλεί μέσω του Internet. Στον παραλήπτη,το πακέτο αποκωδικοποιείται και διαβάζεται από μμία συσκευή που έχει καθορίσει ο αποστολέας.
Το IPSec αποτελείται από τρεις διαφορετικούς μηχανισμούς ασφαλείας: την επικεφαλίδα ελέγχου ταυτότητας, το ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας και το κλειδί διαχείρισης. Οι τρεις μηχανισμοί χρησιμοποιούνται σε συνδυασμό μεταξύ τους, για καλύτερα αποτελέσματα ασφαλείας.

Επικεφαλίδα ελέγχου ταυτότητας
Ο πρώτος μηχανισμός είναι η επικεφαλίδα ελέγχου ταυτότητας (authentication header – AH). Το AH επικεντρώνεται στον έλεγχο ταυτότητας των ατόμων που στέλνουν τις πληροφορίες και βεβαιώνεται ότι δεν έχουν αλλοιωθεί στη διαδρομή. Το AH μπαίνει μμετά στην IP επικεφαλίδα, αλλά πριν από τις άλλες πληροφορίες που πρόκειται να πιστοποιηθούν.

Ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας
Ο δεύτερος μηχανισμός είναι το ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας (encapsulating security payload – ESP). Το ESP πιστοποιεί επίσης την ταυτότητα του χρήστη, αλλά υποστηρίζει και την κρυπτογράφηση των δεδομένων.

Πρωτόκολλο διαχείρισης κλειδιού Internet
Το Πρωτόκολλο διαχείρισης κλειδιού Internet (Internet Key Management Protocol) λέγεται ότι είναι ο πυρήνας του IPSec. Αυτός ο μηχανισμός επιτρέπει να ανταλλάσσουν δύο μμέρη τα δημόσια κλειδιά τους και να διαμορφώνουν μμια ασφαλή σύνοδο. Αφού

ανταλλαχθούν τα δημόσια κλειδιά, ορίζεται ένα προσδιοριστικό συνόδου. Ένα προσδιοριστικό συνόδου (session identifier) είναι ο ορισμός της Internet σχέσης που μοιράζονται τα δύο μμέρη.

Το IPSec είναι όπως το PKI στο τρόπο που ορίζει την εμπιστοσύνη μεταξύ διαφορετικών πλευρών. Σαν καθολική βάση, το IPSec παρέχει τρεις πολύ σημαντικές λειτουργίες ασφαλείας για Internet συναλλαγές: εμπιστοσύνη, ακεραιότητα και έλεγχο ταυτότητας.

Εμπιστοσύνη

Το IPSec βεβαιώνεται ότι όλες οι συναλλαγές είναι εμπιστευτικές, με τον ίδιο τρόπο που το κάνει ο μηχανισμός PKI. Η λειτουργία ESP κρυπτογραφεί τα πακέτα πριν σταλούν μέσω του Internet. Αφού κρυπτογραφηθεί η συναλλαγή, μμπορεί μόνο να αποκρυπτογραφηθεί από το Web διακομιστή. Έτσι, ακόμα και αν οι πληροφορίες υποκλαπούν, δεν θα μπορούσαν να αποκρυπτογραφηθούν.

Ακεραιότητα

Ο παραλήπτης, σε αυτή τη περίπτωση ο Web διακομιστής, μπορεί επίσης να βεβαιωθεί ότι τα δεδομένα δεν έχουν αλλαχθεί ή υποκλαπεί με κάποιον τρόπο. Επειδή η συναλλαγή κρυπτογραφείται πριν σταλεί, θα αποκρυπτογραφηθεί αν το μήνυμα δεν αλλοιωθεί. Έτσι, αν υπάρχει κάποια αλλαγή στο μήνυμα, δεν θα μμεταφραστεί σε αναγνώσιμο υλικό όταν φτάσει στο Web διακομιστή.

Έλεγχος ταυτότητας

Ο παραλήπτης μπορεί επίσης να πιστοποιήσει την πηγή από την οποίαν προέρχονται τα πακέτα, εξ αιτίας των πληροφοριών που παρέχονται στην επικεφαλίδα.

6. Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks-VPN)

Το εικονικό ιδιωτικό δίκτυο (VPN-virtual Private Network) επιτρέπει την δημιουργία και συντήρηση ιδεατών ιδιωτικών καναλιών μεταφοράς δεδομένων μέσω Internet με απόλυτη αξιοπιστία και ασφάλεια. Ως προηγμένη υπηρεσία δικτύωσης, τα VPN καλύπτουν ένα ευρύ φάσμα μορφών επικοινωνίας και εμπορικής δραστηριότητας, από ανταλλαγή ηλεκτρονικών μηνυμάτων, μεταφοράς φωνής, ενημέρωσης εταιρικών βάσεων δεδομένων εώς και ανάπτυξης ηλεκτρονικού εμπορίου με τον βέλτιστο τρόπο.
Με την χρήση της τεχνολογίας VPN, οι επιχειρήσεις έχουν πλέον την δυνατότητα μόνιμης διασύνδεσης των απομακρυσμένων γραφείων ή συνεργατών τους, αυξάνοντας έτσι την παραγωγικότητα τους και δημιουργώντας ένα ισχυρό ανταγωνιστικό δίκτυο μεταξύ των συνεργατών, των προμηθευτών και των πελατών.
Τα VPNς μειώνουν το κόστος δικτύωσης των επιχειρήσεων, αφού αποτελούν μια οικονομική λύση συγκριτικά με αυτή των ανεξάρτητων και ασύνδετων μεταξύ τους μισθωμένων κυκλωμάτων. Η έννοια του κόστους περιλαμβάνει την μειωμένη απαίτηση εξοπλισμού, την ευκολία συντήρησης και διαχείρισης του δικτύου, την ευελιξία αφού μπορούν να χρησιμοποιηθούν σαν βάση για επιπλέον υπηρεσίες, καθώς και την άμεση επεκτασιμότητα για την άριστη κάλυψη των αναγκών των επιχειρήσεων.

6.1 Τι είναι τα VPN;

Για να κατανοήσουμε τι είναι τα VPN θα χρησιμοποιήσουμε ένα παράδειγμα:

Έστω μία εταιρία που έχει έδρα της την Αθήνα, θέλει να στείλει ένα μήνυμα στην θυγατρική της που εδρεύει στο Λονδίνο. Η εταιρία στην Αθήνα αποφασίζει να στείλει το μήνυμα μέσω ηλεκτρονικού ταχυδρομείου. Όμως, καθώς το μήνυμα ταξιδεύει μέσα στο Internet για να φτάσει στο Λονδίνο μπορεί να υποκλαπεί ή να αλλοιωθεί από κάποιο.

Έτσι στην πρώτη περίπτωση ή θυγατρική δεν θα λάβει το μήνυμα, ή θα το λάβει αλλοιωμένο. Αυτό το πιθανό ενδεχόμενο, θα δημιουργήσει μεγάλο οικονομικό κόστος στην εταιρία, και αλλοίωση της εμπιστοσύνης συνεργατών και πελατών της.

Για να αποφύγει αυτό το κόστος, η εταιρία πρέπει να εξασφαλίσει:

1. ***Ιδιωτικότητα.*** *Ότι καμία παρεμβολή δεν θα υπάρξει στην επικοινωνία της εταιρίας με τρίτους. Η εταιρία στην Αθήνα θέλει να είναι σίγουρη, ότι μόνο η θυγατρική της στο Λονδίνο θα μπορέσει να πάρει το μήνυμα. Η ιδιωτικότητα μπορεί να επιτευχθεί, και επιτυγχάνεται μέσω της κρυπτογράφησης.*
2. ***Ακεραιότητα.*** *Κανείς δεν μπορεί να ανακατευθεί στην επικοινωνία της εταιρίας. Η εταιρία θέλει μα είναι σίγουρη, ότι η θυγατρική της θα λάβει τα ακριβή σχέδια που της έστειλε.*
3. ***Αυθεντικότητα.*** *Η θυγατρική στο Λονδίνο πρέπει να είναι σίγουρη, ότι το μήνυμα το έχει στείλει όντως η εταιρία στην Αθήνα. Η αυθεντικότητα ενός μηνύματος μπορεί να επιτευχθεί με την χρήση* ***ψηφιακών υπογραφών.***

Η λύση σε αυτά τα προβλήματα είναι η δημιουργία ενός VPN. Το VPN προστατεύει την επικοινωνία μέσα στο Ίντερνετ και επιτρέπει στην εταιρία να φτιάξει το δικό της ιδιωτικό εικονικό δίκτυο, χρησιμοποιώντας κομμάτια του ιδιωτικού της δικτύου και του δημοσίου δικτύου.
Τι είναι όμως ένα VPN;

Σύμφωνα με την CISCO, το VPN είναι ένα δίκτυο που δημιουργείται με κρυπτογράφηση, μέσα σ' ένα άλλο δίκτυο αμφιβόλου ασφάλειας «Internet». Το VPN παρέχει πρόσβαση σε χρήστες που δεν έχουν πρόσβαση στο δίκτυο από σταθερό σημείο, σε εταιρίες που έχουν γραφεία σε διάφορες γεωγραφικές τοποθεσίες.
Σε γενικές γραμμές το VPN μπορεί να θεωρηθεί σαν ένα **τούνελ** από το τέλος μίας γραμμής σε μία πύλη. Επειδή, μέσα από τα VPN μεταδίδονται συνήθως ευαίσθητες πληροφορίες κρίνεται αναγκαία η χρήση του πρωτοκόλλου Ipsec για να υπάρξει:

1. Εμπιστοσύνη
2. Ακεραιότητα
3. Υπηρεσίες Πιστοποίησης

Πριν επεκταθούμε στο θέμα των VPN, θα δώσουμε δύο ορισμούς οι οποίοι θα βοηθήσουν στην κατανόηση του θέματος των VPN παρακάτω:

Ψηφιακή υπογραφή είναι ένα κείμενο, το οποίο μπορεί να έχει δημιουργηθεί από κάποιον που ξέρει ένα συγκεκριμένο μυστικό. Η κρυπτογράφηση και ένα προσυμφωνημένο κείμενο, μπορούν να παρουσιαστούνε σαν ψηφιακή υπογραφή, με την προϋπόθεση ότι ο «υπογράφων» είναι γνώστης του κλειδιού κωδικοποίησης.
Το tunneling είναι μία μέθοδος χρησιμοποίησης της υποδομής των δικτύων για την μεταφορά δεδομένων από ένα δίκτυο σε άλλο. Τα δεδομένα προς μεταφορά (payload) μπορεί να είναι σε πλαίσια (frames) ή πακέτα (packets) ενός διαφορετικού πρωτοκόλλου. Αντί να στέλνονται τα πακέτα ή τα πλαίσια όπως έχουν φτιαχτεί, με το tunneling επιθυλακώνεται στα πακέτα μια πρόσθετη κεφαλίδα (header). Η πρόσθετη κεφαλίδα παρέχει πληροφορίες δρομολόγησης. Τα πακέτα αυτά ταξιδεύουν σε ένα λογικό μονοπάτι μέσα στο διαδίκτυο το οποίο ονομάζεται tunnel. Όταν τα πακέτα φτάσουν στον προορισμό τους, τότε αφαιρούνται οι πρόσθετες κεφαλίδες. Ο όρος tunneling περικλείει όλη την παραπάνω διαδικασία.

6.2 Σε ποιους απευθύνονται τα VPN;

Οι λύσεις αυτές απευθύνονται συνήθως σε μεσαίες και μεγάλες επιχειρήσεις που :

- Διαθέτουν περισσότερα από ένα υποκαταστήματα στην Ελλάδα ή το εξωτερικό και υπάρχει ανάγκη επικοινωνίας μεταξύ τους για μεταφορά δεδομένων ή φωνής.
- Διαθέτουν μετακινούμενα στελέχη για τα οποία υπάρχει ανάγκη επικοινωνίας με τα κεντρικά γραφεία για μεταφορά δεδομένων ή για πρόσβαση σε πληροφορίες.
- Θέλουν να δημιουργήσουν ένα ασφαλές και αξιόπιστο περιβάλλον με συνεργάτες ή προμηθευτές τους.
- Λειτουργούν σήμερα ένα παραδοσιακό τηλεπικοινωνιακό δίκτυο και ενδιαφέρονται να μειώσουν τα τηλεπικοινωνιακά τέλη..

