ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εγκατάσταση και παραμετροποίηση συστήματος LDAP

Των σπουδαστών:

Καπράνου Δημήτριου

Πετρουτζάκου Αχιλλέα

Εισηγητής:

Ασημακόπουλος Γεώργιος

Αντίρριο 2015

Ευχαριστίες

Επιτέλους φτάσαμε στο τέλος της φοιτητικής μας ζωής. Όλα αυτά τα όμορφα και δημιουργικά χρόνια τελείωσαν και θα ήταν μεγάλη παράληψη να μην ευχαριστήσουμε κάποιους ανθρώπους που μας στήριξαν και μας βοήθησαν ώστε να φτάσουμε σε αυτό το στόχο. Πάνω απ' όλα θέλουμε να ευχαριστήσουμε τους γονείς μας που με θυσίες και μόχθο μας συντηρούσαν τόσα χρόνια και επένδυσαν πάνω μας ώστε να γίνουμε καλύτεροι άνθρωποι και σημαντικοί για την κοινωνία. Θα πρέπει να ευχαριστήσουμε τους καθηγητές μας που όλα αυτά τα χρόνια προσπάθησαν να κάνουν το καλύτερο για εμάς και να μας καθοδηγήσουν σε νέους ορίζοντες γνώσης. Ειδικότερα θα θέλαμε να ευχαριστήσουμε τον Κ. Γεώργιο Ασημακόπουλο που χάρη σε αυτόν πραγματοποιήσαμε την πρακτική μας άσκηση στο ΤΕΙ μας, ίσως στο πιο μεταβατικό στάδιο της ιστορίας του, και ζήσαμε την μοναδική εμπειρία να βάλουμε και εμείς ένα λιθαράκι ώστε να φτιάξουμε από το μηδέν κάτι πραγματικά πανέμορφο.
Η συνεισφορά τους ήταν σημαντική τόσο σε εργασία όσο και σε ψυχολογική υποστήριξη.

Τέλος, ένα μεγάλο ευχαριστώ στα μέλη της εξεταστικής επιτροπής «κ. Ασημακόπουλο» ,τον « κ. Τριανταφύλλου» και τον « κ.Σκλάβο», που μας έκαναν την τιμή να αξιολογήσουν την προσπάθειά μας.
Σας Ευχαριστούμε!!!

Αχιλλέας & Δημήτρης

ΠΡΟΛΟΓΟΣ

Οι υπηρεσίες καταλόγου αποτελούν ένα σημαντικό μέρος των υπολογιστικών περιβαλλόντων των επιχειρήσεων. Οι υπηρεσίες αυτές μας δίνουν την δυνατότητα να συλλέγουμε πληροφορίες που αφορούν χρήστες, εφαρμογές, αρχεία, πηγές εκτυπωτών, ελέγχους πρόσβασης και άλλους πόρους. Οι πληροφορίες αυτές αποθηκεύονται σε έναν κατάλογο ο οποίος προσπελάζεται από τους χρήστες και τις εφαρμογές ενός δικτύου. Όλες οι εφαρμογές καταλόγου μπορούν να χρησιμοποιηθούν από τις επιχειρήσεις. Αυτό ελαχιστοποιεί τις νησίδες πληροφορίας που δημιουργούνται όταν οι εφαρμογές χρησιμοποιούν τις δικές τους εξειδικευμένες αποθήκες για να διαχειριστούν τις πληροφορίες των πόρων. Επιπλέον οι υπηρεσίες αυτές βελτιώνουν την διοίκηση επειδή η διαχείριση των πληροφοριών είναι συγκεντρωτική. Οποιεσδήποτε προσθήκες ή αλλαγές που γίνονται στις πληροφορίες καταλόγου είναι άμεσα διαθέσιμες σε όλους τους χρήστες και σε όλες τις εφαρμογές που χρησιμοποιούν τον κατάλογο. Παραδείγματος χάριν, αντί της αλλαγής του καταλόγου ελέγχου πρόσβασης ενός πόρου σε κάθε σύστημα που το προσπελάζει, μπορεί να γίνει αλλαγή μόνο μιας πληροφορίας και αυτή να χρησιμοποιείται από κάθε εφαρμογή που ελέγχει την πρόσβαση σε αυτόν τον πόρο. Το LDAP (Lightweight Directory Access Protocol) είναι μια ταχέως αναπτυσσόμενη τεχνολογία για την πρόσβαση σε κοινές πληροφορίες καταλόγου και έχει υιοθετηθεί και εφαρμοσθεί από τα περισσότερα προϊόντα δικτύου. Ως ένα ανοιχτό πρότυπο παρέχει μια αρχιτεκτονική με δυνατότητα επέκτασης για την διαχείριση και συγκέντρωση αποθηκευμένων πληροφοριών οι οποίες πρέπει να είναι διαθέσιμες για τα σημερινά κατανεμημένα συστήματα και τις υπηρεσίες. Ύστερα από μια γρήγορη έναρξη, μπορεί να θεωρηθεί ότι το LDAP έχει γίνει η de facto μέθοδος πρόσβασης σε πληροφορίες καταλόγου, αρκετά παρόμοια με το DNS (Domain Name System) το οποίο χρησιμοποιείται για την αναζήτηση διευθύνσεων IP σχεδόν σε οποιοδήποτε σύστημα ενός Intranet ή στο Internet. Το LDAP πρόσφατα υποστηρίζεται από τα περισσότερα λειτουργικά δικτυακά συστήματα.

