ΤΕΙ ΚΡΗΤΗΣ

ΣΤΕΦ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΙΑΣ

ΜΕΛΕΤΗ ΚΑΙ ΠΡΑΓΜΑΤΩΣΗ ΤΟΠΟΛΟΓΙΑΣ ΔΥΟ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ (LAN) ΣΕ ΑΠΟΜΑΚΡΥΣΜΕΝΑ ΚΤΗΡΙΑ ΚΑΙ ΜΕΤΑΞΥ ΤΟΥΣ ΣΥΝΔΕΣΗ ΜΕΣΩ ΕΙΚΟΝΙΚΟΥ ΙΔΙΩΤΙΚΟΥ ΔΙΚΤΥΟΥ (VPN) ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ ROUTER 1841 ΤΗΣ CISCO.

Σπανός Γεώργιος

Επόπτης Καθηγητής:Εμμανουήλ Δρακάκης

1.Πρόλογος

Η κεντρική ιδέα της πτυχιακής εργασίας έχει ως εξής:Μια εταιρεία ονόματι ΗΛΕΚ Α.Ε η οποία προμηθεύει με ηλεκτρολογικό υλικό ηλεκτρολογικά καταστήματα αγόρασε δύο κτίρια, ένα στην Αθήνα (κυρίως κτίριο) και ένα στο Ηράκλειο (παράρτημα) και στα οποια θέλει να εγκατασταθεί.Μου αναθέτει να μελετήσω και να πραγματώσω το τοπικό δίκτυο του κάθε κτιρίου και να τα συνδέσω μεταξύ τους μέσω ενός εικονικού ιδιωτικού δικτύου (VPN) πραγματοποιώντας ταυτόχρονα και την παραμετροποίηση των δρομολογητών της CISCO που θα χρησιμοποιήσω.

Η εργασία θα χωριστεί σε τέσσερα σκέλη:

- Στο πρώτο σκέλος θα γίνει αναφορά πάνω στα τοπικά δίκτυα (LAN),στα δίκτυα ευρείας περιοχής (WAN) και στις δικτυακές συσκευές και τοπολογίες οι οποίες χρησιμοποιούνται για την διασύνδεση τους.Επίσης θα γίνει αναφορά πάνω στην δομημένη καλωδίωση και τους τύπους των φυσικών μέσων που θα χρησιμοποιηθούν για την σύνδεση των δικτυακών συσκευών μεταξύ τους και με το δίκτυο.
- Στο δεύτερο σκέλος θα γίνει θεωρητική αναφορά πάνω στον τρόπο λειτουργίας της τεχνολογίας Virtual Private Network (VPN) ή Εικονικού Ιδιωτικού Δικτύου το οποίο θα εφαρμοστεί για την ασφαλή επικοινωνία μεταξύ των κεντρικών γραφείων και του υποκαταστήματος.Η τεχνολογία VPN την σημερινή εποχή έχει αποκτήσει εκτετεμένα χαρακτηριστικά.Ένας από του λόγους της ευρείας χρήσης της είναι το χαμηλό κόστος σε σύγκριση με τις μισθωμένες δικτυακές γραμμές που κοστίζουν ακριβά.
- Στο τρίτο σκέλος θα γίνει η οικονομικοτεχνική μελέτη και η πραγμάτωση των τοπικών δικτύων των κεντρικών γραφείων και του υποκαταστήματος, με λογικά και φυσικά σχέδια και αναλυτικές παρουσιάσεις των δομών τους.
- Στο τέταρτο σκέλος (παράρτημα) θα παρουσιάσω την παραμετροποίηση των δρομολογητών και του τείχου προστασίας βασιζόμενος στο λογισμικό των συσκευών Cisco με τις οποίες θα εξοπλίσω τα τοπικά δίκτυα και θα τα συνδέσω μεταξύ τους.Η παραμετροποίηση είναι σημαντική για την ολοκλήρωση της μελέτης και την διασφάλιση της λειτουργίας των τοπικών δικτύων καθώς και της επικοινωνίας μεταξύ τους μέσω του δικτύου ευρείας περιοχής.

Θεωρώ ότι πρόκειται για μια ενδιαφέρουσα εφαρμογή στα δίκτυα που βρίσκει ανταπόκριση στις απαιτήσεις της σημερινής εποχής αφού πολλές εταιρείες διαθέτουν παραρτήματα σε διαφορετικές γεωγραφικά περιοχές και επιθυμούν την ασφαλή επικοινωνία μεταξύ τους.Καθώς μια επιχείρηση μεγαλώνει ενδέχεται να επεκταθεί σε μαγαζιά ή γραφεία σε ολόκληρη την χώρα είτε ακόμα και στο εξωτερικό.Για να διατηρήσουμε την λειτουργικότητα της επιχείρησης θα πρέπει οι εργαζόμενοι σε αυτές τις τοποθεσίες να έχουν ένα γρήγορο,αξιόπιστο και ασφαλή τρόπο προκειμένου να μοιράζονται πληροφορίες κατά μήκος των δικτύων υπολογιστών.Επί προσθέτως οι εργαζόμενοι που ταξιδεύουν, όπως οι πωλητές, χρειάζονται μια εξίσου ασφαλή και

αξιόπιστη μέθοδο μέσω της οποίας θα συνδεθούν στο δίκτυο της επιχείρησης απο απομακρυσμένες τοποθεσίες. Επίσης το φάσμα της εργασίας περιλαμβάνει εξ' ορισμού και τις υποπεριπτώσεις:

(i) Μια εταιρεία επιθυμεί να μεταγκατασταθεί σε κάποιο άλλο κτήριο για λειτουργικούς λόγους οπότε και η μελέτη και πραγμάτωση ενός τοπικού δικτύου είναι παραπάνω από απαραίτητη,

(ii) Μια εταιρεία που έχει μόλις ιδρυθεί και επιθυμεί να εγκατασταθεί σε κάποιο συγκεκριμένο κτίριο.

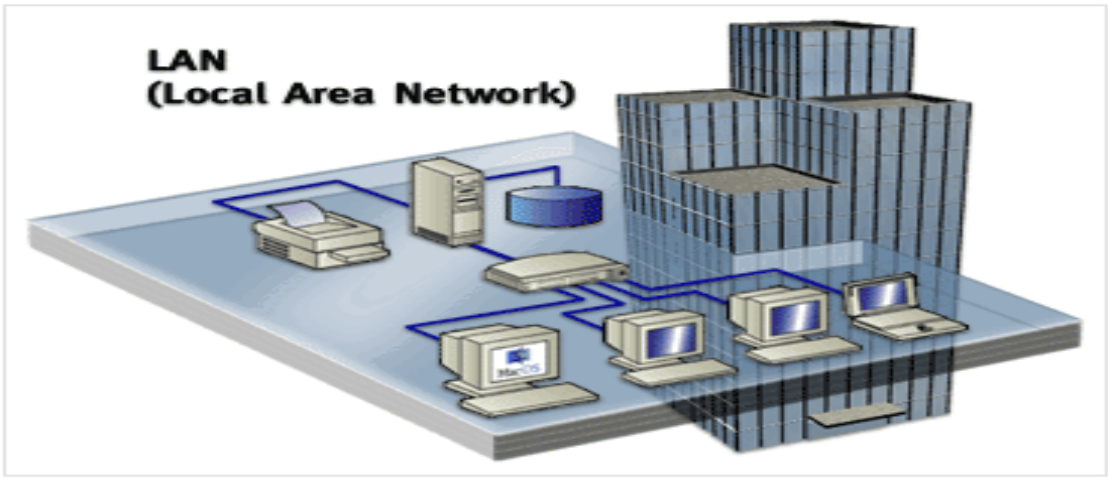
2.Δίκτυα Υπολογιστών

Ένα δίκτυο υπολογιστών είναι μια συλλογή υπολογιστών και άλλων συσκευών οι οποίες είναι συνδεδεμένες μεταξύ τους με τέτοιον τρόπο ώστε να εξασφαλίζεται η επικοινωνία μεταξύ τους.Υπάρχουν πολλοί και διαφορετικοί τύποι δικτύων υπολογιστών οι οποίοι κυμαίνονται σε μέγεθος από τα Personal Area Networks (PANs) ή Δίκτυα Προσωπικής Περιοχής τα οποία και χρησιμοποιούνται για να συνδέσουν τους υπολογιστικούς πόρους ενός άτομου μέχρι τα μεγάλου μεγέθους και πολύπλοκα διαδίκτυα (δίκτυα από διασυνδεμένα δίκτυα) τα οποία συνδέουν ολόκληρο τον κόσμο όπως είναι τα MAN (Metropolitan Area Networks) ή Μητροπολιτικά Δίκτυα Περιοχής.Τα δίκτυα διευκολύνουν πολλές μορφές ηλεκτρονικών επικοινωνιών,επιτρέπουν σε μια μεγάλη και κατανενημένη κοινότητα χρηστών να έχουν πρόσβαση στην κοινόχρηστη πληροφορία και παρέχουν πρόσβαση σε ένα ακόμα μεγαλύτερο εύρος από υπηρεσίες.Η εκθετική αναπτυξη της απαίτησης για δικτυακά προϊόντα και υπηρεσίες σημαίνει ότι η δικτυακή τεχνολογία θα συνεχίσει να εξελίσσεται με ταχύτατους ρυθμούς.

Εικόνα 1: ***Networks***

2.1.Local Area Network (LAN) ή Δίκτυα Τοπικής Περιοχής

Ένα τοπικό δίκτυο Local Area Network (LAN) καλύπτει μια μικρή γεωγραφικά περιοχή (συνήθως ένα κτίριο) και σύνηθως ανήκει ολοκληρωτικά και διατηρείται από ένα οργανισμό.Τα τοπικά δίκτυα χρησιμοποιούνται εκτεταμένα για την σύνδεση προσωπικών υπολογιστών και σταθμών εργασίας που βρίσκονται τοποθετημένοι σε σπίτια,σε γραφεία εταιρειών και σε εργοστασία.Με τον τρόπο αυτό έχουν την ικανότητα να μοιραστούν τους κοινόχρηστους πόρους και να ανταλλάξουν πληροφορίες.Ξεχωρίζουν από τα άλλα είδη δικτύων από το μέγεθος τους,την τεχνολογία μετάδοσης και την τοπολογία τους.Εξαιτίας του σχετικά μικρού μεγεθους τους, η διαχείριση του δικτύου είναι σχετικά εύκολη αφού τα LANs διέπονται από υψηλούς ρυθμούς μετάδοσης δεδομένων,μικρές καθυστερήσεις και μικρό ρυθμό σφαλμάτων.



Εικόνα 2: ***LAN***

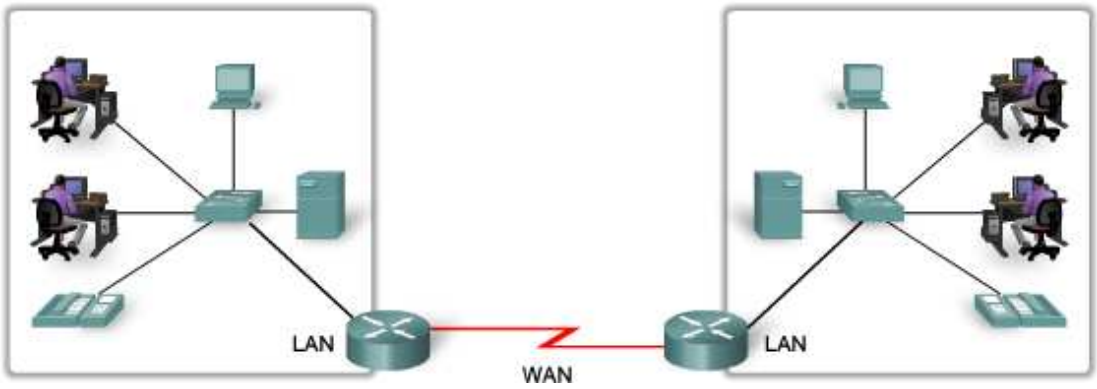
2.2.Wide Area Networks ή Δίκτυα Ευρείας Περιοχής

Όταν μια εταιρεία ή ένας οργανισμός διαθέτει υποκαταστήματα τα οποία τα χωρίζουν γεωγραφικά μεγάλες αποστάσεις είναι απαραίτητο να χρησιμοποιήσουν έναν Telecommunication Service Provider (TSP) δηλαδή ένα οργανισμο παροχής τηλεπικοινωνιών όπως είναι ο ΟΤΕ προκειμένου να διασυνδέσει τα τοπικά δίκτυα τα οποία βρίσκονται σε διαφορετικές περιοχές..Παραδοσιακά οι οργανισμοί παροχής μετέφεραν τις επικοινωνιές της φωνής και των δεδομένων πάνω από διαφορετικά δίκτυα.Πλέον όλο και περισσότερο αυτοί οι πάροχοι τείνουν να προσφέρουν συγκλίνουσες δικτυακές υπηρεσίες στους συνδρομητές τους.

Ανεξάρτητοι οργανισμοί συνήθως μισθώνουν συνδέσεις από το δίκτυο του οργανισμού παροχής τηλεπικοινωνιών.Αυτά τα δίκτυα που συνδέουν τοπικά δίκτυα τα οποία βρίσκονται γεωγραφικά σε διαφορετικές τοποθεσίες ονομάζονται Wide Area Networks (WANs) ή Δικτυα Ευρείας Περιοχής.Αν και ο κάθε οργανισμός διατηρεί τον διαχειριστικό έλεγχο των τοπικών δικτύων και στα δύο άκρα των συνδέσεων, ο έλεγχος μέσα στο δίκτυο του οργανισμού παροχής τηλεπικοινωνιών ελέγχεται από τον οργανισμό.

Τα δίκτυα ευρείας περιοχής χρησιμοποιούν συγκεκριμένου σχεδιασμού δικτυακές συσκευές προκειμένου να πραγματοποιήσουν τις διασυνδέσεις μεταξύ των τοπικών δικτύων.Εξαιτίας της σημαντικότητας αυτων των δικτυακών συσκευών η εγκατάσταση και η διατήρηση τους αποτελούν αποκλειστικό προνόμιο των οργανισμών παροχής.

Τα τοπικά και ευρείας περιοχής δίκτυα είναι πολύ χρήσιμα σε ξεχωριστούς οργανισμούς.Συνδέουν τους χρήστες μέσα στον οργανισμό και επιτρέπουν πολλές μορφές επικοινωνιών συμπεριλαμβανομένων την ανταλλαγή ηλεκτρονικής αλληλογραφίαςς,την εταιρική εκπαίδευση και την πρόσβαση σε κοινόχρηστους πόρους.



Εικόνα 3: ***WAN***

2.3.Δικτυακές Συσκευές

Οι δικτυακές συσκευές είναι μονάδες που χρησιμοποιούνται για να συνδέσουν μεταξύ τους υπολογιστές ή άλλες ηλεκτρονικές συσκευές έτσι ώστε να μοιράζονται φακέλους ή κοινόχρηστους πόρους όπως οι εκτυπωτές και τα μηχανήματα φαξ.Οι συσκευές οι οποίες χρησιμοποιούνται για να διαμορφώσουν ένα τοπικό δίκτυο είναι οι πιο συνηθισμένοι τύποι δικτυακών συσκευών.Ένα τοπικό δίκτυο απαιτεί ένα κόμβο (hub) ένα δρομολογητή (router),καλώδια ή ασύρματη τεχνολογία,δικτυακές κάρτες και ένα μόντεμ αν απαιτείται η πρόσβαση στο διαδίκτυο.

Εικόνα 4: ***Δρομολογητής***

Σ’ ένα δίκτυο ένας υπολογιστής χαρακτηρίζεται σαν διακομιστής (server) και οι υπόλοιποι σαν πελάτες (clients).Ο διακομιστής συνδέεται σε ένα εξωτερικό κόμβο στον οποίο συνδέονται και οι πελάτες.Απο την στιγμή που οι υπολογιστές έχουν πρόσβαση σε μια κοινή ηλεκτρονική πόρτα, δηλαδή τον κόμβο, μπορούν να τον χρησιμοποιήσουν για να περάσουν σήματα προς τα εμπρός και προς τα πίσω.Προκειμένου να κατευθύνουμε αυτά τα σήματα ο κόμβος περιέχει μια συσκευή η οποία είναι γνωστή και ως δρομολογητής.Ο δρομολογητής μοιάζει με ένα ηλεκτρονικό τροχονόμο ο οποίος διαχειρίζεται την κυκλοφορία των δεδομένων μεταξύ των υπολογιστών.

Πως όμως ο δρομολογητής μπορεί να ξεχωρίσει ένα υπολογιστή από κάποιον άλλο;Η απάντηση στο ερώτημα μας είναι πως ο κάθε υπολογιστής μέσα στο δίκτυο θα πρέπει να έχει εγκατεστημένη μια δικτυακή κάρτα.Αυτές οι δικτυακές κάρτες περιέχουν μια μοναδική διεύθυνση (MAC).Σε ένα καλωδιωμένο δίκτυο μια ειδική καλωδίωση η οποία ονομάζεται Ethernet συνδέει την δικτυακή κάρτα στον κόμβο.Σ’ ένα ασύρματο

δίκτυο οι δικτυακές κάρτες και ο δρομολογητής/κόμβος επικοινωνούν μέσω ασύρματων συχνοτήτων.

Εικόνα 5: ***Δικτυακή κάρτα***

Οι δικτυακές κάρτες ταυτοποιούν την παρουσία τους στο δίκτυο με την αποστολή αιτήσεων στον δρομολογητή.Ο δρομολογητής διαβάζει τις διεύθυνσεις «από» και «προς» και ανάλογα δρομολογεί την κυκλοφορία.Υπάρχουν τύποι δικτύων όπου όλες οι αιτήσεις οι οποίες πραγματοποιούνται στο τοπικό δίκτυο μεταδίδονται από τον δρομολογητή προς όλες τις συσκευές (broadcast) που είναι τοποθετημένες στο δίκτυο αλλά τελικά μόνο η συσκευή με την διεύθυνση που ταιριάζει αποκρίνεται.Παρόλαυτα κάτι τέτοιο δεν είναι ασφαλές γιατί άλλες συσκευές μπορούν να παγιδεύσουν κυκλοφορία η οποία δεν απευθύνεται σ' αυτές.

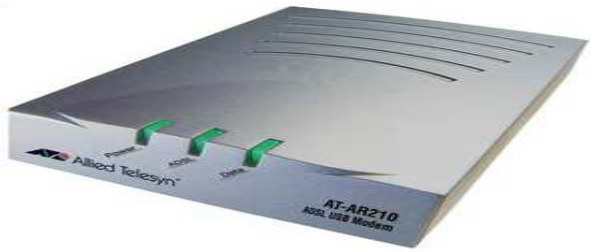
Εικόνα 6: ***Ασύρματη δικτυακή κάρτα***

Η πρόσβαση στο διαδίκτυο είναι προαιρετική σε ένα τοπικό δίκτυο αλλά σε περίπτωση που περιλαμβάνεται, τότε ένας λογαριασμός σε μια ενεργοποιημένη γραμμή του διαδικτύου μπορεί να είναι κοινόχρηστος απ' όλους τους υπολογιστές του δικτύου.Όταν η πρόσβαση στο διαδίκτυο είναι διαθέσιμη, ο δρομολογητής όχι μόνο κατευθύνει την κυκλοφορία στο τοπικό δίκτυο αλλά επίσης διαχειρίζεται τις αιτήσεις οι οποίες απευθύνονται στο διαδίκτυο και τις επακόλουθες αποκρίσεις τους.Ο δρομολογητής λειτουργεί σαν έξοδος προς το διαδίκτυο και επίσης εξυπηρετεί σαν τοίχος προστασίας (firewall) για να διατηρήσει την αυθαίρετη κυκλοφορία μακριά από το τοπικό δίκτυο.

Η σύνδεση στο διαδίκτυο μπορεί να γίνει με την προσάρτηση ενός δρομολογητή/κόμβου σ' ένα υψηλής ταχύτητας μοντεμ ή μέσω ενός υψηλής ταχύτητας μόντεμ το οποίο έχει ενσωματωμένο ένα δρομολογητή/κόμβο.Το υψηλής ταχύτητας μόντεμ θα πρέπει να είναι συμβατό με την ενεργοποιημένη γραμμή προς το διαδίκτυο.

Όταν εγκαθιστούμε ένα τοπικό δίκτυο όλες οι δικτυακές συσκευές θα πρέπει να είναι συμβατές.Αν διαμορφώνουμε ένα καλωδιωμένο τοπικό δίκτυο χρησιμοποιώντας την Ethernet καλωδίωση οι δικτυακές κάρτες θα πρέπει να είναι σχεδιασμένες με μια

Ethernet πόρτα.Αν διαμορφώνουμε ένα ασύρματο δίκτυο όλες οι δικτυακές συσκευές θα πρέπει να είναι σχεδιασμένες όχι μόνο για ασύρματη χρήση αλλά και για να «μιλάνε» την ίδια ασύρματη «γλώσσα», δηλαδή να τρέχουν το ίδιο πρωτόκολο.



Εικόνα 7: ***Μόντεμ***

2.4.Κριτήρια για την επιλογή δικτυακών συσκευών

Προκειμένου το τοπικό δίκτυο να συναντήσει τις απαιτήσεις του χρήστη θα πρέπει να σχεδιαστεί κατάλληλα.Ο σχεδιασμός εξασφαλίζει οτι όλες οι απαιτήσεις, όπως είναι οι παράγοντες σχετικά με το κόστος και οι δυνατότητες ανάπτυξης, θα ληφθούν υπόψην μας.Όταν επιλέγουμε μια συσκευή για ένα συγκεκριμένο τοπικό δίκτυο υπάρχουν μια σειρά από παράγοντες οι οποίοι θα πρέπει να ληφθούν υπόψην μας.Αυτοί οι παράγοντες είναι οι ακόλουθοι:

- Κόστος.
- Ταχύτητα και τύποι πορτών και interfaces.
- Ικανότητα επέκτασης.
- Ικανότητα διαχείρησης.
- Επιπρόσθετα χαρακτηριστικά και υπηρεσίες.

Εικόνα 8: ***Παράγοντες που λαμβάνουμε υπόψιν μας κατά την επιλογή των δικτυακών συσκευών.***

2.5.Switch ή Μεταγωγέας

Ο μεταγωγέας (switch) είναι μια ηλεκτρονική συσκευή η οποία χρησιμοποιείται για την δικτύωση και η οποία συνδέει δύο ή περισσότερα δικτυακά τμήματα (segments).Αυτή η μέθοδος σύνδεσης των δικτύων μαζί ονομάζεται γεφύρωση (bridging).Επειδή ο μεταγωγέας γεγυρώνει δύο δικτυακά τμήματα λέμε ότι λειτουργεί σαν μια συσκευή γεφύρωσης.Ένας μεταγωγέας μπορεί να συνδέσει περισσότερα από δύο δικτυακά τμήματα ενώ ταυτόχρονα προωθεί την κυκλοφορία έξυπνα και η λειτουργία του είναι διαφανής στο δίκτυο.Το γεγονός ότι ο μεταγωγέας έχει πολλές πόρτες όπως επίσης και το ότι μαθαίνει δυναμικά τις Mac διευθύνσεις το κάνει να διαφέρει από μια συνηθισμένη συσκευή γεφύρωσης.

Ο μεταγωγέας μειώνει σημαντικά τις μεταδόσεις των Mac διευθύνσεων καθώς και τις ARP/RARP αιτήσεις.Ο μεταγωγέας λαμβάνει δεδομένα από μια πόρτα και τα προωθεί στην σωστή πόρτα όπου η Mac διεύθυνση προορισμού είναι τοποθετημένη.Όταν ένας μεταγωγέας γνωρίζει την πόρτα στην οποία μια Mac διεύθυνση είναι τοποθετημένη προωθεί το πακέτο προς το συγκεκριμένο interface.Αν η Mac διεύθυνση δεν είναι γνωστή τότε το πακέτο πλημμυρίζει όλες τις πόρτες εκτός από εκείνη στην οποία ελήφθει το πακέτο.Ο μεταγωγέας «ακούει» και διατηρεί στην μνήμη του τις Mac διευθύνσεις όλων των σταθμών εργασίας οι οποίοι συνδέονται σ' αυτό, σ' ένα ειδικό πίνακα προώθησης.Αυτός ο πίνακας επιτρέπει στον μεταγωγέα να αναζητήσει τον συσχετισμό ανάμεσα στην Mac διεύθυνση και σε μια πόρτα και στη συνέχεια να προωθήσει το πακέτο βασιζόμενο στην Mac address.Στις περιπτώσεις που η Mac διεύθυνση δεν βρίσκεται στον ειδικό πίνακα προώθησης θα πρέπει να γίνει μια αίτηση για αυτή την διεύθυνση σ' όλες τις πόρτες του μεταγωγέα το οποίο συσχετίζεται με το τοπικό δίκτυο.

Εικόνα 9: ***Switches***

2.5.1.Παράγοντες που οφείλουμε να λάβουμε υπόψην μας κατά την επιλογή ενός μεταγωγέα.

Αν και υπάρχουν πολλοί παράγοντες τους οποίους θα πρέπει να λάβουμε υπόψην μας κατά την επιλογή ενός μεταγωγέα εμείς θα επικεντρωθούμε σε δύο:

- Κόστος.
- Χαρακτηριστικά των interfaces.

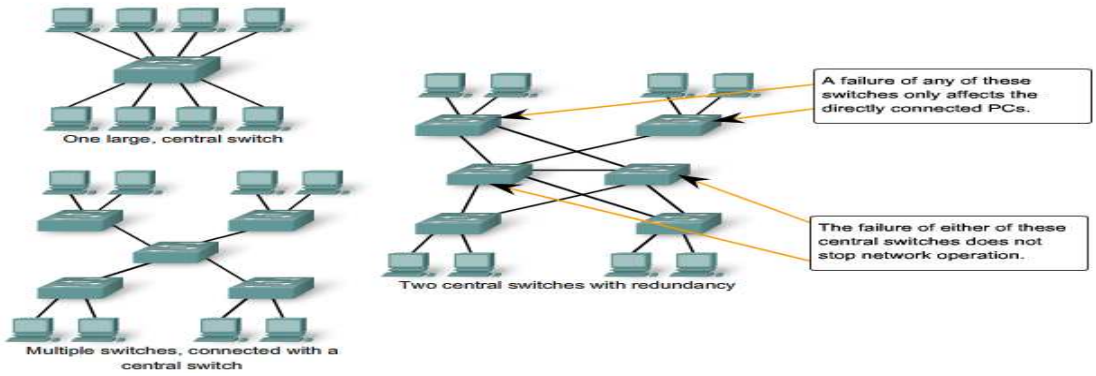
2.5.2.Κόστος

Το κόστος ενός μεταγωγέα καθορίζεται από την χωρητικότητα και τα χαρακτηριστικά του.Η χωρητικότητα του μεταγωγέα περιλαμβάνει τον αριθμό και τους τύπους των πορτών οι οποίες είναι διαθέσιμες καθώς και την ταχύτητα τους.Άλλοι παράγοντες οι οποίοι επηρεάζουν το κόστος είναι οι δικτυακές διαχειριστικές ικανότητες του μεταγωγέα,οι ενσωματωμένες τεχνολογίες ασφάλειας και οι προαιρετικές προηγμένες τεχνολογίες μεταγωγής.

Χρησιμοποιώντας ένα απλό «κόστος ανα πόρτα» υπολογισμό μπορεί να δημιουργηθεί μια καταρχήν αίσθηση ότι η καλύτερη επιλογή είναι να αναπτύξουμε ένα μεγάλο μεταγωγέα σ' ένα κεντρικό σημείο.Παρόλαυτα η προφανής εξοικονόμηση του κόστους από την παραπάνω επιλογή μπορεί να επιβαρυνθεί σημαντικά από το κόστος των μεγαλύτερων μήκους καλωδίων τα οποία θα απαιτηθούν για την σύνδεση της κάθε συσκευής του τοπικού δικτύου στον μεταγωγέα.Αυτή η επιλογή θα πρέπει συγκριθεί με το κόστος της ανάπτυξης ενός τοπικού δικτύου μέσα από ένα αριθμό μικρότερων μεταγωγέων τα οποία συνδέονται μ' ένα κεντρικό μεταγωγέα.

Ένας άλλος παράγοντας τον οποίο θα πρέπει να λάβουμε υπόψην μας είναι το κόστος το οποίο θα πρέπει να επενδύσουμε στον πλεονασμό (redundancy).Η λειτουργία ολόκληρου του φυσικού δικτύου επηρεάζεται σε περίπτωση που προκύψει πρόβλημα σε ένα δίκτυο που διαθέτει μόνο ένα κεντρικό μεταγωγέα.

Ο πλεονασμός μπορεί να παρασχεθεί με περισσότερους από ένα τρόπους.Μπορούμε να διαθέσουμε ένα δευτερεύον κεντρικό μεταγωγέα ο οποιός θα λειτουργεί ταυτόχρονα με τον κεντρικό μεταγωγέα.Μπορούμε επίσης να παράσχουμε επιπρόσθετη καλωδίωση προκειμένου να δημιουργήσουμε πολλές διασυνδέσες μεταξύ των μεταγωγέων.Ο σκοπός των πλεονασματικών συστημάτων είναι να επιτρέψει την λειτουργία του φυσικού δίκτυο του ακόμα και αν μια συσκευή αποτύχει.



Εικόνα 10: ***Παράγοντες που καθορίζουν την επιλογή των μεταγωγέων***

2.5.3.Ταχύτητες και τύποι πορτών/interfaces

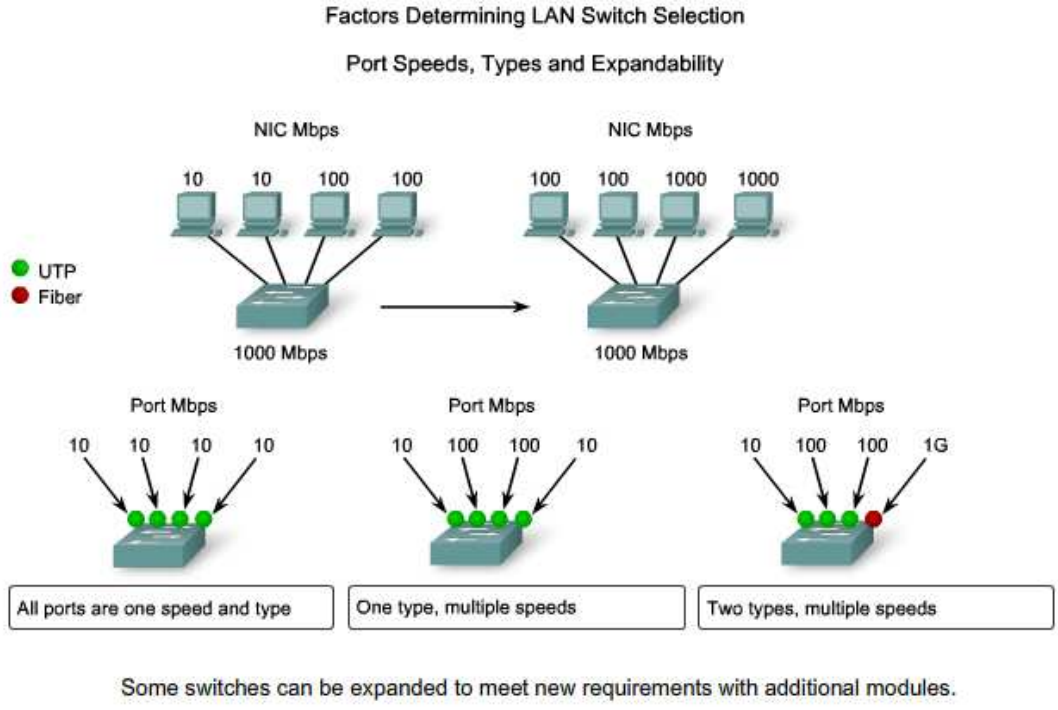
Η ανάγκη για ταχύτητα ήταν πάντα παρούσα σ' ένα περιβάλλον τοπικού δικτύου.Πλέον υπάρχουν διαθέσιμοι καινούργιοι υπολογιστές με εσωτερικές κάρτες

δικτύου (NICs) στα 10/100/1000 Mbps.Η επιλογή επιπέδου 2 συσκευών οι οποίες μπορούν να εξυπηρετήσουν αυξημένες ταχύτητες επιτρέπουν στο δίκτυο να αναπτυχθεί χωρίς την αντικατάσταση των κεντρικών συσκευών.

Όταν επιλέγουμε ένα μεταγωγέα,η επιλογή του αριθμού και του τύπου των πορτών αποτελεί μια κρίσιμη απόφαση.Επομένως κατά την αγορά ενός μεταγωγέα θα πρέπει να κάνουμε τις εξής ερωτήσεις:

- Διαθέτει αρκετές πόρτες για τις ανάγκες της σημερινής εποχής;
- Διαθέτει ένα μείγμα από UTP ταχύτητες;
- Διαθέτει τόσο UTP όσο και Fiber πόρτες;

Αναρωτηθείτε προσεκτικά πόσες UTP πόρτες και πόσες fiber πόρτες θα χρειαστούν.Παρόμοια αναρωτηθείτε πόσες πόρτες θα χρειαστεί να διαθέτουν 1 Gbps bandwidth και πόσες πόρτες θα χρειαστεί να έχουν 10/100 Mbps bandwidth.Επίσης θα πρέπει να αναρωτειθείτε πόσο σύντομα νέες πόρτες θα χρειαστούν.



Εικόνα 11: ***Ταχύτητες των πορτών,τύποι των switches και επεκτασιμότητα***

2.6.Routers ή Δρομολογητές

Στο επίκεντρο των δικτύων βρίσκονται οι δρομολογητές.Ένας απλός ορισμός είναι ότι οι δρομολογητές χρησιμοποιούνται για την σύνδεση ενός δικτύου με ένα άλλο.Γι' αυτό το λόγο ο δρομολογητής είναι υπεύθυνος για την παράδοση πακέτων κατά μήκος των διαφορετικών δικτύων.Ο προορισμός ενός IP πακέτου μπορεί να είναι ένας web διακομιστής σε μια άλλη χώρα ή ένας διακομιστής ηλεκτρονικού ταχυδρομείου σ' ένα τοπικό δίκτυο.Αποτελεί ευθύνη των δρομολογητών να παραδώσουν αυτά τα πακέτα μέσα σ'ένα εύλογο χρονικό διάστημα.Η αποτελεσματικότητα των διαδικτυακών επικοινωνιών εξαρτάται σ' ένα μεγάλο βαθμό από την ικανότητα των δρομολογητών να προωθήσουν τα πακέτα με τον πιο αποτελεσματικό τρόπο.