6.3 Κατηγορίες VPN

Intranet VPNs

Τα Intranet VPNs αφορούν στη σύνδεση των γραφείων και υποκαταστημάτων μιας εταιρείας. Στόχος εδώ είναι να υπάρχει κεντρικός έλεγχος της υποδομής της εταιρείας, να επιτραπεί δηλαδή στα απομακρυσμένα σημεία να χρησιμοποιούν την υποδομή (εφαρμογές λογιστικής, αποθήκης, ανθρώπινων πόρων, μισθοδοσίας, ή άλλες εξειδικευμένες εφαρμογές) απευθείας από τα κεντρικά γραφεία της εταιρείας. Η λειτουργικότητα που επιτυγχάνεται είναι προφανής: όλα τα γραφεία και υποκαταστήματα της εταιρείας είναι άμεσα συνδεδεμένα με τα κεντρικά της γραφεία, έχουν άμεση και αυτόβουλη πρόσβαση στα δεδομένα που τους αφορούν και η εταιρεία ενημερώνεται αυτόματα για όλες τις κινήσεις των περιφερειακών της γραφείων και υποκαταστημάτων. Εδώ εφαρμόζεται και η ενδοεταιρική τηλεφωνία, επιτρέποντας την επικοινωνία μεταξύ όλων αυτών των σημείων με εσωτερικές κλήσεις.

Extranet VPNs

Σ' αυτή την περίπτωση, το ιδεατό ιδιωτικό δίκτυο επεκτείνεται και στους συνεργάτες, πελάτες, προμηθευτές, δίκτυο μεταπωλητών, κτλ. Η λειτουργικότητα είναι η ίδια, με εξαίρεση την εκτενέστερη διαβαθμισμένη πρόσβαση του κάθε μέλους του VPN στους πόρους της εταιρείας, ανάλογα με τα δικαιώματα που επιθυμεί η εταιρεία να αναθέσει. Η τηλεφωνία μεταξύ των εταιρειών, μέσω του VPN, εφαρμόζεται και εδώ, προσφέροντας μηδενικό κόστος για την επικοινωνία μεταξύ των εταιρειών που συμμετέχουν στο Ιδεατό Ιδιωτικό Δίκτυο.

Access VPNs

Τα access VPNs αφορούν στη σύνδεση μεμονωμένων στελεχών στο εταιρικό δίκτυο, από το σπίτι ή σε περιοδεία (είναι γνωστά και ως VPDNs, Virtual Private Dialup Networks). Με τα access VPNs είναι δυνατό κάποιο στέλεχος να αποκτήσει πλήρη πρόσβαση στο εταιρικό δίκτυο, ίδια με την πρόσβαση που θα είχε αν βρισκόταν στο γραφείο του μέσα στην επιχείρηση, αυτή τη φορά όμως από το σπίτι του, ή σε κάποιο ταξίδι. Μπορεί μάλιστα να χρησιμοποιήσει την ενδοεταιρική τηλεφωνία μέσω του προσωπικού του υπολογιστή

6.4 Βασικές απαιτήσεις VPN

Συνήθως, όταν μία εταιρεία εγκαθιστά ένα VPN είναι απαραίτητη η ελεγχόμενη πρόσβαση των χρηστών. Είναι δηλαδή πολύ σημαντικό ο κάθε χρήστης να έχει πρόσβαση μόνο στις πληροφορίες που του επιτρέπεται και επίσης πολύ σημαντικό είναι σε περίπτωση απομακρυσμένης πρόσβασης να υπάρχει εγγύηση της ασφάλειας των δεδομένων που διακινούνται δια μέσω του Internet.

Για τους παραπάνω λόγους ένα VPN πρέπει να παρέχει τουλάχιστον τα παρακάτω :

· User Authentication. Η λύση που θα επιλέξει η κάθε επιχείρηση θα πρέπει να ελέγχει την ταυτότητα του χρήστη και να περιορίζει την πρόσβαση στο VPN μόνο σε εξουσιοδοτημένα πρόσωπα. Επίσης θα πρέπει να ελέγχει και να καταγράφει ποιος και πότε και σε ποιες πληροφορίες είχε πρόσβαση.

· Address Management. Θα πρέπει να υπάρχει αντιστοίχηση (από τον VPN server) της διεύθυνσης του πελάτη σε ένα τοπικό δίκτυο και θα πρέπει να διασφαλιστεί το απόρρητο αυτής της διεύθυνσης.

· Data Encryption. Τα δεδομένα που θα στέλνονται μέσω του δημόσιου δικτύου (Internet) θα πρέπει να μην μπορούν να διαβαστούν από τρίτους.

· Key Management. Θα πρέπει να υπάρχει η δυνατότητα παραγωγής και ανανέωσης encryption keys για τον client και τον server.

· Multiprotocol Support. Θα πρέπει να υποστηρίζονται τα κοινά πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο, όπως τα IP, Internet Packet Exchange (IPX), κ.λ.π.

Μία λύση VPN που βασίζεται στο Point-to-Point Tunneling Protocol (PPTP) ή Layer 2 Tunneling Protocol (L2TP) πληροί όλα τα παραπάνω και εκμεταλλεύεται τις ευρείες δυνατότητες του Internet.

6.5 Βασικά πλεονεκτήματα των VPN

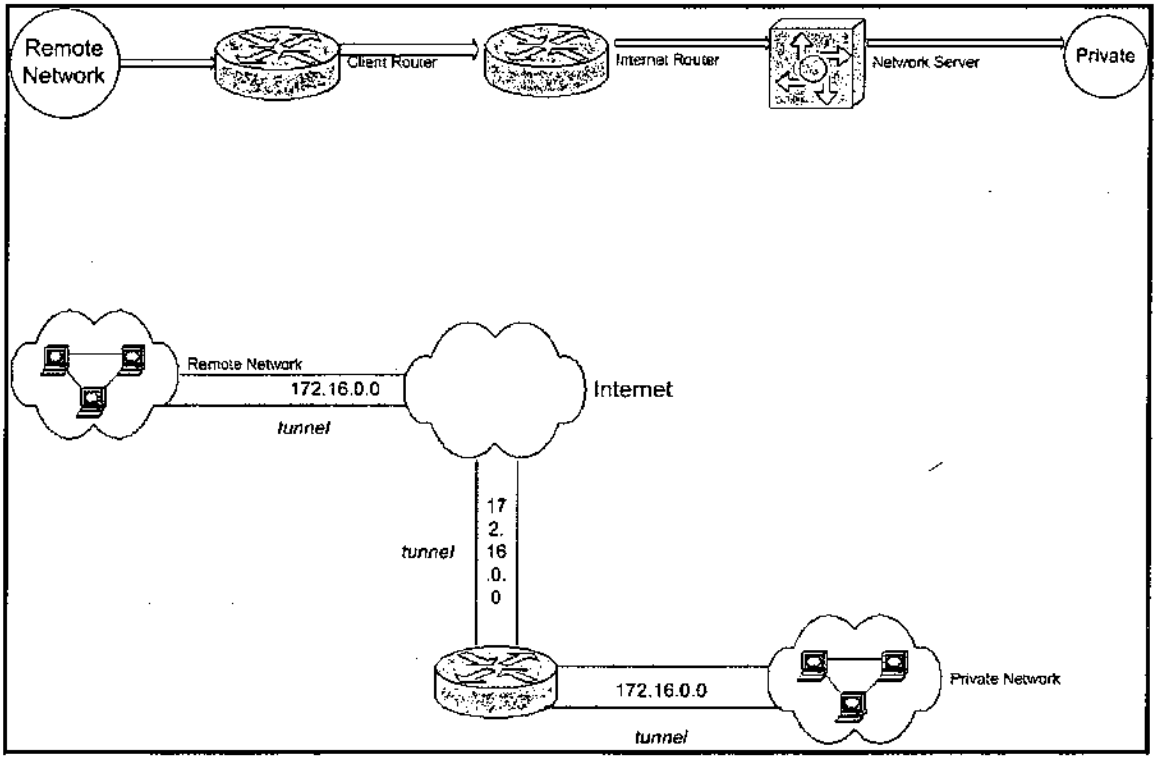
Τα κύρια πλεονεκτήματα του VPN είναι :

- Ουσιαστική, χωρίς όρια, αύξηση της χωρητικότητας
- Επέκταση δικτύου σε διαφορετικούς τόπους
- Πολλές νέες ευκολίες
- Ευελιξία και δημιουργία πακέτων ευκολιών επί παραγγελία
- Δεν υπάρχει ρίσκο λόγο απαρχαίωσης ή αχρηστίας
- Εξοικονόμηση (μείωση κόστους αφού δεν απαιτούνται επενδύσεις για την αγορά πρόσθετου εξοπλισμού)
- Τεχνική υποστήριξη από το διαχειριστή δικτύου
- Υψηλή αξιοπιστία
- Η χρήση του δημοσίου δικτύου σημαίνει πολύ μικρότερα τηλεπικοινωνιακά κόστη, της τάξης του 20-80% ανάλογα με τον αριθμό των σημείων που θα συνδεθούν και των μεταξύ τους αποστάσεων. Αυτό συμβαίνει γιατί το δημόσιο δίκτυο ήδη υπάρχει. Το κόστος ενός ακόμα πελάτη σε ένα υπάρχον δίκτυο είναι πολύ μικρότερο από το κόστος δημιουργίας ενός νέου δικτύου. Ο εξοπλισμός που απαιτείται για την υλοποίηση των VPN συνήθως περιλαμβάνεται στην τιμή διάθεσης τους με την μορφή ενοικίασης. Για την επιχείρηση, αυτό σημαίνει ένα ταμειακό όφελος κατά την έναρξη και μεγαλύτερη ασφάλεια σε περίπτωση που χρειαστεί αναβάθμιση της υπηρεσίας και του εξοπλισμού σε μικρό χρονικό διάστημα.

- Τα εφεδρικά κυκλώματα (συνήθως στην μορφή ISDN γραμμών) επίσης περιλαμβάνονται στο συνολικό σχεδιασμό και κόστος. Την εγκατάσταση, συντήρηση και ενεργοποίηση τους αναλαμβάνει συνήθως ο παροχέας των VPNs.
- Η διαχείριση, παρακολούθηση και συντήρηση των VPNs (μισθωμένα κυκλώματα, εξοπλισμός κ.τ.λ) συνήθως περιλαμβάνεται στην τιμή τους, πράγμα που μεταφράζεται σε μηδενικό επιπλέον κόστος συντήρησης σε προσωπικό και τεχνογνωσία για την επιχείρηση. Δυνατότητα αναβάθμισης σε περίπτωση που χρειαστεί η υπηρεσία και ο εξοπλισμός σε μικρό χρονικό διάστημα.

6.6 Πώς δουλεύει

Για να δημιουργηθεί ένα VPN, πρέπει να δημιουργηθεί ένα ασφαλές τούνελ μεταξύ των δύο δικτύων και να υπάρξει δρομολόγηση IP μέσα από αυτά.



Εικόνα 1

Το παραπάνω διάγραμμα δείχνει πώς πρέπει να είναι στημένο το δίκτυο για να λειτουργήσει.
Ο πελάτης router λειτουργεί σαν μία πύλη για το κινητό δίκτυο. Το κινητό δίκτυο χρησιμοποιεί την τοπική διεύθυνση IP 192,168,12,0. Για την απλοποίηση και την κατανόηση του διαγράμματος, δεν θα αναφερθούμε σε πλοήγηση των routers. Η βασική ιδέα σε αυτό το διάγραμμα είναι να κατευθυνθεί η κυκλοφορία για όλα τα ιδιωτικά δίκτυα (10.0.0.0, 172.16.0.0 και 192.168.0.0) μέσα από το τούνελ. Το σχήμα κατασκευάστηκε για δρομολόγηση δεδομένων προς μία πλευρά. Έτσι, ενώ το κινητό δίκτυο μπορεί να «δει» το ιδιωτικό δίκτυο, το ιδιωτικό δίκτυο δεν μπορεί να «δει» το

κινητό δίκτυο. Για να μπορεί και το ιδιωτικό δίκτυο να βλέπει το κινητό δίκτυο πρέπει οι server να είναι δύο-κατευθύνσεων.

6.7 Διαφορές του VPN από ένα Extranet.

Τα δίκτυα VPN μπορεί να έχουν σχεδιαστεί για να δουλεύουν σαν Extranet, αλλά δεν είναι όλα τα Extranet ένα VPN.
Το Extranet είναι ένας γενικός όρος που μπορεί να σημαίνει πολλά πράγματα. Ο τυπικός ορισμός του Extranet είναι: *Το Extranet είναι ένα δίκτυο, που παρέχει σε εξωτερικούς χρήστες πρόσβαση στο εταιρικό δίκτυο.* Οι χρήστες έχουν πρόσβαση στο εταιρικό δίκτυο μέσω ενός φυλλομετρητή (browser), και για να αποκτήσουν είσοδο πρέπει να εισάγουν το όνομα χρήστη και τον κωδικό που τους έχει δοθεί.
Ένα VPN, μπορεί να χρησιμοποιηθεί με τον ίδιο τρόπο, αλλά παρέχει υψηλότερη ασφάλεια. Συγκεκριμένα ένα VPN, απαιτεί την εγκατάσταση ενός «τούνελ» μέσα στο εταιρικό δίκτυο, και την κρυπτογράφηση των δεδομένων που περνάνε από τον υπολογιστή του χρήστη στον server της εταιρίας.