ΚΕΦΑΛΑΙΟ 1

Τι είναι LDAP :

Άτομα και επιχειρήσεις βασίζονται όλο και περισσότερο στα δικτυωμένα συστήματα υπολογιστών για να υποστηρίξουν κατανεμημένες εφαρμογές. Αυτές οι εφαρμογές ίσως να αλληλεπιδρούν με υπολογιστές που βρίσκονται στο ίδιο τοπικό δίκτυο (LAN), το οποίο είναι μέρος ενός εταιρικού δικτύου (Intranet) ή οπουδήποτε στο παγκόσμιο διαδίκτυο (Internet). Για την βελτίωση της λειτουργίας, της ευκολίας της χρήσης και για να είναι επιτρεπτή η οικονομικώς αποδοτική διαχείριση των κατανεμημένων εφαρμογών πληροφοριών που αφορούν υπηρεσίες, πόρους, χρήστες και άλλα αντικείμενα που είναι προσβάσιμα μέσω των εφαρμογών, χρειάζεται να είναι οργανωμένες με ένα σαφή και συνεπή τρόπο. Ένα μεγάλο μέρος αυτών των πληροφοριών μπορεί να διαμοιραστεί μεταξύ πολλών εφαρμογών, αλλά συγχρόνως πρέπει να προστατεύεται για να αποτρέπεται η παράνομη τροποποίηση ή η κοινοποίηση των ιδιωτικών πληροφοριών.

Οι πληροφορίες που χαρακτηρίζουν τους διάφορους χρήστες, τις εφαρμογές, τα αρχεία, τους εκτυπωτές και άλλους πόρους που προσπελαύνονται από ένα δίκτυο, συχνά συγκεντρώνονται σε μια ειδική βάση δεδομένων που μερικές φορές αποκαλείται «κατάλογος». Καθώς έχει αυξηθεί ο αριθμός των διαφορετικών δικτύων και εφαρμογών, έχει επίσης αυξηθεί ο αριθμός των εξειδικευμένων καταλόγων πληροφοριών με αποτέλεσμα να δημιουργούνται νησίδες πληροφοριών οι οποίες δεν μπορούν να είναι κοινόχρηστες και είναι πολύ δύσκολο να διατηρούνται. Εάν όλες αυτές οι πληροφορίες μπορούσαν να διατηρούνται και να είναι προσπελάσιμες κατά τρόπο συνεχή και ελεγχόμενο θα παρεχόταν ένα σημείο συγκέντρωσης για την ενσωμάτωση ενός κατανεμημένου περιβάλλοντος σε ένα συνεπές και χωρίς όρια σύστημα.

Το Ελαφρύ Πρωτόκολλο Πρόσβασης Καταλόγου (LDAP) είναι ένα ανοιχτό βιομηχανικό πρότυπο το οποίο έχει εξελιχθεί για να ικανοποιήσει αυτές τις ανάγκες. Το LDAP καθορίζει μια πρότυπη μέθοδο για την πρόσβαση και ενημέρωση των πληροφοριών σε ένα κατάλογο. Το LDAP κερδίζει ευρεία αποδοχή ως μέθοδος πρόσβασης καταλόγου του Internet και επομένως γίνεται στρατηγικό μέσο στα εταιρικά Intranets. Υποστηρίζεται από έναν αυξανόμενο αριθμό προμηθευτών λογισμικού και είναι ενσωματωμένο σε ένα μεγάλο αριθμό εφαρμογών που συνεχώς αυξάνεται.