Οι δρομολογητές πλέον τοποθετούνται σε δορυφόρους στο διάστημα.Αυτοί οι δρομολογητές έχουν την ικανότητα να δρομολογήσουν την IP κυκλοφορία μεταξύ των δορυφόρων στο διάστημα με τον ίδιο τρόπο που τα πακέτα μετακινούνται στην Γή.

Μαζί με την προώθηση των πακέτων οι δρομολογητές παρέχουν και άλλες υπηρεσίες.Προκειμένου να συναντήσουν τις απαιτήσεις της σημερινης εποχής χρησιμοποιούνται επίσης:

- Για να διασφαλίσουν την διαθεσιμότητα του δικτύου για 24 ώρες την ημέρα και 7 ημέρες την εβδομάδα.Για να βοηθήσουν στην προσβασιμότητα των δικτύων οι δρομολογητές χρησιμοποιούν εναλλακτικές διαδρομές σε περίπτωση που η πρωτεύον διαδρομή αποτύχει.
- Παρέχουν ενσωματωμένες υπηρεσίες δεδομένων,video και φωνής πάνω από ενσύρματα και ασύρματα δίκτυα.Οι δρομολογητές χρησιμοποιούν την Quality of Service (Qos) ή Την Υπηρεσία Ποιότητας η οποία θέτει σε προτεραιότητα συγκεκριμένα IP πακέτα προκειμένου να εξασφαλίσει ότι η πραγματικού χρόνου κυκλοφορία (όπως είναι η φωνή ,το video και κρίσιμα δεδομένα) δεν θα πέσει και δεν θα καθυστερήσει.
- Μετριάζει την επίδραση των ιών και άλλων επιθέσεων πάνω στο δίκτυο επιτρέποντας ή απαγορεύοντας την προώθηση ορισμένων πακέτων.

Όλες αυτές οι υπηρεσίες χτίζονται γύρω από τον δρομολογητή ο οποίος έχει σαν πρωταρχική ευθύνη την προώθηση των πακέτων από το ένα δίκτυο στο άλλο.

Όταν επιλέγουμε ένα δρομολογητή θα πρέπει να ταιριάξουμε τα χαρακτηριστικά του με τον σκοπό για τον οποίο επιλέχτηκε.Παρόμοια με την επιλογή του μεταγωγέα έτσι και στην επιλογή του δρομολογητή, το κόστος, οι τύποι των interfaces και οι ταχύτητες θα πρέπει να ληφθούν υπόψιν μας.Επιπλέον παράγοντες που θα πρέπει να λάβουμε υπόψιν μας κατά την επιλογή του είναι οι ακόλουθοι:

- Δυνατότητα επέκτασης.
- Τα φυσικά μέσα.
- Τα χαρακτηριστικά των λειτουργικών συστημάτων.

Εικόνα 12: ***Routers ή Δρομολογητές***

2.6.1.Δυνατότητα Επέκτασης

Οι δικτυακές συσκευές όπως οι μεταγωγείς και οι δρομολογητές παράγονται τόσο με προκαθορισμένες (fixed) όσο και με επιπρόσθετες (modular) φυσικές παραμετροποιήσεις.Οι προκαθορισμένες παραμετροποιήσεις έχουν ένα συγκεκριμένο αριθμό και τύπο πορτών και interfaces.Οι συσκευές με επιπρόσθετες υποδοχές επέκτασης μας παρέχουν την ευελιξία στο να προσθέσουμε καινούργια εξαρτήματα καθώς οι απαιτήσεις του δικτύου μας αναπτύσσονται.Οι περισσότερες συσκευές αυτού του τύπου είναι διαθέσιμες με ένα βασικό αριθμό προκαθορισμένων πορτών όπως επίσης και με μια υποδοχή επέκτασης.Απο την στιγμή που οι δρομολογητές μπορούν να χρησιμοποιηθούν για την σύνδεση διαφορετικών τύπων και αριθμών δικτύων θα πρέπει να είμαστε προσεκτικοί για την επιλογή των κατάλληλων εξαρτημάτων και interfaces για συσγκεκριμένα φυσικά μέσα.

2.6.2.Χαρακτηριστικά λειτουργικών συστημάτων

Ανάλογα με την έκδοση του λειτουργικού συστήματος ο δρομολογητής μπορεί να υποστηρίζει συγκεκριμένα χαρακτηριστικά και υπηρεσίες όπως:

- Ασφάλεια.
- Ποιότητα Υπηρεσίας (QoS).
- Voice over IP (VoIP).
- Πολλά πρωτόκολα δρομολόγησης επιπέδου 3.
- Ειδικές υπηρεσίες όπως είναι τα Network Address Translation (NAT) ή Μετάφραση Δικτυακών Διευθύνσεων και Dynamic Host Configuration Protocol (DHCP) ή Δυναμική Παραμετροποιήση Πρωτοκόλλου Χρήστη.

Κατά την επιλογή των συσκευών ο προυπολογισμός είναι ένα σημαντικό κριτήριο.Οι δρομολογητές μπορεί να είναι ακριβοί,κάτι το οποίο εξαρτάται από τα interfaces και τα απαιτούμενα χαρακτηριστικά.Επιπρόσθετες υποδοχές επέκτασης όπως οι οπτικές ίνες μπορεί να αυξήσουν το κόστος.Τα φυσικά μέσα τα οποία χρησιμοποιούνται για να συνδέσουν τον δρομολογητή θα πρέπει να υποστηριζονται χωρίς να προκύψει η ανάγκη αγοράς επιπρόσθετων εξαρτημάτων.

2.7. Servers ή Διακομιστές

Ένας διακομιστής είναι ένα δικτυακός υπολογιστής ο οποίος παρέχει πρόσβαση σε διάφορους δικτυακους πόρους.Τα μοντέρνα δίκτυα κάθε μεγέθους είναι είτε βασισμένα σε διακομιστή (server-based) είτε σε διακομιστή-πελάτη (server-client).

Οι διακομιστές φακέλων (file servers) είναι ηλεκτρονικοί υπολογιστές οι οποίοι διαθέτουν δίσκους με μεγάλη χωρητικότητα αποθήκευσης,επεξεργαστές υψηλής ταχύτητας,μέγαλες ποσότητες από μνήμη RAM και παρέχουν πρόσβαση στους κοινόχρηστους χώρους αποθήκευσης στους πιστοποιημένους χρήστες ενός δικτύου.

Οι Web διακομιστές (web servers) είναι υπολογιστές οι οποίοι παραδίδουν τις Web σελίδες.Κάθε Web διακομιστής έχει μια IP διεύθυνση και πιθανότατα ένα πεδίο ονόματος(domain name).Για παράδειγμα αν εισάγουμε το URL http://www.teicrete.gr/tei/en/index.php στο πρόγραμμα περιήγησης διαδικτύου μας (browser) αυτό θα στείλει ένα αίτημα στον Web διακομιστή, του οποίου το πεδίο ονόματος είναι teicrete.gr.Ο διακομιστής στη συνέχεια ανακτά την σελίδα η οποία ονομάζεται Index.html και την στέλνει στο πρόγραμμα περιήγησης διαδικτύου μας.

Ένας διακομιστής ηλεκτρονικού ταχυδρομείου (mail server) συνήθως αποτελείται από μια περιοχή αποθήκευσης όπου αποθηκεύεται το ηλεκτρονικό ταχυδρομείο το οποίο προορίζεται για τους τοπικούς χρήστες και διέπεται από μια σειρά κανόνων οι οποίοι καθορίζουν τον τρόπο που ο διακομιστής θα πρέπει να αντιδράσει σ' ένα συγκεκριμένο μήνυμα και στον προορισμό για τον οποίο αυτό απευθύνεται.Επίσης διαθέτει μια βάση δεδομένων με τους λογαριασμούς των χρηστών που αναγνωρίζει και τους οποίους διαχειρίζεται τοπικά.Ο διακομιστής ηλεκτρονικού ταχυδρομείου παρέχει επικοινωνιακά συστατικά τα οποία αναλαμβάνουν την μεταφορά των μηνυμάτων από και προς άλλους διακομιστές ηλεκτρονικού ταχυδρομείου και προς άλλους πελάτες ηλεκτρονικού ταχυδρομείου.

Ένας διακομιστής εκτυπωτή επιτρέπει στους υπολογιστές σ' ένα δίκτυο να έχουν πρόσβαση σ' ένα δικτυακό εκτυπωτή.Επομενως οι διακομιστές εκτυπωτών είναι χρήσιμοι ακόμα και σε μικρά δίκτυα από την στιγμή που αποφεύγουμε να μετακινήσουμε τους φακέλους από υπολογιστή σε υπολογιστή πριν τους εκτυπώσουμε.

Εικόνα 13: ***Server***

2.8.Firewall ή Τοίχος Προστασίας

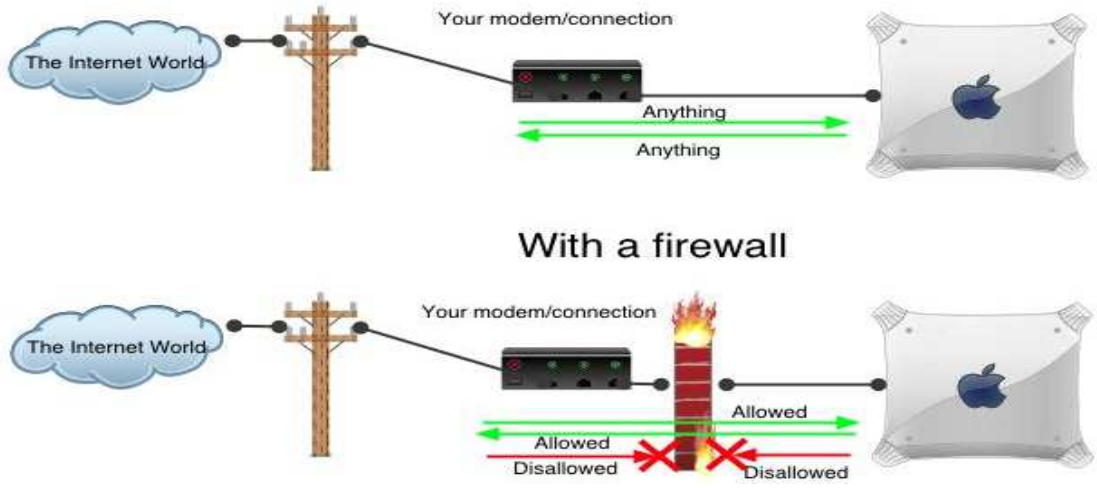
Ο τοίχος προστασίας (firewall) είναι μια συσκευή ασφαλείας.Ο κύριος σκοπός του είναι να ξεχωρίσει μια ασφαλή περιοχή,όπως είναι το δίκτυο μας, από μια μη ασφαλή περιοχή όπως είναι το διαδίκτυο και να ελέγξει την επικοινωνία ανάμεσα στις δύο περιοχές.Ο τοίχος προστασίας μπορεί να πραγματοποιήσει μια ποικιλία από λειτουργίες αλλά πρώτιστα είναι υπεύθυνο για τις εισερχόμενες και τις εξερχόμενες επικοινωνίες.Χωρίζονται σε δύο κατηγορίες:

- **Software firewall ή Λογισμικό τείχος προστασίας**
- **Hardware firewall ή Τεχνικού εξοπλισμού τείχος προστασίας**

2.8.1. Λογισμικό τείχος προστασίας

Το λογισμικό τείχος προστασίας, ο οποίος συχνά ονομάζεται και προσωπικός τοίχος προστασίας (personal firewalls), έχει σχεδιαστεί έτσι ώστε να τρέχει σ' ένα προσωπικό υπολογιστή.Συνήθως χρησιμοποιείται στους υπολογιστές που βρίσκονται σε σπίτια ή σε μικρά γραφεία τα οποία έχουν σύνδεση στο διαδίκτυο.Κύριος σκοπός του είναι η αποτροπή μιας ανεπιθύμητη πρόσβασης του υπολογιστή πάνω από μια δικτυακή σύνδεση.Οι υπολογιστές επικοινωνούν πάνω από από διαφορετικές και αναγνωρίσιμες πόρτες.Ο τείχος προστασίας τείνει να επιτρέπει την πρόσβαση σ' αυτές τις πόρτες χωρίς να ειδοποιεί τον χρήστη.Για παράδειγμα οι υπολογιστές έχουν πρόσβαση στις Web σελίδες πάνω από την πόρτα 80 και χρησιμοποιούν την πόρτα 443 για ασφαλείς Web επικοινωνίες.Ένας υπολογιστής θα περίμενε να δεχτεί δεδομένα πάνω από τις συγκεκριμένες πόρτες.Απο την άλλη το λογισμικό τείχος προστασίας πιθανότατα θα απαγόρευε κάθε πρόσβαση στο διαδίκτυο πάνω από την πόρτα 421, από την οποία δεν περιμένει να δεχτεί κάποια δεδομένα.Επιπρόσθετως η πόρτα 421 έχει χρησιμοποιηθεί στο παρελθόν από συγκεκριμένους Trojans (προγράμματα που εκκινούν επιβλαβείς διαδικασίες χωρίς την συναίνεση του χρήστη).Το λογισμικό τείχος προστασίας μπορούν επίσης να ανιχνεύσει ύποπτες ενέργειες από το διαδίκτυο και να παρεμποδίσει την πρόσβαση στον υπολογιστή μας.

Επίσης ένα λογισμικό τείχος προστασίας επιτρέπει σε συγκεκριμένα προγράμματα στον υπολογιστή του χρήστη να έχουν πρόσβαση στο διαδίκτυο.Τα windows update ,ένα πρόγραμμα antivirus και το Microsoft Word αποτελούν ενδεικτικά προγράμματα τα οποία ο χρήστης θα περιμένει να έχουν νόμιμη πρόσβαση στο διαδίκτυο.Παρόλαυτα ένα πρόγραμμα το οποίο ονομάζεται gator.exe και το οποίο επιχειρεί να αποκτήσει πρόσβαση στο διαδίκτυο, ενώ το πρόγραμμα δεν τρέχει, θα πρέπει να μας ανησυχήσει.



Εικόνα 14: ***Software Firewall***

2.8.2.Τεχνικού Εξοπλισμού Τείχος Προστασίας

Τα τεχνικού εξοπλισμού τείχη προστασίας είναι περισσότερο πολύπλοκα.Διαθέτουν επίσης λογισμικά συστατικά τα οποία όμως τρέχουν πάνω από μια συγκεκριμένη συσκευή όπως είναι η Cisco ASA firewall 5510 ή πάνω από διακομιστές οι οποίοι χρησιμοποιούνται αποκλειστικά ως τείχος προστασίας.Στις συσκευές αυτές κανένα άλλο λογισμικό δεν τρέχει στις συσκευές αυτές ενώ η παραμετροποίηση η οποία διαθέτει έχει διαμορφωθεί κάτω από προσεκτική σκέψη.Τα παραπάνω στοιχεία προσδίδουν στην συσκευή την δυνατότητα να μας παρέχει εξαιρετική ασφάλεια.

Το τεχνικού εξοπλισμού τείχος προστασίας τοποθετείται ανάμεσα σ' ένα ασφαλές δίκτυο,όπως είναι το δίκτυο μιας επιχείρησης και σε μια λιγότερη ασφαλή περιοχή όπως είναι το διαδίκτυο.Εκδοχές των συσκευών τείχου προστάσίας είναι διαθέσιμες και σε οικιακούς χρήστες οι οποίοι επιθυμούν μεγαλύτερη προστασία από πιθανές διαδικτυακές επιθέσεις.Υπάρχουν πολλές προεπιλεγμένες παραμαμετροποιήσεις γι' αυτές τις συσκευές ,μερικές από τις οποίες δεν επιτρέπουν καμμιά εξωτερική επικοινωνία και θα πρέπει να παραμετροποιηθούν από την αρχή χρησιμοποιώντας κανόνες.Οι κανόνες μπορεί να είναι τόσο απλοί όσο το να επιτρέπουν την κυκλοφορία να ρέει μέσα από το τείχος προστασίας και προς τις δύο κατευθύνσεις από την πόρτα 80 ή τόσο πολύπλοκοι όσο το να επιτρέπουμε μόνο στην 443 (SQL Server) κυκλοφορία να ρέει από μια συγκεκριμένη εξωτερική IP διεύθυνση, η οποία βρίσκεται εκτός του δικτύου και μέσω του τείχους προστασίας προς μια συγκεκριμένη IP address, η οποία βρίσκεται εντός του δικτύου μας.

Τα τείχη προστασίας επίσης χρησιμοποιούνται για το Network Address Translation (NAT).Αυτό επιτρέπει σ' ένα δίκτυο να χρησιμοποιεί ιδιωτικές IP διευθύνσεις οι οποίες και δεν δρομολογούνται στο διαδίκτυο.Ο μηχανισμός των ιδιωτικών IP διευθύνσεων επιτρέπουν στους οργανισμούς να περιορίσουν τον αριθμό των δημόσιων δρομολογημένων IP διευθύνσεων που χρησιμοποιούν.Οι δημόσιες IP διευθύνσεις είναι απαραίτητες για τους Web διακομιστές και για τον υπόλοιπο εξωτερικά προσβάσιμο δικτυακό εξοπλισμό.Το NAT επιτρέπει στους διαχειριστές να

χρησιμοποιήσουν μια δημόσια IP address προκειμένουν να έχουν πρόσβαση στο διαδίκτυο όλοι οι χρήστες εντός του δικτύου.Το NAT επίσης επιτρέπει στους χρήστες εντός του δικτύου να επικοινωνήσουν με ένα διακομιστή στο ίδιο δίκτυο χρησιμοποιώντας μια ιδιωτική IP address ενώ οι χρήστες οι οποίοι βρίσκονται εκτός του δικτύου θα πρέπει να συνδεθούν στον ίδιο διακομιστή χρησιμοποιώντας μια εξωτερική IP διεύθυνση.

Παράλληλα με τους κανόνες που θέτουν οι συσκευές του τείχου προστασίας για τις πόρτες και τις IP διευθύνσεις μπορούν να έχουν μια ευρεία ποικιλία λειτουργιών.Για παράδειγμα μπορούν να λειτουργήσουν σαν VPNs, δρομολογητές ή και άλλες μορφές.

Οι συσκευές τείχου προστασίας είναι ζωτικής σημασίας για την δικτυακή διαχείριση.Χωρίς αυτό τον έλεγχο πάνω από τους υπολογιστές και την δικτυακή πρόσβαση τα μεγάλα δίκτυα δεν θα μπορούσαν αποθηκεύσουν ευαίσθητα δεδομένα τα οποία προορίζονται για επιλεκτική ανάκτηση.

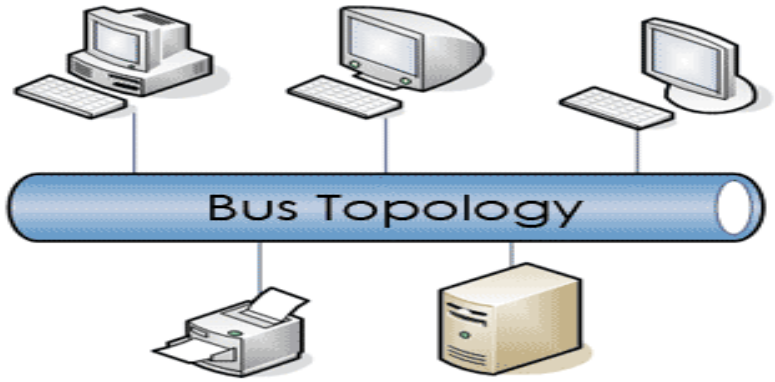
Εικόνα 15: ***Hardware Firewall – Cisco ASA 5510***

3.Δικτυακές Τοπολογίες

Η τοπολογία ενός δικτύου περιγράφει το λογικό σχέδιο του δικτύου ή με άλλα λόγια τον τρόπο με τον οποίο οι δικτυακές συσκευές συνδέονται μεταξύ τους με την βοήθεια των φυσικών μέσων μετάδοσης.Ο συνδιασμός διαφορετικών τοπολογιών ονομάζεται υβριδικός.Οι δικτυακές τοπολογίες τις οποίες συναντάμε στα δίκτυα υπολογιστών είναι οι ακόλουθες:

3.1.Τοπολογία bus

Η παραμετροποιήση αυτού του δικτύου βασίζεται σ' ένα μοναδικό δικτυακό καλώδιο πάνω στο οποίο όλες οι συσκευές είναι προσαρτημένες.Μια συσκευή σ' ένα bus δίκτυο μπορεί να μεταδόσει οποιαδήποτε στιγμή σε οποιαδήποτε συσκευή.Όμως με αυτόν τον τρόπο οι συγκρούσεις είναι αναπόφευκτες και επομένως θα πρέπει να εισαχθεί μια μορφή διαιτησίας.Τα πλαίσια των δεδομένων συνήθως διευθυνσιοδοτούνται σε μια συγκεκριμένη συσκευή προορισμού και χρησιμοποιούν την MAC διεύθυνση της συσκευής αυτής.Αν και τα δεδομένα μεταδίδονται και προς τους δύο κατευθύνσεις κατά μήκος του bus, επομένως παραλαμβάνονται από όλες τις συσκευές του δικτύου, μόνο η συσκευή για την οποία προορίζονται θα μπορέσει να τα επεξεργαστεί. Το καλώδιο θα πρέπει να τερματίζεται σωστά σε κάθε άκρο.Η bus τοπολογία η οποία απεικονίζεται παρακάτω εμφανίζεται πολύ σπάνια στα μοντέρνα LANs.

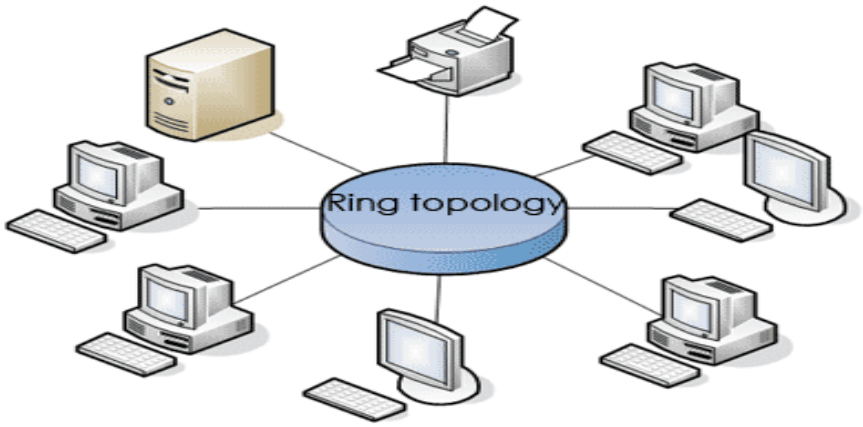


Εικόνα 16: ***Τοπολογία bus***

3.2.Τοπολογία δαχτυλιδιού (ring)

Σε ένα δίκτυο δαχτυλίδι τα πλαίσια των δεδομένων μεταδίδονται από συσκευή σε συσκευή γύρω από ένα κλειστό βρόχο και προς μια κατεύθυνση μόνο.Κάθε συσκευή στον βρόχο επικοινωνεί μόνο με την συσκευή στην οποία μεταδίδει τα πλαίσια.Εν συνεχεία η συσκευή αυτή που περάλαβε τα πλαίσια είναι υπεύθυνη για την μεταβίβαση των ληφθέντων πλαισίων στην επόμενη συσκευή στον βρόχο, συχνά επανενεργοποιώντας το σήμα πριν τη μεταβιβάση.Τα δίκτυα δαχτυλιδιού ελέγχουν την πρόσβαση στα μέσα χρησιμοποιώντας ένα σύστημα γνωστό και σαν token (ενδεικτικό) πέρασμα.Αυτό το πέρασμα χρησιμοποιεί ένα μικρό πλαίσιο δεδομένων, το token, το οποίο και μεταδίδεται γύρω από το δαχτυλίδι και από συσκευή σε συσκευή.Μια συσκευή η οποία θέλει να μεταδόσει κάποια δεδομένα θα πρέπει να

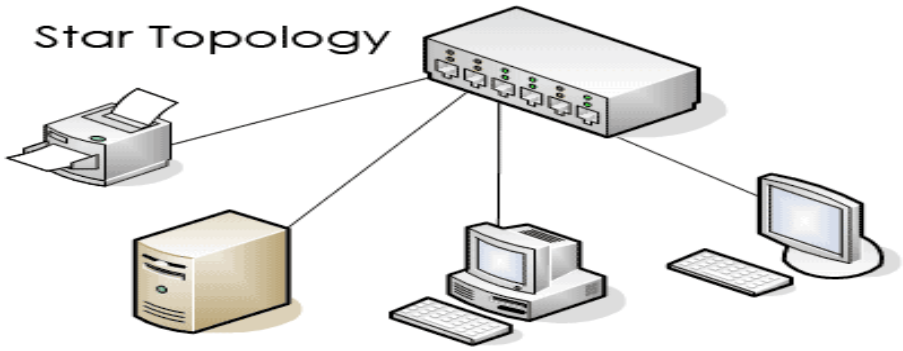
περιμένει μέχρι να παραλάβει το token.Αν το token δεν χρησιμοποιείται ήδη τότε η συσκευή θα μπορέσει να προσθέσει τα δεδομένα και τις πληροφορίες ελέγχου πάνω στο token μετατρέποντας το με αυτόν τον τρόπο σε ένα πλαίσιο δεδομένων.Όταν το πλαίσιο αναγνώρισης παραλαμβάνεται από την συσκευή προορισμού το token απελευθερώνεται προς χρήση από άλλους σταθμούς.



Εικόνα 17: ***Τοπολογία δαχτυλιδιού***

3.3.Τοπολογία αστέρα

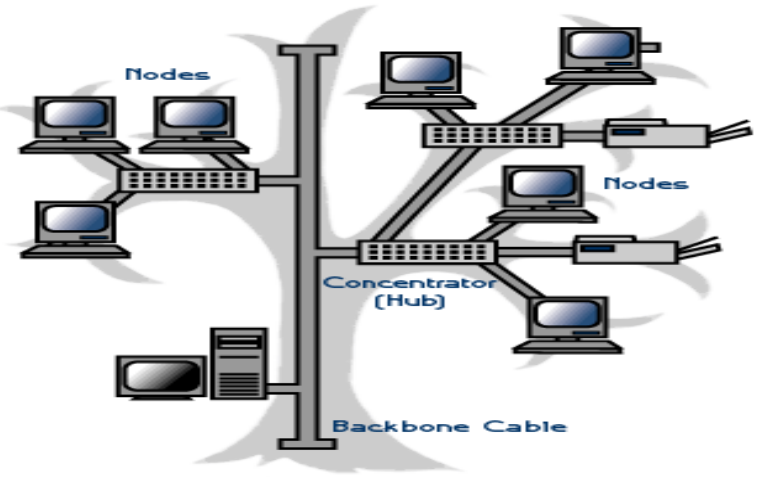
Στην τοπολογία του αστέρα κάθε συσκευή συνδέεται σε ένα καλωδιωμένο κέντρο το οποίο είναι υπεύθυνο για την μεταβίβαση των πακέτων σε άλλες συσκευές που βρίσκονται τοποθετημένες στο ίδιο δικτυακό τμήμα.Τα περισσότερα μοντέρνα δίκτυα χρησιμοποιούν μια παραλαγή της τοπολογίας αστέρα αν και ηλεκτρονικά συμπεριφέρονται σαν τοπολογία bus ή τοπολογία δαχτυλίδι.Ένα μεγάλο πλεονέκτημα των δικτύων αστέρα αποτελεί η ευκολία με την οποία επιπρόσθετες συσκευές μπορούν να προστεθούν στο δίκτυο επιτυγχάνοντας την επέκταση του.Κάθε συσκευή έχει την δικιά της αφοσιωμένη σύνδεση στο καλωδιωμένο κέντρο με αποτέλεσμα την απομόνωση των σφαλμάτων, ενώ οποιοδήποτε πρόβλημα προκύψει στο καλώδιο το οποίο συνδέει το δικτυακό κέντρο με ένα σταθμό εργασίας θα έχει επίπτωση μόνο στο σταθμό αυτό και δεν θα επηρεάσει το υπόλοιπο δικτυακό τμήμα.



Εικόνα 18: ***Τοπολογία αστέρα***

3.4.Τοπολογία δέντρου

Αυτή η τοπολογία αποτέλεί μια διακλαδωμένη έκδοση της bus τοπολογίας.Κάθε διακλάδωση θα πρέπει να τερματίζεται έτσι ώστε να αποτρέπει την αντανάκλαση του σήματος ενώ τα πλαίσια των δεδομένων μεταδίδονται σε όλες τις συσκευές οι οποίες είναι προσαρτημένες στο δίκτυο.

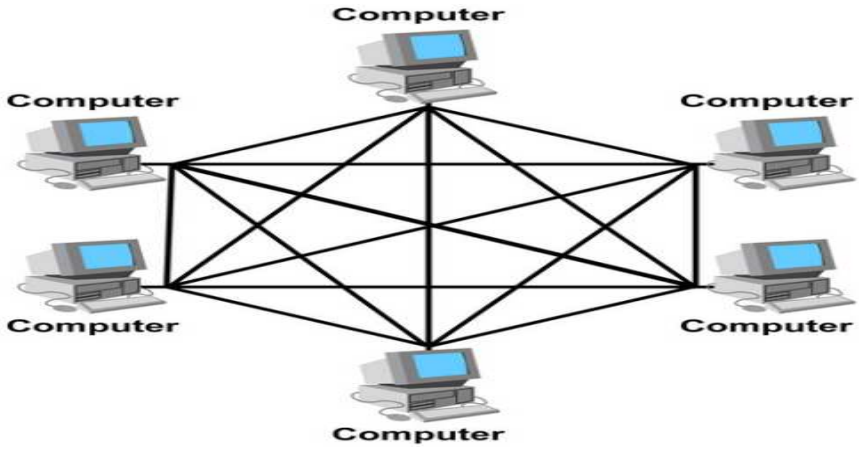


Εικόνα 19: ***Τοπολογία Δέντρου***

3.5.Τοπολογία πλέγμα (mesh)

Στην τεχνολογία πλέγμα κάθε συσκευή συνδέεται με τις υπόλοιπες συσκευές Η αξιοπιστία αυξάνεται γιατί υπάρχουν ενναλακτικές διαδρομές μέσω των οποίων τα πλαίσια των δεδομένων μπορούν να προσπελάσουν τον προορισμό τους σε περίπτωση που μια σύνδεση αποτύχει.Το κύριο μειονέκτημα είναι ο αριθμός των συνδέσεων που απαιτούνται.Αν κάθε συσκευή συνδέεται με όλες τις υπόλοιπες συσκευές στο δίκτυο, ο συνολικός αριθμός των συνδέσεων που απαιτούνται μπορούν να υπολογιστουν από τον παρακάτω τύπο:

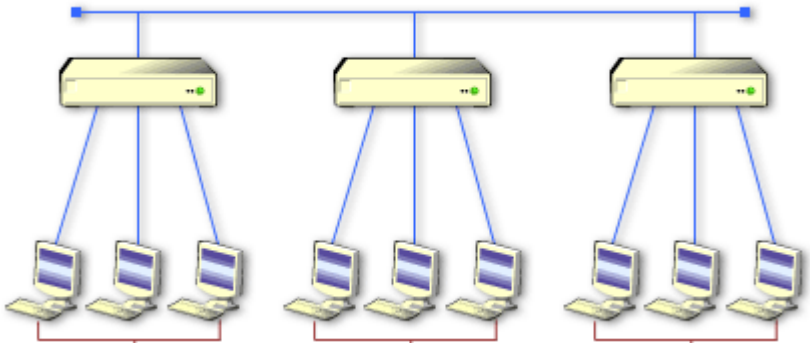
Αριθμός των συνδέσεων = ν x (ν-1)/2 *όπου n ο αριθμός των συσκευών*



Εικόνα 20: ***Τοπολογία Πλέγμα***

3.6.Τοπολογία αστέρα-bus

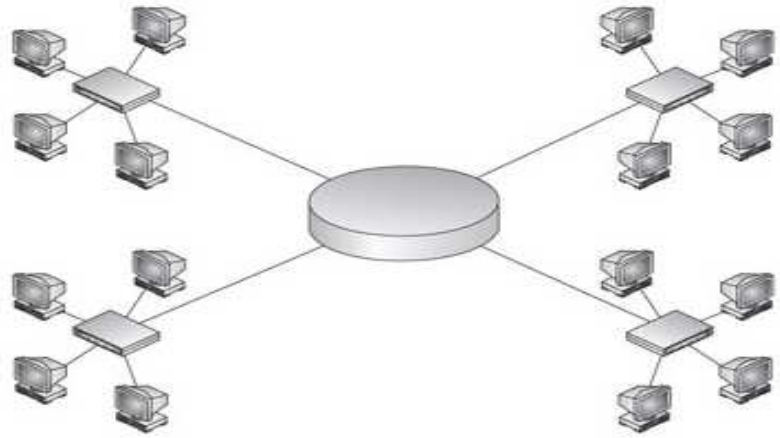
Σ’ αυτή την παραμετροποίηση της τοπολογίας ένα bus χρησιμοποιείται για να συνδεσει ένα αριθμό δικτυακών τμημάτων καθένα από τα οποία διατηρεί μια τοπολογία αστέρα.Αυτή η υβριδική τεχνολογία έχει εφαρμοστεί εκτεταμένα στα τοπικά δίκτυα κατά το παρελθόν και παρέχει ένα εύκολο τρόπο επέκτασης του δικτύου.



Εικόνα 21: ***Τοπολογία Αστέρα - Bus***

3.7.Τοπολογία αστέρα-δαχτυλίδι

Ηλεκτρονικά αυτή η παραμετροποίηση είναι μια τοπολογία δαχτυλιδιού αλλά με τις τερματικές συσκευές συνδεδεμένες σε αστέρα σε ένα ή σε περισσότερα καλωδιωμένα κέντρα.Αυτή η παραμετροποίηση συνήθως χρησιμοποιείται σε Token Ring LANs και παρέχει ένα εύκολο τρόπο επέκτασης του δικτύου δαχτυλιδιού.Επιπρόσθετα καλωδιωμένα κέντρα μπορούν να προστεθούν στο δίκτυο για να επιτρέψουν σε περισσότερες δικτυακές συσκευές να προστεθούν.