6.8 ISPs για VPN

Πριν αρχίσουμε να αναφερόμαστε στους ISPs που παρέχουν υπηρεσίες για VPN, πρέπει να δώσουμε έναν ορισμό των ISPs.
Το ISP είναι το ακρωνύμιο της λέξης (Internet Service Provider-ISP). Εταιρία που εξειδικεύεται στην παροχή υπηρεσιών διασύνδεσης με το Internet. Οι υπηρεσίες αυτές μπορεί να απευθύνονται σε τελικούς χρήστες και να αφορούν πρόσβαση μεμονωμένων ατόμων από γραμμές του επιλεγμένου τηλεφωνικού δικτύου ή να αφορά υπηρεσίες παροχής συνδεσιμότητας σε μισθωμένες γραμμές εταιριών.

Υπηρεσίες που παρέχει ένας ISP σε εταιρίες.

Όπως αναφέραμε παραπάνω, ένας ISP είναι μία εταιρία που παρέχει υπηρεσίες διασύνδεσης στο Internet. Ας δούμε λοιπόν τις υπηρεσίες που προσφέρουν οι εταιρίες αυτές :

- Πρόσβαση στο Internet και υπηρεσίες TCP/IP (VPN)
- Φιλοξενία δεδομένων
- Υπηρεσίες Frame Relay
- Μισθωμένες γραμμές
- Υπηρεσίες **ATM**

Ποία είναι όμως τα κριτήρια ποιότητας υπηρεσίας;

- Πρόσβαση στο Internet και υπηρεσίες TCP/IP (VPN)
- Διαθεσιμότητα κυκλώματος και διασύνδεσης
- Ποσοστό χαμένων πακέτων
- Μέση καθυστέρηση πακέτων
- Διαχείριση δικτύου, παρακολούθηση κυκλοφορίας

- Βοήθεια στην σχεδίαση του δικτύου της εταιρίας
- Λεπτομέρεια και συνέπεια στην χρέωση
- Εγγύηση ποιότητας υπηρεσίας
- Εξυπηρέτηση πελατών
- Κόστος υπηρεσίας

Υπηρεσίες Φιλοξενίας σελίδων (κριτήρια επιλογής)

- Διαθεσιμότητα δικτύου
- Χρόνος απόκρισης των Server
- Διαχείριση (μέτρηση κυκλοφορίας, στατιστικά στοιχεία)
- Επίδοση δικτύου ISP
- Λεπτομέρεια και συνέπεια στην χρέωση
- Εγγύηση ποιότητας υπηρεσίας
- Εξυπηρέτηση πελατών
- Κόστος υπηρεσίας

Υπηρεσίες Διασύνδεσης –Frame Relay, μισθωμένες γραμμές, ATM VPs (κριτήρια ποιότητας και επιλογής)

- Διαθεσιμότητα κυκλώματος
- Ποιότητα κυκλώματος, ποσοστά χαμένων πακέτων
- Διαθέσιμη χωρητικότητα επιπλέον του CIR (Frame relay μόνο)
- Βοήθεια στην σχεδίαση του δικτύου της εταιρίας
- Δυσκολίες και χρόνος στην εγκατάσταση, επισκευές
- Εγγύηση ποιότητας υπηρεσίας
- Εξυπηρέτηση πελατών

6.9 Κόστος ενός VPN

Το VPN είναι μία λύση που απαντά σε συγκεκριμένες ανάγκες της επιχείρησης σας και άρα το κόστος υλοποίησης του εξαρτάται από τις ανάγκες που καλείται να καλύψει. Πιο συγκεκριμένα εξαρτάται από:

- Τον αριθμό των σημείων που θα το απαρτίζουν.
- Την χωρητικότητα (bandwidth) σύνδεσης των σημείων.
- Τα κανάλια φωνής που θα υποστηρίζει (ταυτόχρονες κλήσεις)
- Την ταχύτητα πρόσβασης στο Internet που θα επιλέγει,
- Τον αριθμό των απομακρυσμένων χρηστών που θα έχουν πρόσβαση μέσω τηλεφωνικών συνδέσεων.
- Την ανάθεση προτεραιοτήτων στην κοινή χρήση εφαρμογών.
- Τα τηλεπικοινωνιακά έξοδα που ποικίλουν, ανάλογα με την εταιρία που παρέχει υπηρεσίες διασύνδεσης στο Internet.

7. Voice over IP (VOIP)

Η τεχνολογία VOIP, που είναι επίσης γνωστή και σαν τηλεφωνία πακέτων, αναφέρεται στην μεταφορά τηλεφωνικών φωνητικών συνομιλιών μέσα από ένα IP δίκτυο πακέτων. Η τεχνολογία VOIP επιτρέπει μια νέα σειρα υπηρεσιών και δυνατοτήτων ή οποίες στηρίζονται σε μία ακριβή κατασκευή. Η απαίτηση για λύσεις VOIP, ιδιαίτερα σε ένα διεθνή χώρο, καθώς επιχειρήσεις βλέπουν τρόπους να μειώσουν τα τηλεφωνικά τους κόστη, να αυξήσουν τα οφέλη τους και να γευθούν νέες υπηρεσίες. Οι ειδικοί πολλές φορές, όταν πρόκειται για την αξιολόγηση μίας λύσης VOIP πρέπει να κάνουν συγκριτικές αναλύσεις μεταξύ των μηχανημάτων για την VOIP τεχνολογία και των μηχανημάτων για την **TDM** τεχνολογία. Κάποιοι εκτιμητές οι οποίοι δεν είναι γνώστες της τεχνολογίας VOIP κάνουν το λάθος να βασίζουν τις αναλύσεις κόστους στο κόστος ανά θύρα. Το αποτέλεσμα μίας τέτοιας σύγκρισης δεν είναι αντικατροπτίζουν ακριβώς τα οικονομικά οφέλη από την τεχνολογία VOIP, τα οποία υπερβαίνουν κατά πολύ τα αντίστοιχα της τεχνολογίας TDM. Το λάθος το οποίο κάνουν οι περισσότεροι είναι το γεγονός ότι δεν γνωρίζουν ότι η τεχνολογία VOIP χρειάζεται μόνο μία θύρα για κάθε πύλη. Στα παραδοσιακά κυκλικά κυκλώματα , κάθε LD κλήση απασχολεί δύο θύρες για κάθε διακόπτη της κλάσης 4. Έτσι, ο πραγματικός αριθμός κλήσεων είναι ίσως με τις μισές συνολικά θύρες για κάθε διακόπτη.

7.1 Περιγραφή των λύσεων VOIP.

Τι είναι όμως η τηλεφωνία μέσα από το πρωτόκολλο IP; Η τηλεφωνική κλήση με την χρήση του πρωτοκόλλου IP επιτρέπει σε δεδομένα, φωνή, και πολυμέσα να εκπέμπονται μέσα από ένα δομημένο δίκτυο.
Οι τηλεφωνικές εταιρίες προωθούν τις φωνητικές κλήσεις, από το δημόσιο δίκτυο τηλεφωνίας σε δίκτυα VOIP, τα αρχικά VOIP προκύπτουν από το Voice over IP Protocol, γιατί είναι οικονομικότερο να μεταφέρεις φωνητικά δεδομένα μέσα από δίκτυα (IP). Στο μέλλον , τα δίκτυα IP τηλεφωνίας αναμένεται να παρουσιάσουν νέες υπηρεσίες για πολυμέσα, καθώς θα λειτουργούν σχεδόν όπως τα τηλεφωνικά δίκτυα.

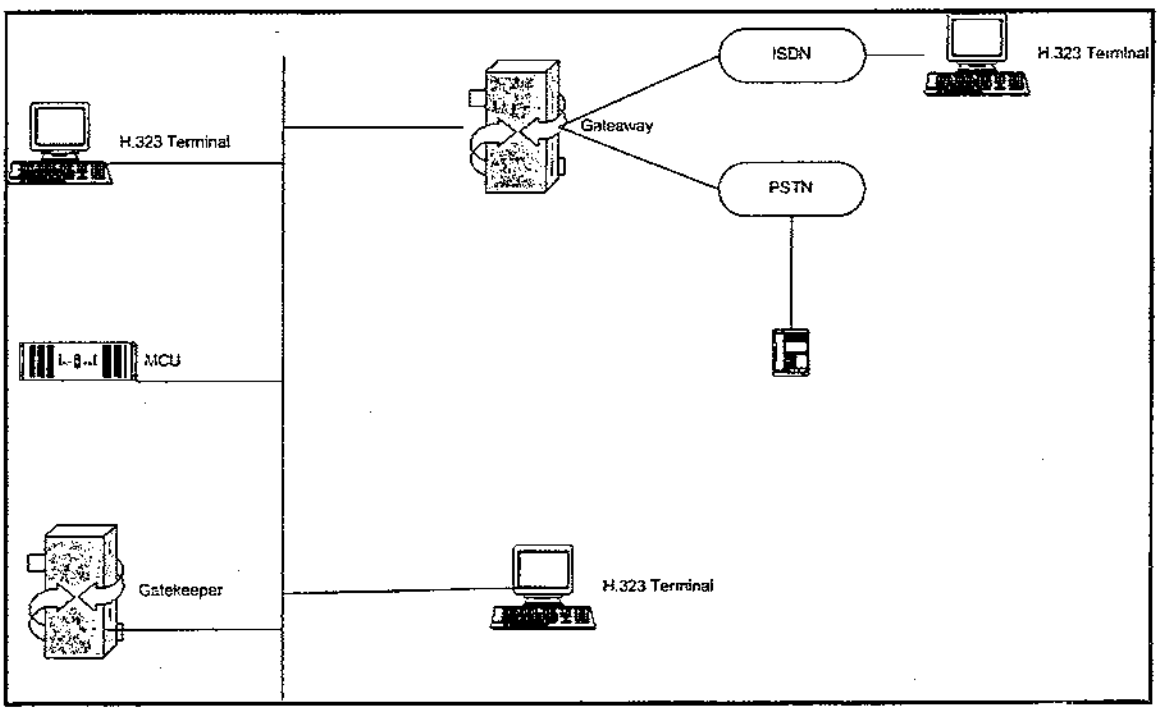
7.2 Τεχνολογία που απαιτείται για την δημιουργία ενός τέτοιου δικτύου.

Τα συστήματα Voip μετατρέπουν σε ψηφιακά τα αναλογικά σήματα φωνής, και τα μεταφέρουν σαν ένα σύνολο πακέτων μέσα από ένα ψηφιακό δίκτυο δεδομένων. Τα δίκτυα IP, επιτρέπουν σε κάθε πακέτο να βρεί το αποτελεσματικότερο και γρηγορότερο μονοπάτι για να πάει στον προορισμό του, χρησιμοποιώντας τους πόρους του δικτύου κατά τον δυνατότερο δυνατό τρόπο. Τα πακέτα που συνδέονται με μία μοναδική πηγή μπορεί να πάρουν πολλά διαφορετικά μονοπάτια για τον προορισμό, όταν βρίσκονται στο δίκτυο. Με την επιλογή διαφορετικών μονοπατιών, η άφιξη των πακέτων θα διαφέρει σημαντικά λόγω και των καθυστερήσεων που θα αντιμετωπίσουν μέσα στο δίκτυο. Μπορεί να φτάσουν εκτός χρόνου ή μπορεί να μην φτάσουν. Όταν τα πακέτα φτάσουν στον προορισμό τότε ανασυνθέτονται ώστε να δημιουργήσουν το αρχικό μήνυμα φωνής. Η τεχνολογία Voip δίνει εγγυήσεις για την σωστή ανασύνθεση των

φωνητικών πακέτων, επανορθώνοντας την ηχώ που μπορεί να δημιουργήθηκε από την end-to-end καθυστέρηση, τα χαμένα πακέτα και το τρέμουλο.
Το δίκτυο IP που χρησιμοποιείται για αυτόν τον σκοπό, μπορεί να είναι ένα LAN, μισθωμένες γραμμές ή και το Internet. Παρόλο, που το Internet είναι μια πολύ συμπαθητική λύση λόγω του οικονομίας που προσφέρει, δεν προτείνεται γιατί δημιουργεί πληθώρα σφαλμάτων, όπως αναίτιες καθυστερήσεις και απώλειες πακέτων. Για την δημιουργία ενός τέτοιου δικτύου προτείνεται η χρήση μισθωμένων γραμμών , που έχουν εξασφαλισμένο εύρος κύματος και υπηρεσίες ποιότητας τις οποίες μπορούμε να ελέγξουμε.