1.1 Έννοια Καταλόγου και Υπηρεσίας Καταλόγου

Ένας κατάλογος (directory) είναι μια λίστα πληροφοριών για αντικείμενα τα οποία είναι τακτοποιημένα με κάποια σειρά και δίνει λεπτομέρειες για κάθε αντικείμενο χωριστά. Κοινά παραδείγματα αποτελούν ο τηλεφωνικός κατάλογος μιας πόλης και ο κατάλογος καρτών μιας βιβλιοθήκης. Για έναν τηλεφωνικό κατάλογο, τα αντικείμενα τα οποία ταξινομούνται είναι άτομα. Τα ονόματά τους τακτοποιούνται αλφαβητικά και οι λεπτομέρειες που δίνονται για κάθε άτομο είναι η διεύθυνσή του και ο τηλεφωνικός αριθμός του. Τα βιβλία σε έναν κατάλογο καρτών μιας βιβλιοθήκης διατάσσονται σύμφωνα με τον συγγραφέα και τον τίτλο του βιβλίου και δίνονται πληροφορίες όπως ο αριθμός
ISBN του βιβλίου ή οποιαδήποτε άλλη πληροφορία που αφορά τις εκδόσεις. Στην ορολογία των υπολογιστών, ένας κατάλογος είναι μια εξειδικευμένη βάση δεδομένων, αποκαλούμενη επίσης «αποθήκη δεδομένων», στην οποία αποθηκεύονται τυποποιημένες και διατεταγμένες πληροφορίες για τα αντικείμενα. Ένας ειδικός κατάλογος μπορεί να απαριθμεί πληροφορίες για τους εκτυπωτές (αντικείμενα) οι οποίες περιέχουν τυποποιημένες πληροφορίες όπως η θέση των εκτυπωτών (ένα μορφοποιημένο string χαρακτήρων), η ταχύτητα των σελίδων ανά λεπτό (αριθμητικό), οι ροές εκτύπωσης που υποστηρίζονται (π.χ PostScript ή ASCII) και ούτω καθεξής. Οι κατάλογοι επιτρέπουν στους χρήστες ή στις εφαρμογές να βρουν πηγές που έχουν τα χαρακτηριστικά που χρειάζονται για ένα συγκεκριμένο σκοπό. Για παράδειγμα, ένας κατάλογος χρηστών μπορεί να χρησιμοποιηθεί για την ανεύρεση της ηλεκτρονικής διεύθυνσης ενός ατόμου ή ενός αριθμού FAX. Ή ένας κατάλογος που αποτελείται από εξυπηρετητές εφαρμογής μπορεί να αναζητήσει στα περιεχομενά του έναν εξυπηρετητή (server) ο οποίος παρέχει πρόσβαση σε πληροφορίες τιμολόγησης πελατών.

Μια υπηρεσία καταλόγου (directory service) αποθηκεύει πληροφορίες στον κατάλογο και ανακτά πληροφορίες από αυτόν εξ ονόματος ενός ή περισσοτέρων εξουσιοδοτημένων χρηστών. Οι υπηρεσίες καταλόγου υλοποιούνται με σκοπό την παροχή ορισμένων τύπων πληροφορίας για τις ανάγκες εφαρμογών. Ωστόσο, διαφορετικές υπηρεσίες καταλόγου μπορούν να μοιράζονται τον ίδιο κατάλογο. Για παράδειγμα, ας υποθέσουμε ότι διαθέτουμε δυο τηλεφωνικούς κατάλόγους, έναν White Pages κατάλογο και έναν Yellow Pages κατάλογο. Και οι δύο διαθέτουν τηλεφωνικούς αριθμούς αλλά με διαφορετικό τρόπο. Ο κατάλογος των «λευκών σελίδων» μας δίνει την δυνατότητα να βρούμε τον τηλεφωνικό αριθμό ενός ατόμου, ενώ ο κατάλογος των «κίτρινων σελίδων» μας επιτρέπει να αναζητούμε κατηγορίες πληροφοριών και να ανακτούμε ποικίλους τηλεφωνικούς αριθμούς. Για την εφαρμογή των δύο υπηρεσιών μπορεί να χρησιμοποιηθεί ο ίδιος κατάλογος. Στο παράδειγμα αυτό, ο συγκεκριμένος κατάλογος θα περιείχε το μοντέλο των

δεδομένων για να περιγράψει τον διαφορετικό τύπο χρηστών και πληροφοριών. Στην πραγματικότητα υπάρχουν δύο διαφορετικές υπηρεσίες καταλόγου. Η μια δίνει πρόσβαση στα δεδομένα των White Pages και η άλλη στα δεδομένα των Yellow Pages. Εντούτοις, και οι δύο μπορούν να χρησιμοποιούν τον ίδιο κατάλογο. Αυτό που συμβαίνει είναι ότι το μοντέλο δεδομένων της υπηρεσίας «λευκών σελίδων» επεκτείνεται ώστε να ταιριάζει με τις πιο σύνθετες ανάγκες της υπηρεσίας των «κίτρινων σελίδων».Το παράδειγμα αυτό δείχνει επίσης ότι οι υπηρεσίες καταλόγου συνήθως λειτουργούν με ένα συγκεκριμένο τρόπο. Παραδείγματος χάριν δεν μπορούμε να δώσουμε τον τηλεφωνικό αριθμό ενός ατόμου στην υπηρεσία White Pages και να αναμένουμε να μας δοθεί (με εύκολο τρόπο) το άτομο στο οποίο αντιστοιχεί ο αριθμός.
Κατά συνέπεια οι όροι «λευκές» και «κίτρινες» σελίδες χρησιμοποιούνται για να περιγράψουν το πώς χρησιμοποιείται ένας κατάλογος. Εάν το όνομα ενός αντικειμένου (άτομο, εκτυπωτής) είναι γνωστό, τότε τα χαρακτηριστικά του (τηλεφωνικός αριθμός, σελίδες ανά λεπτό) μπορούν να ανακτηθούν. Εάν το όνομα ενός μεμονωμένου αντικειμένου δεν είναι γνωστό, ο κατάλογος μπορεί να ψάξει στις αποθηκευμένες πληροφορίες του για μια λίστα αντικειμένων που καλύπτουν μια ορισμένη απαίτηση. Έτσι, οι κατάλογοι που αποθηκεύονται σε ένα ηλεκτρονικό υπολογιστή εν αντιθέσει με τους τηλεφωνικούς, είναι περισσότερο ευέλικτοι γιατί συνήθως μπορούν να εξερευνηθούν με συγκεκριμένα κριτήρια και όχι από ένα σύνολο προκαθορισμένων κατηγοριών.