Εικόνα 22: ***Τοπολογία Αστέρα - Δαχτυλίδι***

4.Καλωδίωση εξοπλισμού

Όταν σχεδιάζουμε την εγκατάσταση της καλωδίωσης ενός τοπικού δικτύου υπάρχουν τέσσερις φυσικές περιοχές τις οποίες και θα πρέπει να λάβουμε υπόψην μας:

- Η περιοχή εργασίας.
- Το δωμάτιο των επικοινωνιών γνωστό επίσης και ως εγκατάσταση διανομής.
- Η ραχοκοκκαλιά της καλωδίωσης γνωστή επίσης και σαν κάθετη καλωδίωση.
- Η καλωδίωση διανομής γνωστή επίσης και σαν οριζόντια καλωδίωση.

4.1.Δομημένη καλωδίωση

Το σύστημα της καλωδίωσης αποτελεί ένα κρίσιμο σημείο κάθε δικτύου.Είναι γενικά αποδεκτό ότι ένας σημαντικός αριθμό δικτυακών σφαλμάτων προκαλούνται κυρίως από προβλήματα τα οποία σχετίζονται με τα καλώδια.Η τοποθέτηση του συστήματος καλωδίωσης με τον σωστό τρόπο είναι σημαντική για την εξασφάλιση ένος αποτελεσματικού συστήματος επικοινωνιών.Έχοντας λάβει τα παραπάνω υπόψην της, η βιομηχανία προτύπων συμπεριέλαβε τα πρότυπα των καλωδίων στην ανάπτυξη του δικτύου και στην τεχνολογία της επικοινωνίας.Παγκόσμια και εθνικά τηλεπικοινωνιακά πρότυπα καλωδίωσης έχουν υιοθετηθεί ευρέως και όλα βασίζονται στο αμερικανικό ANSI/TIA/EIA πρότυπο καλωδίωσης.

4.1.1.Το πρότυπο ANSI/TIA/EIA

Το παραπάνω είναι ευρύτερα γνωστό και ως Commercial Building Telecommunications Cabling Standards και το οποίο μεταφράζεται σαν Πρότυπο Καλωδίωσης Τηλεπικοινωνιών Εμπορικών Κέντρων.Είναι το κυριότερο πρότυπο το οποίο προδιαγράφει ένα γενικό σύστημα εξυπηρέτησης δικτύων δομημένης καλωδίωσης και είναι ικανό να ανταπεξέλθει σε περιβάλλον πολλών προϊόντων.Αναφέρεται ότι βρίσκουν εφαρμογή άλλα δύο πρότυπα:

- **ANSI/TIA/EIA-569-A** μέσω του οποίου παρέχονται οδηγίες για δωμάτια,χώρους και διαδρομές,στις οποίες βρίσκουν εφαρμογή οι τηλεπικοινωνιακοί εξοπλισμοί.Το πρότυπο αυτό είναι γνωστό και ως Commercial Building Standard For Telecommunications Pathways and Spaceways.
- **ANSI/TIA/EIA-606-A** το οποίο προδιαγράφει τον χαρακτηρισμό,τον χρωματικό κώδικα και την τεκμηρίωση μιας εγκατεστημένης δομημένης καλωδίωσης και είναι γνωστό ως Administration Standard for the Telecommunication Infrastructure of Commercial Buildings.Το πολυαναφερόμενο πρότυπο ANSI/TIA/EIA-569-A καθορίζει τις ελάχιστες απαιτήσεις μιας εγκατεστημένης δομημένης καλωδίωσης σ’ ένα κτίριο ή και σε πολλά κτήρια μαζί-το λεγόμενο πολυκτηριακό περιβάλλον-μέχρι και την τηλεπικοινωνιακή έξοδο.

Τα πρότυπα καθορίζουν τον τρόπο με τον οποίο θα πρέπει να σχεδιάσουμε,να δαμορφώσουμε και να διαχειριστούμε ένα σύστημα καλωδίωσης το οποίο θα πρέπει

να είναι δομημένο.Αυτό σημαίνει ότι το σύστημα αποτελείται από ένα αριθμό διακριτών υποσυστημάτων καθένα από τα οποία έχει συγκεκριμένα χαρακτηριστικά.Τα υποσυστήματα οργανώνονται ιεραρχικά μέσα σε ένα ενοποιημένο σύστημα επικοινωνιών.Για παράδειγμα μια ομάδα εργασίας σε ένα υποσύστημα τοπικού δικτύου έχει μικρές απαιτήσεις απόδοσης συγκριτικά με ένα υποσύστημα ραχοκοκαλιάς η οποία συνήθως απαιτεί μια υψηλή απόδοση.Η υψηλή αυτή απόδοση μπορεί να εξασφαλίστεί από ένα καλώδιο οπτικής ίνας.Τα πρότυπα αναπτύχθηκαν έτσι ώστε να υποστηρίξουν τις υψηλές ταχύτητες δικτυακής τεχνολογίας όπως το Gigabit Ethernet και προηγμένους τύπους καλωδίων όπως τα Category 6 και Category 7 καλώδια συνεστραμμένων ζευγών.

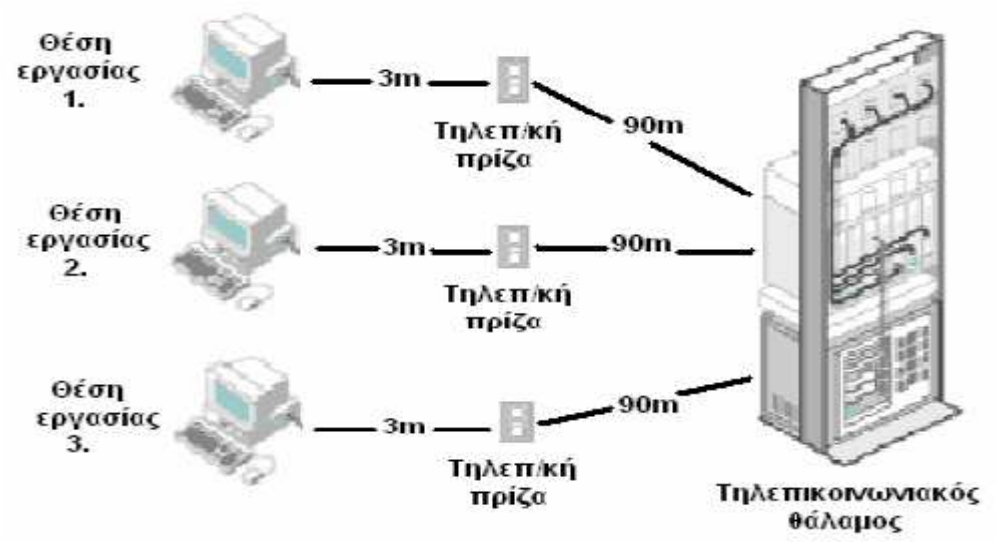
Η δομημένη καλωδίωση καθορίζει ένα γενικό τηλεπικοινωνιακό σύστημα καλωδίωσης για εμπορικά κτίρια και περιλαμβάνει:την καλωδίωση,τους κονέκτορες και όλα τα εξαρτήματα τα οποία χρησιμοποιούνται για να συνδέσουν τον εξοπλισμό ενός τοπικού δικτύου και ενός τηλεφωνικού συστήματος μέσα σ’ ένα κτίριο.Η δομημένη καλωδίωση διαχωρίζει το σύστημα καλωδίωσης σε δύο βασικά συστατικά στοιχεία:

- Την οριζόντια καλωδίωση και
- Την κάθετη καλωδίωση ή διαφορετικά την καλωδίωση ραχοκοκαλιάς.

Τα πρότυπα της δομημένης καλωδίωσης καθορίζουν τα μέσα,την τοπολογία,τα τερματικά σημεία και τα σημεία σύνδεσης.

4.1.2.Οριζόντια καλωδίωση

Περιλαμβάνει όλη την καλωδίωση μια περιοχής εργασίας (η οποία αναπτύσσεται μεταξύ των τηλεπικοινωνιακών πριζών και της οριζόντιας σταυρωτής σύνδεσης στον τηλεπικονωνιακό θαλάμο),τις τηλεπικοινωνιακές πριζές,ένα προαιρετικό σημείο σύνδεσης και την οριζόντια σταυρωτή σύνδεση.Η οριζόντια καλωδίωση όπως αναφέρει η ονομασία της συνήθως τρέχει οριζόντια (πάνω από ψευδοροφές ή κάτω από ψευδοπατώματα) και δεν πηγαίνει πάνω ή κάτω μεταξύ των ορόφων σ’ ένα κτήριο.Η μέγιστη επιτρεπτή απόσταση μεταξύ των τηλεπικοινωνιακών θαλάμων και των τηλεπικοινωνιακών πριζών είναι 90 μέτρα ανεξάρτητα του τύπου του καλωδίου.Επιπρόσθετα 6 μέτρα επιτρέπονται για τα patch καλώδια στον τηλεπικοινωνιακό θαλάμο και στην περιοχή εργασίας αλλά το συνδιασμένο μήκος αυτών των καλωδίων δεν μπορεί να ξεπερνά τα 10 μέτρα.Το καλώδιο που χρησιμοποιείται για την οριζόντια καλωδίωση θα πρέπει να είναι ή ένα τεσσάρων ζευγαριων UTP 100 Ω ή two-fibre 62.5/125-mm καλώδιο οπτικής ίνας ή 50/125-mm multimode καλώδιο οπτικής ίνας.



Εικόνα 23: ***Οριζόντια Καλωδίωση***

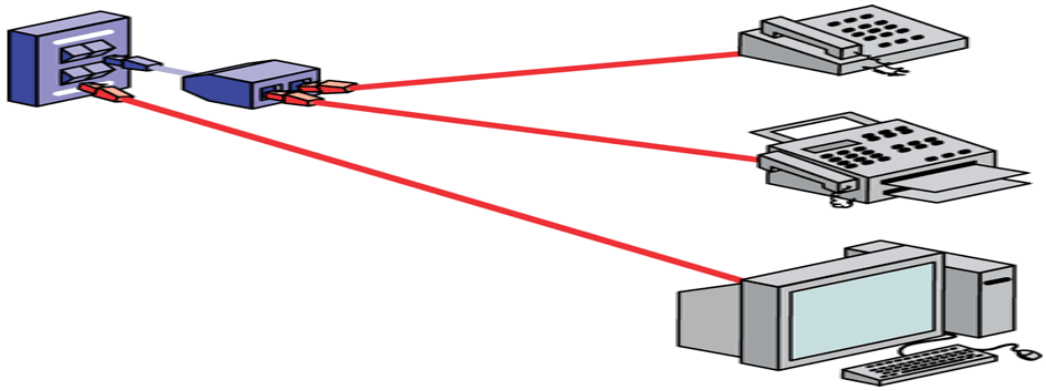
4.1.3.Κάθετη καλωδίωση

Τρέχει μέσα από τα πατώματα των κτηριών και αποτελεί την καλώδιωση που χρησιμοποιείται μεταξυ των τηλεπικοινωνιακών θαλάμων ,των εγκαταστάσεων εισόδου ,των δωμάτιων εξοπλισμου και των κτηρίων ,συμπεριλαμβανομένων όλων των καλωδίων,των τερματικών τους και των ενδιάμεσων σταυρωτών συνδέσεων.Καθορίζεται πάνω στα πρότυπα μιας ιεραρχημένης τοπολογίας αστέρα μέσα στον οποίο όλες οι καλωδιώσεις εκτείνονται γύρω απο ένα κεντρικό σημείο με την μορφή ακτινών (αστερας) **και το οποίο ονομάζεται σταυρωτή σύνδεση (cross connect) και την οποία αποτελεί συνήθως ο τηλεπικοινωνιακός θάλαμος**.Κάθε τηλεπικοινωνιακός θάλαμος ή κάθε εγκατάσταση εισόδου είναι καλωδιωμένή/ός είτε απ' ευθείας στη κεντρική σταυρωτή σύνδεση είτε μέσω ενδιάμεσων σταυρωτών συνδέσεων.Οι περιορισμοί της απόστασης γι' αυτού του τύπου καλωδίωσης εξαρτάται από τον τύπο του καλωδίου που χρησιμοποιείται και τις εγκαταστάσεις τις οποίες συνδέει.

Εικόνα 24: ***Κάθετη καλωδίωση***

4.1.4.Περιοχή εργασίας

Η περιοχή εργασίας καθορίζεται σαν μια περιοχή του κτιρίου μέσα στην οποία αξιοποιείται ο τηλεπικοινωνιακός εξοπλισμός.Περιλαμβάνει όλα τα συστατικά των καλωδίων που εκτείνονται μεταξύ των τηλεπικοινωνιακών πριζών και του τηλεπικοινωνιακού εξοπλισμού του τερματικού χρήστη όπως είναι τα τηλέφωνα,οι σταθμοί εργασιές και οι εκτυπωτές.Τα συστήμα καλωδίωσης των περιοχών εργασίας είναι έτσι σχεδιασμένο ώστε να είναι ευέλικτο αλλά ακόμα και έτσι απαιτεί προσεκτική διαχείριση.Κατά την διαδικασία εγκτάστασης μιας πρότυπης δομημένης καλωδίωσης θα πρέπει να ελέγχουμε την εγκατάσταση των τηλεπικοινωνιακών πρίζων ενώ οι τερματισμοί των καλωδίων θα πρέπει να πραγματοποιούνται χρησιμοποιώντας το ίδιο πρότυπο (T568A ή T568B).Το T568B είναι το πιο συνηθισμένο πρότυπο στις εφαρμογές των δικτυακών συσκευών.Το πρότυπο απαιτεί ότι δύο έξοδοι θα πρέπει να παρέχονται σε κάθε πριζάκι: μια για τα δεδομένα και μια για την φωνή.



Εικόνα 25: ***Περιοχή Εργασίας***

4.1.5.Τηλεπικοινωνιακός θάλαμος

Αποτελεί μια κλειστή περιοχή όπως ένα δωμάτιο ή ένας θάλαμος που προορίζεται για την στέγαση του τηλεπικοινωνιακού εξοπλισμού,την κατανομή των πλαισίων,τους τερματισμούς των καλωδίων και τις σταυρωτές συνδέσεις.Με άλλα λόγια όλος ο τεχνικός εξοπλισμός ο οποιός απαιτείται για την συνδέση της οριζόντιας καλωδίωσης με την κάθετη καλωδίωση.Αυτή η περιοχή πολύ συχνά στεγάζει βοηθητικό εξοπλισμό όπως τους δικτυακούς διακομιστές φακέλων.Κάθε κτήριο θα πρέπει να διαθέτει τουλάχιστον ένα τηλεπικοινωνιακό θάλαμο ενώ το πρότυπο καθορίζει ένα για κάθε όροφο.Συγκεκριμένων διαστάσεων τηλεπικοινωνιακοι θάλαμοι συνιστώνται και οι οποίοι εξαρτώνται από το μέγεθος της περιοχής υπηρεσίας.Θα πρέπει να υπάρχει ικανοποιητικός χώρος για το προσωπικό υπηρεσίας προκειμένου να παρέχουν την συντήρηση και την ολοκλήρωση άλλων καθηκόντων πάνω στον τηλεπικοινωνιακό εξοπλισμό.Ο φωτισμός ,οι τροφοδοσιες του ρεύματος και οι περιβαλλοντολογικοι παράγοντες θα πρέπει επίσης να συναντούν τις απαιτήσεις του συγκεκριμένου προτύπου.

Εικόνα 26: ***Τηλεπικοινωνιακός Θάλαμος***

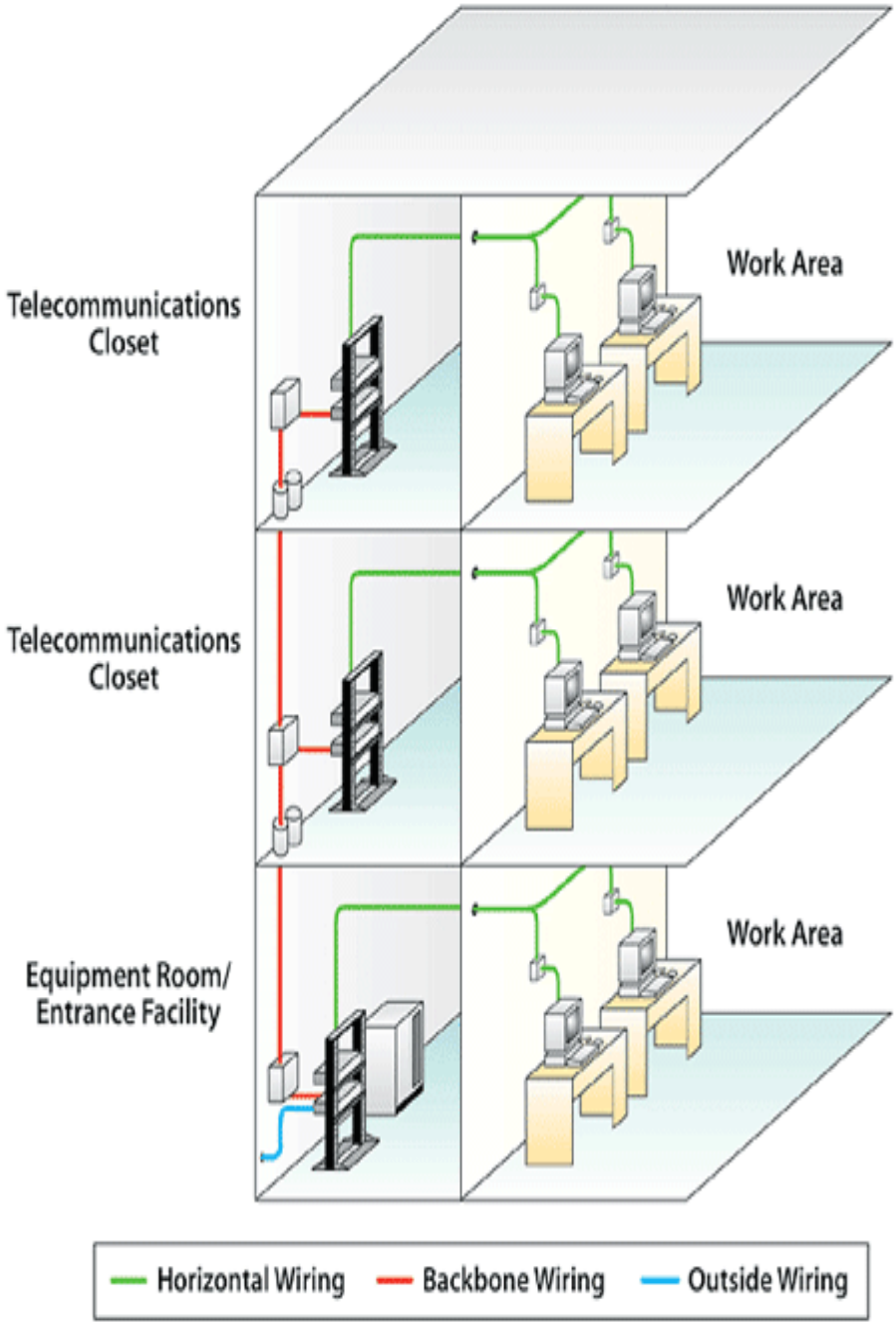
4.1.6.Δωμάτιο εξοπλισμού

Ο χώρος ο οποίος στεγάζει τηλεπικοινωνιακά συστήματα του κτιριου όπως τα PBXs,τους διακομιστές,τους μεταγωγείς,τους δρομολογητές και τους μηχανικούς τερματισμούς του τηλεπικοινωνιακού συστήματος καλωδίωσης.Θεωρείται διαφορετικός από ένα τηλεπικοινωνιακό θάλαμο εξαιτίας της πολυπλοκότητας των συστατικών που στεγάζει.Ένα δωμάτιο εξοπλισμού μπορεί είτε να αντικαταθιστά τον τηλεπικοινωνιακό θάλαμο, αφου οι λειτουργίες του δωματίου εξοπλισμού μπορούν να συγχωνεύονται σε αυτόν, είτε να αποτελεί μια διαφορετική εγκτάσταση.Το δωμάτιο εξοπλισμού παρέχει τερματικά σημείο για την κάθετη καλωδίωση.Το κάθε τερματικό σημείο συνδέεται με έναν ή και περισσότερους τηλεπικοινωνιακούς θαλάμους.Σ’ ένα περιβάλλον μιας μεγάλης εταιρείας κάθε κτίριο μπορεί να διαθέτει το δικό του δωμάτιο εξοπλισμού στο οποίο συνδέεται ο κάθε τηλεπικοινωνιακός θάλαμος. Ο εξοπλισμός αυτού του δωματίου μπορεί εν συνεχεία να συνδεθεί στις κεντρικές εγκαταστάσεις της εταιρείας,οι οποίες παρέχουν το κεντρική σταυρωτή σύνδεση για όλα τα κτίρια.

Εικόνα 27: ***Δωμάτιο Εξοπλισμού***

4.1.7.Εγκαταστάσεις εισόδου

Περικλείει την είσοδο της τηλεπικοινωνιακής υπηρεσίας στο κτίριο.Επίσης περικλείει το δικτυακό σημείο οριοθέτησης, δηλαδή το σημείο που πραγματοποιείται η διασύνδεση με τις εγκαταστάσεις του τοπικού τηλεπικοινωνιακού φορέα.



Εικόνα 28: ***Δομημένη Καλωδίωση***

4.1.8.Διευθέτηση εξοπλισμού

Όποιο και αν είναι το μέγεθος του δικτύου θα πρέπει να παρέχουμε ικανοποιητικό χώρο για την διευθέτηση των δικτυακών διακομιστών ,τις συσκευές μεταγωγής και τις εφεδρικές παροχές ηλεκτρικού ρεύματος.Αυτός ο εξοπλισμός είναι ζωτικής σημασίας για την λειτουργία του δικτύου και το κόστος της επιδιόρθωσης ή

αντικατάστασης του είναι μεγάλο.Γι’ αυτό το λόγο θα πρέπει να στεγάζεται σ’ ένα ασφαλές σημείο για την αποτροπή κλοπής του εξοπλισμού ή της οποίας ενδεχόμενης ζημιάς.Επομένως θα πρέπει να χρησιμοποιούνται σχάρες εξοπλισμού ή θάλαμοι οι οποίοι είναι αποκλειστικά σχεδιασμένοι για την ασφαλή και λειτουργική χωροταξική διευθέτηση του δικτυακού εξοπλισμού.

Εικόνα 29: ***Σχάρα και Θάλαμος***

Η σχάρα (rack) είναι μια ανοιχτά πλαισιωμένη περίφραξη στην οποία ο εξοπλισμός μπορεί να τοποθετηθεί ώστε να έχουμε την δυνατότητα κυκλικής πρόσβασης σε αυτόν.Ο θάλαμος είναι κυκλικά πλαισιωμένος εκτός από το μπροστινό μέρος οπού έχουμε την δυνατότητα πρόσβασης μέσω μιας πόρτας.Και οι δύο τύποι της περίφραξης παρέχουν δύο κάθετες ράγες με ενσωματωμένες τρύπες ανά τακτικά διαστήματα επι του μήκους της και πάνω στις οποίες δικτυακός εξοπλισμός μπορεί να τοποθετηθεί.

Η σταθερότητα ενός θαλάμου αποτελεί πελεονέκτημα αν εκεί θα πρέπει να γίνει διευθέτηση εξοπλισμών μεγάλου μεγέθους ή βάρους.Ο θάλαμος επίσης παρέχει προστασία απέναντι σε περιβαλλοντολογικούς παράγοντες όπως η σκόνη ενώ προσφέρει μεγαλύτερη ασφάλεια απ’ ότι μια ανοιχτή σχάρα.Απο την άλλη μεριά αν απαιτείται για τον εξοπλισμό μια συχνή κυκλική πρόσβαση ή αν ο εξαερισμός αποτελεί ένα ζήτημα εξαιτίας της παραγωγής θερμότητας τότε μια ανοιχτή σχάρα θα προτιμηθεί για την τοποθέτηση του εξοπλισμού αντί για ένα θάλαμο.Ο εξοπλισμός ο οποίος είναι τοποθετημένος σε περιοχή η οποία είναι προσβάσιμη στο κοινό θα πρέπει να είναι στεγασμένος σε ένα κλειδωμένο θάλαμο.Αν ο εξοπλισμός παράγει μεγάλη θερμότητα ο θάλαμος θα πρέπει να εξοπλιστεί με ανεμιστήρες.

Τόσο οι σχάρες όσο και οι θάλαμοι είναι διαθέσιμοι σε διάφορα μεγέθη και μπορούν να είναι είτε επιδαπέδιοι είτε εντοιχισμένοι.Οι επιδαπέδιοι θα πρέπει να βιδώνονται στο πάτωμα ή στον τοίχο για μεγαλύτερη σταθερότητα.Η τοποθέτηση των θαλάμων

θα πρέπει να είναι τέτοια ώστε να παρέχει την ικανοποιητική πρόσβαση στον εξοπλισμό για λόγους συντήρησης.

4.1.9.Patch panels

Το patch panel παρέχει ένα βολικό μέρος για τον τερματισμό των καλωδίων, τα οποία προέρχονται από διαφορετικά δωμάτια και καταλήγουν στο rack του κάθε ορόφου.Φυσικά κάποιο καλώδιο θα μπορούσε να παρακάμψει το patch panel και να τερματιστεί απ' ευθείας στο switch με ένα RJ-45 κονέκτορα αλλά θα έχανε τα πλεονεκτήματα που περιγράφονται παρακάτω:

Μπορούμε να τοποθετήσουμε ετικέτες στο patch panel έτσι ώστε να γνωρίζουμε το καλώδιο το οποίο τερματίζεται σ' αυτό από ποιο δωμάτιο προέρχεται.Η τοποθέτηση των ετικετών στα καλώδια είναι δυσκολότερη στην ανάγνωση συγκριτικά με την τοποθέτηση ετικετών στο patch panel ενώ υπάρχει πάντα το ενδεχόμενο οι ετικέτες των καλωδίων να φθαρούν.Το RJ-45 στο μπροστινό μέρος παρέχει ένα σημείο στο οποίο θα κουμπωθεί ένα patch καλώδιο το οποίο θα καταλήξει στον μεταγωγέα.Οι τύποι των κονεκτόρων στο πίσω μέρος του patch panel συνήθως είναι χρωματικά κωδικοποιημένοι είτε με το πρότυπο 568A είτε με το πρότυπο 568B.Είναι σημαντικό ότι ο τύπος (568A ή 568B) πάνω στο patch panel να ταιριάζει με τον τύπο της τηλεπικοινωνιακής πρίζας.

Εικόνα 30: ***Patch Panels***

5.Οι τύποι των φυσικών μέσων

Η επιλογή των καλωδίων προκειμένου να δημιουργήσουμε μια τοπική ή μια ευρείας περιοχής σύνδεση απαιτεί να λάβουμε υπόψην μας τους διαφορετικούς τύπους των φυσικών μέσων.Υπάρχουν διαφορετικές εφαρμογές σε φυσικό επίπεδο οι οποίες υποστηρίζουν διαδορετικά φυσικά μέσα:

- UTP (Κατηγορία 5,5e,6 και 7)
- Οπτικές ίνες
- Ασύρματα

Κάθε φυσικό μέσο έχει τα πλεονεκτήματα και τα μειονεκτήματα του.Μερικοί από τους παράγοντες που θα πρέπει να λάβουμε υπόψιν μας είναι:

- Το μήκος του καλωδίου – Θα πρέπει το καλώδιο να συνδέθεί κατά μήκος ενός δωματίου ή από κτίριο σε κτίριο;
- Κόστος – Μας επιτρέπει ο προυπολογισμός την χρήση ακριβότερων τύπων φυσικών μέσων;
- Εύρος ζώνης ή ταχύητα – Η τεχνολογία η οποία χρησιμοποιήθηκε με τα φυσικά μέσα παρέχει ικανοποιητική ταχύτητα;
- Ευκολία εγκατάστασης – Μπορεί η ομάδα εγκτάστασης να εγκαταστήσει το καλώδιο ή θα πρέπει να απευθυνθούμε στην εταιρεία προμήθευσης του καλωδίου;
- Ευαισθησία στο EMI/RFI – Υπάρχει το ενδεχόμενο το τοπικό περιβάλλον να παρέμβει στο σήμα;

Εικόνα 31: ***Τύποι διασύνδεσης των συσκευών (Οπτικές ίνες,UTP καλώδια,ασύρματη σύνδεση)***

5.1.Το μήκος του καλωδίου

Το μέγιστο μήκος του καλωδίου το οποίο απαιτείται προκειμένου να συνδέσει μια συσκευή, περιλαμβάνει όλο το μήκος των καλωδίων από τις τερματικές συσκευές που βρίσκονται τοποθετημένες στην περιοχή εργασίας μέχρι τις ενδιάμεσες συσκευές που βρίσκονται εγκαταστημένες στο δωμάτιο επικοινωνιας (συνήθως ένας μεταγωγέας).Επίσης περιλαμβάνει το καλώδιο από τις συσκευές μέχρι την πρίζα του τοίχου,το καλώδιο από την πρίζα του τοίχου και μέσα από τους τοίχους του κτίριου στο σημείο της σταυρωτής σύνδεσης ή στο patch panel και την καλωδίωση από το patch panel στον μεταγωγέα.Αν οι μεταγωγείς βρίσκονται εγκατεστημένοι σε δωμάτια επικοινωνίας σε διαφορετικούς ορόφους ενός κτηρίου ή σε διαφορετικά κτήρια, το μήκος του καλωδίου μεταξύ αυτών των σημείων θα πρέπει να περιληφθούν στο συνολικό μήκος.

Η εξασθένιση (attenuation) είναι η μείωση της δύναμης ενός σήματος καθώς μετακινείται στα φυσικά μέσα.Όσο μεγαλύτερο το μήκος των φυσικών μέσων τόσο μεγαλύτερη η εξασθένιση του σήματος.Αυτό θα έχει σαν αποτέλεσμα σε κάποιο σημείο το σήμα να μην είναι ανιχνεύσιμο.Η απόσταση της καλωδίωσης αποτελεί ένα σημαντικό παράγοντα στην απόδοση των σημάτων των δεδομενων.Η εξασθένιση του σήματος και η έκθεση του σε πιθανές παρεμβολές αυξάνεται με το μήκος του καλωδίου.

Για παράδειγμα όταν χρησιμοποιούμε τη UTP καλωδίωση για Ethernet ,το μήκος της οριζόντιας καλωδίωσης θα πρέπει να παραμείνει μέσα στα προτεινώμενα όρια της μέγιστης απόστασης των 90 μέτρων προκειμένου να αποφύγει την εξασθένιση του σήματος.Τα καλώδια των οπτικών ινών παρέχουν μια μεγαλύτερη απόσταση καλωδίωσης η οποία ξεκινάει από τα 500 μέτρα και φτάνει μέχρι αρκετά χιλιόμετρα ανάλογα με την τενολογία που χρησιμοποιείται.Παρόλαυτα το καλώδιο της οπτικής ίνας μπορεί επίσης να προσβληθεί από την εξασθένιση όταν προσεγγίζει τα παραπάνω όρια.

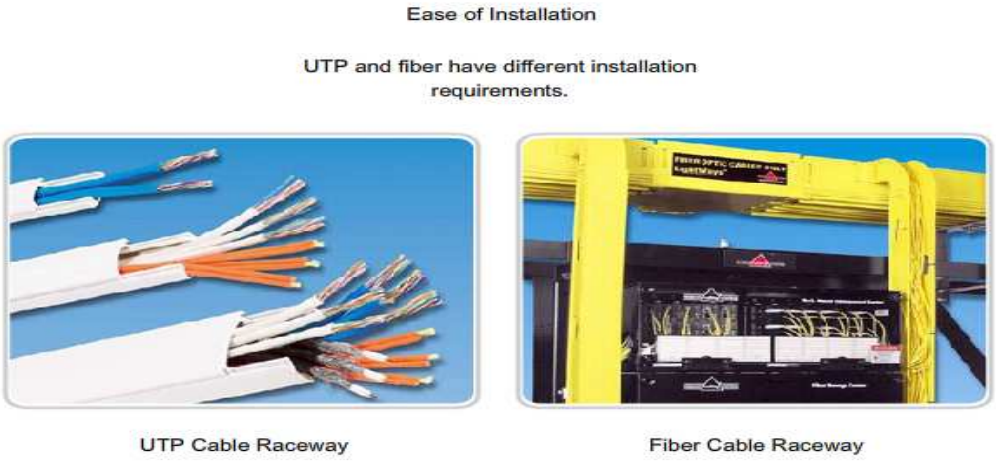
5.2.Ευκολία της εγκατάστασης

Η ευκολία της εγκατάστασης των καλωδίων ποικίλει ανάλογα με τον τύπο του καλωδίου και την αρχιτεκτονική του κτιρίου.Η πρόσβαση στους ορόφους ή στους χώρους των ψευδοροφών και των ψευδοπατωμάτων,τα φυσικά μεγέθη των καλωδίων και τα χαρακτηριστικά τους,επηρεάζουν το πόσο εύκολα ένα καλώδιο μπορεί να εγκατασταθεί σε διάφορα κτήρια.Τα καλώδια στα κτήρια είναι συνήθως προστατευμένα κάτω από ένα κλειστό πλαίσιο.Όπως φαίνετε στο σχήμα ένα πλαίσιο αποτελεί μια περίφραξη ή ένα σωλήνα το οποίο περικλείει το καλωδίο.

Το UTP καλώδιο είναι σχετικά ελαφρύ,ευέλικτο και έχει μικρή διάμετρο κάτι το οποίο του επιτρέπει να χωράει σε μικρούς χώρους.Οι RJ45 κονέκτορες είναι σχετικά εύκολοι στην εγκατάσταση τους και αποτελούν ένα πρότυπο για όλες τις Ethernet συσκευές.

Πολλά καλώδια οπτικών ινών περιέχουν ένα λεπτό γυαλί ίνας.Το γεγονός αυτό δημιουργεί θέμα όσο αναφορά την ακτίνα κάμψης του καλωδίου.Οι τσακίσεις ή το αιχμηρό λύγισμα του καλωδίου ενδέχεται να σπάσει την ίνα.Ο τερματισμός στους κονέκτορες (ST, SC, MT-RJ) του καλωδίου είναι πολύ δύσκολος και απαιτεί ειδικό εξοπλισμό.