Τεχνολογία για το H.323 στάνταρ

Το H.323 στάνταρ προτείνει μία αρχιτεκτονική ή οποία αποτελείται από τέσσερα μέρη τα : *τερματικά, Πύλες, Φύλακες πυλών και τα μονάδες ελέγχου πολλών σημείων (MCUs-Multiple Control Units).* Η αρχιτεκτονική H.323 απεικονίζεται γραφικά στο παρακάτω σχήμα.



Εικόνα 2

Για τα στοιχεία που αποτελούν αυτό το διάγραμμα, αναφερόμαστε παρακάτω:
Τερματικά.
Αυτά είναι τερματικά σημεία ενός πελάτη σ ένα δίκτυο LAN, που παρέχουν επικοινωνία σε πραγματικό χρόνο και διπλής κατευθύνσεως.

Πύλη.
Μία πύλη είναι ένα τελικό σημείο στο δίκτυο που παρέχουν επικοινωνία διπλής κατευθύνσεως και πραγματικού χρόνου, μεταξύ τερματικών σε δίκτυο IP με άλλα τερματικά που είναι συνδεδεμένα σε άλλο δίκτυο.

Φύλακες Πύλης

Αυτό είναι ένα σημαντικό στοιχείο στην αρχιτεκτονική H.323, και λειτουργεί σαν ένας «μάνατζερ». Είναι το κέντρο για όλες τις εισερχόμενες κλήσεις στο εύρος που καλύπτει και παρέχει υπηρεσίες για όλα τα εγγεγραμμένα τελικά σημεία. Οι φύλακες πύλης παρέχουν υπηρεσίες όπως: μετάφραση διεύθυνσης, έλεγχος εισαγωγής, σηματοποίηση κλήσης, πιστοποίηση κλήσης, διαχείριση κλήσης, διαχείριση εύρους δεδομένων.

Multipoint Control Units

Το MCU λειτουργεί σαν ένα τελικό σημείο του δικτύου και δίνει την ικανότητα σε τρία ή περισσότερα τερματικά και πύλες να συμμετέχουν σε μία διάσκεψη. Το MCU αποτελείται από δύο κομμάτια : το υποχρεωτικό Multipoint controller (MC) , και τον προαιρετικό (MC). Οι λειτουργίες του MC's είναι να καθορίζει τις βασικές λειτουργίες της συνδιάσκεψης τερματικών, χρησιμοποιώντας το H.245 πρωτόκολλο.

7.3 Που απευθύνονται;

Οι προτεινόμενες λύσεις απευθύνονται σε μεσαίες και μεγάλες επιχειρήσεις που έχουν ένα ιδιαίτερα μεγάλο μηνιαίο κόστος τηλεφωνικών κλήσεων, αστικών, υπεραστικών, διεθνών και κλήσεων σε κινητά και επιθυμούν να το μειώσουν δραστικά. Απαραίτητη προϋπόθεση συνήθως για την παροχή της υπηρεσίας αυτής, είναι η επιχείρηση να διαθέτει σύγχρονο τηλεφωνικό κέντρο το οποίο δίνει την δυνατότητα διασύνδεσης με ενεργό δικτυακό εξοπλισμό.

7.4 Οφέλη VOIP υπηρεσιών

- Αύξηση των πηγών εσόδων καθοδηγώντας τους υπάρχοντες συνδρομητές και προσελκύοντας νέους πελάτες.
- Η επένδυση σε υποδομές νέας εποχής μεγιστοποιεί τη δυνατότητα ομαδοποίησης των υπηρεσιών, ενισχύει την αφοσίωση των πελατών και μειώνει τις λειτουργικές δαπάνες.
- Οι υπηρεσίες μπορούν να παρέχονται σε ευρύ κοινό: Διεθνείς υπηρεσίες μεγάλων αποστάσεων ή εθνικές υπηρεσίες καρτών κλήσης μπορούν να υλοποιηθούν με τον καλύτερο τρόπο σε κάθε ευρωπαϊκή, αφρικάνικη ή της Μέσης Ανατολής χώρα, στοχεύοντας σχεδόν στο 100% του πληθυσμού.

- Έχοντας το πλεονέκτημα του χαμηλού κόστους έναρξης ενός νέου σημείου υπηρεσίας (Points of Presence), οι παροχείς υπηρεσιών μπορούν να κλιμακώσουν την επέκτασή τους με γοργούς ρυθμούς σε σημαντικό αριθμό κρατών.
- Ανοίγουν την πόρτα για μελλοντικά έσοδα και αυξημένη ικανοποίηση πελατών μέσα από επεκτάσιμη παροχή υπηρεσιών, όπως είναι η εικονική δεύτερη γραμμή και η διαδικτυακή υπηρεσία αναμονής (call waiting).
- Μειώνουν το κόστος υποδομής και κεφαλαίου χρησιμοποιώντας την ίδια υποδομή για δεδομένα, φωνή και μελλοντικές υπηρεσίες video. Οι τρέχουσες παροχές από άλλους προμηθευτές βασίζονται σε διαχωρισμένες δικτυακές υποδομές που δομούνται ειδικά για την παροχή των επιπλέον υπηρεσιών.

7.5 Πύλες VOIP

Η τεχνολογία VOIP, τρέχει πάνω σε ένα γνήσιο δίκτυο IP, αλλά μεμονωμένες κλήσεις μπορούν να γίνουν ή να ληφθούν χρησιμοποιώντας ένα αναλογικό ή ψηφιακό IP τηλέφωνο. Οι πύλες VOIP, συνήθως είναι ένας μισθωμένος server, λειτουργούν σαν μία γέφυρα μεταξύ των κλασικών δικτύων PSTN με τα IP δίκτυα. Μία κλήση μπορεί να προωθηθεί από ένα κλασικό δίκτυο PSTN στον πλησιέστερο server πύλη, ο οποίος κάνει ψηφιακό το αναλογικό φωνητικό σήμα , το συμπιέζει σε πακέτα IP και τα προωθεί στο Internet για να μεταφερθούν σε μία πύλη κοντά στον δέκτη. Με την χρήση των πυλών VOIP, κλήσεις από υπολογιστές σε τηλέφωνα, κλήσεις από τηλέφωνα σε υπολογιστές και κλήσεις από τηλέφωνο σε τηλέφωνο μπορούν να πραγματοποιηθούν με ευκολία.

Η πρόσβαση σε μία τοπική πύλη VOIP για την αναγνώριση των κλήσεων μπορεί επίσης να υποστηριχτεί με μια ποικιλία τρόπων. Για παράδειγμα, ένα συνεταιρικό PBX (Private Branch Exchange) μπορεί να μορφοποιηθεί έτσι ώστε όλες οι διεθνείς κλήσεις να δρομολογούνται προς την πλησιέστερη πύλη. Τα τηλεφωνήματα υψηλής αξίας (όπως διεθνείς κλήσεις) υποστηρίζονται από το VOIP, και έτσι επιτυγχάνεται μείωση του κόστους.

Για να εξασφαλιστεί ή διαλειτουργικότητα μεταξύ διαφορετικών VOIP πυλών, οι κατασκευαστές πρέπει να συμπεριλαμβάνουν στις πύλες ένα στάνταρ κοινής κλήσης και ένα πρωτόκολλο ελέγχου.

7.6 Πλεονεκτήματα της χρήσης VoIP

- Τεράστια μείωση κόστους που σχετίζεται με την χρήση του τηλεφωνικού δικτύου (πάγια, χρεώσεις ανά δευτερόλεπτο κ.α
- Χρήστες που ταξιδεύουν και απομακρυσμένα γραφεία, μπορούν να προωθήσουν τις κλήσεις μεγάλης απόστασης μέσα από το Internet, και να αποφύγουν τις τηλεφωνικές χρεώσεις. Η πρόσβαση στο Internet για την μεταφορά φωνής γίνεται με την πληρωμή ενός μηνιαίου ποσού.

- Ενσωματωμένη υποδομή. Μικρές επιχειρήσεις είναι ικανές να αναπτύξουν ένα δίκτυο για φωνή και επικοινωνία δεδομένων, μειώνοντας ακόμη περισσότερο το κόστος.
- Εξελιξιμότητα. Αυτά τα δίκτυα μπορούν εύκολα να μορφοποιηθούν σύμφωνα με τις ανάγκες των χρηστών.

7.7 Πλεονεκτήματα της IP τηλεφωνίας

Με την IP τηλεφωνία, επιχειρήσεις με ένα κατάστημα ή πολλά υποκαταστήματα μπορούν να χρησιμοποιήσουν το δίκτυο δεδομένων σαν το πρωτεύον δίκτυο μετάδοσης φωνής και το κλασικό δημόσιο τηλεφωνικό δίκτυο σαν το εναλλακτικό. Αυτό έχει σαν αποτέλεσμα την μείωση των τηλεπικοινωνιακών τελών. Όμως μία λύση IP τηλεφωνίας προσφέρει πολλά περισσότερα από μία μείωση του κόστους: ένα ενιαίο δίκτυο τηλεπικοινωνιών, οπού οι χρήστες τους θα έχουν ταυτόχρονη πρόσβαση, σε ιστοσελίδες, εφαρμογές, αρχεία, εικόνες, βίντεο, ενώ ταυτόχρονα θα μιλάνε στο τηλέφωνο τους. Συνοψίζοντας τα πλεονεκτήματα της IP τηλεφωνίας είναι:

- Ευκολία στην υλοποίηση
- Πιστοποιημένη δια-λειτουργικότητα
- Επεκτασιμότητα
- Μειωμένο επικοινωνιακό και διαχειριστικό κόστος
- Αυξημένη παραγωγικότητα
- Μειωμένο κόστος σε ταξίδια και αυξημένη ομαδικότητα
- Αυξημένος έλεγχος, ασφάλεια και κεντρική διαχείριση.

8. Τεχνολογικό υπόβαθρο

8.1 Αναφορά στις απαιτήσεις σε υλικό, λογισμικό και εξειδικευμένο προσωπικό που χρειάζεται.

VPN

Υπάρχουν δύο είδη αρχιτεκτονικών για τα VPN. Είναι τα προϊόντα που είναι βασισμένα στο πρωτόκολλο Ipsec και άλλα που είναι βασισμένα σε πρωτόκολλο τούνελ σημείου προς σημείο (PPTP-Point to Point Tunneling Protocol) ή το L2TP (Layer 2 Tunneling Protocol). Παρόλο που το Ipsec έχει γίνει μία de-facto κατάσταση για τα δίκτυα LAN και τα LAN VPNs, και είναι εφαρμόσιμη από τους VPNs servers, τα PPTP και L2TP σπάνια χρησιμοποιούνται για την δημιουργία ενός VPN.

Για να δημιουργήσετε ένα LAN προς LAN ή πελάτης προς LAN VPN, χρειάζεστε τουλάχιστον έναν VPN server. Υπάρχει ποικιλία επιλογών για την απόκτηση ενός VPN server. Μερικές αναφέρονται παρακάτω :

- Χρησιμοποιείστε υπηρεσίες VPN από Microsoft Windows NT/2000 στον server που ήδη έχετε.
- Χρησιμοποιείστε υπηρεσίες VPN που είναι διαθέσιμες σε servers Unix / Linux.
- Χρησιμοποιείστε ένα VPN server που θα βρείτε σε πολλές εταιρίες, όπως η VPNet ή η RedCreek
- Υπηρεσίες VPN που θα βρείτε σε πολλούς 'τοίχους προστασίας' σαν το CheckPoint
- Χρησιμοποιείστε υπηρεσίες VPN που είναι διαθέσιμες σε πολλούς δρομολογητές.

Για την τηλεφωνική σύνδεση δύο γραφείων που βρίσκονται στις αντίθετες πλευρές της Αμερικής χρειάζεται να δαπανάει η εταιρία περίπου το ποσό των $8.600, ενώ με την χρήση ενός VPN το ποσό αυτό θα μειωνόταν σε $2.100. Μεγάλη μηνιαία διαφορά, τέτοια που δικαιολογεί την χρήση VPN. Στο βιβλίο *Building and Manging Virtual Private Network του **Dave Kosiur,*** ένα δίκτυο που θα συμπεριλάμβανε πολλές πόλεις παγκοσμίως, θα κόστιζε περίπου $71.455 με την χρήση γραμμών T1, ενώ ένα VPN που θα κάλυπτε τις απαιτήσεις αυτές θα κόστιζε $17.100. Το κόστος του VPN θα ήταν ακόμη μικρότερο εάν δεν είχαμε απαιτήσεις για υψηλή απόδοση και ασφάλεια.