1.1.1 Χαρακτηριστικά ενός Καταλόγου

Οι κατάλογοι έχουν πέντε σημαντικά χαρακτηριστικά:

- Η αποθήκευση των πληροφοριών προσαρμόζεται έτσι ώστε οι πληροφορίες να διαβάζονται συχνότερα παρά να ενημερώνονται.

  Οι κατάλογοι είναι κατάλληλοι για την εκτέλεση μεγάλου μήκους αναζητήσεων αλλά δεν ενδείκνυνται για την εφαρμογή λειτουργιών που απαιτούν συχνή ενημέρωση (π.χ συστήματα αεροπορικών κρατήσεων).

• Οι πληροφορίες αποθηκεύονται με τρόπο ιεραρχικό.

Η δομή των πληροφοριών βασίζεται στις σχέσεις πρώτου ανιόντος-πρώτου κατιόντος (father-child).

• Οι πληροφορίες του καταλόγου βασίζονται στα χαρακτηριστικά.

Ο κατάλογος αποτελείται από ένα σύνολο αντικειμένων (objects). Καθένα από τα αντικείμενα διαθέτει μια ομάδα χαρακτηριστικών (attributes) τα οποία περιέχουν πληροφορίες. Κατά συνέπεια, η πληροφορία διοχετεύεται στα χαρακτηριστικά των αντικειμένων τα οποία σχηματίζουν την υποδομή του καταλόγου.

• Οι κατάλογοι παρέχουν ένα ενοποιημένο namespace για όλους τους πόρους για τους οποίους διαθέτουν πληροφορία.

Οι κοινές πληροφορίες εντοπίζονται και διαμοιράζονται από διαφορετικούς πελάτες καταλόγου επειδή κάθε εφαρμογή μπορεί να χρησιμοποιήσει την ίδια μέθοδο παραπομπής ενός αντικειμένου. Ένα ενοποιημένο namespace δίνει την δυνατότητα στα στοιχεία του δικτύου και των υπηρεσιών να ενοποιούνται με άλλους τύπους πληροφοριών, όπως χρήστες, εφαρμογές και servers.

• Οι κατάλογοι μπορούν να διανείμουν αποτελεσματικά την πληροφορία σε ένα κατανεμημένο σύστημα μέσω της πολλαπλότητας υλικού.

Ο server καταλόγου έχει την ικανότητα να ελέγχει το είδος της πληροφορίας που κατανέμεται, τη χρονική στιγμή που συμβαίνει αυτό και σε ποιους κόμβους του συστήματος.

1.1.2 Directories vs. Databases

Ένας κατάλογος συχνά περιγράφεται ως Βάση Δεδομένων αλλά είναι μια εξειδικευμένη Βάση Δεδομένων η οποία έχει χαρακτηριστικά που την κάνουν να

ξεχωρίζει από το γενικό σκοπό των Σχεσιακών Βάσεων Δεδομένων. Ένα ειδικό χαρακτηριστικό των καταλόγων είναι ότι προσπελάζονται (μέσω της ανάγνωσης ή της αναζήτησης) πολύ πιο συχνά απ' ότι ενημερώνονται (μέσω της εγγραφής). Εκατοντάδες άνθρωποι μπορούν να ανατρέξουν στα χαρακτηριστικά ενός τηλεφωνικού αριθμού ή χιλιάδες χρήστες εκτυπωτών ίσως να ανατρέξουν στα χαρακτηριστικά ενός συγκεκριμένου εκτυπωτή. Όμως ο τηλεφωνικός αριθμός ή τα χαρακτηριστικά του εκτυπωτή σπάνια αλλάζουν.