Οι ασύρματες συσκευές απαιτούν καλωδίωση μόνο μέχρι κάποιο σημείο και προκειμένου να συνδέσει συσκευές όπως είναι τα σημεία πρόσβασης στο καλωδιωμένο τοπικό δίκτυο.Επειδή υπάρχει σημαντικά μειωμένη καλωδίωση στα ασύρματα δίκτυα τα καθιστά ευκολότερο στην εγκατάσταση του συγκριτικά με την UTP καλωδίωση ή την καλωδίωση με οπτική ίνα.Παρόλαυτα ένα ασύρματο τοπικό δίκτυο απαιτεί ενδελεχή σχεδιασμό και έλεγχο.Επιπλέον υπάρχουν και πολλοί εξωτερικοί παράγοντες, όπως άλλες ηλεκτρομαγνητικές συσκευές και η δομή του κτηρίου, οι οποίοι μπορούν να επηρεάσουν την λειτουργία του.



Εικόνα 32: ***Τρόποι εγκατάστασης UTP καλωδίων και οπτικών ινών***

5.3.Ηλεκτρομαγνητική παρεμβολή/Παρεμβολή ραδιοσυχνότητας

Η ηλεκτρομαγνητική παρεμβολή (EMI) και η παρεμβολή της ραδιοσυχνότητας (RFI) θα πρέπει να ληφθούν υπόψιν μας όταν επιλέγουμε το φυσικό μέσο γα ένα τοπικό δίκτου.Το EMI/RFI σε ένα εργοστασιακό περιβάλλον μπορεί να επηρεάσει σημαντικά την επικοινωνία των δεδομένων αν διαλέξουμε λάθος φυσικό μέσο.Η παρεμβολή μπορεί να δημιουργηθεί από ηλεκτρικές μηχανές,το φωτισμό και άλλες συσκευές επικοινωνίας συμπεριλαμβανομένων τον υπολογιστών και τον ασύρματο εξοπλισμό.

Σαν παράδειγμα θεωρήστε μια εγκατάσταση στην οποία οι συσκευές μεταξύ δυο ξεχωριστών δικτύων διασυνδέονται.Τα φυσικά μέσα τα οποία χρησιμοποιούνται προκειμένου να διασυνδέσουμε τα κτίρια μεταξύ τους θα είναι εκτεθειμένα σε περίπτωση ενός κεραυνού.Επιπροσθέτως μπορεί να υπάρχει μεγάλη απόσταση μεταξύ αυτών των δύο κτιρίων.Για την συγκεκριμένη εγκατάσταση το καλώδιο της οπτικής ίνας αποτελεί την καλύτερη λύση.

Το ασύρματο αποτελεί το μέσο το οποίο είναι περισσότερο ευάλωτο στο RFI.Πριν να εφαρμόσουμε τις ασύρματες τεχνολογίες θα πρέπει να αναγνωρίσουμε και να περιορίσουμε όσο αυτό είναι δυνατόν τις πιθανές πηγές παρεμβολής.

5.4.Καλώδια Συνεστραμμένων Ζευγών

Η συστροφή στα τηλεπικοινωνιακά καλώδια εφαρμόστηκε για πρώτη φορά την δεκαετία του 1880 στα τηλεγραφικά καλώδια προκειμένου να περιοριστεί η επίδραση από γειτνιάζοντες αγωγούς ηλεκτρικής τροφοδοσίας των TPAM και αργότερα της παράλληλης όδευσης καλωδίων ηλεκτροδότησης.Τα ρεύματα εξ' επαγωγής που δημιουργούνται εξαιτίας των γειτονικών ηλεκτρομαγνητικών πεδίων αλληλοεξουδετερώνονται σε κάθε συστροφή με αποτέλεσμα να περιορίζεται ο εισαγώμενος ηλεκτρομαγνητικός θόρυβος στο τηλεπικοινωνιακό καλώδιο.Για τις εφαρμογές του τηλεγράφου αρκούσαν τέσσερις συστροφές ανα χιλιόμετρο.Στην σημερινή εποχή η συστροφή με το να περιρίζει τον θόρυβο κάνει εφικτούς υψηλότερους ρυθμούς μετάδοσης δεδομένων.

Κατηγορία Καλωδίου	**Εύρος Φάσματος Συχνοτήτων σε MHz**	**Κατάλληλο για Χρήση**
1	-	Απλή χρήση
2	1	Τηλεφωνική καλωδίωση
3	16	Τηλεφωνική καλωδίωση, 10Base-T
4	20	Token-Ring , 10Base-T
5	100	100Base-TX, 10Base-T
5e	100	1000Base-T, 100Base-TX
6	250	1000Base-T, 100Base-TX
6a	500	10GBase-T
7	600	

Πίνακας 1

Οι μεγαλύτερες κατηγορίες είναι συμβατές με τις κατώτερες.

5.4.1.Unshielded Twisted Pair (UTP) ή Απροστάτευτα Συνεστραμμένα Ζεύγη

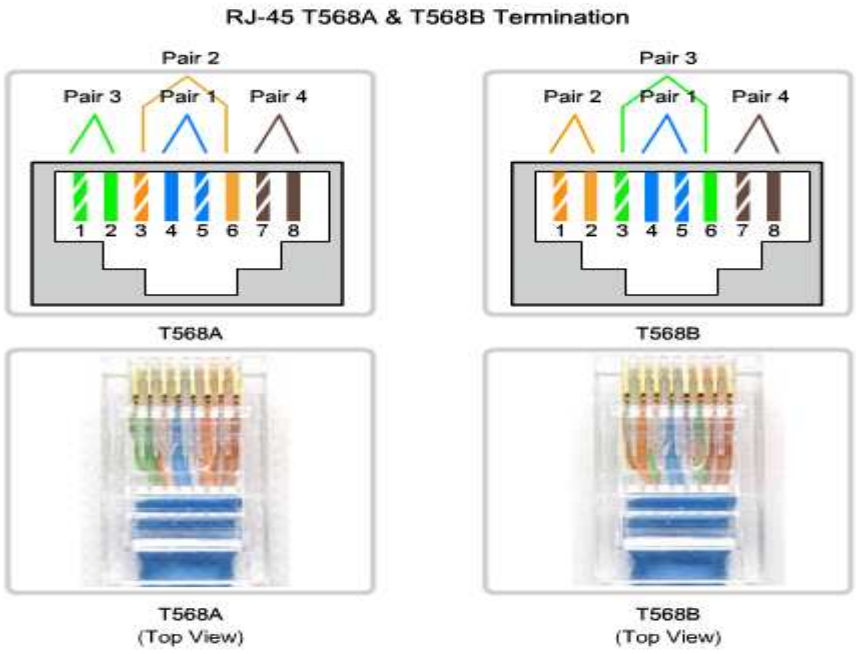
Είναι τα απλούστερα που υπάρχουν και δεν διαθέτουν πρόσθετη εξωτερική μόνωση για θωράκιση.Υπάρχουν πολύζευγα και τα πλεόν διαδεδομένα είναι τα 25ζευγα (50 αγωγοί) και τα 4ζεύγα (8 αγωγοί).Τα πρώτα χρησιμοποιούνται κυρίως για τηλεφωνικές διασυνδέσεις μεταξύ ορόφων κτηρίων ή μεταξύ διαφορετικών κτηρίων ενώ τα 4ζεύγα για εσωτερική δομημένη καλωδίωση σε δίκτυα υπολογιστών.Οι χρωματισμοί είναι δεδομένοι και διευκολύνουν τον εγκαταστάτη.Οι χρωματισμοί διαφέρουν ελάχιστα από κατασκευαστή σε κατασκευαστή.Σε 4ζεύγο καλώδιο έχουμε τα εξής ζεύγη:

- Άσπρο-πορτοκαλί και πορτοκαλί
- Άσπρο-πράσινο και πράσινο
- Άσπρο-μπλέ και μπλέ
- Άσπρο-καφέ και καφέ.

Αρκετές φορές τα δίχρωμα είναι απλά λευκά οπότε διακρίνονται μόνο από το ζευγάρι τους με το οποίο τυλίγονται.Οι συστροφές είναι σημαντικές για τον περιορισμό των παρεμβολών συνεπώς κατά την εφαρμογή στο patch panel / ακροδέκτη θα πρέπει να αποσυστρέφονται κατά το ελάχιστο μήκος.

5.5.Ακροδέκτες καλωδίων δικτύου – RJ45

Οι αρσενικοί ακροδέκτες των καλωδίων δικτύου είναι τυποποιημένοι και ονομάζονται RJ45 (Registered Jack).Η ονομασία δόθηκε από την Telecommunication Industry Association (TIA) και υπάρχουν δύο πρότυπα αναφορικά με την αντιστοίχιση των αγωγών των ζευγών στους 8 ακροδέκτες: το 568A και το 568B.Όταν αντικρίζουμε το RJ45 από την μπροστινή πλευρά τα pins αριθμούνται από το 8 στο 1.Όταν το αντικρίζετε από την ανοιχτή πλευρά της εισόδου των καλωδίων τα pins αριθμούνται από το 1 στο 8. Η μόνη διαφορά μεταξύ των χρωματικών κωδικών 568A και 568B είναι ότι τα ζεύγη του πορτοκαλί χρώματος και του πράσινου χρώματος ανταλλάσονται.



Εικόνα 33: ***Τερματισμός 568A και 568B***

5.6.Straight through and crossover cables ή Καλώδια απ’ ευθείας σύνδεσης και σταυρωτή σύνδεσης.

Μέχρι και τις αρχές τις δεκαετίας υπήρχαν δύο τρόποι διαδύνδεσης με καλώδιο Ethernet:

- Ο απ’ ευθείας τρόπος (straight through) για διασύνδεση υπολογιστών (MDI-medium dependent interface) με κάποιο μεταγωγέα/κόμβο/δρομολογητή και
- Ο χιαστί (crossover) για διασύνδεση όμοιων συστημάτων μεταξύ τους χωρίς την παρεμβολή κάποιου μεταγωγέα (MDIX).

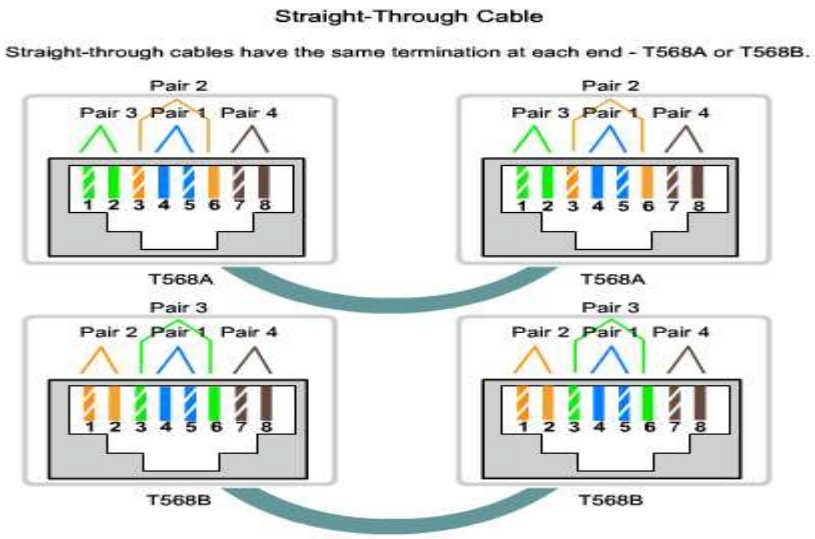
Η διαφοροποίηση αυτή δεν είναι τόσο έντονη σήμερα μιας και οι περισσότερες κάρτες δικτύου και οι μεταγωγείς διαθέτουν πόρτες τύπου MDI και MDIX οπότε λειτουργούν με ότι τύπο καλωδίου και αν τις συνδέσουμε.

Το Media Dependent Interface (MDI) χρησιμοποιεί το πρότυπο Ethernet εξόδου των pins.Τα pins 1 και 2 χρησιμοποιούνται για την μετάδοση και τα pins 3 και 6 χρησιμοποιούνται για την λήψη.Συσκευές όπως οι προσωπικοί υπολογιστές,οι διακομιστές και οι δρομλογητές δέχονται MDI συνδέσεις.

Οι συσκευές οι οποίες παρέχουν την συνδεσιμότητα του LAN-συνήθως οι κόμβοι και οι μετγαωγείς-χρησιμοποιούν τα Media Dependent Interface, crossover (MDIX) συνδέσεις.Η MDIX σύνδεση ανταλλάσει το ζεύγος της μετάδοσης εσωτερικά.Αυτή η ανταλλαγή επιτρέπει στις τερματικές συσκευές να συνδεθούν στον κόμβο ή στον μεταγωγέα χρησιμοποιώντας ένα straight through καλώδιο.

5.6.1.Straight Through UTP καλώδιο

Το straight-through UTP καλώδιο έχει κονέκτορες και στα δύο άκρα οι οποίοι τερματίζονται με τον ίδιο τρόπο σύμφωνα με τα πρότυπα είτε του T568A είτε του T568B.Αναγνωρίζοντας το πρότυπο του καλωδίου το οποίο θα χρησιμοποιηθεί σας βοηθάει να καθορίσετε αν έχετε το κατάλληλο καλώδιο για την εργασία σας.Επίσης πολύ σημαντικό είναι να χρησιμοποιήσουμε το ίδιο χρωματικό κώδικα σ' ολόκληρο το τοπικό δίκτυο.



Εικόνα 34: ***Τερματισμός άκρων straight through με 568A και 568B***

RJ45 Ακροδέκτης #	Περιγραφή Χρώματος Αγωγού (T568A)	Χρώμα Αγωγού (T568A)	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	White/Green		Transmit+	BI_DA+
2	Green		Transmit-	BI_DA-
3	White/Orange		Receive+	BI_DB+
4	Blue		Αχρησιμοποίητο	BI_DC+
5	White/Blue		Αχρησιμοποίητο	BI_DC-
6	Orange		Receive-	BI_DB-
7	White/Brown		Αχρησιμοποίητο	BI_DD+
8	Brown		Αχρησιμοποίητο	BI_DD-

Εικόνα 35: ***Χρωματικός κώδικας 568A για straight through καλωδίωση***

RJ45 Ακροδέκτης #	Περιγραφή Χρώματος Αγωγού (T568B)	Χρώμα Αγωγού (T568B)	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	White/Orange		Transmit+	BI_DA+
2	Orange		Transmit-	BI_DA-
3	White/Green		Receive+	BI_DB+
4	Blue		Αχρησιμοποίητο	BI_DC+
5	White/Blue		Αχρησιμοποίητο	BI_DC-
6	Green		Receive-	BI_DB-
7	White/Brown		Αχρησιμοποίητο	BI_DD+
8	Brown		Αχρησιμοποίητο	BI_DD-

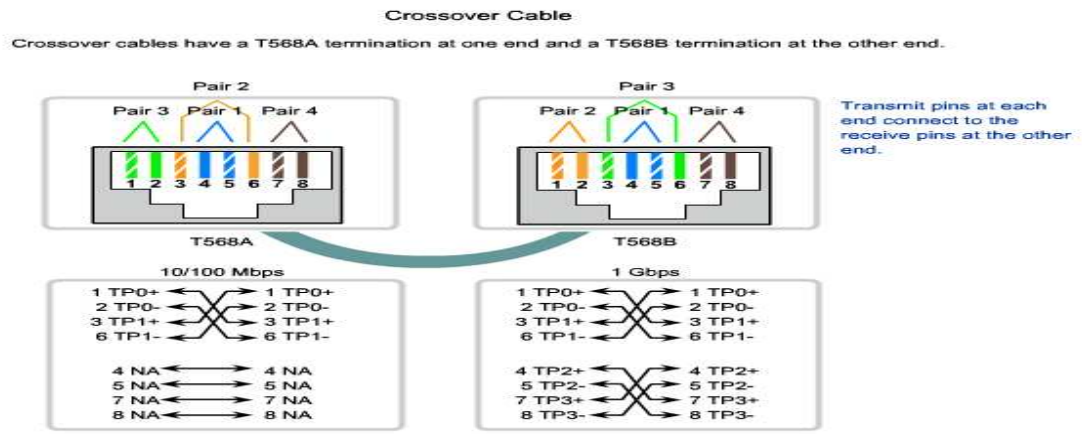
Εικόνα 36: ***Χρωματικός κώδικας 568B για straight through καλωδίωση***

5.6.2.Crossover UTP καλώδιο

Προκειμένου δύο συσκευές να επικοινωνήσουν μέσω ενός καλωδίου το οποίο είναι απ' ευθείας συνδεδεμένο μεταξύ τους, το τερματικό πομπού μιας συσκευής θα πρέπει να συνδεθεί με το τερματικό δέκτη της άλλης συσκευής.

Το καλώδιο θα πρέπει να τερματιστεί έτσι ώστε το pin μετάδοσης, δηλαδή το Tx το οποίο παίρνει το σήμα από την συσκευή Α που βρίσκεται στο ένα άκρο, να καλωδιώνεται με το pin λήψης Rx της συσκευής Β.Παρόμοια το pin μετάδοσης Tx της συσκευής Β θα πρέπει να συνδεθεί με το pin λήψης Rx.Αν το Tx pin της μιας συσκευής είναι αριθμημένο με το 1 και το Rx pin είναι αριθμημένο με το 2 τότε το καλώδιο συνδέει το pin 1 στο ένα άκρο με το pin 2 του άλλου άκρου.Αυτή η διασταύρωση (crossover) μεταξύ των pin συνδέσεων δίνει σ' αυτό τον τύπο του καλωδίου το όνομα του.

Προκειμένου να πραγματοποιήσουμε αυτού του είδους την σύνδεση σ' ένα UTP καλώδιο το ένα άκρο θα πρέπει να τερματιστεί με το πρότυπο EIA/TIA T568A και το άλλο άκρο θα πρέπει να τερματιστει σύμφωνα με το πρότυπο EIA/TIA T568B.



Εικόνα 37: ***Τερματισμός άκρων crossover με 568A τερματισμό στο ένα άκρο και 568B τερματισμό στο άλλο άκρο***

Cross over Cable (T568A άκρο 1 – T568B άκρο 2):

RJ45 Ακροδέκτης #(Άκρο 1)	Wire Color	Diagram End #1	RJ45 Ακροδέκτης #(Άκρο 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Συνήθως όταν συνδέουμε διαφορετικούς τύπους συσκευών χρησιμοποιούμε ένα straight-through καλώδιο και όταν συνδέουμε τον ίδιο τύπο συσκευής συνήθως χρησιμοποιούμε ένα crossover καλώδιο.

5.7.Patch Cord

Το patch cord είναι ένα καλώδιο UTP μικρού μήκους (από 1 εως 10 μέτρα) το οποίο τερματίζει σε βίσματα RJ-45 και χρησιμοποιείται για την σύνδεση δικτυακών συσκευών.Ακολουθεί τους ίδιους διαχωρισμούς των UTP καλωδίων που περιγράψαμε παραπάνω και επομένως τα διακρίνουμε σε:

- Straight patch cord
- Crossover patch cord

Εικόνα 38*: UTP patch cords*

6.Τύποι των συνδέσεων ευρείας περιοχής

Εξ' ορισμού οι ευρείας περιοχής συνδέσεις καλύπτουν πολύ μεγάλες αποστάσεις.Αυτές οι αποστάσεις κυμαίνονται αφού περιλαμβάνουν τις συνδέσεις των επικοινωνιών τις οποίες χρησιμοποιούμε προκειμένου να διαχειριστούμε τους λογαριασμούς των ηλεκτρονικών ταχυδρομείων και το άνοιγμα μιας web σελίδας μέχρι την δημιουργία μια τηλεδιάσκεψης μ' ένα πελάτη.

Οι Wide Area συνδέσεις μεταξύ των δικτύων παίρνουν μια σειρά από μορφές περιλαμβανομένων των:

- RJ11 κονεκτόρων των τηλεφωνικών γραμμών για dialup ή Digital Subscriber Line (DSL).
- 60pin σειριακές συνδέσεις.

Εικόνα 39: ***RJ11 κονέκτορας 4 pins –σύνδεση στην τηλεφωνική πρίζα***

Εικόνα 40: ***60pin σειριακές συνδέσεις προς DCE συσκευές***

Εικόνα 41: ***Σύνδεση Router σε τηλεφωνική πρίζα (DSL σύνδεση)***

Data Communication Equipment ή Εξοπλισμός Επικοινωνίας Δεδομένων : Μια συσκευή η οποία παρέχει τις υπηρεσίες χρονισμού σε μια άλλη συσκευή.Συνήθως

αυτή η συσκευή βρίσκεται στο άκρο της σύνδεσης του πάροχου του δικτύου ευρείας περιοχής.

Data Terminal Equipment ή Τερματικός Εξοπλισμός Δεδομένων : Μια συσκευή η οποία δέχεται υπηρεσίες χρονισμού από μια άλλη συσκευή και προσαρμόζεται ανάλογα με τον χρονισμό αυτό.Συνήθως η συσκευή αυτή βρίσκεται το άκρο στο οποίο βρίσκεται ο πελάτης του δικτύου ευρείας περιοχής.

Αν μια σειριακή σύνδεση γίνεται απ' ευθείας στον τηλεπικοινωνιακό πάροχο ή σε μια συσκευή η οποία παρέχει το σήμα του χρονισμού όπως αποτελεί μια Channel Service Unit/Data Service Unit (CSU/DSU) ,ή Κανάλι Υπηρεσίας Μονάδας/Δεδομένα Υπηρεσίας Μονάδας, όπως ένα modem τότε ο δρομολογητής θεωρείται ότι αποτελεί μια DTE συσκευή και θα χρησιμοποιήσει ένα DTE σειριακό καλώδιο.

Τα DTE και τα DCE χρησιμοποιούνται για τις συνδέσεις ευρείας περιοχής.Η επικοινωνία μέσω μιας σύνδεσης διατηρείται παρέχοντας ένα ρυθμό χρονισμού το οποίο είναι αποδεκτό και από τις δύο πλευρές δηλαδή τόσο την συσκευή αποστολής όσο και της συσκευή λήψης.Στις περισσότερες περιπτώσεις ο τηλεπικοινωνιακός πάροχος παρέχει την υπηρεσία χρονισμού η οποία συγχρονίζει το μεταδιδόμενο σήμα.

Τοποθετώντας ένα ρυθμό χρονισμού στον δρομολογητή εφαρμόζεται ένας χρονισμός.Αυτός επιτρέπει στον δρομολογητή να προσαρμόσει τις ταχύτητες στην λειτουργία των επικοινωνιών του και επομένως να συγχρονίζεται με τις συσκευές που είναι συνδεδεμένες σ' αυτόν.

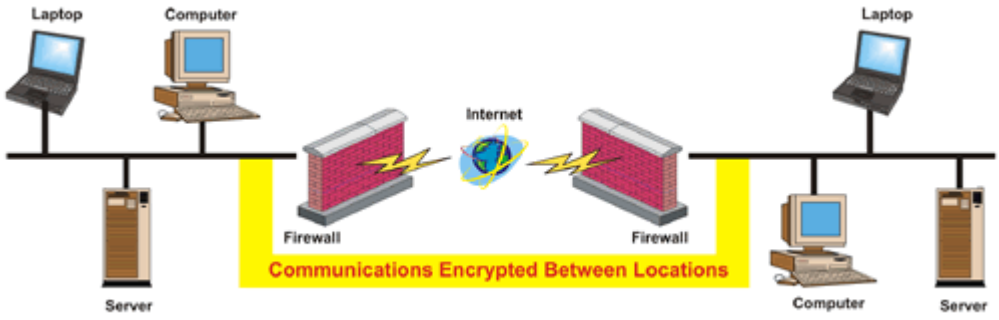
Εικόνα 42: ***WAN σύνδεση μέσω DCE και DTE συσκευών***

Οι δρομολογητές αποτελούν DTE συσκευές εξ' ορισμού αλλά μπορούν να παραμετροποιηθούν για να συμπεριφέρονται σαν DCE συσκευές.

7.Virtual Private Network ή Εικονικό Ιδιωτικό Δίκτυο

Το διαδίκτυο αποτελεί ένα παγκόσμιο ,δημόσια προσβάσιμο IP δίκτυο.Εξαιτίας του γρήγορου και παγκόσμιου πολλαπλασιασμού του, έχει γίνει ένας ελκυστικός τρόπος προκειμένου να διασυνδέσει απομακρυσμένα sites.Το γεγονός ότι αποτελεί μια δημόσια υποδομή μετατοπίζει τους κινδύνους, από τα κενά της ασφάλειας που μπορεί να παρουσιάζει, στους οργανισμούς και στα εσωτερικά τους δίκτυα.Ευτυχώς όμως η VPN τεχνολογία δίνει την δυνατότητα στους οργανισμούς να δημιουργήσουν ιδιωτικά δίκτυα πάνω από την δημόσια υποδομή του διαδικτύου.Τα δίκτυα αυτά διατηρούν την εμπιστευτικότητα και την ασφάλεια.

Οι οργανισμοί χρησιμοποιούν τα VPNs προκειμένου να παράσχουν μια εικονική υποδομή δικτύου ευρείας περιοχής που να συνδέει υποκαταστήματα, οικιακά γραφεία, sites συνεργατών και απομακρυσμένη τηλεεργασία από κάθε κομμάτι του δικτύου του οργανισμού.Για να διατηρήσουμε την ιδιωτικότητα η κυκλοφορία κρυπτογραφείται.Αντι για να χρησιμοποιήσουμε μια αφοσιωμένη επιπέδου 2 σύνδεση, όπως είναι η μισθωμένη γραμμη, το VPN χρησιμοποιεί εικονικές συνδέσεις οι οποίες δρομολογούνται μέσα από το διαδίκτυο.



Εικόνα 43: ***VPN σύνδεση***

Φανταστείται το διαδίκτυο σαν ένα γήπεδο το οποίο αποτελεί μια δημόσια τοποθεσία.Όταν ο αγώνας τελείωσει οι φίλαθλοι φεύγουν μέσα από τους κοινόχρηστους διαδρόμους και τις κοινόχρηστες πόρτες στριμώχνοντας και παρεμποδίζοντας ο ένας τον άλλο καθόλη την διαδρομή.Όλο αυτό τον συνωστισμό μπορούν να τον εκμεταλλευτούν πιθανοί κλέφτες.

Φέρτε στο μυαλό σας την εικόνα για το πώς φεύγουν οι υψηλοί προσκεκλημένοι.Οι άντρες της ασφάλειας του γηπέδου δημιουργούν ένα ασφαλή διάδρομο και προστατεύουν τους προσκεκλημένους προκειμένου να μην έρθουν σε επαφή με τον υπόλοιπο κόσμο.Οι άντρες της ασφάλειας μπορούμε να πούμε ότι δημιουργούν ένα τούνελ.Οι προσκεκλημένοι οδηγούνται μέσα από το εικονικό τούνελ στα αυτοκίνητα τους τα οποία και τελικά τους οδηγούν στους προορισμούς τους.Το VPN δουλεύει με ανάλογο τρόπο συσκευάζοντας τα δεδομένα και μεταφέροντας τα με ασφάλεια κατά μήκος του διαδικτύου και μέσα από προστατευμένα τούνελ.

7.1.Αντιστοιχία:Κάθε τοπικό δίκτυο αποτελεί ένα νησί

Θα χρησιμοποιήσουμε ακόμα μια αναλογία προκειμένου να συλλάβουμε την εικόνα του VPN.Φανταστείτε ότι κατοικείται σ' ένα νησί στην μέση ενός ωκεανού.Υπάρχουν χιλιάδες άλλα νησιά γύρω από το δικό σας, μερικά πιο κοντινά και μερικά περισσότερο απονμακρυσμένα.Ο φυσιολογικός τρόπος για να ταξιδέψετε σε κάποιο από αυτά είναι να πάρετε το πλοίο που κατευθύνεται προς το νησί αυτό.Το ταξίδι με ένα πλοίο σημαίνει ότι διατηρείται εν μέρει την ιδιωτικότητα σας.Οτι και αν κάνετε θα είναι ορατό και από άλλους επιβάτες.

Υποθέστε ότι κάθε νησί αναπαριστά ένα ιδιωτικό τοπικό δίκτου και ότι ο ωκεανός αποτελεί το διαδίκτυο.Όταν ταξιδεύετε με το πλοίο είναι παρόμοιο με την σύνδεση σας σ' ένα web διακομιστή ή σε κάποια άλλη συσκευή μέσα από το διαδίκτυο.Δεν έχετε τον έλεγχο πάνω από τα καλώδια και τους δρομολογητές οι οποίοι διαμορφώνουν το διαδίκτυο με παρόμοιο τρόπο με τον οποίο δεν έχετε τον έλεγχο στους συνεπιβάτες που σας αντικρίζουν πάνω στο πλοίο.Το γεγονός αυτό σας αφήνει εκτεθειμένους σε ζητήματα ασφάλειας, στην προσπάθεια σας να συνδέσετε δύο ιδιωτικά δίκτυα με την χρησιμοποίηση ενός δημόσιου πόρου.

Το νησί στο οποίο κατοικείται αποφασίζει να χτίσει μια γέφυρα προς κάποιο άλλο νησί έτσι ώστε να υπάρχει ένας ευκολότερος,περισσότερο ασφαλής και ευθύς δρόμος για τους ανθρώπους προκειμένου να ταξιδέψουν ανάμεσα στα δύο νησιά.Είναι όμως ακριβό να χτίσεις και να διατηρήσεις μια γέφυρα ακόμα και αν το νησί με το οποίο θα συνδεθεί είναι πολύ κοντά.Αλλά η ανάγκη για αξιοπιστία και ασφάλεια σας οδηγεί να πραγματοποιήσετε το εγχείρημα.

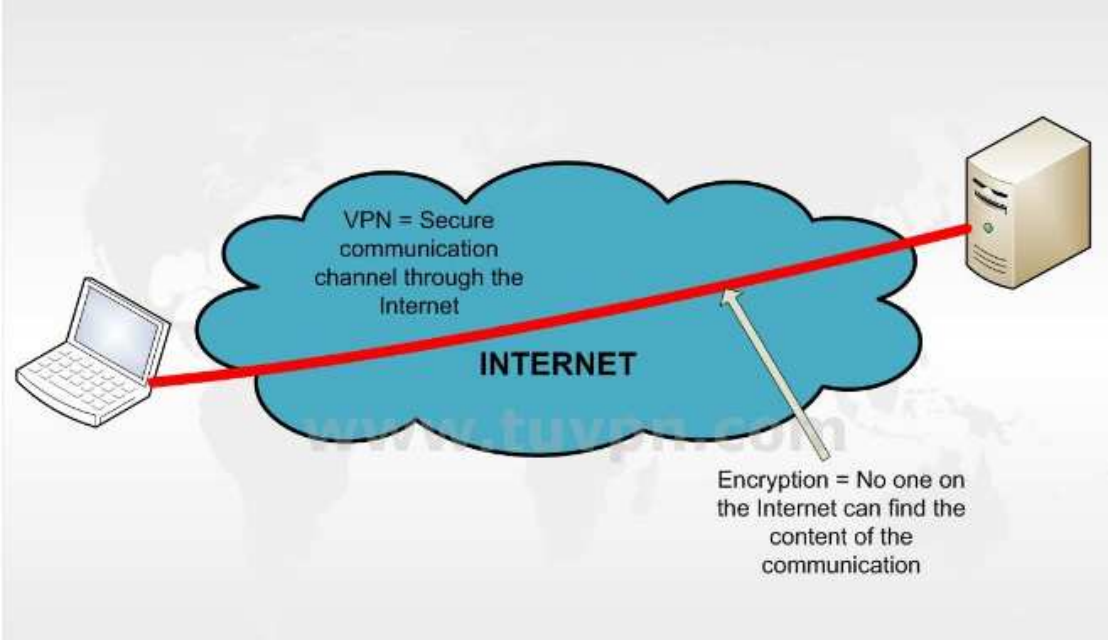
Η παραπάνω κατάσταση είναι σαν να έχεις μια μισθωμένη γραμμή.Οι γέφυρες (μισθωμένες γραμμές) είναι ανεξάρτητες από τον ωκεανό (διαδίκτυο) αλλά μπορούν να συνδεθούν στα νησιά (τοπικά δίκτυα).Πολλές εταιρείες επέλεξαν αυτή την κατεύθυνση εξαιτίας της ανάγκης για αξιοπιστία και ασφάλεια προκειμένου να συνδεθούν στα απομακρυσμένα γραφεία τους.Παρόλαυτα αν τα απομακρυσμένα γραφεία είναι πολύ μακριά το κόστος είναι απαγορευτικό – σαν να προσπαθήσουμε να χτίσουμε μια γέφυρα που να καλύπτει μια πολύ μεγάλη απόσταση.

Με ποιο τρόπο λοιπόν το VPN αναμειγνύεται σε αυτή την κατάσταση;Θα μπορούσαμε να δώσουμε σε κάθε κάτοικο του νησιού ένα μικρό υποβρύχιο με τα ακόλουθα χαρακτηριστικά:

- Ταχύτητα
- Ευκολία στην μετακίνηση
- Ικανότητα να μας κρύψει εντελώς από άλλα πλοία ή υποβρύχια
- Αξιόπιστο
- Μικρό κόστος η επιπρόσθετη απόκτηση και άλλων υποβρυχίων τα οποία θα εμπλουτίσουν τον στόλο σας από την στιγμή που αποκτήσατε το πρώτο σας.

Αν και ταξιδεύουν στον ωκεανό μαζί με άλλα πλοία, οι κάτοικοι των δύο νησιών μπορούν να ταξιδέψουν μπροστά και πίσω όποτε και αν το θελήσουν διατηρώντας

την ιδιωτικότητα και την ασφάλεια τους.Αυτός είναι ο τρόπος με τον οποίο ένα VPN δουλεύει.Κάθε απομακρυσμένο μέλος του δικτύου σας μπορεί να επικοινωνήσει με ένα ασφαλή και αξιόπιστο τρόπο χρησιμοποιώντας το διαδίκτυο σαν το μέσο προκειμένου να συνδεθεί σ' ένα ιδιωτικό τοπικό δίκτυο.Το VPN μπορεί να αναπτυχθεί προκειμένου να εξυπηρετήσει περισσότερους χρήστες και περισσότερες τοποθεσίες με μεγαλύτερη ευκολία από ότι μια μισθωμένη γραμμή.Στην πραγματικότητα η επεκτασιμότητα αποτελεί ένα μεγάλο πλεονέκτημα που διαθέτουν τα VPN σε σύγκριση με τις μισθωμένες γραμμές.Αντίθετα με τις μισθωμένες γραμμές όπου το κόστος αυξάνεται ανάλογα με τις αποστάσεις,οι γεωγραφικές τοποθεσίες των απομακρυσμένων γραφείων δεν παίζουν ρόλο κατά την δημιουργία των VPN.