Διαμόρφωση λύσης

Προκειμένου να προδιαγραφεί η τελική λύση VPN και να καθοριστεί το είδος και το πλήθος των πόρων που απαιτούνται για να υλοποιηθεί, απαιτείται η συλλογή συγκεκριμένων πληροφοριών από τον πελάτη. Συνήθως αυτές οι πληροφορίες συλλέγονται με την εξής σειρά :

1.**Κεντρικό σημείο (α) του εταιρικού δικτύου VPN :** Ως τέτοια συνήθως ορίζονται όλα τα σημεία παρουσίας του πελάτη στα οποία διαθέτει εταιρικούς servers στους οποίους

μπορούν να έχουν πρόσβαση όλα τα υπόλοιπα σημεία παρουσίας του. Πιο συγκεκριμένα για κάθε τέτοιο σημείο πρέπει να συλλεχθούν οι εξής πληροφορίες :

- Πλήρη διεύθυνση και τηλέφωνο.
- Ποιες εφαρμογές λειτουργούν σε αυτό το σημείο.
- Πόσοι χρήστες έχουν πρόσβαση σε κάθε μία από τις παραπάνω εφαρμογές.
- Ποια είναι η ανάγκη διακίνησης δεδομένων ανά χρήστη της κάθε εφαρμογής / δευτερόλεπτο.
- Ποια δικτυακά πρωτόκολλα χρησιμοποιούνται στο LAN του κεντρικού σημείου.
- Ποίες από αυτές τις εφαρμογές είναι Time Sensitive.
- Ποιο είναι το αποδεκτό Response Time /εφαρμογή.
- Υπάρχει ανάγκη για δημιουργία κλειστού δικτύου φωνής (VOIP).
- Εάν ναι, πόσα ταυτόχρονα κανάλια φωνής απαιτούνται;
- Τι είδους τηλεφωνικό κέντρο διαθέτει ο πελάτης; Ποιες οι δυνατότητες σύνδεσης αυτού με άλλα περιφερειακά;
- Τι πολιτική ασφαλείας διαθέτουν οι εταιρικές εφαρμογές;
- Υπάρχει κάποιο Security Company Policy; Ποιο είναι αυτό;
- Υπάρχουν ανάγκες υλοποίησης υποδομών;

2. **Απομακρυσμένα σημεία του εταιρικού δικτύου :** Ως τέτοια ορίζονται όλα τα υπόλοιπα σημεία παρουσίας του πελάτη, τα οποία α) εξυπηρετούνται από τα κεντρικά σημεία για πρόσβαση σε εταιρικά δεδομένα ή εφαρμογές και β) διαθέτουν φυσικό σημείο παρουσίας. Ποιο συγκεκριμένα για κάθε τέτοιο σημείο πρέπει να συλλεχθούν οι εξής πληροφορίες :

- Πλήρη διεύθυνση και τηλέφωνο
- Αριθμός χρηστών.
- Πόσοι από τους χρήστες εχουν πρόσβαση σε κάθε μία από τις εταιρικές εφαρμογές.

Μετακινούμενα Στελέχη : Ως τέτοια ορίζονται όλοι οι υπάλληλοι του τελικού πελάτη που μετακινούνται συνεχώς και έχουν ανάγκη για πρόσβαση στα εταιρικά δεδομένα.

VOIP

Οι λύσεις τηλεφωνίας μέσω μισθωμένων κυκλωμάτων, συνήθως, προσεγγίζουν συνολικά και ολοκληρωμένα τις τηλεφωνικές ανάγκες της επιχείρησης καθώς περιέχουν όλους τους απαραίτητους πόρους που απαιτούνται για να λειτουργήσουν. Πίο συγκεκριμένα μια τέτοια λύση μπορεί για κάθε σημείο παρουσίας του πελάτη, που χρειάζεται μια τέτοια λύση, να προσφέρει :

- Το βασικό τηλεπικοινωνιακό κύκλωμα σύνδεσης
- Το εφεδρικό κύκλωμα σύνδεσης
- Τον απαραίτητο εξοπλισμό σύνδεσης

- Την σχετική πύλη πρόσβασης στο δίκτυο κορμού για το βασικό κύκλωμα σύνδεσης, η οποία εξασφαλίζει και την πρόσβαση στο Internet, εάν αυτό είναι ζητούμενο για ένα σημείο παρουσίας.
- Την απαραίτητη υπηρεσία διαμόρφωσης άκρου και μεταφοράς δεδομένων εντός του δικτύου κορμού, η οποία εξασφαλίζει την ποιότητα της παρεχόμενης υπηρεσίας.
- Την απαραίτητη υπηρεσία τερματισμού κλήσεων.

Όλοι οι παραπάνω πόροι υλοποίησης (Βασικές υπηρεσίες) εμπεριέχονται στις εξειδικευμένες λύσεις τηλεφωνίας , με σύνθεση και πλήθος ανάλογο των σημείων παρουσίας του πελάτη και των ειδικών αναγκών που πρέπει να εξυπηρετηθούν.

Διαμόρφωση της λύσης

Προκειμένου να προδιαγραφεί η τελική λύση τηλεφωνίας και να καθοριστεί το είδος και το πλήθος των πόρων που απαιτούνται για να υλοποιηθεί απαιτείται η συλλογή συγκεκριμένων πληροφοριών από τον πελάτη. Συνήθως οι πληροφορίες που απαιτούνται είναι οι εξής :

- Πλήρη διεύθυνση και τηλέφωνο
- Πόσοι χρήστες έχουν πρόσβαση στο τηλεφωνικό κέντρο.
- Πόσες γραμμές πόλεως χρησιμοποιεί η επιχείρηση και αν αυτές είναι αναλογικές ή ψηφιακές;
- Που τερματίζουν οι γραμμές πόλεως, σε τηλεφωνικό κέντρο ή απευθείας σε τηλεφωνική συσκευή;
- Πόσες γραμμές χρησιμοποιούνται ταυτόχρονα από τα στελέχη της επιχείρησης για εξερχόμενες κλήσεις σε ώρες αιχμής;
- Τι τηλεφωνικό κέντρο διαθέτει ο πελάτης και τι δυνατότητες παρέχει;
- Τι ποσοστό των εξερχόμενων κλήσεων αφορούν αστική επικοινωνία, υπεραστική, διεθνή ή κλήσεις σε κινητά; Υπάρχουν κάποιοι διεθνείς προορισμοί που αποτελούν τον κύριο όγκο των διεθνών κλήσεων.

Υποδομή IP τηλεφωνίας

Εφόσον έχει φτιαχτεί η σωστή δικτυακή υποδομή, είναι πλέον εύκολο η IP τηλεφωνία να ενσωματωθεί στην υποδομή αυτή, χωρίς να αντιμετωπίσει κανένα πρόβλημα. Η υποδομή της IP τηλεφωνίας περιλαμβάνει :

- Εξυπηρετητές διαχείρισης κλήσεων (agents).
- Μηχανισμούς ελέγχου υποβολής κλήσεων που διασχίζουν το δίκτυο WAN
- Πύλες πρόσβασης φωνής, fax, modem
- Πηγές για συνδιάσκεψη και μετάφραση μεταξύ κωδικοποιήσεων συμπίεσης
- Τηλεφωνικές συσκευές

8.2 Κοστολογική ανάλυση

VOIP

Το τελικό τίμημα αποτελείται :

1. Από ένα εφάπαξ τίμημα που αφορά κυρίως τη προμήθεια των απαραίτητων τηλεπικοινωνιακών κυκλωμάτων από τον παροχέα και την επίσκεψη των συνεργείων για εγκατάσταση της υπηρεσίας.
2. Από ένα μηνιαίο πάγιο τίμημα που συμπεριλαμβάνει την χρήση όλων των παραπάνω υπηρεσιών

VPN

Το τελικό τίμημα αποτελείται :

1. Από το κόστος αγοράς του απαραίτητου εξοπλισμού.
2. Από ένα μηνιαίο πάγιο που θα πληρώνεται στον ISP για την παροχή των υπηρεσιών του.

9. Case Studie

Ιστορικό

Μεγάλη εισαγωγική εταιρία ηλεκτρολογικού εξοπλισμού με έδρα την Αθήνα, οπού βρίσκεται και η κεντρική αποθήκη, διαθέτει υποκατάστημα και αποθήκη διανομής στην Πάτρα, το οποίο καλύπτει τις ανάγκες της Πελοποννήσου.

Υπάρχων εξοπλισμός:

Α. Αθήνα

Τοπικό δίκτυο (LAN) με 15 Η/Υ και 2 Database Servers οπού βρίσκεται εγκατεστημένη μία εφαρμογή ERP, η οποία καλύπτει όλο το φάσμα των λειτουργιών του λογιστηρίου και της εμπορικής διαχείρισης και 1 Web Server ο οποίος φιλοξενεί την ιστοσελίδα της εταιρίας και συνδέεται με τους Database Servers για παραγγελίες από την ιστοσελίδα. Η σύνδεση με το Internet γίνεται μέσω μισθωμένης γραμμής Hellascom με τον ISP.

Β. Πάτρα

Τοπικό δίκτυο LAN με 5 Η/Υ. Η σύνδεση με το Internet γίνεται ανεξάρτητα μέσω dial-up σύνδεσης με την χρήση ISDN router.

Για την on-line επικοινωνία της Πάτρας με την Αθήνα χρησιμοποιείται μία μισθωμένη γραμμή Hellaspac στα 128Kbps με την χρήση Baseband modems, με μηνιαίο πάγιο χρήσης.

Υπάρχουν πωλητές οι οποίοι ταξιδεύουν και είναι εφοδιασμένοι με φορητούς υπολογιστές για την λήψη παραγγελιών.

Η πρόκληση

Να μειωθεί το κόστος της on-line σύνδεσης και να καταργηθεί η γραμμή Hellascom με την χρήση του Internet και DSL συνδέσεων. Να χρησιμοποιηθεί η σύνδεση αυτή και για την τηλεφωνική επικοινωνία μεταξύ των δύο καταστημάτων. Η όλη σύνδεση να είναι ασφαλής και να επιτρέπεται η πρόσβαση και των δύο δικτύων στο Internet.

Επίσης να παρέχεται η δυνατότητα σύνδεσης των πωλητών με το δίκτυο της εταιρίας μέσω απλών PSTN συνδέσεων με το Internet.

Τέλος και στις δύο αποθήκες θα εγκατασταθούν ασύρματα τερματικά για τις ανάγκες φόρτωσης / εκφόρτωσης τα οποία θα συνδέονται ασύρματα με τα δίκτυα των καταστημάτων.

Η λύση

Για την δικτύωση της επιχείρησης θα χρησιμοποιήσουμε προϊόντα της εταιρίας CISCO.
Ο νέος Easy VPN Server , που συμπεριλαμβάνει το λειτουργικό σύστημα IOS 12.2 T ή νεότερες εκδόσεις, επιτρέπει στους router να τερματίζουνε τις συνδέσεις VPN που χρησιμοποιούνται από τους κινητούς χρήστες.
Για τους κινητούς χρήστες , δεν είναι αρκετό να έχουν μία καλή σύνδεση με το Internet. Για να μπορούν να είναι ανταγωνιστικοί πρέπει να έχουν ασφαλή πρόσβαση σε ηλεκτρονικές πηγές της επιχείρησης από την δουλεία ή από το σπίτι, και αυτό γίνεται με την δημιουργία ενός VPN με αλγόριθμους πιστοποίησης και δυνατότητα κρυπτογράφησης των δεδομένων. Αυτό γίνεται με την χρήση ενός server που παρέχει VPN πλατφόρμες (Cisco VPN Easy Server).
Για να έχουν πρόσβαση σε τοπικά δίκτυα οι κινητοί χρήστες πρέπει να συνδεθούν με το Internet μέσω του δημοσίου τηλεφωνικού δικτύου και να δημιουργήσουν ένα κανάλι VPN με το τοπικό δίκτυο που θέλουν χρησιμοποιώντας το λογισμικό **CISCO VPN Client** , μία εφαρμογή που υποστηρίζεται από τα Windows και άλλα λειτουργικά συστήματα. Η εφαρμογή διευκολύνει την επιχείρηση, αφού αφαιρεί πολλές από τις αναγκαίες ρυθμίσεις της δημιουργίας ενός VPN μεταξύ των κεντρικών γραφείων και των γραφείων στην Πάτρα. Ο Router των κεντρικών γραφείων πρέπει να έχει πολιτικές ασφαλείας, τέτοιες ώστε να καθορίζουν ποίες παράμετροι του VPN, παράμετροι όπως οι αλγόριθμοι κρυπτογράφησης και πιστοποίησης , θα χρησιμοποιηθούν για την επικοινωνία με κινητά μηχανήματα (Laptop, palmtop). Αυτές οι πολιτικές ασφαλείας εισάγονται στις κινητές συσκευές πολύ εύκολα.