Επειδή οι κατάλογοι πρέπει να είναι σε θέση να υποστηρίζουν μεγάλο όγκο αιτημάτων ανάγνωσης, είναι βελτιστοποιημένοι για πρόσβαση ανάγνωσης. Η πρόσβαση εγγραφής μπορεί να επιτρέπεται στους διαχειριστές συστήματος ή στους δικαιούχους κάθε μέρους της πληροφορίας. Από την άλλη πλευρά, ο γενικός σκοπός της Βάσης Δεδομένων χρειάζεται να υποστηρίζει εφαρμογές όπως αεροπορικές κρατήσεις και τραπεζικές συναλλαγές με μεγάλο βαθμό ενημέρωσης.

Επειδή οι κατάλογοι προορίζονταν για την αποθήκευση σχετικά στατικών πληροφοριών και συνεχίζουν να παραμένουν σε αυτόν τον σκοπό, δεν είναι κατάλληλοι για αποθήκευση πληροφορίας που διαρκώς μεταβάλλεται. Για παράδειγμα, ο αριθμός των εργασιών που βρίσκονται προσωρινά στην ουρά ενός εκτυπωτή πιθανόν να μην πρέπει να αποθηκεύεται στον κατάλογο του εκτυπωτή επειδή οι συγκεκριμένες πληροφορίες θα έπρεπε να ενημερώνονται συχνά για να μπορεί να επαληθεύεται η ορθότητά τους. Αντί για αυτό, η καταχώρηση καταλόγου του εκτυπωτή θα μπορούσε να περιέχει την διεύθυνση δικτύου ενός εκτυπωτή server. Ο εκτυπωτής server θα μπορούσε να ερωτηθεί ώστε να γίνει γνωστό το μήκος της τρέχουσας ουράς. Η πληροφορία που βρίσκεται στον κατάλογο (η διεύθυνση του εκτυπωτή server) είναι στατική, ενώ ο αριθμός των εργασιών στην ουρά εκτύπωσης είναι δυναμικός.

Μια άλλη σημαντική διαφορά μεταξύ των καταλόγων και των -γενικού σκοπού- Βάσεων Δεδομένων είναι ότι οι κατάλογοι μπορεί να μην υποστηρίζουν δοσοληψίες. Οι δοσοληψίες είναι διαδικασίες που συντελούνται συνολικά ή καθόλου. Για παράδειγμα, κατά την μεταφορά χρηματικού ποσού από έναν τραπεζικό λογαριασμό σε έναν άλλο, τα χρήματα πρέπει να χρεωθούν πρώτα στον έναν λογαριασμό και έπειτα στον άλλο και όλα αυτά να γίνουν σε μια και μόνο δοσοληψία. Εάν ολοκληρωθεί μόνο το μισό μέρος αυτής της δοσοληψίας ή κάποιος παρέμβει στους λογαριασμούς κατά την διάρκεια μεταφοράς των χρημάτων, οι λογαριασμοί δεν θα είναι ισορροπημένοι. Συνήθως οι -γενικού σκοπού- Βάσεις Δεδομένων υποστηρίζουν τέτοιου είδους δοσοληψίες οι οποίες κάνουν δύσκολη την εφαρμογή τους. Επειδή οι κατάλογοι ασχολούνται περισσότερο με αιτήματα ανάγνωσης, οι δυσκολίες των δοσοληψιών μπορούν να αποφευχθούν. Εάν δυο άτομα ανταλλάξουν γραφεία, θα πρέπει να ενημερωθούν οι καταχωρήσεις καταλόγου τους με νέους τηλεφωνικούς αριθμούς, με τις καινούριες θέσεις των σταθμών εργασίας και ούτω καθεξής. Εάν ενημερωθεί μια καταχώρηση καταλόγου και στη συνέχεια μια άλλη, υπάρχει μια σύντομη χρονική περίοδος που ο κατάλογος θα δείξει ότι και τα δύο άτομα έχουν τον ίδιο αριθμό τηλεφώνου. Επειδή οι ενημερώσεις είναι σχετικά σπάνιες, τέτοιες ανωμαλίες θεωρούνται αποδεκτές.

Το είδος των πληροφοριών που αποθηκεύεται σε έναν κατάλογο συνήθως δεν απαιτεί ακριβή συνέπεια. Μπορεί να είναι ανεκτό το γεγονός ότι μια πληροφορία, όπως ένας τηλεφωνικός αριθμός, ίσως να βρίσκεται προσωρινά εκτός λειτουργίας. Επειδή οι κατάλογοι δεν είναι κατάλληλοι για δοσοληψίες, δεν είναι καλή ιδέα να χρησιμοποιούνται για την αποθήκευση πληροφοριών που είναι ευαίσθητες σε ασυνέπειες όπως οι ισορροπίες τραπεζικών λογαριασμών.