Εικόνα 44: VPN - κανάλι ασφαλούς επικοινωνίας μέσα από το Internet

7.2.Τα VPNs και τα πλεονεκτήματα τους

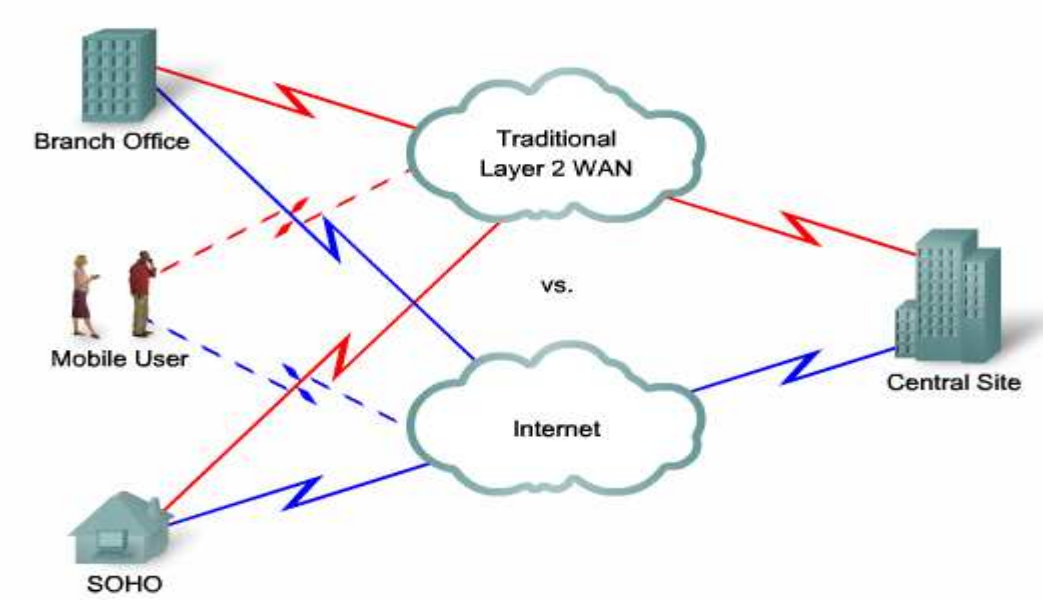
Οι οργανισμοί οι οποίοι χρησιμοποιούν τα VPNs επωφελούνται από την ελαστικότητα και την παραγωγικότητα τους.Τα απομακρυσμένα sites και οι τηλεεργαζόμενοι μπορούν να συνδεθούν με ασφάλεια στο εταιρικό δίκτυο από οποιοδήποτε τοποθεσία.Τα δεδομένα σ' ένα VPN είναι κρυπτογραφημένα και ακατανόητα σε κάποιον ο οποίος δεν δικαιούται να έχει πρόσβαση σ' αυτά.Τα VPNs φέρνουν τους απομακρυσμένους χρήστες μέσα στον τείχο προστασίας δίνοντας τους πρόσβαση στις δικτυακές συσκευές σε επίπεδα ανάλογα σαν να βρίσκονταν στα εταιρικά γραφεία.

Η εικόνα 45 απεικονίζει τις μισθωμένες γραμμές με το κόκκινο χρώμα.Οι μπλέ γραμμές αναπαριστούν τις VPN συνδέσεις.Θα πρέπει να λάβετε υπόψιν σας τα ακόλουθα πλεονεκτήματα όταν χρησιμοποιείται τα VPNs:

- **Είναι οικονομικά** – Οι οργανισμοί μπορούν να χρησιμοποιήσουν μια αποτελεσματικού κόστους και έμμεσου τρόπου, μεταφορά μέσα από το

διαδίκτυο προκειμένου να συνδέσουν απομακρυσμένους χρήστες στο εταιρικό site.Το γεγονός αυτό εξαλείφει τις ακριβές αφοσιωμένες συνδέσεις ευρείας περιοχής.Χρησιμοποιώντας μια γρήγορη σύνδεση τα VPNs μείωνουν τα κόστη της συνδεσιμότητας την ίδια στιγμή που αυξάνουν την ευρυζωνικότητα της απομακρυσμένης σύνδεσης.

- **Είναι ασφαλή** – Πρωτόκολα προηγμένης κρυπτογράφησης και πιστοποίησης προστατεύουν τα δεδομένα από την αυθαίρετη πρόσβαση.
- **Έχουν δυνατότητα επέκτασης** – Τα VPNs χρησιμοποιούν την υποδομή του Internet μέσα από τους Internet Service Providers (ISPs) δηλαδή τους τηλεπικοινωνιακούς παρόχους καθιστώντας εύκολη την πρόσθεση νέων χρηστών από τους οργανισμούς.Οι οργανισμοί μεγάλοι και μικροί είναι ικανοί να προσθέσουν μεγάλη ποσότητα χωρητικότητας χωρίς να χρειάζεται να προσθέσουν σημαντική υποδομή.



Εικόνα 45: ***Σύγκριση μισθωμένων γραμμών και VPN συνδέσεων***

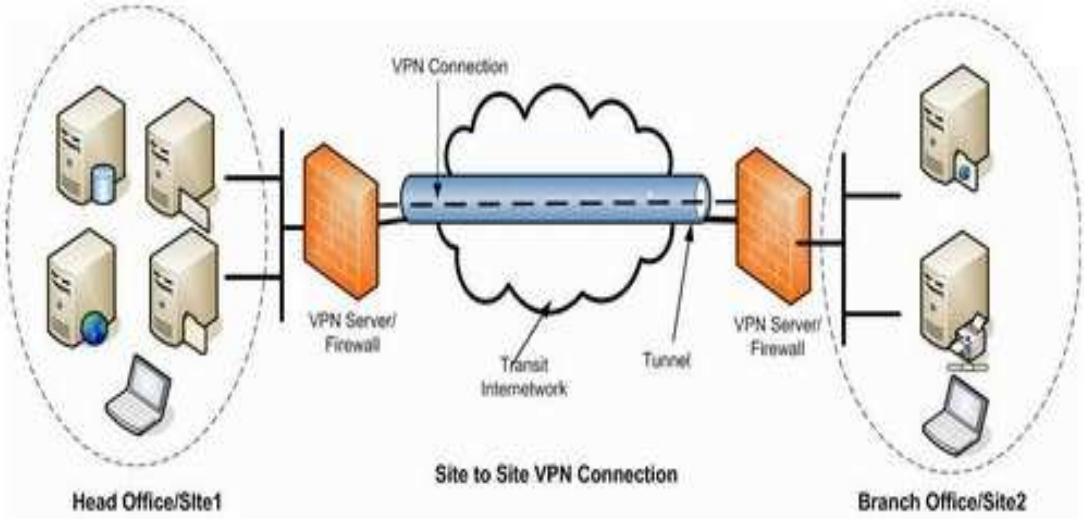
Τύποι των VPNs

7.3.Site to site VPNs

Οι οργανισμοί χρησιμοποιούν site-to-site VPNs προκειμένου να συνδέσουν απομακρυσμένες τοποθεσίες με τον ίδιο τρόπο όπως μια μισθωμένη γραμμή ή μια σύνδεση μέσω Frame-Relay.Επειδή οι περισότεροι οργανισμοί έχουν πρόσβαση στο διαδίκτυο αποκτά νόημα να εκμεταλλευτούμε τα πλεονεκτήματα που συνοδευούν τα site-to-site VPNs.Όπως φαίνετε στο σχήμα τα site-to-site VPNs επίσης υποστηρίζουν τα εταιρικά intranet και τα extranet των συνεργαζόμενων εταιρειών.

Το site-to-site (από τοποθεσία σε τοποθεσία) VPN αποτελεί μια προέκταση του κλασικού δικτύου ευρείας περιοχής συνδέοντας ολόκληρα δίκτυα μεταξύ τους.Για παράδειγμα μπορούν να συνδέσουν ένα υποκατάστημα μιας εταιρείας στο κεντρικό δίκτυο της εταιρείας.

Στα site-to-site VPNs οι χρήστες στέλνουν και δέχονται TCP/IP κυκλοφορία μέσα από μια VPN έξοδο (gateway) η οποία μπορεί να είναι ένας δρομολογητής,μια εφαρμογή τείχου προστασίας ή μια συσκευή Adaptive Security Appliance (ASA) ή μια Εφαρμογή Δυναμικής Ασφλαλειας.Η VPN έξοδος είναι υπεύθυνη για την ενθυλάκωση και την κρυπτογράφηση της εξωτερικής κυκλοφορίας από ένα συγκεκριμένο site και την αποστολή της μέσα από ένα VPN τούνελ πάνω από το διαδίκτυο και μέχρι μια ομότιμη VPN έξοδο η οποία βρίσκεται στο site στο οποίο απευθυνόμαστε.Κατα την αποδοχή των δεδομένων από την VPN έξοδο του παραλήπτη αφαιρούνται οι επικεφαλίδες, αποκρυπτογραφούνται τα περιεχόμενα και μεταφέρονται τα πακέτα προς τον χρήστη προορισμού μέσα στο ιδιωτικό δίκτυο.



Εικόνα 46: ***Site to site VPN***

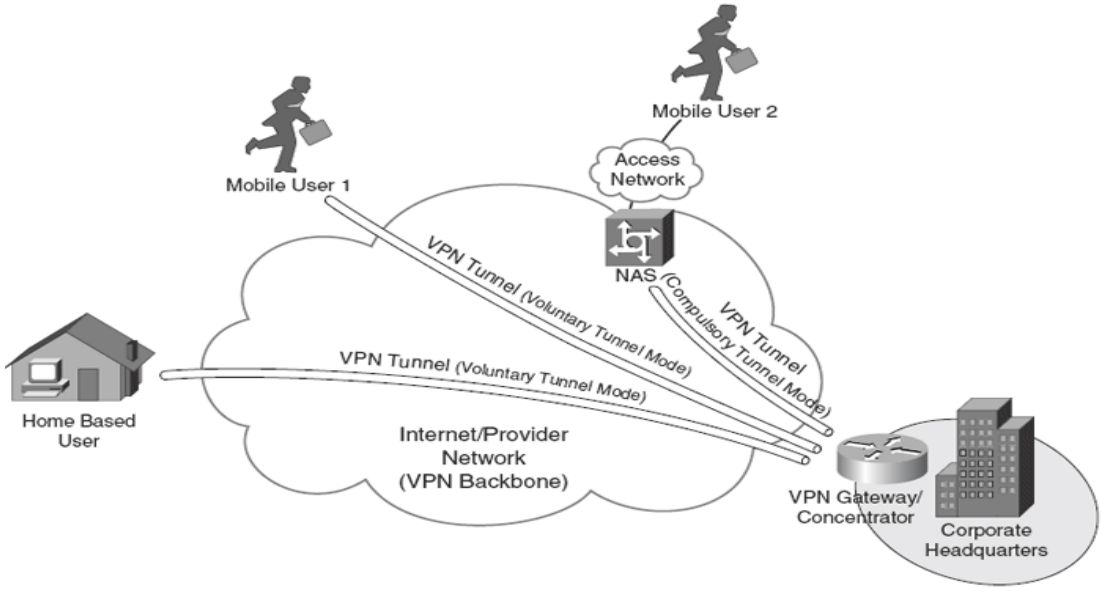
7.4.VPN για απομακρυσμένοι χρήστες

Οι κινητοί χρήστες και οι τηλεεργαζόμενοι χρησιμοποιούν τα VPNs απομακρυσμένης πρόσβασης εκτεταμένα.Στο παρελθόν οι επιχειρήσεις υποστήριζαν τους απομακρυσμένους χρήστες μέσα από σύνδεση δικτύων μέσω τηλεφώνου (dialup).Αυτό περιλάμβανε μια κλήση από ένα τηλέφωνο, και η οποία επιβάρυνε την εταιρεία με μεγάλο κόστος.

Οι περισσότεροι τηλεεργαζόμενοι πλέον έχουν πρόσβαση στο διαδίκτυο από τα σπίτια τους και μπορούν να εγκαταστήσουν απομακρυσμένα VPNs χρησιμοποιώντας γρήγορες συνδέσεις.Παρόμοια ένα κινούμενος χρήστης μπορεί να πραγματοποιήσει μια τοπική κλήση σ’ έναν τοπικό τηλεπικοινωνιακό πάροχο προκειμένου να έχει πρόσβαση στην εταιρεία μέσα από το διαδίκτυο.Σαν αποτέλεσμα, το παραπάνω, αποτελεί μια επαναστατική προσέγγιση σε σχέση με τα δίκτυα μέσω τλεφώνου.Τα απομακρυσμένα πρόσβασης VPNs μπορούν να υποστηρίξουν τις ανάγκες των τηλεεργαζόμενων όπως επίσης και των κινούμενων χρηστών.

Σ’ ένα VPN απομακρυσμένης πρόσβασης κάθε χρήστης συνήθως έχει ένα VPN λογισμικό.Κάθε φορά που ο χρήστης προσπαθεί να αποστείλει κυκλοφορία, το VPN λογισμικό ενθυλακώνει και κρυπτογραφεί αυτή την κυκλοφορία πριν την στείλει στο

διαδίκτυο και στη VPN έξοδο στην άλλη άκρη του δικτύου προορισμού.Κατα την παράδοση η VPN έξοδος διαχειρίζεται τα δεδομένα με τον ίδιο τρόπο όπως θα διαχειριζόταν από ένα site-to-site VPN.



Εικόνα 47: ***VPN για απομακρυσμένους χρήστες***

7.5.Συστατικά VPN

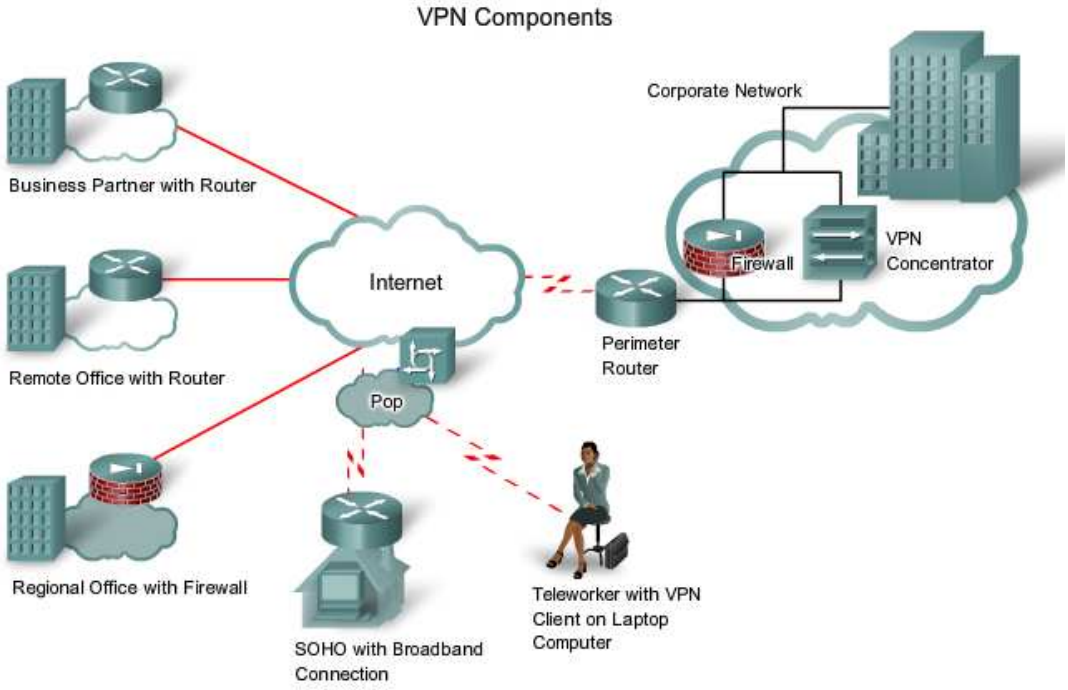
Το VPN δημιουργεί ένα ιδιωτικό δίκτυο πάνω από την υποδομή ενός δημόσιου δικτύου ενώ παράλληλα διατηρεί την εμπιστευτικότητα και την ασφάλεια.Τα VPNs χρησιμοποιούν πρωτόκολα κρυπτογραφημένων τούνελ για να παράσχουν προστασία απέναντι στην υποκλοπή πακέτων,στην πιστοποίηση του αποστολέα και την ακεραιότητα των μηνυμάτων.

Το σχήμα απεικονίζει μια τυπική VPN τοπολογία.Τα συστατικά τα οποία απαιτούνται προκειμένου να εγκαταστήσουμε αυτό το VPN περιλαμβάνουν:

- Ένα δίκτυο με διακομιστέςκαι σταθμούς εργασίας
- Μια σύνδεση στο διαδίκτυο
- VPN εξόδους όπως είναι οι δρομολογητές,τα τείχη προστασίας,οι VPN συγκεντρωτές (concentrators) και τα ASAs τα οποία και λειτουργούν σαν τερματικά σημεία που εγκαθιστούν,διαχειρίζονται και ελέγχουν τις VPN συνδέσεις.
- Κατάλληλο λογισμικό προκειμένου να δημιουργηθούν και να διαχειρίστούν τα VPN τούνελ.

Το κλειδί για την αποτελεσματικότητα του VPN είναι η ασφάλεια.Τα VPNs ασφαλίζουν τα δεδομένα μέσα από την ενθυλάκωση ή την κρυπτογράφηση.Τα περισσότερα VPNs μπορούν να πραγματοποιήσουν και τα δύο.

- Η ενθυλάκωση αναφέρεται και σαν tunneling γιατί η ενθυλάκωση μεταδίδει τα δεδομένα ευκρινός από δίκτυο σε δίκτυο μέσα από μια κοινόχρηστη δικτυακή υποδομή.
- Οι κώδικες κρυπτογράφούν τα δεδομένα σε διαφορετικές μορφές χρησιμοποιώντας ένα μυστικό κλειδί.Η αποκρυπτογράφηση αποκωδικοποιεί τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή.



Εικόνα 48: ***Συστατικά διαμόρφωσης VPN***

7.6.Χαρακτηριστικά ασφάλειας των VPNs

Τα VPNs χρησιμοποιούν προηγμένη κρυπτογράφηση και την κατασκευή σήραγγας (tunneling) προκειμένου να δίνει την δυνατότητα στους οργανισμούς να παρέχουν ασφάλεια από άκρο σε άκρο πάνω από ιδιωτικές συνδέσεις δικτύου στο διαδίκτυο.

Το θεμέλιο της ασφάλειας ενός VPN αποτελεί η εμπιστευτικότητα των δεδομένων,η ακεραιότητα και η πιστοποίηση:

- **Η εμπιστευτικότητα των δεδομένων** – Κάτι το οποία λαμβάνουμε συχνά υπόψιν μας, όσο αναφορά την ασφάλεια, αποτελούν οι ωτακουστές (κρυφακούω).Χαρακτηριστικό του αρχικού σχεδιασμού αποτελεί η προστασία του περιεχομένου των μηνυμάτων από εξωτερικές παρεμβάσεις.Τα VPNs επιτυγχάνουν την εμπιστευτικότητα χρησιμοποιώντας μηχανισμούς ενθυλάκωσης και κρυπτογράφησης.
- **Η ακεραιότητα των δεδομένων** – Οι παραλήπτες δεν έχουν κανένα έλεγχο πάνω στην διαδρομή πάνω από την οποία τα δεδομένα μεταφέρθηκαν και επομένως δεν μπορούν να γνωρίζουν αν τα δεδομένα έχουν παρακολουθηθεί ή αν έχουν διαχειριστεί από κάποιον καθώς ταξίδεψαν μέσα από το διαδίκτυο.Υπάρχει πάντα η πιθανότητα τα δεδομένα να έχουν τροποιηθεί.Η

ακεραιότητα των δεδομένων εγγυάται ότι καμμία αλλοίωση ή μετατροπή δεν πραγματοποιήθηκαν στα δεδομένα κατά την διαδρομή τους από την πηγή προς τον προορισμό.Τα VPNs συνήθως χρησιμοποιούν τους κατακερματισμούς (hashes) για να διασφαλίσουν την ακεραιότητα των δεδομένων.Ο κατακερμαστισμός είναι κάτι σαν ελεγκτικό άθροισμα ή σαν σφράγισμα το οποίο και εγγυάται ότι κανένας δεν έχει διαβάσει το περιεχόμενο τους.

- **Πιστοποίηση** – Η πιστοποιήση διασφαλίζει ότι τα μηνύματα προέρχονται από μια αυθεντική πηγή και πηγαίνουν προς ένα αυθεντικό προορισμό.Η ταυτοποιήση του χρήστη αποτελεί τη πιστοποιήση ότι το κομμάτι του δικτύου με το οποίο ο χρήστης εγκαθιδρύει μια σύνδεση είναι ακριβώς το κομμάτι το οποίο εκείνος επικοινωνεί και όχι κάποιο άλλο.Τα VPNs μπορούν να χρησιμοποιήσουν κωδικούς πρόσβασης και ψηφιακές πιστοποιήσεις προκειμένου να διαμορφώσουν την ταυτότητα των τμημάτων στην άλλη άκρη του δικτύου.

7.7.Κατασκευή σήραγγας VPN (Tunneling)

Ενσωματώνοντας τις δυνατότητες εμπιστευτικότητας στα δεδομένα μέσω του VPN, διασφαλίζεται ότι μόνο οι επιδιωκόμενες πηγές και οι επιδιωκόμενοι προορισμοί είναι ικανά να μεταφράσουν το περιεχόμενο των δεδομένων.

Η κατασκευή σήραγγας επιτρέπει τη χρήση των δημόσιων δικτύων όπως είναι το διαδίκτυο προκειμένου να μεταφέρει τα δεδομένα στους χρήστες με τέτοιο τρόπο σαν να είχαν πρόσβαση οι χρήστες σ’ ένα ιδιωτικό δίκτυο.Η κατασκευή σήραγγας ενθυλακώνει ολόκληρο το πακέτο μέσα σ’ ένα άλλο πακέτο και στέλνει το νέο διαμορφωμένο πακέτο στο δίκτυο.Το σχήμα ταξινομεί της τρείς τάξεις των πρωτοκόλων που το tunneling χρησιμοποιεί.

Προκειμένου να αντιληφθούμε την έννοια της κατασκευής σήραγγας και τις τάξεις των tunneling πρωτοκόλλων θεωρείστε ότι είμαστε σ’ ένα νησί και στέλνουμε μια κάρτα διακοπών μέσα απο το παραδοσιακό ταχυδρομείο.Η κάρτα έχει γραμμένο ένα μήνυμα πάνω της.Η κάρτα αποτελεί τον επιβάτη του πρωτοκόλλου.Ο αποστολέας τοποθετεί την κάρτα μέσα σ’ ένα φάκελο (πρωτόκολλο ενθυλάκωσης) με την κατάλληλη διεύθυνση γραμμένη.Ο αποστολέας στην συνέχεια ρίχνει το φάκελο στο ταχυδρομικό κουτί για την μεταφορά του.Το ταχυδρομικό σύστημα (το πρωτόκολλο μεταφοράς) παίρνει και μεταφέρει τον φάκελο στο ταχυδρομικό κουτί του παραλήτη.Τα δύο τερματικά σημεία στο σύστημα μεταφοράς αποτελούν τα tunnel interfaces.Ο παραλήπτης αφαιρεί την κάρτα από τον φάκελο (αποσπά το πρωτόκολο του επιβάτη) και διαβάζει τα μηνυμα.

Η εικόνα απεικονίζει ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο μεταφέρεται μέσα από το διαδίκτου και πάνω από μια VPN σύνδεση.Το Point-to-Point (από σημείο σε σημείο) πρωτόκολο μεταφέρει το μήνυμα στην VPN συσκευή όπου το μήνυμα ενθυλακώνεται μέσα σ’ ένα Generic Route Encapsulation (GRE) πακέτο ή σε μια Γενικής Δρομολόγησης Ενθυλάκωση.Το GRE αποτελεί ένα tunneling πρωτόκολο

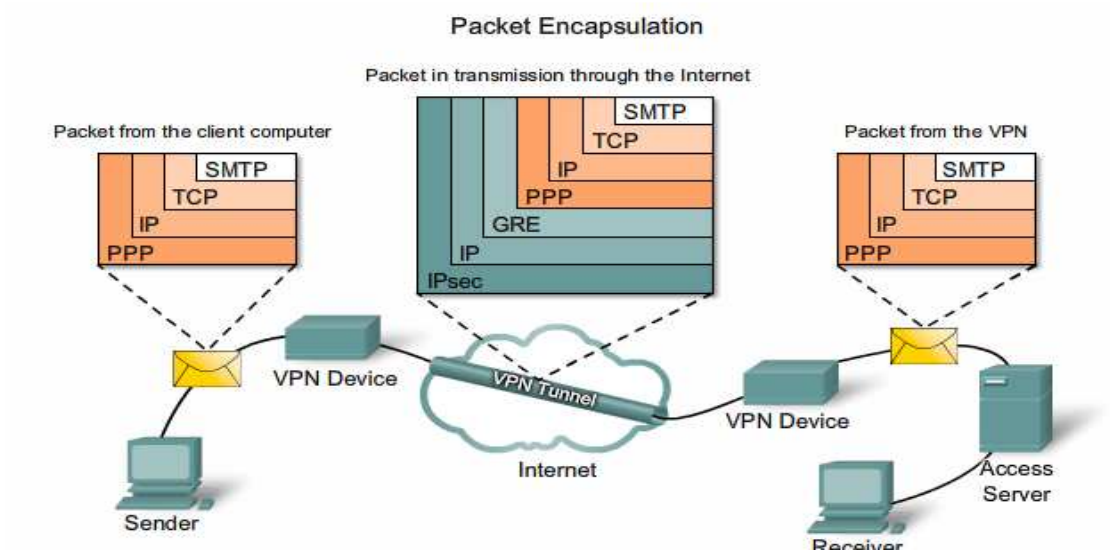
το οποίο μπορεί και ενθυλακώνει μια μεγάλη ποικιλία από διαφορετικούς τύπους πρωτοκόλων που φέρουν τα πακέτα, μέσα σε IP tunnels και δημιουργεί μια εικονική Point-to-point σύνδεση με δρομολοογητές σε απομακρυσμένα σημεία και πάνω από ένα IP δίκτυο.Στο σχήμα το εξωτερικό πακέτο της πηγής και η διεύθυνση του προορισμού αναθέτονται στα tunnel interfaces και καθίστονται δρομολογητέα κατά μήκος του δικτύου.Απο την στιγμή που ένα σύνθετο πακέτο προσσεγίζει το tunnel interface του προρισμού το εσωτερικό πακέτο αποσπάται.

7.8.Πρωτόκολλα tunneling

Carrier Protocol ή Πρωτόκολλο Μεταφοράς: Το πρωτόκολο πανω από το οποίο η πληροφορία ταξιδεύει (Frame Relay, ATM, MPLS).

Encapsulating Protocol ή Πρωτόκολλο Ενθυλάκωσης: Το πρωτόκολο το οποίο τυλίγεται πάνω από τα αρχικά δεδομένα (GRE, L2F, PPTP, L2TP).

Passenger Protocol ή Πρωτόκολλο Επιβάτη: Το πρωτόκολο πάνω από το οποίο τα αρχικά δεδομένα μεταφέρθηκαν (IPX, AppleTalk, IPv4, IPv6).



Εικόνα 49: ***Πρωτόκολλα tunneling***

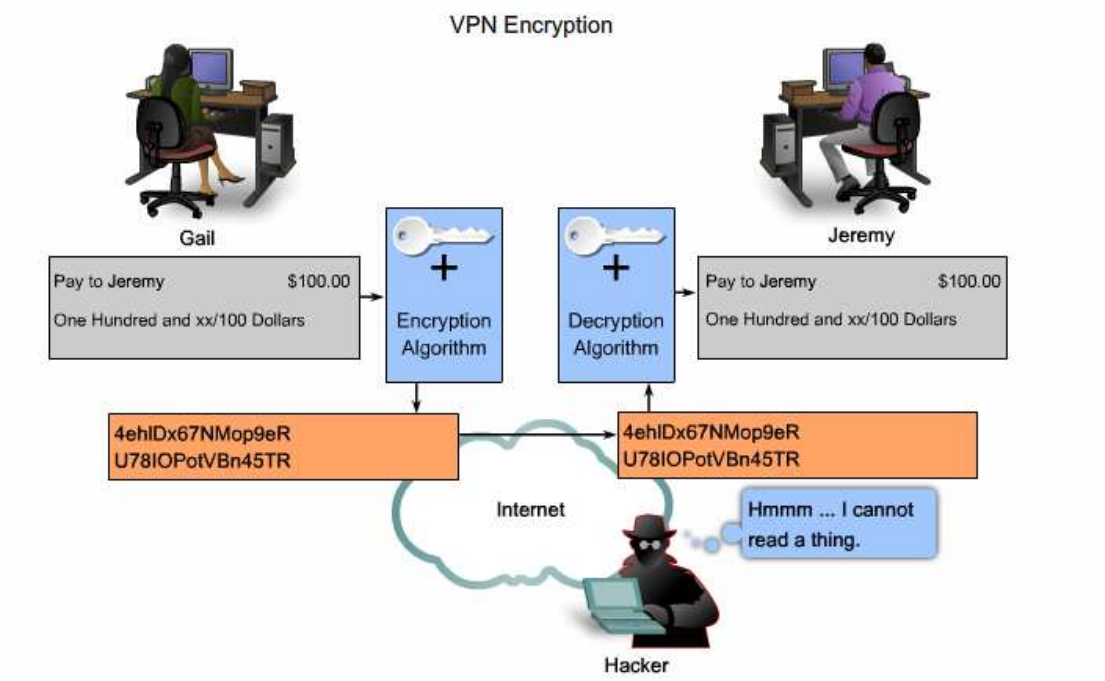
7.9.VPN κρυπτογράφηση

Αν τα δεδομένα ενός απλού κειμένου μεταφέρονται πάνω από ένα δημόσιο δίκτυο μπορούν να υποκλαπούν και να διαβαστούν.Προκειμένου να διατηρήσουμε τα δεδομένα ιδιωτικά θα πρέπει να τα κρυπτογραφήσουμε.Η VPN κρυπτογράφηση κρυπτογραφεί τα δεδομένα και τα καθιστά μη αναγνώσιμα σε αυθάιρετους αποδέκτες.

Προκειμένου να λειτουργήσει η κρυπτογράφηση τόσο ο αποστολέας όσο και ο παραλήπτης θα πρέπει να γνωρίζουν τους κανόνες οι οποίες χρησιμοποιήθηκαν προκειμένου να μεταμορφωθεί το αρχικό μήνυμα στην κωδικοποιημένη μορφή του.Οι κανόνες κρυπτογράφησης του VPN περιλαμαμβάνουν ένα αλγόριθμο και ένα κλειδί.Ο αλγόριθμος αποτελεί μια μαθηματική λειτουργία η οποία συνδιάζει ένα

μήνυμα , ένα κείμενο, κάποια ψηφία ή και τα τρία, με ένα κλειδί.Το αποτέλεσμα είναι μια μη αναγνώσιμη κρυπτογραφημένη συμβολοσειρά.Η αποκωδικοποίηση είναι αδύνατη χωρίς το σωστό κλειδί.

Στο παρακάτω παράδειγμα η Gail θέλει να στείλει ένα οικονομικό έγγραφο στον Jeremy μέσα από το Internet.Η Gail και ο Jeremy συμφώνησαν προηγουμένως για ένα κοινόχρηστο κλειδί.Στο άκρο της Gail, το VPN λογισμικό συνδιάζει το έγγραφο με το κοινόχρηστο κλειδί και τα περνάει μέσα από τον αλγόριθμο κρυπτογράφησης.Το αποτέλεσμα είναι ένα μη αναγνώσιμο κρυπτογραφημένο κείμενο.Το κρυπτογραφημένο κείμενο στη συνέχεια στέλνεται μέσα από το VPN tunnel πάνω από το διαδίκτυο.Στο άλλο άκρο το μήνυμα επανασυνδίαζεται με το ίδιο κοινόχρηστο μυστικό κλεδί και επεξεργάζονται από τον ίδιο αλγόριθμο κρυπτογράφησης.Το αποτέλεσμα είναι το αρχικό οικονομικό έγγραφο το οποίο πλέον είναι αναγνώσιμο από τον Jeremy.



Εικόνα 50: ***VPN κρυπτογράφηση***

7.9.1.Ακεραιότητα των δεδομένων στο VPN

Το επίπεδο ασφάλειας που παρέχεται από ένα αλγόριθμο κρυπτογράφησης εξαρτάται από το μήκος του κλειδιού.Ο χρόνος ο οποίος απαιτείται για κάθε κλειδί προκειμένου αυτό να επεξεγαστεί όλες τις πιθανότητες προκειμένου να αποκρυπτογραφήσει το κωδικοποιημένο κείμενο είναι μια λειτουργία η οποία εξαρτάται από την υπολογιστική ικανότητα του υπολογιστή μας.Επομένως όσο μικρότερο το κλειδί τόσο

ευκολότερο να σπάσει αλλά την ίδια στιγμή και τόσο ευκολότερο να εμφανιστεί το κρυπτογραφημένο μήνυμα.