Χρησιμοποιώντας την πλατφόρμα Cisco Unified VPN Framework, ο Cisco VPN Remote Feature επιτρέπει την αυτόματη ρύθμιση των περισσοτέρων παραμέτρων στον router της Πάτρας από τον VPN 3000 Concentrator. Σε αυτό το σενάριο, VPN 3000 Concetrator λειτουργεί σαν ένας server Ipsec και ο router της Πάτρας λειτουργεί σαν πελάτης Ipsec
Η αυτόματη ρύθμιση των παραμέτρων περιλαμβάνει τα εξής:

- Εσωτερική διεύθυνση IP
- Internal Dynamic Host Control Protocol (DHCP) server address
- Internal Server Wins address
- Διαχωρισμό τούνελ με επιτρεπόμενη σημαία

Έτσι εάν ο router της σειράς 1700 έχει ρυθμιστεί με την χρήση ενός Easy Remote VPN, μια VPN σύνδεση με τον Concentrator της σειράς 3000 μπορεί να πραγματοποιηθεί κάνοντας ελάχιστες ρυθμίσεις. Ένας easy VPN server, προωθεί τις IPsec παραμέτρους και τις πολιτικές ασφαλείας στον router της σειράς 1700 και δημιουργεί ένα VPN tunnel (Επειδή μεγάλο μέρος του στησίματος ενός VPN δικτύου είναι αυτοματοποιημένο, η διαδικασία δημιουργίας ενός VPN απλοποιήθηκε πολύ με το Cisco easy VPN Remote Feature. Για να ανταποκριθεί στις δικτυακές ανάγκες διαφόρων χρηστών το Cisco easy VPN Remote Feature χωρίζεται σε δύο κατηγορίες :

1. **Client Mode.** Αυτή είναι στάνταρ κατηγορία στην οποία επιτρέπεται σε μηχανήματα στα γραφεία της Πάτρας ή σε μηχανήματα πωλητών να

έχουν πρόσβαση σε πηγές του τοπικού δικτύου της Αθήνας, χωρίς να είναι αμφίδρομη αυτή η σχέση.

2. **Network Extension mode.** Οι χρήστες και στα δύο καταστήματα θα μπορούν να έχουν πρόσβαση σε πηγές που βρίσκονται οπουδήποτε μέσα στο

Έτσι στα κεντρικά γραφεία στην Αθήνα θα πρέπει να προστεθεί ένας ακόμη server που θα υποστηρίζει την δημιουργία δικτύων VPN. Προτείνεται η αγορά ενός Cisco VPN Server. Ο νέος server θα συνδεθεί στο *catalyst switch* που είναι συνδεδεμένοι οι RDBMS και ο Web Server μίας και υπάρχει θύρα ελεύθερη.

Catalyst switch

Η σύνδεση των υπολογιστών με το *Catalyst switch* θα γίνει με *(Ethernet Cable<100m)* Το *catalyst switch* των server επικοινωνεί με την χρήση *Ethernet Cable* με το *Catalyst switch* του τοπικού δικτύου. Στους server με τις βάσεις δεδομένων τρέχει ακόμη η εφαρμογή ERP η οποία καλύπτει ακόμη τις ανάγκες του λογιστηρίου και της Εμπορικής διαχείρισης.

Χαρακτηριστικά του (Catalyst 6000- Integrated Cisco IOS software)

Ο Cisco Catalyst Switch Manager (CSM) είναι βασισμένος στο σύστημα (EMS) για να παρέχει υπηρεσίες δικτύου υψηλής απόδοσης. Το προϊόν αυτό έχει γραφικό περιβάλλον διεπαφής για τον έλεγχο του

Concentrator

Ο Concentrator 3005 είναι μία πλατφόρμα σχεδιασμένη για επιχειρήσεις μεγάλης δυναμικότητας που ζητάνε bandwidth από T1/E1 μέχρι T3/E3 (50Mbps μέγιστη ταχύτητα). Ο 3020 προσφέρει υποστήριξη σε πάνω από 750 συνεδρίες Ipsec ή σε 200 clientless.

Τι προσφέρει ο 3020;

- Μία εφαρμογή SEP για κρυπτογράφηση βασισμένη στο hardware
- Ένα τροφοδοτικό
- Τρεις 10/100 BASE-T Ethernet διεπαφές
- Επιπλέον κάρτα κρυπτογράφησης
- Μνήμη Flash για την διαχείριση αρχείων.

Router (Cisco 836 ADSL)

Ο router 836 ADSL υποστηρίζει ασύμμετρο DSL μέσα από δίκτυο ISDN και προσφέρει ένα 4-θύρο Ethernet Lan Switch για την σύνδεση πολλών υπολογιστών ή δικτυακών συσκευών σε ένα δίκτυο.

Προσφέρει ασφάλεια και απόδοση για VPN δίκτυα επιχειρήσεων, ασφάλεια που σχετίζεται με ασφαλές πρωτόκολλα (Ipsec), στάνταρ τριπλής κρυπτογράφησης (3DES) για εικονικά ιδιωτικά δίκτυα., Firewall , Cisco Easy VPN Remote.

Ο 836 router της Cisco, προσφέρει εξελιγμένο QoS και υψηλά επίπεδα κρυπτογράφησης και έτσι μπορεί να παρέχει υπηρεσίες φωνής και βίντεο σε πολύ υψηλές αποδόσεις. Όταν συνδεθούν τα IP τηλέφωνα τότε ο router μπορεί να δώσει προτεραιότητα στην διευθυντιοδότηση της φωνής και των δεδομένων και να εξασφαλίσει μίας υψηλής απόδοσης σύνδεση για την μεταφορά φωνής μέσω του πρωτοκόλλου IP

Router (Cisco 1760) + call manager express

Ο router 1760 της Cisco, που μπορεί να διαχειριστεί φωνή και δεδομένα και να παρέχει λειτουργικότητα VOIP και μεταφορά φωνής (π.χ τηλεφωνικές κλήσεις, φάξ). Χρησιμοποιώντας μία ή δύο συνδέσεις WAN, ο router συνδέει τα δίκτυα LAN (Ethernet Fast Ethernet) με τα κεντρικά γραφεία.
Επιπλέον οι δρομολογητές των υποκαταστημάτων ενσωματώνουν την λειτουργία SRST (Survivable Remote Site Telephony), που επιτρέπει στα τηλέφωνα του καταστήματος να λειτουργούν σε περίπτωση βλάβης του εξυπηρετητή Call Manager ή της γραμμής ISDN.

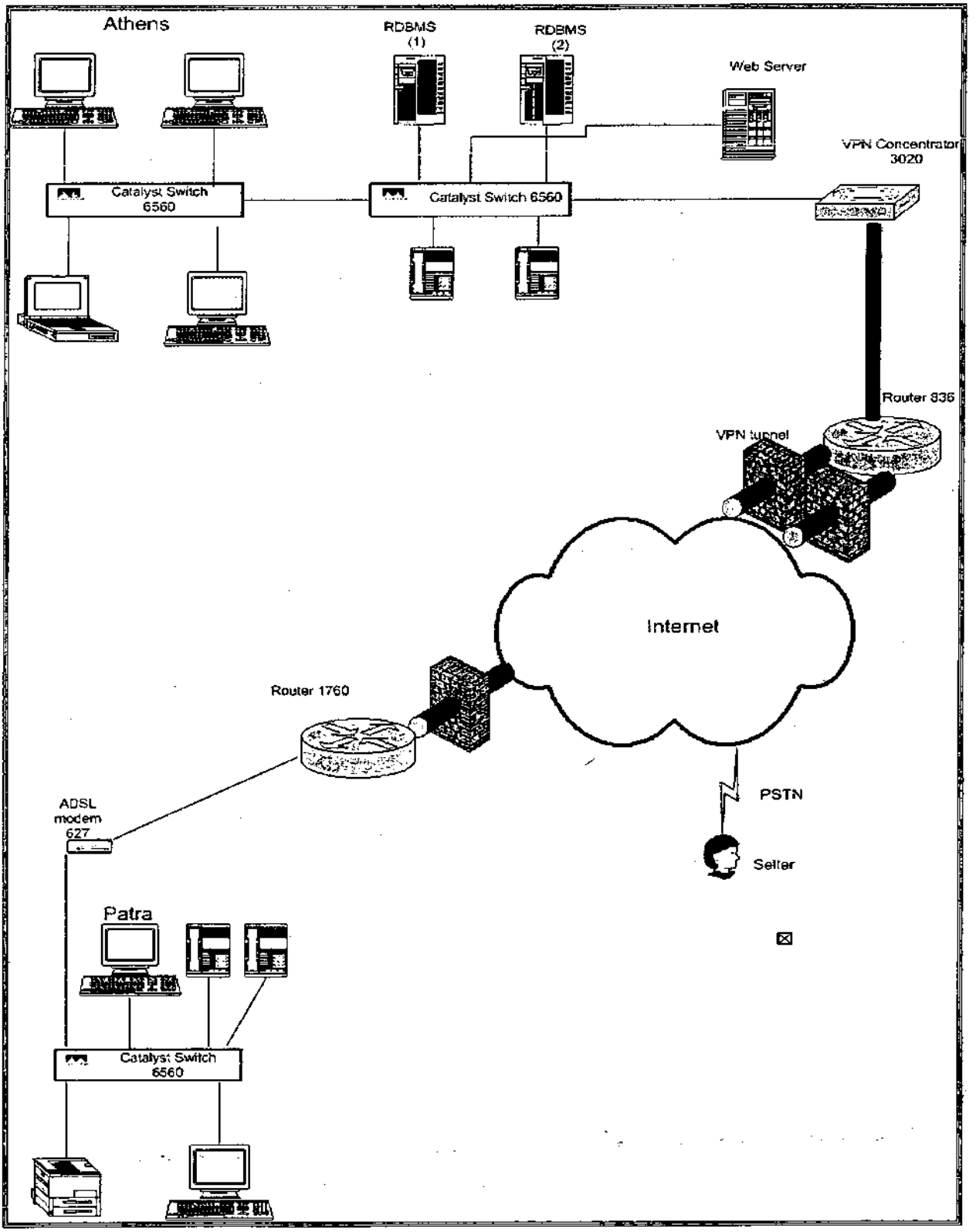
Call Manager

Ο call manager είναι ένα λογισμικό βασισμένο στην προώθηση κλήσεων της IP τηλεφωνίας. Το λογισμικό αυτό χρησιμοποιήται από την AVVID (Architecture for Voice, Video and integrated data) και επεκτείνει τις δυνατότητες της τηλεφωνίας σε μορφές όπως ή μετάφορα πακέτων δεδομένων μέσα απο τα δίκτυα της τηλεφωνίας με την χρήση IP τηλεφώνων, συσκευές επεξεργασίας πολυμέσων , πύλες VOIP, και εφαρμογές πολυμέσων. Επιπλέον υπηρεσίες φώνής και βίντεο, όπως ενοποιημένα μηνύματα , τηλεδιάσκεψη, κέντρα συνεργασίας και ενεργή βοήθεια σε περιβάλλον πολυμέσων. Το Cisco Call Manager είναι εγκατεστημένο στους Media Convergence Servers (MCSs) και σε επιλεγμένους τρίτους server.