Επειδή οι -γενικού σκοπού- Βάσεις Δεδομένων πρέπει να υποστηρίζουν αυθαίρετες εφαρμογές όπως τον έλεγχο τραπεζικών εργασιών, επιτρέπουν να αποθηκεύονται αυθαίρετες συλλογές δεδομένων. Οι κατάλογοι μπορούν να περιορίζονται στον τύπο των δεδομένων που επιτρέπουν για αποθήκευση (αν και η αρχιτεκτονική δεν επιβάλλει έναν τέτοιο περιορισμό). Για παράδειγμα, ένας κατάλογος που ειδικεύεται στις πληροφορίες επικοινωνίας πελατών μπορεί να περιοριστεί μόνο στην αποθήκευση προσωπικών πληροφοριών όπως ονομάτων, διευθύνσεων και τηλεφωνικών αριθμών. Εάν ένας κατάλογος είναι επεκτάσιμος,

μπορεί να διαμορφωθεί με τρόπο που να αποθηκεύει ποικίλους τύπους πληροφοριών που τον καθιστούν πιο χρήσιμο σε πολλά και διαφορετικά προγράμματα.

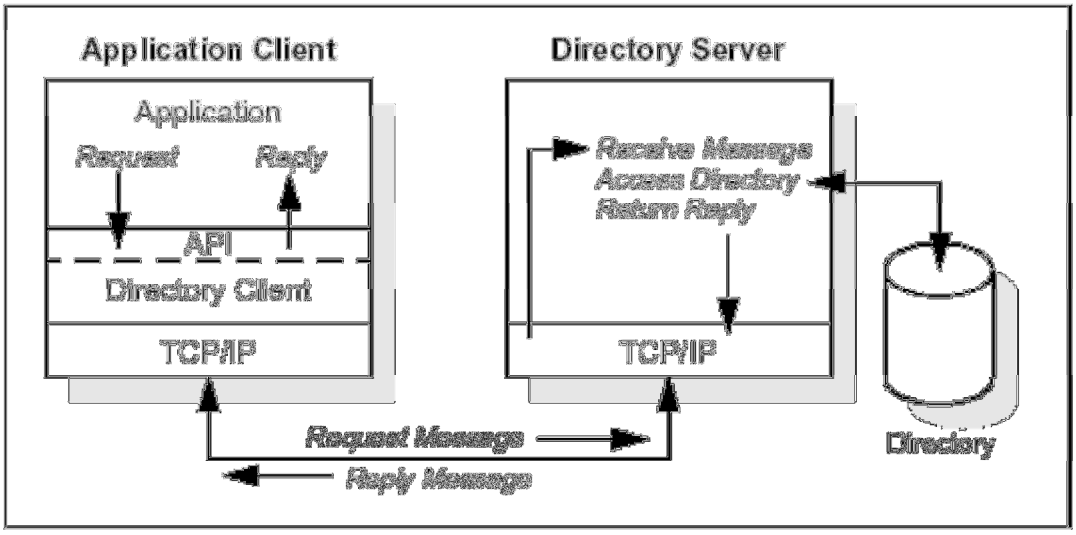
Μια άλλη σημαντική διαφορά μεταξύ των καταλόγων και των –γενικού σκοπού- Βάσεων Δεδομένων βρίσκεται στον τρόπο με τον οποίο προσεγγίζονται οι πληροφορίες. Οι περισσότερες Βάσεις Δεδομένων υποστηρίζουν μια ισχυρή τυποποιημένη μέθοδο πρόσβασης που ονομάζεται Δομημένη Γλώσσα Ερωτημάτων (SQL). Η SQL επιτρέπει πολύπλοκες ενημερώσεις και συναρτήσεις ερωτημάτων με κόστος το μέγεθος των προγραμμάτων και την πολυπλοκότητα των εφαρμογών. Από την άλλη πλευρά, οι κατάλογοι LDAP χρησιμοποιούν ένα απλουστευμένο και βελτιωμένο πρωτόκολλο πρόσβασης το οποίο μπορεί να εφαρμοσθεί σε μικρές και σχετικά απλές εφαρμογές.

Επειδή οι κατάλογοι δεν είναι προορισμένοι να παρέχουν τόσες λειτουργίες όσες προσφέρουν οι Βάσεις Δεδομένων, μπορούν να βελτιωθούν με οικονομικό τρόπο ώστε να παρέχουν περισσότερες λειτουργίες με άμεση πρόσβαση στα δεδομένα του καταλόγου σε μεγάλα κατανεμημένα συστήματα. Επειδή η εκτενής χρήση των καταλόγων είναι προορισμένη περισσότερο για ανάγνωση και όχι για δοσοληψίες μπορούν κατά συνέπεια να απλοποιηθούν ο πελάτης (client) και ο εξυπηρετητής (server) καταλόγου.