Μερικοί από τους πιο συνηθισμένους αλγόριθμους κρυπτογράφησης μαζί με το μήκος του κλειδιού που αυτοί χρησιμοποιούνε είναι οι ακόλουθοι:

- **Data Encryption Standard** ή Πρότυπο Κρυπτογράφησης Δεδομένων (DES) αλγόριθμος – Ανεπτυγμένος από την IBM το DES χρησιμοποιεί ένα 56-bit κλειδί εξασφαλίζοντας υψηλή απόδοσης κρυπτογράφηση.Το DES αποτελεί ένα συμμετρικό κλειδί κρυπτογράφησης.
- **Triple DES** (3DES) αλγόριθμος – Μια καινούργια παραλλάγη του DES το οποίο κρυπτογραφεί με ένα κλειδί ,αποκρυπτογραφεί με ένα άλλο κλειδί και στην συνέχεια κρυπτογραφεί για μια τελευταία φορά με κάποιο άλλο κλειδί.Το 3DES παρέχει πολύ μεγαλύτερο σθένος στην διαδικασία κρυπτογράφησης.
- **Advanced Encryption Standard (AES)** ή Πρότυπο Ανεπτυγμένης Κρυπτογράφησης – Το διεθνές ινστιτούτο των προτύπων και τεχνολογίας (NIST) υιοθέτησε το AES προκειμένου να αντικαταστήσει την υπάρχουσα DES κρυπτογράφηση στις κρυπτογραφικές συσκευές.Το AES παρέχει μεγαλύτερη ασφάλεια συγκριτικά με το DES και έχει μεγαλύτερη υπολογιστική ισχύ από το 3DES.Το AES προσφέρει τρία διαφορετικά μήκη κλειδιών :128,192 και 256 bit κλειδιά.
- **Rivest ,Shamir και Adleman (RSA)** – Ένα ασσύμετρο κλειδί κρυπτογράφησης.Τα κλειδιά έχουν μήκος 512, 768, 1024 ή και μεγαλύτερο.

7.9.2.Συμμετρική Κρυπτογράφηση

Οι αλγόριθμοι κρυπτογράφησης όπως οι DES και 3DES απαιτούν ένα κοινόχρηστο κλειδί προκειμένου να πραγματοποιήσουν την κρυπτογράφηση και την αποκρυπτογράφηση.Καθένας από τους δύο υπολογιστές θα πρέπει να γνωρίζει το κλειδί προκειμένου να αποκωδικοποιήσει την πληροφορία.Με το κλειδί της συμμετρικής κρυπτογράφησης, το οποίο επίσης ονομάζεται και μυστικό κλειδί κρυπτογράφησης, κάθε υπολογιστής κρυπτογραφεί την πληροφορία πριν να την στείλει στο δίκτυο στο οποίο βρίκεται τοποθετημένος ο άλλος υπολογιστής.Το κλειδί της συμμετρικής κρυπτογράφησης απαιτεί γνώση για το ποιοί υπολογιστές θα επικοινωνήσουν μεταξύ τους έτσι ώστε το ίδιο κλειδί να εφαρμοστεί σε κάθενα απ' αυτούς.

Για παράδειγμα ένας αποστολέας δημιουργεί ένα κωδικοποιημένο μήνυμα όπου το κάθε γράμμα αντικαθιστάται με το γράμμα που βρίσκεται δύο σειρές πιο κάτω στην αλφαβήτα.Για παράδειγμα το Α αντικάθισταται από το Γ,το Β από το Ε κ.ο.κ.Σ' αυτή την περίπτωση η λέξη ΚΡΥΦΟ γίνετε ΜΤΧΨΡ.Ο αποστολέας έχει ήδη πεί στον παραλείπτη ότι το μυστικό κλειδί έχει «μετακινηθεί κατά 2».Όταν ο παραλήπτης λαμβάνει λαμβάνει το μήνυμα ΜΤΧΨΡ ο υπολογιστής αποκωδικοποιεί το μήνυμα μετατοπίζοντας κάθε γράμμα προς τα πίσω κατά δύο και υπολογίζει την λέξη

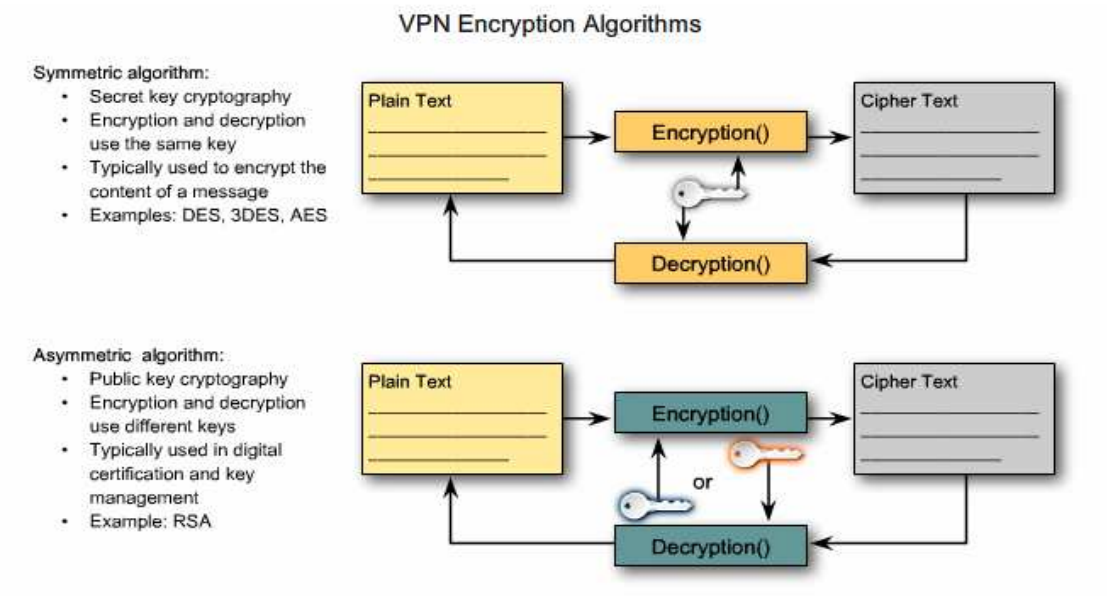
ΚΡΥΦΟ.Οποιοσδήποτε άλλος βλέπει αυτό το μήνυμα βλέπει την κρυπτογραφημένη μορφή του και δεν κατανοεί τι γράφει εκτός και ξέρει το μυστικό κλειδί.

Η ερώτηση είναι το πώς οι συσκευές κρυπτογράφησης και αποκρυπτογράφησης έχουν και οι δύο το ίδιο κοινόχρηστο κλειδι.

7.9.3.Ασσύμμετρη Κρυπτογράφηση

Η ασσύμετρη κρυπτογράφηση χρησιμοποιεί διαφορετικά κλειδιά κατά την κρυπτογράφηση και αποκρυπτογράφηση.Γνωρίζοντας μόνο ένα από τα δύο κλειδιά ένας χάκερ δεν μπορεί να συμπεράνει το δεύτερο κλειδί και να αποκωδικοποιήσει το μήνυμα.Είναι αδύνατο να κωδικοποιήσει και να αποκωδικοποιήσει με το ίδιο κλειδί.

Η κρυπτογράφηση του δημοσίου κλειδιού είναι μια παραλλαγή της ασσύμετρης κρυπτογράφησης η οποία χρησιμοποιεί τον συνδιασμό ενός ιδιωτικού και ενός δημόσιου κλειδιού.Ο παραλήπτης δίνει ένα δημόσιο κλειδί σε κάθε αποστολέα με τον οποίο και θέλει να επικοινωνήσει.Ο αποστολέας χρησιμοποιεί ένα ιδιωτικό κλειδί συνδιασμένο με το δημόσιο κλειδί του παραλήπτη προκειμένου να κρυπτογραφήσει ένα μήνυμα.Επίσης και ο αποστολέας θα πρέπει να μοιραστεί ένα δημόσιο κλειδί με τον παραλήπτη.Ο παραλήπτης για να απακρυπτογραφήσει θα χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα σε συνδιασμό με το δικό του ιδιωτικό κλειδί.



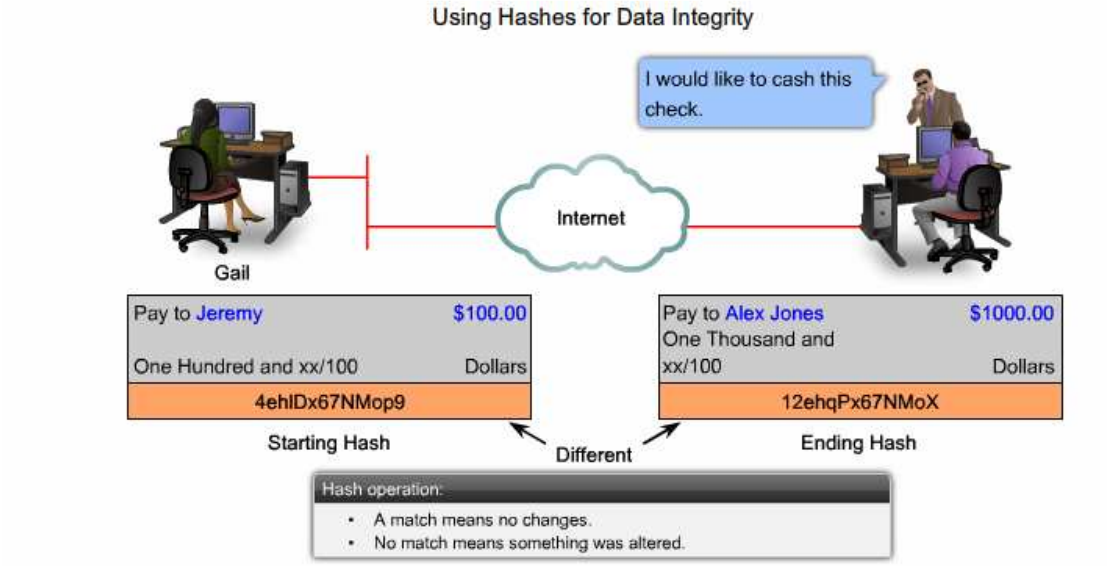
Εικόνα 51: ***Συμμετρική και ασσύμετρη κρυπτπγράφηση***

7.9.4.Η VPN ακεραιότητα των δεδομένων

Οι κατακερματισμοί (hashes) συνεισφέρουν στην ακεραιότητα των δεδομένων και την πιστοποίηση διασφαλίζοντας ότι μη εξουσιοδοτημένα άτομα δεν θα αλλοιώσουν τα μεταδιδόμενα μηνύματα.Ο κατακερματισμός είναι ένας αριθμός ο οποίος ενεργοποιείται από μια ακουλουθία κειμένου και είναι μικρότερος από το ίδιο το κείμενο.Ενεργοποιείται χρησιμοποιώντας ένα τύπο με τέτοιον τρόπο ώστε είναι σχεδόν αδύνατο κάποιο άλλο κείμενο να παράξει την ίδια κατκερματισμένη τιμή.

Ο αρχικός αποστολέας ενεργοποιεί ένα κατακερματισμό του μηνύματος και το στέλνει μαζί με το μήνυμα αυτό καθευατό.Ο παραλήπτης αποκρυπτογραφεί το μήνυμα και τον κατακερματισμό,παράγει κάποιο άλλο κατακερματισμό από το μήνυμα που παρέλαβε και συγκρίνει τους δύο κατακερματισμούς.Αν είναι τα ίδια ο αποστολέας μπορεί να συμπεράνει λογικά ότι η ακεραιότητα του μηνύματος δεν επηρεάστηκε.

Στο σχήμα κάποιος προσπαθεί να στείλει στον Jeremy μια επιταγή των 100 δολαρίων.Στο απομακρυσμένο άκρο ο Alex Jones,πιθανότητα κάποιος απατεώνας,προσπαθεί να εισπράξει μια επιταγή των 1000 δολαρίων.Καθώς η επιταγή μετακινήθηκε μέσα από το διαδίκτυο με κάποιο τρόπο μορφοποιήθηκε.Τόσο ο παραλήπτης όσο και το ποσό της επιταγής υπέστησαν αλλαγές.Σ' αυτή την περίπτωση αν ένας αλγόριθμος χρησιμοποιήθει τότε οι κατακερματισμοί δεν θα ταίριαζουν και η συναλλαγή δεν θα ήταν έγκυρη.



Εικόνα 52: ***Χρησιμοποιήση κατακερματισμών (hashes) για την διασφάλιση της ακεραιότητας των δεδομένων***

Τα VPN δεδομένα μεταφέρονται μέσα από το δημόσιο διαδίκτυο.Όπως φαίνετε υπάρχει το ενδεχόμενο τα δεδομένα αυτά να υποκλαπούν και να τροποποιηθούν.Για να προστατευτούμε από τέτοιου τύπου απειλές, οι χρήστες μπορούν να προσθέσουν ένα κατακερματισμό στο μήνυμα.Αν ο μεταδιδόμενος κατακερματισμός ταιριάζει με το παλαμβανόμενο κατακερματισμό τότε συμπεραίνουμε οτι διατηρήθηκε η ακεραιότητα του μηνύματος.Αν όμως δεν υπάρχει αντιστοιχία το μήνυμα τροποποιήθηκε.

Τα VPNs χρησιμοποιούν ένα κώδικο πιστοποίησης του μηνύματος προκειμένου να επαληθεύσει την ακεραιότητα και την αυθεντικότητα του μηνύματος χωρίς την χρησιμοποίηση κάποιων πρόσθετων μηχανισμών.Το Hashed Message Authentication Code (HMAC) ή το Κατακερματισμένο Μήνυμα Πιστοποιήσης Κωδικού αποτελεί ένα αλγόριθμο ακεραιότητας δεδομένων ο οποίος εγγυάται την ακεραιότητα του μηνύματος.

Ένα HMAC έχει δύο παραμέτρους: ένα εισαγμένο μήνυμα και ένα μυστικό κλειδί, το οποίο είναι γνωστό μόνο στον αποστολέα του μηνύματος και τους επιδιωκόμενους παραλήπτες.Ο αποστολέας του μηνύματος χρησιμοποιεί μια HMAC λειτουργία προκειμένου να παράγει μια τιμή (τον κώδικο πιστοποίησης του μήνυματος) ,διαμορφωμένο έτσι ώστε να λαμβάνει υπόψιν του το μυστικό κλειδί και το εισαγμένο μήνυμα.Ο κωδικός πιστοποίησης του μηνύματος αποστέλεται μαζί με το μήνυμα.Ο παραλήπτης υπολογίζει των κωδικό πιστοποίησης του μηνύματος στο παραλαμβανόμενο μήνυμα χρησιμοποιώντας το ίδιο κλειδί και την HMAC λειτουργία που χρησιμοποίησε ο αποστολέας και συγκρίνει τα αποτελέσματα.Αν οι δυο τιμές ταιριάζουν το μήνυμα έχει παραληφθεί σωστά και ο παραλήπτης διαβεβαιώνεται ότι ο αποστολέας ανήκει στην κοινότητα των χρηστών που μοιράζονται το κλειδί.Η κρυπτογραφική δύναμη του HMAC εξαρτάται από την κρυπτογραφική δύναμη της υποκείμενης λειτουργίας του κατακερματισμού,από το μέγεθος και την ποιότητα του κλειδιού και από το μέγεθος του παραγμένου κατακερματισμού σε bits.

Υπάρχουν δύο συνηθισμένοι HMAC αλγόριθμοι:

- **Message Digest 5 (MD5)** ή Αφομοίωση Μηνύματος 5 – Χρησιμοποιεί ένα 128 bit κοινόχρηστο μυστικό κλειδί.Το μεταβλητού μήκους μήνυμα και το 128 bit κοινόχρηστο κλειδί συνδιάζονται και τρέχουν μέσα από τον HMAC-MD5 αλγόριθμο.Το παραγμένο αποτέλεσμα είναι ένας κατακερματισμός 128-bit.Ο κατακερματισμός επισυνάπτεται στο αρχικό μήνυμα και προωθείται στο απομακρυσμένο άκρο.
- **Secure Hash Algorithm 1 (SHA-1)** ή Αλγόριθμος Ασφάλειας Κατακερματισμου – Χρησιμοποιεί ένα 160-bit κοινόχρηστο κλειδί.Το μεταβλητού μήκους μήνυμα και το 160-bit κοινόχρηστο μυστικό κλειδί συνδιάζονται κα τρέχουν μέσα από τον HMAC SHA-1 hash αλγόριθμο.Το παραγμένο αποτέλεσμα είναι ένας κατακερματισμός 160-bit.Το hash επισυνάπτεται στο αρχικό μήνυμα και προωθείται στο απομακρυσμένο άκρο.

Όταν πραγματοποιούμε επικοινωνίες από μακρινή απόσταση είναι απαραίτητο να γνωρίζουμε ποιος είναι στην άλλη άκρη του τηλεφώνου,του ηλεκτρονικού ταχυδρομείου και του fax.Η ίδια ανάγκη υπάρχει και στα VPN δίκτυα.Η συσκευή στην άλλη άκρη του VPN τούνελ θα πρέπει να πιστοποιηθεί πριν το μονοπάτι επικοινωνίας να θεωρηθεί ασφαλές.Υπάρχουν δύο ομότιμες μέθοδοι πιστοποίησης:

- **Pre-shared key (PSK)** ή Κοινόχρηστο Κλειδί – Αποτελεί ένα μυστικό κλειδί το οποίο μοιράζεται μεταξύ των δύο πλευρών χρησιμοποιώντας ένα ασφαλές κανάλι πριν αυτό να χρησιμοποιηθεί.Τα PSKs χρησιμοποιούν κρυπτογραφικούς αλγορίθμους συμμετρικών κλειδιών.Ένα PSK εισάγεται σε κάθε πλευρά χειροκίνητα και χρησιμοποιείται για την πιστοποίηση τους.Σε κάθε άκρο το PSK συνδιάζεται με άλλες πληροφορίες προκειμένου να διαμορφώσουν το κλειδί πιστοποίησης.

- **RSA signature** ή Υπογραφή RSA – Χρησιμοποιεί την ανταλλαγή ψηφιακών πιστοποιήσεων προκειμένου να πιστοποιήσει και τις δύο πλευρές.Η τοπική συσκευή αποκομίζει τον κατακερματισμό και τον κρυπτογραφεί με το ιδιωτικό του κλειδί.Ο κρυπτογραφημένος κατακερματισμός (ψηφιακή υποφραφή) επισυνάπτεται στο μήνυμα και προωθείται στο απομακρυσμένο άκρο.Στο απομακρυσμένο άκρο ο κρυπτογραφημένος κατακερματισμός αποκρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί στο τοπικό άκρο.Αν το αποκρυπτογαφημένο hash ταιριάζει με το επανυπολογισμένο κατακερματισμό τότε η υπογραφή είναι αυθεντική.

Εικόνα 53: ***Πιστοποίηση VPN***

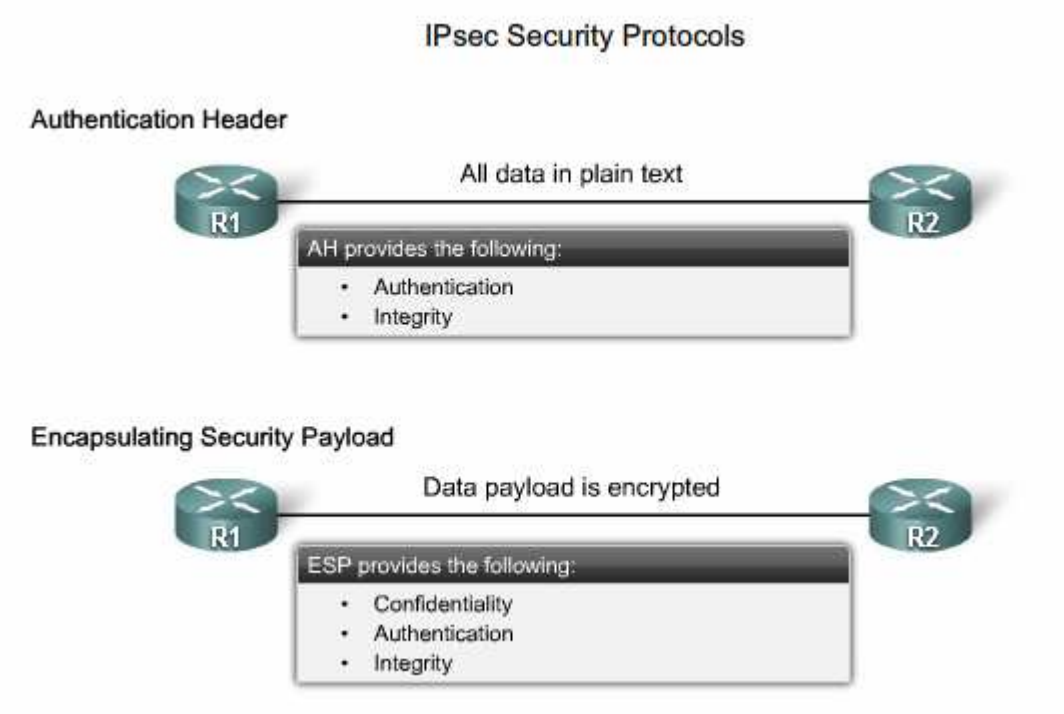
7.10.IPsec security protocols ή IPsec πρωτόκολλα ασφαλείας

Το IPsec αποτελεί μια ακολουθία πρωτοκόλου το οποίο διασφαλίζει της IP επικοινωνίες και το οποίο παρέχει κρυπτογράφηση,ακεραιότητα και πιστοποίηση.Το IPsec συλλαβίζει το μήνυμα το οποίο είναι απαραίτητο για την διασφάλιση των VPN επικοινωνιών αλλά στηρίζεται στους υπάρχοντες αλγόριθμους.

Υπάρχουν δύο κύρια IPsec πρωτόκολα:

- **Authentication header (AH)** ή Επικεφαλίδα Πιστοποίησης– Χρησιμοποιείται όταν η εμπιστευτικότητα δεν απαιτείται.Το AH παρέχει πιστοποίηση και ακεραιότητα των δεδομένων για τα IP πακέτα τα οποία μεταφέρονται μεταξύ δύο συστημάτων.Επαληθεύει ότι κάθε μήνυμα το οποίο μεταφέρται από το R1 στον R2 δεν τροποποιήθηκε κατά την διάρκεια της μετάδοσης του.Επίσης επαληθεύει ότι η προέλευση των δεδομένων αποτελούσε είτε ο R1 είτε ο R2.Το AH δεν παρέχει εμπιστευτικότητα των δεδομένων ,δηλαδή κρυπτογράφηση των πακέτων.Όταν το AH χρησιμοποιείται μόνο του παρέχει αδύναμη προστάσία.Στην συνέχεια χρησιμοποιείται με το ESP πρωτόκολο για να παράσχει κυπτογράφηση των δεδομένων.
- **Encapsulating Security Payload (ESP)** ή Ασφάλεια Φορτίου Ενθυλάκωσης – Παρέχει εμπιστευτικότητα και πιστοποίηση κρυπτογραφώντας το IP πακέτο.Η κρυπτογράφηση του IP πακέτου αποκρύπτει τα δεδομένα και τις ταυτότητες τόσο της πηγής όσο και του προορισμού.Το ESP πιστοποιεί το εσωτερικό IP πακέτο και την ESP επικεφαλίδα.Η πιστοποίηση παρέχει πιστοποίηση της προέλευσης των δεδομένων και την ακεραιότητα τους.Τόσο

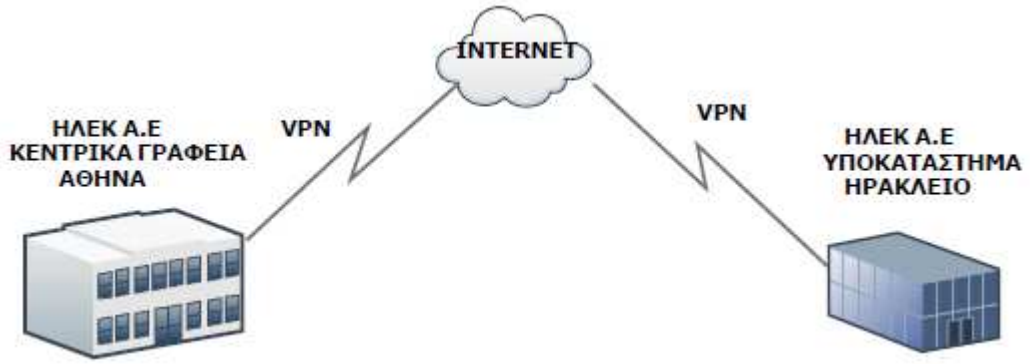
η κρυπτογράφηση όσο και η πιστοποίηση είναι προαιρετικές στο ESP αλλά θα πρέπει μια από τις δύο να χρησιμοποιείται.



Εικόνα 54: ***Πρωτόκολα Ασφαλείας IPsec***

8. Εταιρεία Προμήθευσης Ηλεκτρολογικού Υλικού ΗΛΕΚ Α.Ε

Η νεοσύστατη εταιρεία ΗΛΕΚ Α.Ε πουλάει ηλεκτρολογικό υλικό σε ηλεκτρολογικά καταστήματα στην Αθήνα και στο Ηράκλειο Κρήτης.Στην Αθήνα βρίσκονται τα κεντρικά γραφεία της εταιρείας μας, ενώ υποκατάστημα της εταιρείας υπάρχει και στο Ηράκλειο.Η εργασία που μας αναθέτει η εν λόγω εταιρεία είναι να δικτυώσουμε τα κεντρικά της γραφεία στην Αθήνα και του υποκαταστήματος της στο Ηράκλειο ανάλογα με τις απαιτήσεις που εκείνη μας δίνει και στη συνέχεια να διαμορφώσουμε την επικοινωνία μεταξύ τους μέσω VPN.



Σχέδιο 1: ***Σύνδεση Αθήνας - Ηρακλείου***

8.1.Κεντρικά Γραφεία Αθήνας

Τα κεντρικά γραφεία της Αθήνας αποτελούνται από τέσσερις ορόφους.Οι απαιτήσεις τις εταιρείας ανά όροφο ξεχωριστά είναι οι εξής:

Υπόγειο: Communication Room.

1ος Όροφος: Τρείς χρήστες και ένας εκτυπωτής.

2ος Όροφος: Οκτώ χρήστες και ένα εκτυπωτής.

3ος Όροφος: Έξι χρήστες και ένας εκτυπωτής.

4ος Όροφος: Τρείς χρήστες και ένας εκτυπωτής.

8.2.Επιλογή δικτυακών συσκευών

Το δίκτυο το οποίο πρέπει να διαμορφώσουμε είναι ένα σχετικά μικρό δίκτυο.Θα τοποθετήσουμε ένα μεταγωγέα ανα όροφο και ένα κεντρικό μεταγωγέα (backbone switch) στο δωμάτιο εξοπλισμού.Εκεί θα τοποθετήσουμε επίσης ένα δρομολογητή,ένα τείχο προστασίας και τρείς διακομιστές.

Οι μεταγωγείς οι οποία θα χρησιμοποιήσουμε ανήκουν στην σειρά Cisco Catalyst 2960 τα οποία περιέχουν από 24 πόρτες 10/100/1000 Mbps.Το δίκτυο θα λειτουργήσει στα 100 Mbps ενώ η δυνατότητα του μεταγωγέα στο Gigabit Ethernet (1000 Mbps) θα μας βοηθήσει σε μια μελλοντική ανάπτυξη του δικτύου σε τεχνολογίες όπως οι οπτικές ίνες.Η uplink πόρτα που χρησιμοποιειται για την σύνδεση του μεταγωγέα του κάθε ορόφου με τον κέντρικό μεταγωγέα (backbone

switch) είναι 1000 Mbps.Εμείς θα διαλέξουμε την 24 port του κάθε μεταγωγέα για την αντιπροσώπευση της uplink πόρτας.

Εικόνα 55: ***Switch Catalyst 2960***

Η συσκευή του τείχους προστασίας την οποία θα χρησιμοποιήσουμε είναι το Cisco ASA 5510.Εμπεριέχει ένα κατανοητό και αποτλεσματικό Intrusion Prevention System (IPS) ή Σύστημα Αποτροπής Εισβολών που σε συνδιασμό με ένα υψηλής απόδοσης VPN και την δυνατότητα συνεχού ελέγχου από μακρινή πρόσβαση το κάνουν πολύ αποδοτικο .Την ίδια στιγμή παρέχει μεγάλη προστάσια από κακοβούλες επιθέσεις προερχόμενες από το διαδίκτυο.Η συσκευή firewall αποτελείται από τεσσέρις πόρτες.Εμείς θα χρησιμοποιήσουμε την πόρτα 0 και την πόρτα 1.Η πόρτα 0 θα ορίσει το εξωτερικό δίκτυο (outside),δηλαδή το διαδίκτυο και η πόρτα 1 θα ορίσει την πόρτα εσωτερικού δικτύου (inside).Το outside interface συνδέεται με τον Router και το inside interface συνδέεται με τον μεταγωγέα.Οι υπόλοιπες πόρτες είναι για μελλοντική χρήση και την δημιουργία νέων ζωνών ασφαλείας δικτύου.

Εικόνα 56: ***Cisco ASA Firewall 5510***

Ο δρομολογητής μας είναι το μοντέλο 1841 της εταιρείας Cisco και μας παρέχει την διασύνδεση της εταιρείας από και προς το διαδίκτυο.Οι γραμμές που θα χρησιμοποιήσουμε είναι δύο: η κύρια γραμμή ADSL στα 24 Mbit και μια εφεδρική στα 24 Mbit επίσης.

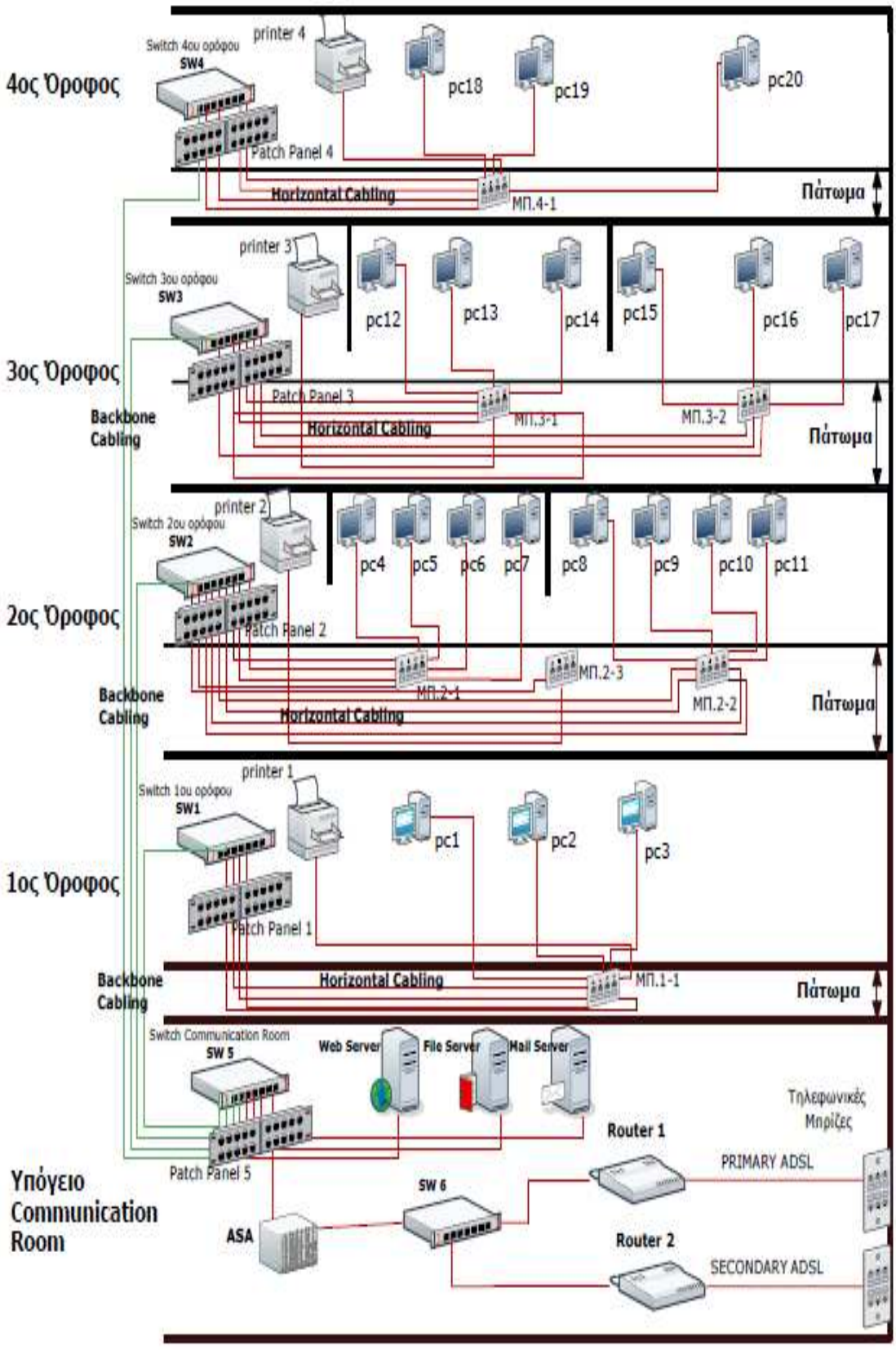
Εικόνα 57: ***Cisco Router 1841***

Οι διακομιστές οι οποίοι θα επιλέξουμε είναι το μοντέλο PowerEdge R210 II της DELL. Εύκολος στη διαχείριση και πλήρως κλιμακούμενος.Με την απόδοση και τα

χαρακτηριστικά που διαθέτει για την εκτέλεση των εφαρμογών και τη διευκόλυνση της κοινής χρήσης και της προστασίας δεδομένων, είναι ιδανικός για μικρές επιχειρήσεις και απομακρυσμένα γραφεία.

Εικόνα 58: ***Server DELL PowerEdge R210 II***

8.3.Φυσική τοπολογία κεντρικών γραφείων Αθήνας



Σχέδιο 2: ***Φυσική τοπολογία κεντρικών γραφείων Αθήνα***

8.4.Δομημένη Καλωδίωση

Σε κάθε όροφο θα τοποθετήσουμε ένα μεταγωγέα στο οποίο θα συνδεθούν οι προσωπικοί υπολογιστές (PCs) και ο εκτυπωτής.

8.4.1.Οριζόντια καλωδίωση

Η σύνδεση μεταξύ των προσωπικών υπολογιστών και του εκτυπωτή με το ανα όροφο μεταγωγέα θα γίνει με καλώδια straight through UTP κατηγορίας CAT5e.Τα καλώδια θα συνδεθουν σ' ένα τερματικό πριζάκι δικτύου τοποθετημένο κάτω από το πάτωμα.Απο εκεί καλώδια υποδομής τερματίζουν σ' ένα patch panel το οποίο είναι εγκατεστημένο σ' ένα μικρό Rack στον τηλεπικοινωνιακό θάλαμο που υπάρχει ανά όροφο και στον οποίο έχει τοποθετηθεί ο μεταγωγέας.Τα καλώδια τερματίζονται στο πίσω μέρος του patch panel σύμφωνα με το πρότυπο του T568-B.Στο μπροστινό μέρος θα κουμπώσουμε καλώδια straight patch cords κατηγορίας CAT5e τα οποία θα καταλήγουν στις πόρτες του switch.