IP Telephony (Cisco IP Phone 7940G)

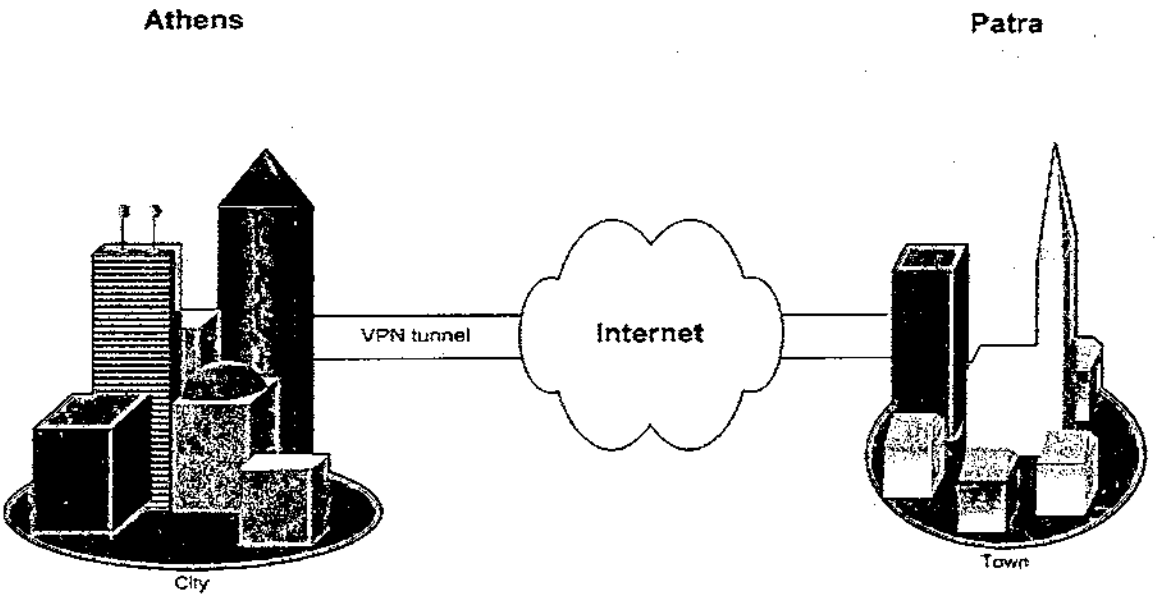
Το τηλέφωνο 7940G αναγνωρίζει τα εισερχόμενα μηνύματα και τα κατηγοριοποιεί για την ευκολία του χρήστη στην οθόνη.Αυτό επιτρέπει στους χρήστες να απαντούν στις εισερχόμενες κλήσεις με ταχύτητα και αποτελεσματικότητα.

Αποτελέσματα


Athens
RDBMS (1)
RDBMS (2)
Web Server
VPN Concentrator 3020
Catalyst Switch 6560
Catalyst Switch 6560
Router 836
VPN tunnel
Internet
Router 1760
ADSL modem 627
PSTN
Seller
Patra
Catalyst Switch 6560

Εικόνα 3

Στο παρακάτω διάγραμμα βλέπουμε την επικοινωνία μέσω ενός ιδιωτικού ιδεατού δικτύου :



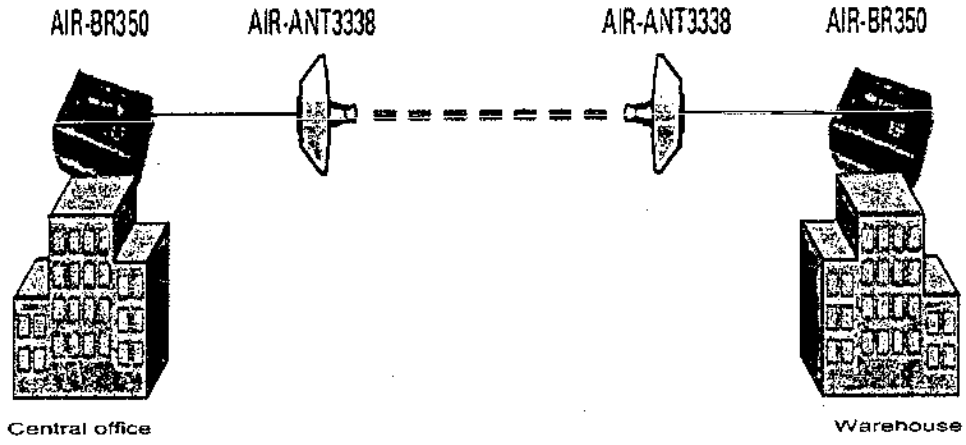
Εικόνα 4

Έτσι η επικοινωνία μεταξύ των καταστημάτων επιτυγχάνεται μέσα από την δημιουργία VPN's. Έτσι καταργεί την μισθωμένη γραμμή (Hellascom), την οποία της παρείχε ο ISP. Αξίζει να αναφέρουμε ότι για την χρήση της γραμμής αυτής εταιρία πλήρωνε τα ακόλουθα ποσά..Για παραχώρηση γραμμής 440 ευρό το κάθε άκρο. Συνολικά για την χρήση (μόνο) της γραμμής 880 ευρό κάθε μήνα.

1. Για πρόσβαση με 128Kbps πρέπει να πληρώνει 60 Ε για κάθε άκρο (60*2=120 Ε) και 4,46 Ε γία κάθε χιλιόμετρο. Η χιλιομετρική απόσταση της Αθήνας από την Πάτρα έιναι περίπου 200Km, οπότε η εταιρία θα έπρεπε να πληρώνει (200*4,46=892 Ε).

Συνολικά ή εταιρία για να μπορεί να χρησιμοποιεί την μισθωμένη γραμμή από τον ISP, πρέπει να δαπανά **1.892 Ε** μηνιαίος

Τέλος η ασύρματη επικοινωνία θα επιτευχθεί με την χρήση της σειράς (AIR) ή οποία παρέχει όλο το απαραίτητο υλικό για την επικοινωνία δύο κτηρίων χωρίς την χρήση τηλεφωνικών γραμμών και οπτικών ινών. Στην εικόνα 5 φαίνετε καθαρά ο τρόπος που θα επικοινωνούν ασύρματα τα κεντρικά γραφεία με τις αποθήκες.
Θα πρέπει εδώ να αναφέρουμε ότι σε περίπτωση που δεν υπάρχει οπτική επαφή μεταξύ των δύο κτηρίων θα πρέπει να τοποθετηθεί και ένας αναμεταδότης σε υψηλό σημείο ώστε να βλέπει και τα δύο κτήρια.



Εικόνα 5

Κοστολογική ανάλυση

Η εταιρία έχει σταθερό κόστος γραμμής 880 ευρό. Το μεταβλητό της κόστος, το οποίο εξαρτάται από την χιλιομετρική απόσταση και το επιθυμητό εύρος ζώνης για την μετάδοση δεδομένων ανέρχεται στα 1012 ευρό. Συνολικά η εταιρία πρέπει να δαπανά **1892 ευρό** μηνιαίος.

Για αυτή την νέα επένδυση θα χρειαστούμε τρία *catalyst switch 6000*, έναν *concentrator 3005*, έναν *router 836 ADSL*, έναν *router 1760*, *το λογισμικό call manager*, *IP τηλέφωνα* καθώς και δύο *ADSL modem*.
Για την δημιουργία ενός ιδεατού ιδιωτικού δικτύου προκύπτουν λοιπόν τα παρακάτω κόστη:

Μοντέλο	**Ποσότητα**	**Τιμή μονάδας ($)**	**Τιμή μονάδας ($)**
Catalyst switch 6000	3	600	1.800
Concentrator 3005	1	2.950	2.950
Router 836 ADSL	1	767	767
Router 1760	1	2.100	2.100
Call manager Software	1	3.500	3.500
IP phones	30	150	4.500
Software for IP phone	2	80	160

Εκτός από τα πάγια έξοδα της επένδυσης η εταιρία θα έχει και ένα μηνιαίο σταθερό κόστος το οποίο είναι μεταβαλλόμενο. Το κόστος αυτό εξαρτάτε απο την ταχύτητα μετάδοσης δεδομένων που επιθυμεί η επιχείρηση καθώς και απο τα εκάστοτε τιμολόγια του ISP φορέα. Παρακάτω παραθέτουμε έναν συγκριτικό πίνακα για τις μηνιαίες

χρεώσεις σε συνδέσεις ADSL αορίστου χρόνου και για ταχύτητες **384,512,1024 Kbps.** Οι χρεώσεις είναι σε ευρό.

	Otenet	**Forthnet**	**HOL**	**Vivodi**	**A.C.N**	**Sparknet**
384 Kbps	32	47,9	47,1	80	67,5	43
512 Kbps	42,7	73	71	100	92,5	66
1024 Kbps	85,5	142	145		161,5	128,5

Συνολικά η εταιρία για αυτήν την επένδυση θα δαπανήσει **15.777 $.**

Στην συγκεκριμένη περίπτωση είναι δύσκολο να προτείνουμε κάποια περίπτωση απο τις δύο γιάτι πρέπει να γίνει οικονομική ανάλυση όλων των στοιχείων που διαδραματίζουν κάποιον ρόλο στις συγκεκριμένες περιπτώσεις. Γεγονός είναι ότι με την κατάργηση της μισθωμένης γραμμής η εταιρία εξοικονομεί το ποσό των 1892 ευρό μηνιαίος και μπορεί να διαθέτει μέρος των χρημάτων αυτών στην απόσβεση της επένδυσης.
Έτσι η επένδυση αυτή είναι αρκετά δελεαστική για την επιχείρηση γιατί αναβαθμίζει τον υπάρχον τεχνολογικό εξοπλισμό της

10. Επίλογος

10.1 Αναφορά σε τεχνολογίες που τώρα αναπτύσσονται.

Η εξέλιξη της τεχνολογίας της κινητής τηλεφωνίας έχει γίνει με τέτοια επιτάχυνση, που δημιούργησε την ανάγκη διαφοροποίησης μεταξύ διαφορετικών τεχνολογιών σε διαφορετικές χρονικές περιόδους. Έτσι η βιομηχανία τηλεπικοινωνιών έχει διαχωρίσει αυτές τις διαφοροποιημένες εποχές αναφερόμενη στο κοινός αποδεκτό όρο «γενιά». Η πρώτη γενιά συστημάτων είναι τα πρώτα κυψελωτά συστήματα, τα οποία τυπικά ήταν αναλογικά. Σε αυτήν την γενιά περιλαμβάνονται το σύστημα AMPS (Advanced Mobile Phone Systems) στην βόρεια Αμερική, το σύστημα TACs (Total Access Systems) στις περισσότερες χώρες της βρετανικής κοινοπολιτείας και την Ιταλία, και τα συστήματα NMT (Nordic Mobile Telephone) 450 και 900 τα οποία ήταν δημοφιλή στις Σκανδιναβικές χώρες. Αυτά τα συστήματα υπήρχαν στα τέλη της δεκαετίας του 70 και καθ' όλη την διάρκεια της δεκαετίας του 80.

Στις αρχές της δεκαετίας του 90, τα πρώτα ψηφιακά συστήματα άρχισαν να κάνουν την εμφάνιση τους. Αυτά ήταν το D-AMPS και το PCS (Personal Communication Systems) 1900 στην βόρεια Αμερική και το GSM στην Ευρώπη. Αυτά τα συστήματα από τότε αναφέρονται σαν συστήματα δεύτερης γενιάς και βρίσκονται σήμερα σε ενέργεια. Τα συστήματα δεύτερης γενιάς στην Ευρώπη, υφίστανται βελτιώσεις που θα τα καταστήσουν ικανά να διαχειρίζονται ευκολότερα και με μεγαλύτερη ταχύτητα τα δεδομένα, περιλαμβανομένων της μετάδοσης αρχείων και της εισαγωγής προηγμένων υπηρεσιών που θα κάνουν πραγματικότητα την ύπαρξη εφαρμογών όπως το ηλεκτρονικό εμπόριο. Αυτή η βελτίωση θα έχει την μορφή των τεχνολογιών GPRS και EDGE (Enhanced Data Rates for Global Evolution), οι οποίες θα δώσουν την δυνατότητα στα υπάρχοντα συστήματα να μεταβιβάζουν δεδομένα με ταχύτητα 115 Kbps μέσω του GPRS και τελικά εως 384 Kbps μέσω του EDGE. Οι τεχνολογίες του GPRS και του EDGE είναι βασισμένες στο σύστημα GSM και κοινός αναφέρονται σαν συστήματα 2,5 γενιάς. Στο παρόν χρονικό διάστημα, οι operators κινητής τηλεφωνίας στήνουν την δικτυακή υποδομή των συστημάτων GPRS στην ελληνική αγορά.

Μετα την εγκατάσταση των συστημάτων GPRS/EDGE από τους operators, το επόμενο λογικό βήμα δεν αντιπροσωπεύει πλέον μία επιμηκυνόμενη εξέλιξη των ψηφιακών δικτύων κινητής τηλεφωνίας, αλλά μάλλον μια τεχνολογική επανάσταση που θα προσφέρει την δυνατότητα παροχής εντελώς νέων υπηρεσιών και ταχύτητας μετάδοσης των δεδομένων 100 φορές ταχύτερη από αυτή των σημερινών συστημάτων. Έτσι θα έχουμε την δυνατότητα της ταχείας μετάδοσης δεδομένων μέσω του Internet, την παροχή ενοποιημένων και ευκολόχρηστων υπηρεσιών ηλεκτρονικού ταχυδρομείου καθώς και την ταχεία και ολοκληρωμένη μετάδοση εικόνων υψηλής ανάλυσης. Αυτά είναι τα κοινώς αποκαλούμενα δίκτυα 3ης γενιάς.