Πολλές διαφορές από τις οποίες αναφέρθηκαν μπορούν να οδηγήσουν στην υποψία ότι ένας κατάλογος δεν είναι κάτι περισσότερο από μια περιορισμένη σε λειτουργία Βάση Δεδομένων. Αυτό είναι πράγματι εν μέρει σωστό δεδομένου ότι ένας από τους σημαντικότερους σχεδιαστικούς στόχους μιας υπηρεσίας καταλόγου είναι ότι μπορεί να προσπελασθεί και να χρησιμοποιηθεί από σχετικά μικρές και απλές εφαρμογές. Επίσης συζητούνται προτάσεις στους οργανισμούς προτύπων για την πρόσθεση μερικών λειτουργιών στις μελλοντικές εκδόσεις του LDAP που ειδικεύονται στις Βάσεις Δεδομένων όπως η υποστήριξη των ενημερώσεων των δοσοληψιών.

1.1.3 Πελάτες και Εξυπηρετητές Καταλόγου

Οι κατάλογοι συνήθως προσπελάζονται με την χρησιμοποίηση του μοντέλου επικοινωνίας πελάτη / εξυπηρετητή (client/server). Μια εφαρμογή που επιθυμεί να διαβάσει ή να εγγράψει πληροφορία σε έναν κατάλογο δεν προσπελαύνει άμεσα τον κατάλογο. Αντί για αυτό καλεί μια λειτουργία, ένα API (Application Programming Interface), που αναγκάζει ένα μήνυμα να σταλεί σε μια άλλη διαδικασία. Η δεύτερη αυτή διαδικασία έχει πρόσβαση στην πληροφορία καταλόγου εξ ονόματος της εφαρμογής αίτησης. Έπειτα, τα αποτελέσματα της ανάγνωσης ή της εγγραφής επιστρέφονται στην εφαρμογή αίτησης (βλέπε σχήμα 1.1.3).



Σχήμα 1.1.3 Αλληλεπίδραση client/server καταλόγου

Το αίτημα εκτελείται από τον πελάτη καταλόγου και η διαδικασία αναζήτησης πληροφοριών σε έναν κατάλογο ονομάζεται εξυπηρετητής καταλόγου. Γενικά, οι εξυπηρετητές παρέχουν μια συγκεκριμένη υπηρεσία στους πελάτες. Μερικές φορές ένας εξυπηρετητής μπορεί να γίνει ο πελάτης άλλων εξυπηρετητών προκειμένου να συγκεντρώσει τις απαραίτητες πληροφορίες για να επεξεργαστεί ένα αίτημα.

Μια υπηρεσία καταλόγου είναι μια μόνο μορφή υπηρεσίας που μπορεί να είναι διαθέσιμη σε περιβάλλον client/server. Άλλα συνηθισμένα παραδείγματα υπηρεσιών είναι οι υπηρεσίες αρχείων, οι υπηρεσίες ηλεκτρονικού ταχυδρομείου, οι υπηρεσίες εκτύπωσης, οι υπηρεσίες ιστοσελίδων και ούτω καθεξής. Οι διαδικασίες του client και του server μπορούν να συντελούνται στο ίδιο μηχάνημα ή και όχι. Ένας server είναι σε θέση να εξυπηρετεί πολλούς πελάτες. Μερικοί servers μπορούν να επεξεργάζονται αιτήματα πελατών παράλληλα. Κάποιοι άλλοι βάζουν σε σειρά τα εισερχόμενα αιτήματα των clients για σειριακή επεξεργασία σε περίπτωση που είναι ήδη απασχολημένοι με την επεξεργασία άλλων αιτημάτων.
Ένα API καθορίζει την διεπαφή προγραμματισμού, μια ιδιαίτερη γλώσσα προγραμματισμού, που χρησιμοποιείται για την πρόσβαση σε μια υπηρεσία. Το format και τα περιεχόμενα των μηνυμάτων που ανταλλάσσονται μεταξύ του client και του server πρέπει να εμμένουν πάνω σε ένα συμφωνημένο πρωτόκολλο. Το LDAP καθορίζει ένα πρωτόκολλο μηνύματος που χρησιμοποιείται από τους clients και servers καταλόγου. Υπάρχει επίσης ένα σχετικό LDAP API για την γλώσσα προγραμματισμού C καθώς και τρόποι με τους οποίους μπορούμε να έχουμε πρόσβαση στο LDAP μέσω μιας εφαρμογής JAVA. Ο client δεν εξαρτάται από μια συγκεκριμένη εφαρμογή του server και ο server μπορεί να εφαρμόσει τον κατάλογο όπως αυτός επιλέξει.