8.4.2.Κάθετη καλωδίωση

Στη συνέχεια θα χρησιμοποιηθεί ένα καλώδιο crossover UTP κατηγορίας CAT5e για την σύνδεση του μεταγωγέα που υπάρχει σε κάθε όροφο με το κεντρικό μεταγωγέα το οποίο είναι εγκατεστημένο σ' ένα τηλεπικοινωνιακό θάλαμο στο δωμάτιο εξοπλισμού.

8.5.Καλωδίωση Δικτυακού εξοπλισμού δωματίου επικοινωνίας

Εκεί βρίσκονται τοποθετημένα επίσης μια συσκευή τείχους προστασίας Cisco ASA firewall 5510,ένας δρομολογητής 1841 της Cisco και τρείς διακομιστές.Η συσκευή του τείχους προστασίας θα συνδεθεί στον μεταγωγέα με καλώδιο straight through UTP κατηγορίας CAT5e.Με τον ίδιο τρόπο θα γίνει η σύνδεση των διακομιστών με τον μεταγωγέα.Το ASA firewall παρεμβάλεται ανάμεσα στο μεταγωγέα και στον δρομολογητή.Το καλώδιο το οποίο θα χρησιμοποιηθεί για να συνδέσει την συσκευή του τείχους προστασίας με τον δρομολογητή είναι επίσης ένα straight through UTP καλώδιο κατηγορίας CAT5e.Αναλυτικά:

Συσκευή	**Συσκευή Σύνδεσης**	**Τύπος καλωδίου**
PC	**Switch**	straight through UTP Cat5e
Printer		straight through UTP Cat5e
Switch		crossover UTP Cat5e
Servers		straight through UTP Cat5e
Router		straight through UTP Cat5e
ASA firewall		straight through UTP Cat5e
	Router	straight through UTP Cat5e

Πίνακας 1: ***Τύποι καλωδίων για την διασύνδεση δικτυακών συσκευών***

Στο σχέδιο 2 αποτυπώνεται η φυσική τοπολογία του δικτύου μας.Σε κάθε όροφο έχουμε τοποθετήσει τις τερματικές συσκευές (προσωπικοί υπολογιστές και εκτυπωτές) σύμφωνα με τις απαιτήσεις τις εταιρείας και ένα μεταγωγέα πάνω στο οποίο θα καταλήξουν τα καλώδια που έρχονται από τις τερματικές συσκευές.Στο δωμάτιο επικοινωνίας το οποίο βρίσκεται στο υπόγειο του δικτύου έχει τοποθετηθεί ο

κεντρικός μας μεταγωγέας,η συσκευή του τείχους προστασίας firewall,ο δρομολογητής και οι διακομιστές της εταιρείας μας.

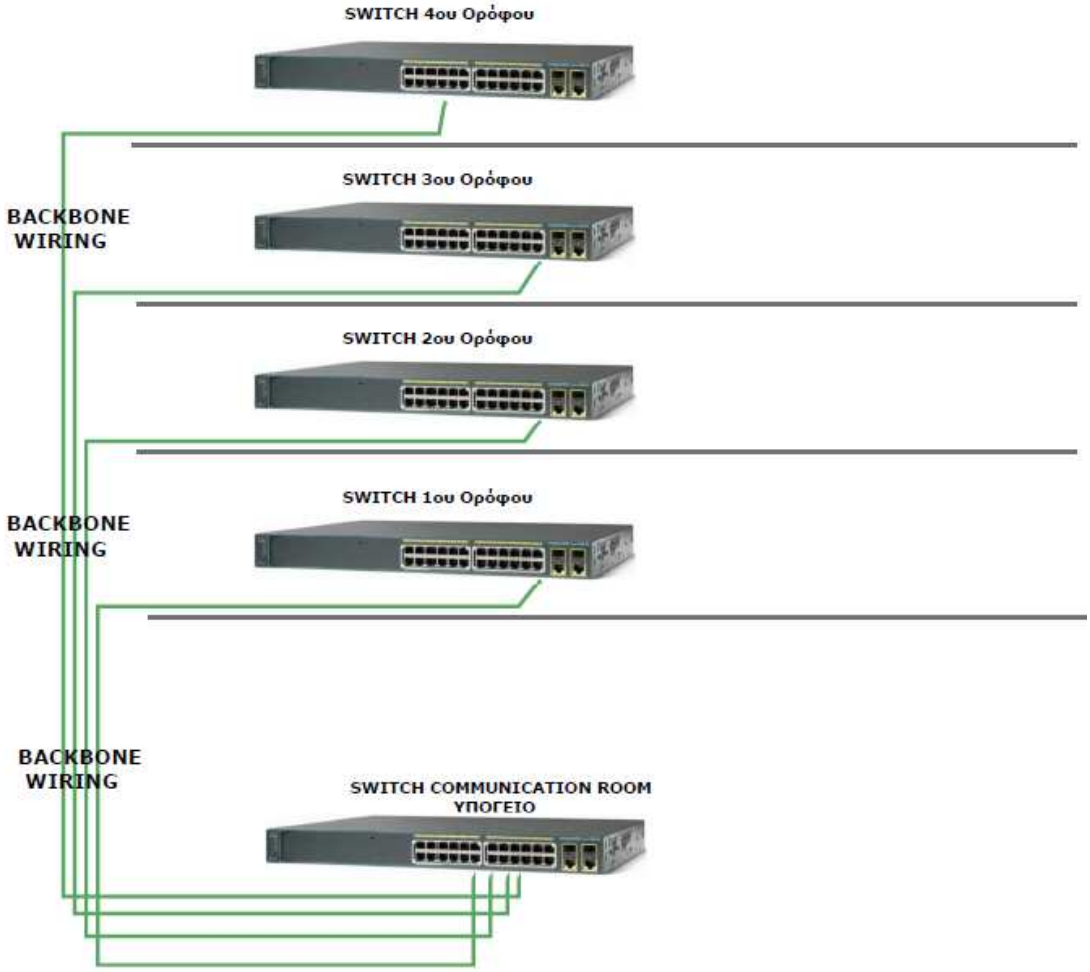
8.6.Συνδέσεις τερματικών συσκευών και δικτυακών συσκευών

Για το παραπάνω σχέδιο θα διαμορφώσουμε ένα cut sheet το οποίο και θα αποτυπώνει λεπτομερώς τις συνδέσεις του δικτύου μας:

Όροφοι	**Τερματικές Συσκευές**	**Αριθμός Δικτυακής πρίζας και πόρτας**	**Αριθμός Patch Panel και πόρτας**	**Αριθμός Switch και πόρτας**
1ος Όροφος	PC01	1-1.1	1.1	1.1
	PC02	1-1.2	1.2	1.2
	PC03	1-1.3	1.3	1.3
	Printer1	1-1.4	1.4	1.4
2ος Όροφος	PC04	2-1.1	2.1	2.1
	PC05	2-1.2	2.2	2.2
	PC06	2-1.3	2.3	2.3
	PC07	2-2.1	2.4	2.4
	PC08	2-2.2	2.5	2.5
	PC09	2-2.3	2.6	2.6
	Printer2	2-1.4	2.7	2.7
3ος Όροφος	PC10	3-1.1	3.1	3.1
	PC11	3-1.2	3.2	3.2
	PC12	3-1.3	3.3	3.3
	PC13	3-1.4	3.4	3.4
	PC14	3-2.1	3.5	3.5
	PC15	3-2.2	3.6	3.6
	PC16	3-2.3	3.7	3.7
	PC17	3-2.4	3.8	3.8
	Printer3	3-3.1	3.9	3.9
4ος Όροφος	PC18	4-1.1	4.1	4.1
	PC19	4-1.2	4.2	4.2
	PC20	4-1.3	4.3	4.3
	Printer4	4-1.4	4.4	4.4
Υπόγειο Communication Room	Web Server	-	5.5	5.1
	File Server	-	5.6	5.2
	Mail Server	-	5.7	5.3
	ASA	-	5.8	5.4
			-	6.3
	RouterA		-	6.1
	RouterB		-	6.2

Πίνακας 2: ***Συνδέσεις τερματικών συσκευών και συσκευών δικτύου***

8.7.Σύνδεση κεντρικού switch με τα switches των ορόφων



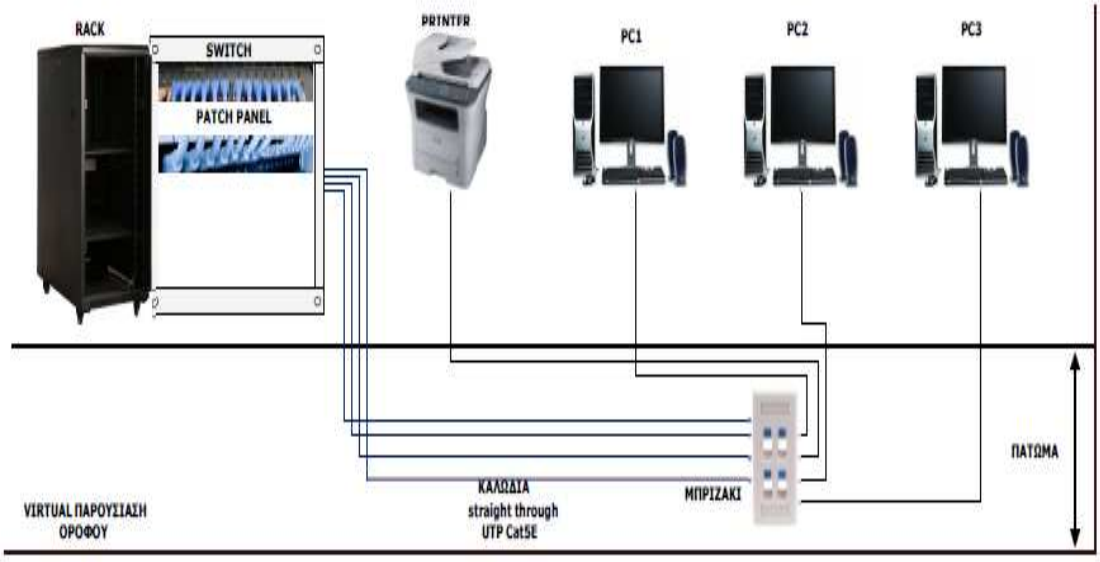
Επίσης θα διαμορφώσουμε ένα cut sheet που θα απεικονίζει την συνδεσμολογία των μεταγωγέων των ορόφων με τον κεντρικό μεταγωγέα στο δωμάτιο επικοινωνίας.

Όροφος	**Πόρτα switch**	**Πόρτα Patch Panel**	**Πόρτα κεντρικού switch**
1ος	1.5	5.1	5.5
2ος	2.8	5.2	5.6
3ος	3.10	5.3	5.7
4ος	4.5	5.4	5.8

Πίνακας 3: ***Συνδέσεις switch ορόφων με κεντρικό switch***

8.8.Εικονική παρουσίαση ορόφου

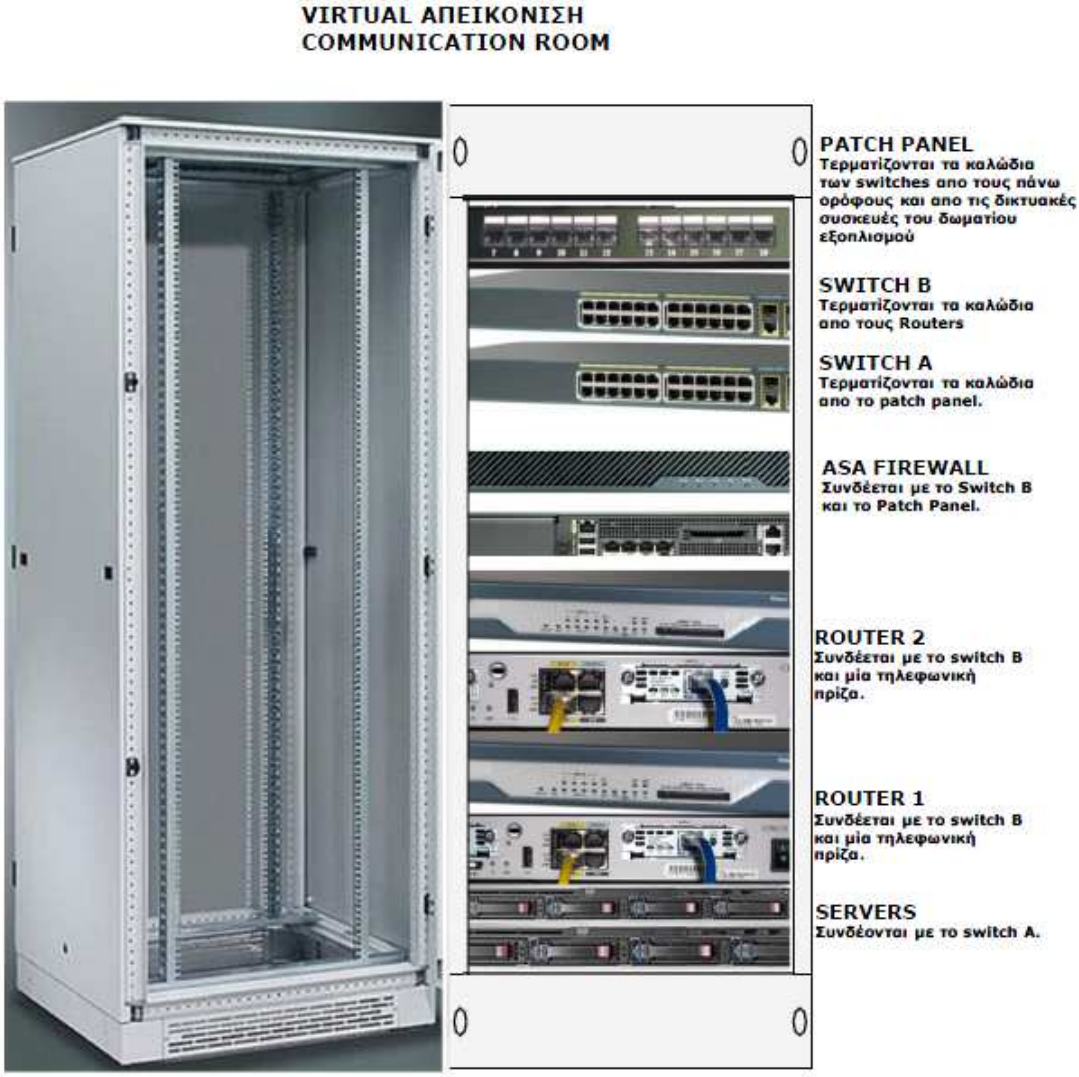
Στη συνέχεια θα παρουσιάσουμε ενδεικτικά μια virtual απεικόνιση ενός ορόφου και του δωματίου επικοινωνίας.



Σχήμα 3: ***Ενδεικτική εικονική παρουσιάση ορόφου***

Στο σχήμα παρατηρούμε τρείς προσωπικούς υπολογιστές και ένα εκτυπωτή.Καθεμιά από τις τερματικές συσκευές θα συνδεθούν με καλώδια straight through UTP κατηγορίας CAT5e τα οποία και θα καταλήξουν στο δικτυακό πριζάκι που είναι εγκατεστημένο κάτω από το ψευδοπάτωμα του κάθε ορόφου.Απο το δικτυακό μπριζάκι επίσης φεύγουν καλώδια υποδομής UTP κατηγορίας CAT5e τα οποία και τερματίζουν στο πίσω μέρος του patch panel του κάθε ορόφου.Απο το μπροστινό μέρος θα φύγουν patch cords καλώδια τα οποία θα τερματιστούν στις πόρτες του μεταγωγέα.

8.9.Εικονική παρουσίαση τηλεπικοινωνιακού θαλάμου στο δωμάτιο εξοπλισμού



Σχήμα 4: ***Εικονική απεικόνιση τηλεπικοινωνιακού θαλάμου τοποθετημένο στο δωμάτιο εξοπλισμού***

Στο δωμάτιο επικοινωνίας όλες οι συσκευές είναι τοποθετημένες σ' ένα τηλεπικοινωνιακό θάλαμο.Η διευθέτηση των δικτυακών συσκευών γίνετε με συγκεντρωτικό τρόπο και κάνει ευκολότερη την πρόσβαση μας σ' αυτές.Οι συνδέσεις των συσκευών στον τηλεπικοινωνιακό θάλαμο του δωματίου επικοινωνίας γίνονται ως εξής:

Switch A,B:Στον μεταγωγέα Α καταλήγουν όλα τα καλώδια που προέρχονται από το patch panel μέσω patch cords και στο μεταγωγέα Β συνδέονται οι δρομολογητές 1,2 και η συσκευή του τείχου προστασίας ASA Firewall.

Servers: Καθένας από τους διακομιστές συνδέεται με ένα καλώδιο crossover UTP κατηγορίας CAT5e στο patch panel του τηλεπικοινωνιακού θαλάμου και από εκεί με crossover patch cords σε μια πόρτα του μεταγωγέα.

ASA Firewall: Η συσκευή του τείχους προστασίας ASA Firewall συνδέεται τόσο στον μεταγωγέα Α όσο και στον μεταγωγέα Β.Η σύνδεση του ASA με τον μεταγωγέα

Α γίνετε μέσω του patch panel και με την βοήθεια ενός crossover patch cord καλωδίου.Η σύνδεση του ASA με τον μεταγωγέα Β γίνετε απ’ ευθείας και με ένα crossover patch cord καλώδιο.

Router 1, 2: Ο δρομολογητής 1 συνδέεται σε μια τηλεφωνική πρίζα που βρίσκεται στο δωμάτιο μέσω ενός τηλεφωνικού καλωδίου.Παρόμοια και ο δρομολογητής 2.

9.Υποκατάστημα Ηρακλείου

Το υποκατάστημα του Ηρακλείου έχει τα γραφεία του εγκατεστημένα σ' ένα όροφο και το δωμάτιο εξοπλισμού βρίσκεται τοποθετημένο στο υπόγειο του κτηρίου.

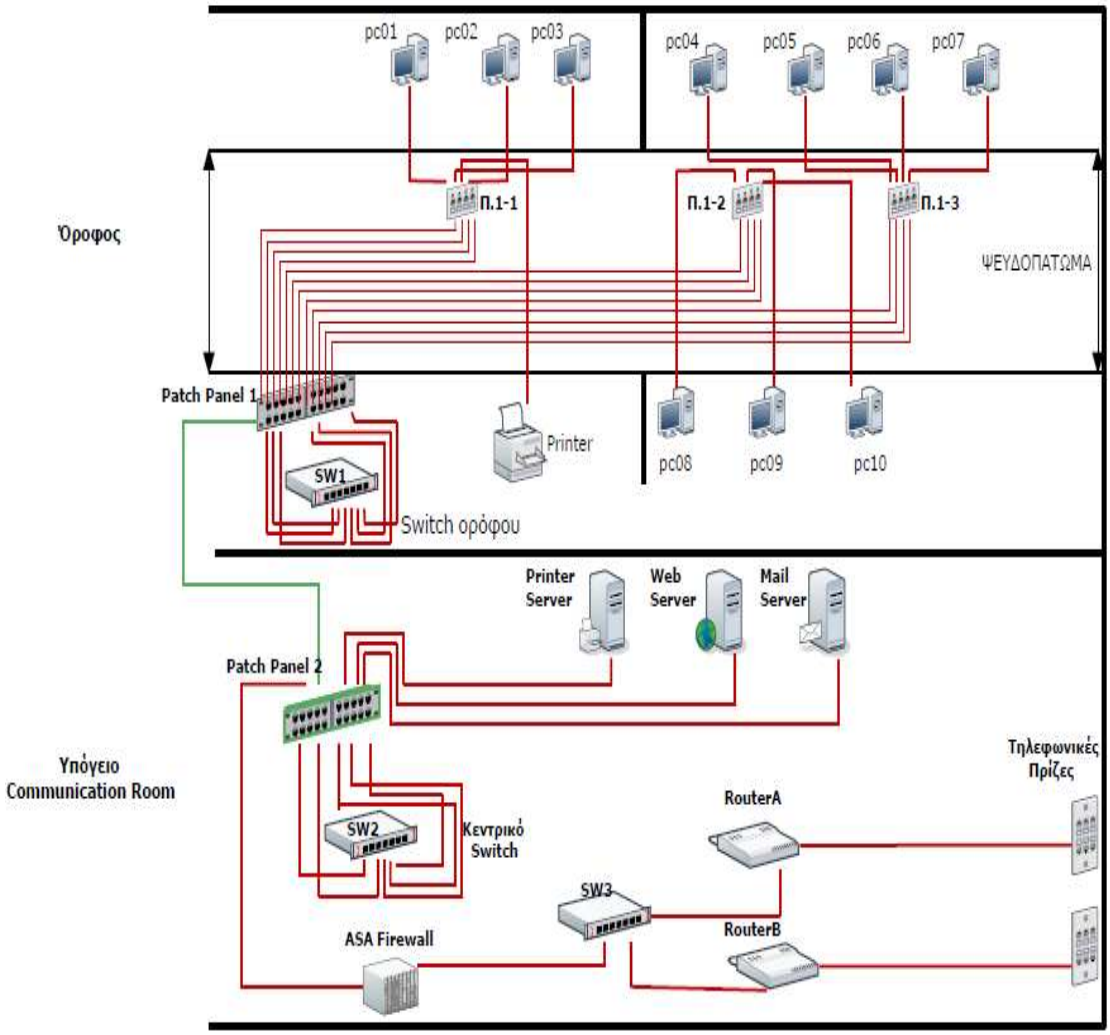
Όροφος: 10 χρήστες και ένας εκτυπωτής

Υπόγειο: Communication Room.

9.1.Δικτυακές Συσκευές

Οι δικτυακές συσκευές οι οποίες θα χρησιμοποιήσουμε για το υποκατάστημα του Ηρακλείου είναι ίδιες με εκείνες των κεντρικών γραφείων στην Αθήνα με την διαφορά ότι το ASA firewall το οποίο θα χρησιμοποιήσουμε, εξαιτίας του μικρού αριθμού χρηστών, είναι ο 5505.Επίσης ο αριθμός των Cisco 2960 switches που θα χρησιμοποιήσουμε θα είναι δύο (ένα στον όροφο και ένα στο δωμάτιο εξοπλισμού).

9.2.Φυσική τοπολογία υποκαταστήματος Ηρακλείου



Σχήμα 5: ***Φυσική τοπολογία υποκαταστήματος Ηρακλείου***

9.3.Συνδέσεις τερματικών συσκευών και δικτυακών συσκευών

Για το παραπάνω σχέδιο θα διαμορφώσουμε ένα cut sheet το οποίο και θα αποτυπώνει λεπτομερώς τις συνδέσεις του δικτύου μας.

Όροφοι	**Συσκευές**	**Αριθμός Δικτυακής πρίζας και πόρτας**	**Αριθμός Patch Panel και πόρτας**	**Αριθμός Switch και πόρτας**
1ος Όροφος	PC01	1-1.1	1.1	1.1
	PC02	1-1.2	1.2	1.2
	PC03	1-1.3	1.3	1.3
	PC04	1-3.1	1.4	1.4
	PC05	1-3.2	1.5	1.5
	PC06	1-3.3	1.6	1.6
	PC07	1-3.4	1.7	1.7
	PC08	1-2.1	1.8	1.8
	PC09	1-2.2	1.9	1.9
	PC10	1-2.3	1.10	1.10
	Printer	1-1.4	1.11	1.11
Υπόγειο Communication Room	Web Server	-	2.1	2.1
	Mail Server	-	2.2	2.2
	File Server	-	2.3	2.3
	ASA	-	2.4	2.4
				3.3
	Router A			3.1
	Router B			3.2

Πίνακας 5: ***Συνδέσεις τερματικών συσκευών και συσκευών δικτύου***

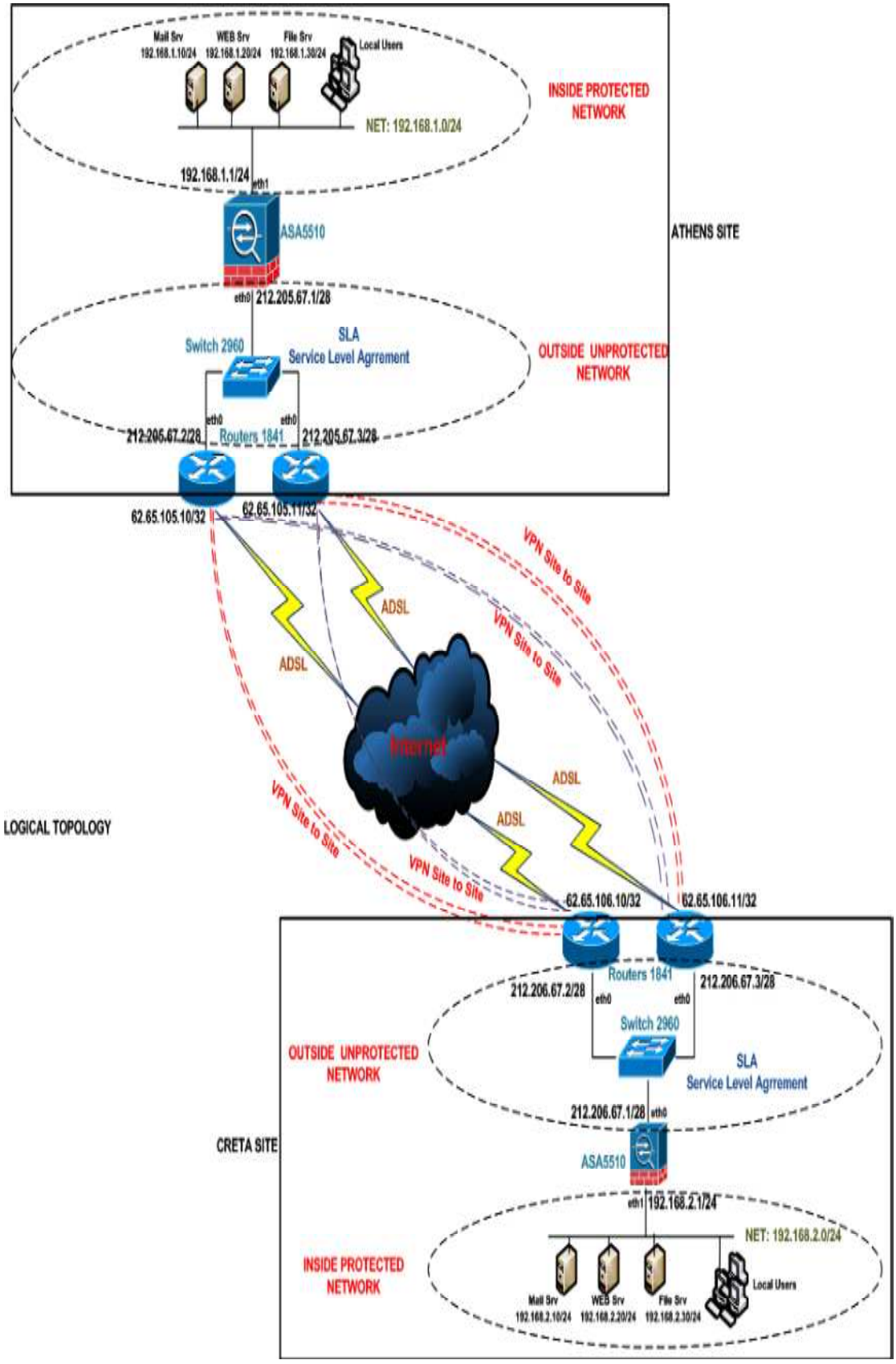
9.4.Σύνδεση κεντρικού switch με τα switches των ορόφων

Επίσης θα διαμορφώσουμε ένα cut sheet που θα απεικονίζει την συνδεσμολογία των switches των ορόφων με το κεντρικό switch στο δωμάτιο επικοινωνίας.

Όροφος	Πόρτα switch	Πόρτα Patch Panel	Πόρτα κεντρικού switch
1ος	1.11	2.5	2.1

Πίνακας 6: ***Συνδέσεις switch με κεντρικό switch***

10.Λογική Τοπολογία



Εικόνα 59:*Λογική τοπολογία Αθήνας-Κρήτης*

Η λογική τοπολογία των τοπικών δικτύων και του δικτύου ευρείας περιοχής, το οποίο συνδέει τα τοπικά δίκτυα μεταξύ τους, απεικονίζεται στο παραπάνω σχήμα.Στο σχέδιο αυτό έχουν τοποθετηθεί οι IP διευθύνσεις των εσωτερικών και εξωτερικών τοπικών δικτύων όπως επίσης και οι IP διευθύνσεις της πρωταρχικής και εφεδρικής ADSL σύνδεσης.

Σαν εσωτερικό δίκτυο έχουμε ορίσει το δίκτυο του κάθε site που οριοθετείται πριν το ASA firewall 5510 και σαν εξωτερικό δίκτυο το δίκτυο που οριοθετείται μετά το ASA firewall 5510.Ο διαχωρισμός αυτός γίνεται προκειμένου να ορίσουμε τις ασφαλείς περιοχές των δικτύων και τις επισφαλείς περιοχές των δικτύων.

	Αθήνα	**Ηράκλειο**
Ιδιωτικές IP διευθύνσεις	192.168.1.1/24	192.168.2.1/24
	212.205.67.1/28	212.206.67.1/28
	212.205.67.2/28	212.206.67.2/28
	212.205.67.2/28	212.206.67.3/28
Δημόσιες IP διευθύνσεις	62.65.105.10/32	62.65.106.10/32
	62.65.105.11/32	62.65.106.11/32

Ιδιωτικές IP διευθύνσεις είναι οι διευθύνσεις που ορίζονται από τον διαχειριστή των τοπικών δικτύων και αφορούν τις δικτυακές συσκευές των δικτύων αυτών ενώ δημόσιες IP διευθύνσεις είναι οι διευθύνσεις που τις παρέχουν οι τηλεπικοινωνιακοί πάροχοι όπως ο ΟΤΕ ή η HOL και αφορούν την σύνδεση των τοπικών δικτύων μέσω του δικτυου ευρείας περιοχής που οι πάροχοι ελέγχουν και διαχειρίζονται.

Η συσκευή ASA firewall,τοποθετημένη και στα δύο άκρα, είναι η συσκευή εκείνη στην οποία τερματίζεται η VPN σύνδεση μεταξύ των κεντρικών γραφείων της Αθήνας και του υποκαταστήματος του Ηρακλείου.Μας εξασφαλίζει πλήρη προστασία των δεδομένων που διακινούνται μέσα από το διαδίκτυο.

Σε κάθε άκρο της σύνδεσης ευρείας περιοχής έχουμε τοποθετήσει δύο δρομολογητές έτσι ώστε να εξασφαλίσουμε την μόνιμη σύνδεσιμότητα μεταξύ των δύο τοπικών δικτύων σε περίπτωση αποτυχίας του δρομολογητή που έχουμε αρχικά ορίσει σαν τον αρχικό δρομολογητή.

11.Οικονομική Μελέτη

Σημαντικός παράγοντας για την μελέτη και την εγκατάσταση του δίκτυου μιας μικρομεσαίας επιχείρησης αποτελεί το οικονομικό κόστος.Το κόστος είναι ανάλογο του μεγέθους του δικτύου της επιχείρησης, τουλάχιστον όσο αναφορά την εγκατάσταση, καθώς και της ποιότητας των δικτυακών συσκευών τις οποίες θα αγοράσουμε.

Κόστος εξοπλισμού:

Εξοπλισμός	**Κόστος**	**Τεμάχια/Μέτρα**	**Συνολικό Κόστος**
Cisco Router 1841	2000euro/ανά τεμάχιο	4	8000 euro
Cisco Switch 2960 24 ports	1200 euro/ανά τεμάχιο	9	10800 euro
Cisco ASA 5510	1800 euro	1	1800 euro
Cisco ASA 5505	500 euro	1	500 euro
Dell Servers PowerEdge R210	960 euro/ανά τεμάχιο	6	5760 euro
Patch Panel	300 euro/ανά τεμάχιο	7	2100 euro
Πρίζες Δικτύου	30 euro/ανά τεμάχιο	10	300 euro
Καλώδια patch cord Cat5e 5m	3.90 euro/ανά τεμάχιο	45	175.5 euro
Καλώδια patch cord Cat5e 2m	1.50 euro/ανά τεμάχιο	45	67.5 euro
Τερματικά jack RJ45	1.33 euro/τεμάχιο	20	26.6 euro
Καλώδια UTP Cat 5e κουλούρα	0.50 λεπτά/ανά μέτρο	100	50 euro
Τελικό Κόστος			**29.579,6 euro**

Κόστος μελέτης και εγκατάστασης:

Εργασία	**Κόστος**
Μελέτη	1000 euro
Εγκατάσταση	3000 euro
Τελικό Κόστος	**4000 euro**

Συνολικό κόστος : 33.579,6

12.Επίλογος

Τα δίκτυα των υπολογιστών μετατρέπονται σ' ένα πολύ χρήσιμο εργαλείο για την αποτελεσματική σύνδεση των ανθρώπων μεταξύ τους.Το διαδίκτυο έφερε επανάσταση στις επικοινωνίες και τις εμπορικές μεθόδους, επιτρέποντας σε διαφορετικά δίκτυα σε ολόκληρο τον κόσμο να διασυνδεθούν μεταξύ τους.Υπάρχει ένα πλήθος από πλεονεκτήματα που σχετίζονται με τα δίκτυα των υπολογιστών.Μερικά πεδία επιτυχημένης εφαρμογής τους αποτελούν οι βιομηχανίες,οι επιχειρήσεις,οι κυβερντικοί οργανισμοί και η εκπαίδευση.