Γλωσσάριο Τεχνικών Όρων

Concentrator : Ένας τύπος πολυπλέκτη που συνδυάζει πολλά κανάλια σε μία μόνο εκπομπή με τέτοιο τρόπο που όλα τα κανάλια μπορούν να είναι ταυτόχρονα ενεργά. Για παράδειγμα, οι ISPs χρησιμοποιούν το hardware αυτό με τέτοιο τρόπο ώστε να το απλό μόντεμ με τις γραμμές T1 για σύνδεση στο Internet.

Modem (μόντεμ) : Ακρωνύμιο της λέξης Modulator/Demodulator (Διαμορφωτής/Αποδιαμορφωτής). Σε γενικές γραμμές το μόντεμ είναι μία συσκευή η οποία διαμορφώνει και αποδιαμορφώνει ένα σήμα. Στην ασύρματη επικοινωνία, το μόντεμ είναι μια συσκευή η οποία παρέχει ένα περιβάλλον διεπαφής για την μεταφορά δεδομένων στο ασύρματο δίκτυο.

Proxy Server: Οι περισσότερες μεγάλες επιχειρήσεις, και πανεπιστήμια χρησιμοποιούν ένα proxy server. Αυτός είναι ένας server από τον οποίο πρέπει να περάσουν όλοι οι υπολογιστές που είναι συνδεδεμένοι στο τοπικό δίκτυο, πριν αποκτήσουν πρόσβαση σε πληροφορίες του Internet.

Hub: Μία συσκευή σύνδεσης για δίκτυα. Επιτρέπει σε πολλούς υπολογιστές να συνδέονται και να μοιράζονται πακέτα πληροφοριών.

Network Interface Card (Κάρτα δικτύου) : Η κάρτα δικτύου είναι μία κάρτα που μπαίνει στον υπολογιστή, ώστε να μπορεί ο υπολογιστής να συνδέεται στο δίκτυο. Οι περισσότερες κάρτες δικτύου είναι σχεδιασμένες για έναν συγκεκριμένο τύπο δικτύου, πρωτοκόλλων, και πολυμέσων, αλλά υπάρχουν και κάποιες που υποστηρίζουν πολλά δίκτυα.

[redacted] ...έονται τα LANs. Μία ...η γέφυρα έχει θύρες σύνδεσης σε δύο ξεχωριστά LANs. Ένα πακέτο που λαμβάνεται από την μία θύρα μπορεί να αναμεταδοθεί σε μία άλλη θύρα. Αντίθετα με τον αναμεταδότη, η γέφυρα δεν θα αρχίσει την αναμετάδοση εάν δεν έχει παραλάβει ολόκληρο το πακέτο. Σαν συνέπεια αυτού, η γέφυρα μπορεί να μεταδίδει ταυτόχρονα χωρίς να δημιουργούνται προβλήματα. Οι γέφυρες όπως και οι αναμεταδότες, δεν τροποποιούν το περιεχόμενο των πακέτων σε καμία περίπτωση. Τέλος αξίζει να αναφέρουμε ότι οι γέφυρες αντίθετα με τους αναμεταδότες μπορεί να προκαλέσει κίνηση στο δίκτυο.

Router (Διακομιστής) : Ο διακομιστής σε γενικές γραμμές είναι μία συσκευή, που χρησιμοποιείται για να τεμαχίσει το δίκτυο, με σκοπό να μειώσει την ευρεία κυκλοφορία και να παρέχει ασφάλεια, έλεγχο και εναλλακτικά μονοπάτια. Είναι μια συσκευή που μπορεί να συνδέσει πολλά LAN στο επίπεδο του δικτύου και έχει πρόσβαση σε διευθύνσεις δικτύου, αλλά λειτουργεί με σεβασμό στα τρέχοντα πρωτόκολλα.

Bandwidth:

1. Το εύρος μιας συχνότητας ή ενός κύματος
2. Η ποσότητα δεδομένων που μπορεί να μεταδοθεί σε συγκεκριμένο χρόνο. Για ψηφιακές συσκευές το bandwidth μετράται σε bits/sec. Για αναλογικές συσκευές το bandwidth μετράται σε κύκλους/sec.

Server: Ένας υπολογιστής ή συσκευή σε ένα δίκτυο που διαχειρίζεται τις πηγές του δικτύου. Για παράδειγμα ένας server αρχείων, είναι ένας υπολογιστής και μια αποθηκευτική συσκευή που σκοπός τους είναι η αποθήκευση αρχείων.

Internet: Ένα παγκόσμιο δίκτυο που συνδέει εκατομμύρια υπολογιστές. Περισσότερες από 100 χώρες είναι συνδεδεμένες και μοιράζονται δεδομένα, ιδέες, απόψεις.

Repeater (Αναμεταδότης) : Μια δικτυακή συσκευή που αναμεταδίδει ένα μήνυμα. Οι αναμεταδότες χρησιμοποιούνται σε συστήματα εκπομπής για να αναμεταδίδουν αναλογικά ή ψηφιακά σήματα που μπορεί να έχουν απώλειες μετάδοσης. Σε δίκτυα δεδομένων, ο αναμεταδότης μπορεί να κατευθύνει μηνύματα μεταξύ υποδικτύων που χρησιμοποιούν διαφορετικά είδη πρωτοκόλλων, ή καλωδίωσης.

Intranet: Ένα δίκτυο βασισμένο στα πρωτόκολλα TCP/IP, που ανήκει σε έναν οργανισμό, συνήθως μια εταιρία στην οποία έχουν πρόσβαση μόνο τα μέλη της ή όσοι έχουν εξουσιοδότηση. Μια ιστοσελίδα Intranet, μοιάζει με τις περισσότερες ιστοσελίδες, μόνο που το τοίχος προστασίας δεν αφήνει μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση.

Extranet : Το extranet είναι ένα intranet το οποίο δίνει πρόσβαση και σε χρήστες που δεν έχουν σχέση με την εταιρία, παρέχοντας σε αυτούς πολλά επίπεδα πρόσβασης στο δίκτυο της εταιρίας.

Ethernet: Μία αρχιτεκτονική LAN που αναπτύχθηκε από την Xerox Corporation σε συνεργασία με την DEC και την INTEL το 1976. Το Ethernet χρησιμοποιεί τοπολογία αστέρα ή γραμμής και υποστηρίζει μεταφορά δεδομένων μέχρι 10Mbps.

FTP: Τα αρχικά του File Transfer Protocol, το πρωτόκολλο που χρησιμοποιείται για την ανταλλαγή αρχείων στο Internet. Το FTP δουλεύει με τον ίδιο τρόπο με το HTTP για την μεταφορά σελίδων από έναν server στον φυλλομετρητή ενός χρήστη.

Telnet: Ένα πρόγραμμα για δίκτυα TCP/IP σαν το Internet. Το πρόγραμμα αυτό τρέχει στον υπολογιστή του χρήστη και το συνδέει σε έναν server στο δίκτυο. Εκεί μπορείς να δώσεις εντολές μέσω του προγράμματος και θα εκτελεστούν σαν να τις έδινε κατευθείαν σε έναν server.

DNS: Το DNS είναι τα αρχικά του (Domain Name System), μια υπηρεσία του Internet που μεταφράζει τα ονόματα των ιστοσελίδων σε διευθύνσεις IP. Το Internet είναι βασισμένο σε διευθύνσεις IP, παρόλο που τα ονόματα ιστοσελίδων είναι ποιο εύκολο να μένουν στην μνήμη. Κάθε φορά που πληκτρολογείται στον browser μια διεύθυνση ή υπηρεσία DNS πρέπει να μεταφράσει το όνομα στην σωστή διεύθυνση, για να μπορέσει να δει ο χρήστης την ιστοσελίδα που επιθυμεί.

IMAP : Τα αρχικά του (Internet Message Access Protocol), ένα πρωτόκολλο που χρησιμοποιείται για την ανάνηψη από τον server, των e-mail μας.

OSI : OSI είναι τα αρχικά του (Open System Interconnection), ένα πρότυπο της ISO για τις διεθνείς επικοινωνίες που ορίζει ένα πλαίσιο για την εφαρμογή των πρωτοκόλλων σε εφτά επίπεδα. Ο έλεγχος περνάει από το ένα επίπεδο στο άλλο, ξεκινώντας από το στρώμα εφαρμογής και φτάνοντας στο φυσικό στρώμα.

Browser (φυλλομετρητής) : Ένα πρόγραμμα που σκοπός του είναι να βρίσκει και να απεικονίζει τις ιστοσελίδες στον χρήστη. Οι ποιο γνωστοί browser, είναι οι Internet Explorer και Netscape Navigation.

ATM : Κατηγορία δικτύων που επιτρέπει την μεταγωγή δεδομένων διαφορετικών μορφών, μέσω σταθερού μεγέθους κελυφών, με αποτέλεσμα να επιτρέπονται υψηλές ταχύτητες μετάδοσης. Ένα δίκτυο ATM πρέπει να είναι εφοδιασμένο με τις κατάλληλες συσκευές αλλά μπορεί να υλοποιηθεί πάνω στις υπάρχουσες γραμμές επικοινωνίας.

Backbone (Δίκτυο κορμού) : Όρος που αποδίδεται στα τμήματα δικτύων που χρησιμοποιούνται για την διασύνδεση και μεταγωγή πληροφοριών μεταξύ άλλων επιμέρους δικτύων.

FDDI (Fiber Distributed Data Interface) : Δίκτυα υλοποιημένα πάνω σε οπτικές ίνες, υλικό που είναι ιδιαίτερα ανθεκτικό σε αντίξοες συνθήκες και προσφέρει μεγάλες ταχύτητες δεδομένων.

Node (Κόμβος) : Ονομάζεται κάθε συσκευή ή ηλεκτρονικός υπολογιστής που είναι συνδεδεμένος στο Internet.

Internet Service Provider (ISP) : Εταιρίες που εξειδικεύονται στην παροχή υπηρεσιών διασύνδεσης με το Internet. Οι υπηρεσίες αυτές μπορεί να απευθύνονται σε τελικούς χρήστες και να αφορούν πρόσβαση μεμονωμένων ατόμων μέσω του τηλεφωνικού δικτύου ή να αφορά υπηρεσίες συνδεσιμότητας σε μισθωμένες γραμμές εταιριών.

Πίνακες και σχεδιαγράμματα

Πίνακες

Εικόνες

Βιβλιογραφία

1. ***http://ietf.org/html.charters/ipsec-charter.html***
2. ***http://web.mit.edu/tytso/www/ipsec/index.html***
3. *www.cisco.com*
4. *www.otenet.gr*
5. *www.hol.gr*
6. *www.lucent.com*
7. *www.3com.com*
8. *www.webopedia.com*
9. *http://www.cisco.com/warp/public/759/ipj_3-3/ipj_3-3_futureTCP.html*
10. *www.flash.gr*
11. *www.go-online.gr*
12. http://www.putergeek.com/home_network_2
13. http://hnet.teipir.gr/HGD/Networks/Main_networks.html
14. http://www.cs.aueb.gr/
15. http://digimedia.oingo.com/apps/domainpark/results.cgi?s=ipsec&client=GOTO2486&domain_name=%26domain_name%3Dhack&sid=0080132544b30000&param=10768&ac=s
16. http://www.isoc.org/
17. www.unitech.com
18. www.voip-info.org
19. www.conta.gr

20. Cisco-Λύσεις ασυρμάτων δικτύων
21. TravelPack Case Studie- BOS.COM
22. Digital Signatures and Public Key Infrastructures – *Wolfang Schneider*
23. Εργαστήριο δικτύων υπολογιστών – *Βασίλης Δαρσινός , Νικόλαος Βώρος, Μανώλης Ψαράκης*
24. Electronic Commerce in Internet – *David Billard*
25. *Τηλεπικοινωνίες: Βασικές έννοιες και κατευθύνσεις- Κ. Κουρκουμπέτης*
26. *IGMP reports*
27. *Internetworking Technology Overview – June 1999*
28. *Επιχειρηματικές λύσεις τηλεφωνίας – Cisco*
29. Local Area Network Concepts and Products: LAN Architecture
30. *Tanenbaum,* Δίκτυα Υπολογιστών
37. Μετάδοση δεδομένων – Επικοινωνία – *πανεπιστήμιο Κρήτης*

38. Ηλεκτρονική διακίνηση αγαθών & κρυπτογραφία – *Αθανάσιος Βασιλόπουλος, Γούτας Δημήτριος*
39. Εισαγωγή στους υπολογιστές – *Peter Norton*
40. Εισαγωγή στην πληροφοριακή σκέψη – *Μιχάλης Σφακιανάκης*
41. Διοίκηση – Διαχείρηση πληροφοριακών συστημάτων – *Αντώνης Δημητριάδης*
42. *Communication Solutions*