Τα δίκτυα των υπολογιστών άνοιξαν τις πύλες της πληροφορίας και ενεργοποίησαν την άμεση πρόσβαση στην πληροφορία.Ο τεράστιος πλούτος της πληροφορίας ο οποίος ρέει στο δίκτυο είναι προσβάσιμος μέσα από τα καλά διασυνδεδεμένα παγκόσμια δίκτυα.Τα δίκτυα συνοδεύτηκαν με μια ψηφιακή επικοινωνία η οποία πλεόν έχει αντίκτυπο στην καθημερινότητα,σε ομάδες ανθρώπων,στην προσωπική ταυτοποίηση,στον πολιτισμό,στην ασφάλεια και με ένα εικονικό τρόπο σε όλες τις πτυχές της ύπαρξης μας.Η ψηφιακή κοινωνία έχει γίνει τόσο διεισδιτική ώστε η αναγνώριση των επιδράσεων που έχουν αυτές οι τεχνολογίες πάνω μας,σαν άτομα,αλλά και σαν μέλη της κοινωνίας,έχει γίνει πολύ σημαντική.Τα δίκτυα πλέον συνεισφέρουν στην παγκοσμιοποίηση της παραγωγής και στις κεφαλαιακές αγορές μέσω της μείωσης του κόστους της πληροφορίας και της επικοινωνίας.Αυτές οι τεχνολογίες έκαναν ευκολότερη στις πολυεθνικές και στις άλλες εταιρείες, την επέκταση των παραγωγικών κέντρων παγκοσμίως,την εναρμόνιση διεθνών διαφημιστικών εκστρατειών και την σύμπραξη σε μελέτες οι οποίες διεξάγονται σε διαφορετικές ηπείρους.

Ακόμα μεγαλύτερο είναι το αντίκτυπο των δικτύων υπολογιστών πάνω στις μικρομεσαίες επιχειρήσεις.Η ολοκληρωμένη οικονομοτεχνική μελέτη των τοπικών δικτύων μιας επιχείρησης και του δικτύου ευρείας περιοχής,για την επιτυχημένη διασύνδεση τους,αποτελεί ίσως το κρισιμότερο σημείο της λειτουργίας της επιχείρησης.Τα κύρια χαρακτηριστικά που οφείλουν να διέπουν τα τοπικά δίκτυα και την διασύνδεση μεταξύ τους είναι η αξιοπιστία και η ασφάλεια.Η αξιοπιστία εξασφαλίζει την αποτελεσματική λειτουργία των τοπικών δικτύων 24 ώρες το 24ώρο και η ασφάλεια εγγυάται την εχεμύθεια και την φερεγγυότητα της πληροφορίας που ανταλλάσαται μεταξύ των τοπικών δικτύων διαμέσου του διαδικτύου.

Η αξιοποστία πραγματοποιείται με την σωστή εγκατάσταση των δικτυακών υποδομών στα κτήρια της επιχείρησης, πάνω στις οποίες θα πρέπει να έχουμε την πλήρη εποπτεία.Η ασφάλεια εγγυάται με την σωστή παραμετροποίηση των συσκευών του τείχου προστασίας και των δρομολογητών.Επομένως η ολοκληρωμένη οικονομοτεχνική μελέτη ξεκινάει από την εφαρμογή των δικτυακών εγκαταστάσεων και φτάνει μέχρι την σωστή παραμετροποίηση του λογισμικού των δικτυακών συσκευών που ορίζουν τα τοπικά και δίκτυα ευρείας περιοχής.

13.Παράρτημα:Configurations-Παραμετροποιήσεις

SITE ATHENS

ASA 5510 CONFIGURATION

```
ASA Version 8.2(1)11
!
hostname ATHENS-ASA
domain-name Athens-comany.gr
enable password PbKEHAhPeHEkZ4A/ encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
name 212.205.67.2 ROUTER1
name 212.205.67.3 ROUTER2
name 192.168.1.10 PRIVATE-IP-MAILSRV
name 192.168.1.20 PRIVATE-IP-WEBSRV
name 192.168.1.30 PRIVATE-IP-FILESRV
name 212.205.67.4 PUBLIC-IP-MAILSRV
name 212.205.67.5 PUBLIC-IP-WEBSRV
name 212.205.67.6 PUBLIC-IP-FILESRV
!
dns-guard
!
interface Ethernet0/0
description *** Connected to Internet ***
nameif OUTSIDE
 security-level 0
 ip address 212.205.67.1 255.255.255.240
 no shutdown
!
interface Ethernet0/1
description *** Connected to 192.168.1.0/24 ***
 nameif INSIDE
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 no ip address
 management-only
!
ftp mode passive
!
dns server-group DefaultDNS
 domain-name Athens-company.gr
!
!
same-security-traffic permit inter-interface
```

```
same-security-traffic permit intra-interface
!
!
!
!
!
access-list INSIDE_access_in extended permit ip 192.168.1.0 255.255.255.0 any
access-list INSIDE_access_in extended permit icmp 192.168.1.0 255.255.255.0 any
access-list OUTSIDE_access_in extended permit tcp any host PUBLIC-IP-MAILSRV eq smtp
access-list OUTSIDE_access_in extended permit tcp any host PUBLIC-IP-WEBSRV eq www
access-list OUTSIDE_access_in extended permit tcp any host PUBLIC-IP-MAILSRV eq https
access-list OUTSIDE_access_in extended permit icmp any host PUBLIC-IP-MAILSRV
access-list OUTSIDE_access_in extended permit icmp any host PUBLIC-IP-WEBSRV
access-list INSIDE_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
!
!
pager lines 24
logging enable
logging asdm informational
!
mtu OUTSIDE 1500
mtu INSIDE 1500
icmp unreachable rate-limit 1 burst-size 1
!
icmp permit any OUTSIDE
icmp permit any INSIDE
!
asdm image disk0:/asdm-623.bin
no asdm history enable
!
arp timeout 14400
!
nat-control
global (OUTSIDE) 1 interface
!
nat (INSIDE) 0 access-list INSIDE_nat0_outbound
!
nat (INSIDE) 1 192.168.1.0 255.255.255.0
!
static (INSIDE,OUTSIDE) PUBLIC-IP-MAILSRV PRIVATE-IP-MAILSRV netmask 255.255.255.255
static (INSIDE,OUTSIDE) PUBLIC-IP-FILESRV PRIVATE-IP-FILESRV netmask 255.255.255.255
static (INSIDE,OUTSIDE) PUBLIC-IP-WEBSRV PRIVATE-IP-WEBSRV netmask 255.255.255.255
!
access-group OUTSIDE_access_in in interface OUTSIDE
access-group INSIDE_access_in in interface INSIDE
!
route OUTSIDE 0.0.0.0 0.0.0.0 ROUTER 1
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
!
dynamic-access-policy-record DfltAccessPolicy
!
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
!
http server enable
http 192.168.1.0 255.255.255.0 INSIDE
!
sysopt noproxyarp INSIDE
!
!
!
telnet 192.168.1.0 255.255.255.0 INSIDE
telnet timeout 5
!
ssh 192.168.1.0 255.255.255.0 INSIDE
ssh timeout 5
ssh version 2
```

```
!
console timeout 0
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
username giorgos password gB9q/m.zrYGMEskE encrypted privilege 15
!
prompt hostname context
!
!
: end
```

SITE ATHENS

ROUTER 1 CONFIGURATION

```
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ1
!
boot-start-marker
boot-end-marker
!
!
logging buffered 52000
enable secret 5 $1$VPDV$Y2wsKarawi6s.SrZWsaTL0
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
memory-size iomem 10
clock timezone PCTime 0 0
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
crypto pki trustpoint ATHENS-COMPANY
 enrollment selfsigned
 serial-number
 ip-address dialer1
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-2692466680
```

```
crypto pki certificate chain ATHENS-COMPANY
 certificate self-signed D9
  30820275 308201DE A0030201 020201D9 300D0609 2A864886 F70D0101 04050030
  56315430 12060355 0405130B 46435A31 34303639 30445130 1A06092A 864886F7
  0D010908 130D3739 2E313239 2E36332E 31313930 2206092A 864886F7 0D010902
  16154851 312E636F 73746163 6F666665 652E6C6F 63616C30 1E170D31 31303531
  37313032 3932305A 170D3230 30313031 30303030 30305A30 56315430 12060355
  0405130B 46435A31 34303639 30445130 1A06092A 864886F7 0D010908 130D3739
  2E313239 2E36332E 31313930 2206092A 864886F7 0D010902 16154851 312E636F
  73746163 6F666665 652E6C6F 63616C30 819F300D 06092A86 4886F70D 01010105
  0003818D 00308189 02818100 EBC3E3F3 51848236 89C90B84 A8BC50AA 621D1BFA
  002726EB 3766F20B 323D05A1 EB510FB1 61931375 D507649B A63C5574 C77A3A94
  378464E3 6F03EA7F EEF00099 4C89C439 ABB3A302 A912B46B 249BFC93 EF3494C5
  2DA29887 8D8E3FDF BF77AE8D 9E2C3FDF 7A498F5F ED7545B2 D8F88B43 C6AD789C
  E15B6A15 AFC250AB 6D7C9357 02030100 01A35330 51300F06 03551D13 0101FF04
  05300301 01FF301F 0603551D 23041830 16801474 941080A4 AE0296A8 125AF422
  DB25BC09 269B5E30 1D060355 1D0E0416 04147494 1080A4AE 0296A812 5AF422DB
  25BC0926 9B5E300D 06092A86 4886F70D 01010405 00038181 00A5AE13 36E86E55
  42CDBC42 60B29E8B E5C1C9B3 30976154 D55A9E6C D8E6A6F2 F47E99FB 8FA96D9F
  7CCD278A 33E56040 58E91206 89ED899E C4EAAB6D C8A7DE55 0053B2CE B25F0B0E
  58D0945A 34702143 DC003097 DF82385E 69CEA20D 65D6F964 AA66C159 23310067
  F3D96D6B FEF4B361 F2C63489 849F29CB 4400ABAB 60D07686 21
       quit
ip source-route
!
!
!
!
!
ip cef
ip domain name Athens-company
ip name-server 195.170.0.1
ip name-server 195.170.2.2
!
!
archive
 log config
  hidekeys
!
!
username giorgos privilege 15 secret 5 $1$JbHo$hj3h0xCJkY33sN27vUEYX.
secure boot-image
secure boot-config
!
!
!
!
!
track 123 ip sla 1 reachability
!
track 456 ip sla 2 reachability
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp key C#om-An1@ address 62.65.106.10 no-xauth
crypto isakmp key C#om-An1@ address 62.65.106.11 no-xauth
!
crypto isakmp fragmentation
crypto isakmp keepalive 10
crypto isakmp xauth timeout 45
!
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
!
!
```

```
!
!
!
!
!
crypto map SDM_CMAP_1  ipsec-isakmp
 description Tunnel  to Creta
 set peer 62.65.106.10  default
 set peer 62.65.106.11
 set transform-set ESP-3DES-SHA
 match address 104
!
!
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
no shutdown

!
!
interface ATM0.4 point-to-point
 pvc 8/35
  pppoe-client dial-pool-number 1
 !
!
!
interface FastEthernet0
 ip address 212.205.67.2 255.255.255.240
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache cef
 no ip route-cache
no shutdown
!
interface Dialer1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly in
 encapsulation ppp
 no ip route-cache cef
 no ip route-cache
 dialer pool 1
 dialer-group 1
 ppp authentication chap pap callin
 ppp chap hostname giorg@otenet.gr
 ppp chap password 0 giorg1
 ppp pap sent-username giorg@otenet.gr password 0 giorg1
 no cdp enable
 crypto map SDM_CMAP_1
 no shutdown
!
!
router rip
 version 2
 redistribute static
 network 212.205.67.0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
!
!
!
!
!
!
!
```

```
ip nat inside source list 192 interface Dialer1 overload
!
ip route 0.0.0.0 0.0.0.0 Dialer1 track 123
ip route 0.0.0.0 0.0.0.0 212.205.67.3 track 456
ip route 0.0.0.0 0.0.0.0 Dialer1
!
ip route 192.168.1.0 255.255.255.0 212.205.67.1 permanent
ip route 195.170.2..1 255.255.255.255 212.205.67.3
!
!
ip sla 1
 icmp-echo 195.170.0.2 source-interface Dialer1
 threshold 3
 frequency 5
ip sla schedule 1 life forever start-time now
!
!
ip sla 2
 icmp-echo 195.170.2.1 source-interface FastEthernet0
 threshold 3
 frequency 5
ip sla schedule 2 life forever start-time now
!
!
access-list 104 remark IPSec Rule
access-list 104 permit ip 192.168.1. 0.0.0.255 192.168.2.0 0.0.0.255
!
access-list 192 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 192 permit ip 192.168.1.0 0.0.0.255  any
access-list 192 permit ip 212.205.67.3 any

!
dialer-list 1 protocol ip permit
!
no cdp run
!
!
banner motd ^CWelcome to Router HQ1 – Athens-company^C
!
line con 0
!
line aux 0
!
line vty 0 4
transport input telnet ssh
!
end
```

SITE ATHENS

ROUTER 2 CONFIGURATION

```
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ2
!
boot-start-marker
boot-end-marker
!
!
```

```
logging buffered 52000
enable secret 5 $1$VPDV$Y2wsKarawi6s.SrZWsaTL0
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
memory-size iomem 10
clock timezone PCTime 0 0
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
crypto pki trustpoint ATHENS-COMPANY
 enrollment selfsigned
 serial-number
 ip-address dialer1
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-2692466680
crypto pki certificate chain ATHENS-COMPANY
 certificate self-signed D9
  30820275 308201DE A0030201 020201D9 300D0609 2A864886 F70D0101 04050030
  56315430 12060355 0405130B 46435A31 34303639 30445130 1A06092A 864886F7
  0D010908 130D3739 2E313239 2E36332E 31313930 2206092A 864886F7 0D010902
  16154851 312E636F 73746163 6F666665 652E6C6F 63616C30 1E170D31 31303531
  37313032 3932305A 170D3230 30313031 30303030 30305A30 56315430 12060355
  0405130B 46435A31 34303639 30445130 1A06092A 864886F7 0D010908 130D3739
  2E313239 2E36332E 31313930 2206092A 864886F7 0D010902 16154851 312E636F
  73746163 6F666665 652E6C6F 63616C30 819F300D 06092A86 4886F70D 01010105
  0003818D 00308189 02818100 EBC3E3F3 51848236 89C90B84 A8BC50AA 621D1BFA
  002726EB 3766F20B 323D05A1 EB510FB1 61931375 D507649B A63C5574 C77A3A94
  378464E3 6F03EA7F EEF00099 4C89C439 ABB3A302 A912B46B 249BFC93 EF3494C5
  2DA29887 8D8E3FDF BF77AE8D 9E2C3FDF 7A498F5F ED7545B2 D8F88B43 C6AD789C
  E15B6A15 AFC250AB 6D7C9357 02030100 01A35330 51300F06 03551D13 0101FF04
  05300301 01FF301F 0603551D 23041830 16801474 941080A4 AE0296A8 125AF422
  DB25BC09 269B5E30 1D060355 1D0E0416 04147494 1080A4AE 0296A812 5AF422DB
  25BC0926 9B5E300D 06092A86 4886F70D 01010405 00038181 00A5AE13 36E86E55
  42CDBC42 60B29E8B E5C1C9B3 30976154 D55A9E6C D8E6A6F2 F47E99FB 8FA96D9F
  7CCD278A 33E56040 58E91206 89ED899E C4EAAB6D C8A7DE55 0053B2CE B25F0B0E
  58D0945A 34702143 DC003097 DF82385E 69CEA20D 65D6F964 AA66C159 23310067
  F3D96D6B FEF4B361 F2C63489 849F29CB 4400ABAB 60D07686 21
       quit
ip source-route
!
!
!
!
!
ip cef
ip domain name Athens-company
ip name-server 195.170.0.1
ip name-server 195.170.2.2
!
!
archive
 log config
  hidekeys
!
```

```
!
username giorgos privilege 15 secret 5 $1$JbHo$hj3h0xCJkY33sN27vUEYX.
secure boot-image
secure boot-config
!
!
!
!
!
track 123 ip sla 1 reachability
!
track 456 ip sla 2 reachability
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp key C#om-An1@ address 62.65.106.10 no-xauth
crypto isakmp key C#om-An1@ address 62.65.106.11 no-xauth
!
crypto isakmp fragmentation
crypto isakmp keepalive 10
crypto isakmp xauth timeout 45
!
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
!
!
!
!
!
!
!
crypto map SDM_CMAP_1  ipsec-isakmp
 description Tunnel  to Creta
 set peer 62.65.106.11  default
 set peer 62.65.106.10
 set transform-set ESP-3DES-SHA
 match address 104
!
!
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
no shutdown

!
!
interface ATM0.4 point-to-point
 pvc 8/35
  pppoe-client dial-pool-number 1
 !
!
!
interface FastEthernet0
 ip address 212.205.67.3 255.255.255.240
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache cef
 no ip route-cache
 no shutdown
!
interface Dialer1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly in
```

```
 encapsulation ppp
 no ip route-cache cef
 no ip route-cache
 dialer pool 1
 dialer-group 1
 ppp authentication chap pap callin
 ppp chap hostname giorg12@otenet.gr
 ppp chap password 0 giorg2
 ppp pap sent-username giorg12@otenet.gr password 0 giorg2
 no cdp enable
 crypto map SDM_CMAP_1
 no shutdown
!
!
router rip
 version 2
 redistribute static
 network 212.205.67.0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
!
!
!
!
!
!
!
ip nat inside source list 192 interface Dialer1 overload
!
ip route 0.0.0.0 0.0.0.0 Dialer1 track 123
ip route 0.0.0.0 0.0.0.0 212.205.67.2 track 456
ip route 0.0.0.0 0.0.0.0 Dialer1
!
ip route 192.168.1.0 255.255.255.0 212.205.67.1 permanent
ip route 195.170.0..2 255.255.255.255 212.205.67.2
!
!
ip sla 1
 icmp-echo 195.170.2.1 source-interface Dialer1
 threshold 3
 frequency 5
ip sla schedule 1 life forever start-time now
!
!
ip sla 2
 icmp-echo 195.170.0.2 source-interface FastEthernet0
 threshold 3
 frequency 5
ip sla schedule 2 life forever start-time now
!
!
access-list 104 remark IPSec Rule
access-list 104 permit ip 192.168.1. 0.0.0.255 192.168.2.0 0.0.0.255
!
access-list 192 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 192 permit ip 192.168.1.0 0.0.0.255  any
access-list 192 permit ip 212.205.67.2 any
!
dialer-list 1 protocol ip permit
!
no cdp run
!
!
banner motd ^CWelcome to Router HQ2 – Athens-company^C
!
line con 0
```

```
!
line aux 0
!
line vty 0 4
transport input telnet ssh
!
end
```

SITE CRETA

ASA 5505 CONFIGURATION

```
ASA Version 8.2(1)11
!
hostname CRETA-ASA
domain-name Creta-comany.gr
enable password PbKEHAhPeHEkZ4A/ encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
name 212.206.67.2 ROUTER1
name 212.206.67.3 ROUTER2
name 192.168.2.10 PRIVATE-IP-MAILSRV
name 192.168.2.20 PRIVATE-IP-WEBSRV
name 192.168.2.30 PRIVATE-IP-FILESRV
name 212.206.67.4 PUBLIC-IP-MAILSRV
name 212.206.67.5 PUBLIC-IP-WEBSRV
name 212.206.67.6 PUBLIC-IP-FILESRV
!
dns-guard
!
interface Vlan1
 description *** Connected to 192.168.2.0/24 ***
 nameif INSIDE
 security-level 100
 ip address 192.168.2.1 255.255.255.0
 no shutdown
!
interface Vlan2
 description *** Connected to Internet ***
 nameif OUTSIDE
 security-level 0
 ip address 212.206.67.1 255.255.255.240
 no shutdown
!
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
!
interface Ethernet0/1
 switchport access vlan 1
no shutdown
!
interface Ethernet0/2
shutdown
!
interface Ethernet0/3
shutdown
!
interface Ethernet0/4
shutdown
!
interface Ethernet0/5
shutdown
```

```
!
interface Ethernet0/6
 shutdown
!
interface Ethernet0/7
 shutdown
!
!
ftp mode passive
!
dns server-group DefaultDNS
domain-name Creta-company.gr
!
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
!
!
!
!
access-list INSIDE_access_in extended permit ip 192.168.2.0 255.255.255.0 any
access-list INSIDE_access_in extended permit icmp 192.168.2.0 255.255.255.0 any
access-list OUTSIDE_access_in extended permit tcp any host PUBLIC-IP-MAILSRV eq smtp
access-list OUTSIDE_access_in extended permit tcp any host PUBLIC-IP-WEBSRV eq www
access-list OUTSIDE_access_in extended permit tcp any host PUBLIC-IP-MAILSRV eq https
access-list OUTSIDE_access_in extended permit icmp any host PUBLIC-IP-MAILSRV
access-list OUTSIDE_access_in extended permit icmp any host PUBLIC-IP-WEBSRV
access-list INSIDE_nat0_outbound extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
!
!
pager lines 24
logging enable
logging asdm informational
!
mtu OUTSIDE 1500
mtu INSIDE 1500
icmp unreachable rate-limit 1 burst-size 1
!
icmp permit any OUTSIDE
icmp permit any INSIDE
!
asdm image disk0:/asdm-623.bin
no asdm history enable
!
arp timeout 14400
!
nat-control
global (OUTSIDE) 1 interface
!
nat (INSIDE) 0 access-list INSIDE_nat0_outbound
!
nat (INSIDE) 1 192.168.2.0 255.255.255.0
!
static (INSIDE,OUTSIDE) PUBLIC-IP-MAILSRV PRIVATE-IP-MAILSRV netmask 255.255.255.255
static (INSIDE,OUTSIDE) PUBLIC-IP-FILESRV PRIVATE-IP-FILESRV netmask 255.255.255.255
static (INSIDE,OUTSIDE) PUBLIC-IP-WEBSRV PRIVATE-IP-WEBSRV netmask 255.255.255.255
!
access-group OUTSIDE_access_in in interface OUTSIDE
access-group INSIDE_access_in in interface INSIDE
!
route OUTSIDE 0.0.0.0 0.0.0.0 ROUTER 1
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
!
dynamic-access-policy-record DfltAccessPolicy
!
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
```

```
aaa authentication telnet console LOCAL
!
http server enable
http 192.168.2.0 255.255.255.0 INSIDE
!
sysopt noproxyarp INSIDE
!
!
!
telnet 192.168.2.0 255.255.255.0 INSIDE
telnet timeout 5
!
ssh 192.168.2.0 255.255.255.0 INSIDE
ssh timeout 5
ssh version 2
!
console timeout 0
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
username giorgos password gB9q/m.zrYGMEskE encrypted privilege 15
!
prompt hostname context
!
!
: end
```

SITE CRETA

ROUTER 1 CONFIGURATION

```
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C-HQ1
!
boot-start-marker
boot-end-marker
!
!
logging buffered 52000
enable secret 5 $1$VPDV$Y2wsKarawi6s.SrZWsaTL0
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
memory-size iomem 10
clock timezone PCTime 0 0
crypto pki token default removal timeout 0
```

```
!
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
crypto pki trustpoint CRETA-COMPANY
 enrollment selfsigned
 serial-number
 ip-address dialer1
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-2692466680
crypto pki certificate chain CRETA-COMPANY
 certificate self-signed D9
  30820275 308201DE A0030201 020201D9 300D0609 2A864886 F70D0101 04050030
  56315430 12060355 0405130B 46435A31 34303639 30445130 1A06092A 864886F7
  0D010908 130D3739 2E313239 2E36332E 31313930 2206092A 864886F7 0D010902
  16154851 312E636F 73746163 6F666665 652E6C6F 63616C30 1E170D31 31303531
  37313032 3932305A 170D3230 30313031 30303030 30305A30 56315430 12060355
  0405130B 46435A31 34303639 30445130 1A06092A 864886F7 0D010908 130D3739
  2E313239 2E36332E 31313930 2206092A 864886F7 0D010902 16154851 312E636F
  73746163 6F666665 652E6C6F 63616C30 819F300D 06092A86 4886F70D 01010105
  0003818D 00308189 02818100 EBC3E3F3 51848236 89C90B84 A8BC50AA 621D1BFA
  002726EB 3766F20B 323D05A1 EB510FB1 61931375 D507649B A63C5574 C77A3A94
  378464E3 6F03EA7F EEF00099 4C89C439 ABB3A302 A912B46B 249BFC93 EF3494C5
  2DA29887 8D8E3FDF BF77AE8D 9E2C3FDF 7A498F5F ED7545B2 D8F88B43 C6AD789C
  E15B6A15 AFC250AB 6D7C9357 02030100 01A35330 51300F06 03551D13 0101FF04
  05300301 01FF301F 0603551D 23041830 16801474 941080A4 AE0296A8 125AF422
  DB25BC09 269B5E30 1D060355 1D0E0416 04147494 1080A4AE 0296A812 5AF422DB
  25BC0926 9B5E300D 06092A86 4886F70D 01010405 00038181 00A5AE13 36E86E55
  42CDBC42 60B29E8B E5C1C9B3 30976154 D55A9E6C D8E6A6F2 F47E99FB 8FA96D9F
  7CCD278A 33E56040 58E91206 89ED899E C4EAAB6D C8A7DE55 0053B2CE B25F0B0E
  58D0945A 34702143 DC003097 DF82385E 69CEA20D 65D6F964 AA66C159 23310067
  F3D96D6B FEF4B361 F2C63489 849F29CB 4400ABAB 60D07686 21
       quit
ip source-route
!
!
!
!
!
ip cef
ip domain name Creta-company
ip name-server 195.170.0.1
ip name-server 195.170.2.2
!
!
archive
 log config
  hidekeys
!
!
username giorgos privilege 15 secret 5 $1$JbHo$hj3h0xCJkY33sN27vUEYX.
secure boot-image
secure boot-config
!
!
!
!
!
track 123 ip sla 1 reachability
!
track 456 ip sla 2 reachability
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
```

```
 authentication pre-share
 group 2
!
crypto isakmp key C#om-An1@ address 62.65.105.10 no-xauth
crypto isakmp key C#om-An1@ address 62.65.105.11 no-xauth
!
crypto isakmp fragmentation
crypto isakmp keepalive 10
crypto isakmp xauth timeout 45
!
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
!
!
!
!
!
!
!
crypto map SDM_CMAP_1  ipsec-isakmp
 description Tunnel  to Athens
 set peer 62.65.105.10  default
 set peer 62.65.105.11
 set transform-set ESP-3DES-SHA
 match address 104
!
!
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
no shutdown

!
!
interface ATM0.4 point-to-point
 pvc 8/35
  pppoe-client dial-pool-number 1
 !
!
!
interface FastEthernet0
 ip address 212.206.67.2 255.255.255.240
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache cef
 no ip route-cache
 no shutdown
!
interface Dialer1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly in
 encapsulation ppp
 no ip route-cache cef
 no ip route-cache
 dialer pool 1
 dialer-group 1
 ppp authentication chap pap callin
 ppp chap hostname c-giorg@otenet.gr
 ppp chap password 0 giorg1
 ppp pap sent-username c-giorg@otenet.gr password 0 giorg1
 no cdp enable
 crypto map SDM_CMAP_1
 no shutdown
!
!
router rip
 version 2
 redistribute static
```

```
 network 212.206.67.0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
!
!
!
!
!
!
!
ip nat inside source list 192 interface Dialer1 overload
!
ip route 0.0.0.0 0.0.0.0 Dialer1 track 123
ip route 0.0.0.0 0.0.0.0 212.206.67.3 track 456
ip route 0.0.0.0 0.0.0.0 Dialer1
!
ip route 192.168.2.0 255.255.255.0 212.206.67.1 permanent
ip route 195.170.2..1 255.255.255.255 212.206.67.3
!
!
ip sla 1
 icmp-echo 195.170.0.2 source-interface Dialer1
 threshold 3
 frequency 5
ip sla schedule 1 life forever start-time now
!
!
ip sla 2
 icmp-echo 195.170.2.1 source-interface FastEthernet0
 threshold 3
 frequency 5
ip sla schedule 2 life forever start-time now
!
!
access-list 104 remark IPSec Rule
access-list 104 permit ip 192.168.2. 0.0.0.255 192.168.1.0 0.0.0.255
!
access-list 192 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 192 permit ip 192.168.2.0 0.0.0.255  any
access-list 192 permit ip 212.206.67.3 any

!
dialer-list 1 protocol ip permit
!
no cdp run
!
!
banner motd ^CWelcome to Router C-HQ1 – Creta -company^C
!
line con 0
!
line aux 0
!
line vty 0 4
transport input telnet ssh
!
end
```

SITE CRETA

ROUTER 2 CONFIGURATION

```
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C-HQ2
!
boot-start-marker
boot-end-marker
!
!
logging buffered 52000
enable secret 5 $1$VPDV$Y2wsKarawi6s.SrZWsaTL0
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
memory-size iomem 10
clock timezone PCTime 0 0
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
crypto pki trustpoint CRETA-COMPANY
 enrollment selfsigned
 serial-number
 ip-address dialer1
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-2692466680
crypto pki certificate chain CRETA-COMPANY
 certificate self-signed D9
  30820275 308201DE A0030201 020201D9 300D0609 2A864886 F70D0101 04050030
  56315430 12060355 0405130B 46435A31 34303639 30445130 1A06092A 864886F7
  0D010908 130D3739 2E313239 2E36332E 31313930 2206092A 864886F7 0D010902
  16154851 312E636F 73746163 6F666665 652E6C6F 63616C30 1E170D31 31303531
  37313032 3932305A 170D3230 30313031 30303030 30305A30 56315430 12060355
  0405130B 46435A31 34303639 30445130 1A06092A 864886F7 0D010908 130D3739
  2E313239 2E36332E 31313930 2206092A 864886F7 0D010902 16154851 312E636F
  73746163 6F666665 652E6C6F 63616C30 819F300D 06092A86 4886F70D 01010105
  0003818D 00308189 02818100 EBC3E3F3 51848236 89C90B84 A8BC50AA 621D1BFA
  002726EB 3766F20B 323D05A1 EB510FB1 61931375 D507649B A63C5574 C77A3A94
  378464E3 6F03EA7F EEF00099 4C89C439 ABB3A302 A912B46B 249BFC93 EF3494C5
  2DA29887 8D8E3FDF BF77AE8D 9E2C3FDF 7A498F5F ED7545B2 D8F88B43 C6AD789C
  E15B6A15 AFC250AB 6D7C9357 02030100 01A35330 51300F06 03551D13 0101FF04
  05300301 01FF301F 0603551D 23041830 16801474 941080A4 AE0296A8 125AF422
  DB25BC09 269B5E30 1D060355 1D0E0416 04147494 1080A4AE 0296A812 5AF422DB
  25BC0926 9B5E300D 06092A86 4886F70D 01010405 00038181 00A5AE13 36E86E55
```

```
  42CDBC42 60B29E8B E5C1C9B3 30976154 D55A9E6C D8E6A6F2 F47E99FB 8FA96D9F
  7CCD278A 33E56040 58E91206 89ED899E C4EAAB6D C8A7DE55 0053B2CE B25F0B0E
  58D0945A 34702143 DC003097 DF82385E 69CEA20D 65D6F964 AA66C159 23310067
  F3D96D6B FEF4B361 F2C63489 849F29CB 4400ABAB 60D07686 21
       quit
ip source-route
!
!
!
!
!
ip cef
ip domain name Creta-company
ip name-server 195.170.0.1
ip name-server 195.170.2.2
!
!
archive
 log config
  hidekeys
!
!
username giorgos privilege 15 secret 5 $1$JbHo$hj3h0xCJkY33sN27vUEYX.
secure boot-image
secure boot-config
!
!
!
!
!
track 123 ip sla 1 reachability
!
track 456 ip sla 2 reachability
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp key C#om-An1@ address 62.65.105.10 no-xauth
crypto isakmp key C#om-An1@ address 62.65.105.11 no-xauth
!
crypto isakmp fragmentation
crypto isakmp keepalive 10
crypto isakmp xauth timeout 45
!
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
!
!
!
!
!
!
!
crypto map SDM_CMAP_1  ipsec-isakmp
 description Tunnel  to Athens
 set peer 62.65.105.11  default
 set peer 62.65.105.10
 set transform-set ESP-3DES-SHA
 match address 104
!
!
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
no shutdown
```

```
!
!
interface ATM0.4 point-to-point
 pvc 8/35
  pppoe-client dial-pool-number 1
 !
!
!
interface FastEthernet0
 ip address 212.206.67.3 255.255.255.240
 ip nat inside
 ip virtual-reassembly in
 no ip route-cache cef
 no ip route-cache
no shutdown
!
interface Dialer1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly in
 encapsulation ppp
 no ip route-cache cef
 no ip route-cache
 dialer pool 1
 dialer-group 1
 ppp authentication chap pap callin
 ppp chap hostname c-giorg12@otenet.gr
 ppp chap password 0 giorg2
 ppp pap sent-username c-giorg12@otenet.gr password 0 giorg2
 no cdp enable
 crypto map SDM_CMAP_1
 no shutdown
!
!
router rip
 version 2
 redistribute static
 network 212.206.67.0
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
!
!
!
!
!
!
!
ip nat inside source list 192 interface Dialer1 overload
!
ip route 0.0.0.0 0.0.0.0 Dialer1 track 123
ip route 0.0.0.0 0.0.0.0 212.206.67.2 track 456
ip route 0.0.0.0 0.0.0.0 Dialer1
!
ip route 192.168.2.0 255.255.255.0 212.206.67.1 permanent
ip route 195.170.0..2 255.255.255.255 212.206.67.2
!
!
ip sla 1
 icmp-echo 195.170.0.2 source-interface Dialer1
 threshold 3
 frequency 5
ip sla schedule 1 life forever start-time now
!
!
ip sla 2
```

```
 icmp-echo 195.170.2.1 source-interface FastEthernet0
 threshold 3
 frequency 5
ip sla schedule 2 life forever start-time now
!
!
access-list 104 remark IPSec Rule
access-list 104 permit ip 192.168.2. 0.0.0.255 192.168.1.0 0.0.0.255
!
access-list 192 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 192 permit ip 192.168.2.0 0.0.0.255  any
access-list 192 permit ip 212.206.67.2 any

!
dialer-list 1 protocol ip permit
!
no cdp run
!
!
banner motd ^CWelcome to Router C-HQ2 – Creta -company^C
!
line con 0
!
line aux 0
!
line vty 0 4
transport input telnet ssh
!
end
```

14.Βιβλιογραφία

Cisco (2007-2009) "*Cisco Networking Academy*"

Cisco (2011),Products and Services

<http://www.cisco.com/>

DLT-FBSC Corporation (2011), IT Infrastructure Services

<http://www.adanmore.com/>

Dr. Roy Winkelman, Director (2006), "*An Educator's Guide to School Networks*"

Florida Department For Education

Μιχάλης Παιγνιγιάννης (2009) "*Δομημένη Καλωδίωση στις πολυκατοικίες,υψηλή τεχνολογία ή απλά προνοητικότητα;*",

Ημερίδα ΕΛΕΜ