1.1.4 Κατανεμημένοι Κατάλογοι

Οι όροι «τοπικός», «παγκόσμιος», «συγκεντρωτικός» και «κατανεμημένος» συχνά χρησιμοποιούνται για να περιγράψουν έναν κατάλογο ή μια υπηρεσία καταλόγου. Γενικά, με τον όρο «τοπικός» εννοούμε κάτι το οποίο βρίσκεται κοντά ενώ με τον όρο «παγκόσμιος» κάτι το οποίο εξαπλώνεται κατά μήκος του περιβάλλοντος που μας ενδιαφέρει. Το περιβάλλον που μας ενδιαφέρει μπορεί να είναι μια εταιρεία, μια χώρα ή ολόκληρη η Γη. Οι όροι «τοπικός» και «παγκόσμιος» είναι τα δύο άκρα μιας συνέχειας. Δηλαδή κάτι μπορεί να είναι περισσότερο ή λιγότερο τοπικό ή παγκόσμιο από κάτι άλλο. Συγκεντρωτικό σημαίνει κάτι το οποίο βρίσκεται σε ένα μέρος και κατανεμημένο κάτι το οποίο βρίσκεται σε περισσότερα από ένα μέρη. Ανάλογα με το τοπικό και το παγκόσμιο, κάτι μπορεί να είναι κατανεμημένο σε μικρότερη ή σε μεγαλύτερη έκταση.

Η αποθηκευμένη πληροφορία σε έναν κατάλογο μπορεί να είναι τοπική ή σφαιρική. Για παράδειγμα, ένας κατάλογος ο οποίος αποθηκεύει τοπική πληροφορία μπορεί να περιέχει ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, δημόσια κλειδιά κρυπτογράφησης και ούτω καθεξής, τα οποία αφορούν τα μέλη ενός τμήματος ή μια ομάδας εργαζομένων. Ένας κατάλογος που αποθηκεύει σφαιρική πληροφορία μπορεί να αποθηκεύσει πληροφορία για μια ολόκληρη εταιρεία. Στην προκείμενη περίπτωση μας ενδιαφέρει η εταιρεία. Οι πελάτες που έχουν πρόσβαση στις πληροφορίες καταλόγου μπορεί να είναι τοπικοί ή παγκόσμιοι. Οι τοπικοί μπορεί να βρίσκονται όλοι στο ίδιο κτίριο ή στο ίδιο τοπικό δίκτυο (LAN). Οι παγκόσμιοι μπορεί να είναι κατανεμημένοι κατά πλάτος της ηπείρου ή του πλανήτη.

Ο ίδιος κατάλογος μπορεί να είναι συγκεντρωτικός ή κατανεμημένος. Εάν ένας κατάλογος είναι συγκεντρωτικός, υπάρχει ένας server καταλόγου που παρέχει πρόσβαση στον κατάλογο ενώ αν είναι κατανεμημένος υπάρχουν περισσότεροι από έναν servers που δίνουν πρόσβαση στον κατάλογο. Όταν αναφερόμαστε σε έναν κατανεμημένο κατάλογο, συνήθως εννοούμε τους κατανεμημένους servers καταλόγου. Όταν ένας κατάλογος είναι κατανεμημένος η αποθηκευμένη πληροφορία του μπορεί να είναι χωρισμένη σε τμήματα ή να έχει αντίγραφα. Στην περίπτωση που η πληροφορία έχει την μορφή κατηγοριών, κάθε server καταλόγου αποθηκεύει ένα μοναδικό και μη επικαλυπτόμενο υποσύνολο της πληροφορίας. Δηλαδή κάθε καταχώρηση καταλόγου είναι αποθηκευμένη από έναν και μόνο έναν server. Όταν υπάρχουν αντίγραφα της πληροφορίας η ίδια καταχώρηση αποθηκεύεται σε περισσότερους από έναν servers. Σε έναν κατανεμημένο κατάλογο, κάποιες πληροφορίες μπορούν να είναι χωριστές και κάποιες να έχουν αντίγραφα.

Οι τρεις ‘’διαστάσεις’’ ενός καταλόγου – πεδίο της πληροφορίας, θέση των clients και διανομή των servers – είναι ανεξάρτητες μεταξύ τους. Παραδείγματος χάριν, οι πελάτες που είναι διασκορπισμένοι παγκοσμίως θα μπορούσαν να έχουν πρόσβαση σε έναν κατάλογο που περιέχει πληροφορία για ένα μόνο τμήμα και αυτός ο κατάλογος θα μπορούσε να αντιγραφθεί για πολλούς servers καταλόγου. Ή πελάτες που βρίσκονται σε μια μόνο θέση θα μπορούσαν να προσπελάσουν έναν κατάλογο ο οποίος περιέχει πληροφορίες για οποιονδήποτε στον κόσμο που είναι αποθηκευμένες από έναν μόνο server.

Το πεδίο των πληροφοριών που αποθηκεύεται σε έναν κατάλογο συχνά αποδίδεται ως μια απαίτηση εφαρμογής. Η διανομή των servers καταλόγου

και ο τρόπος με τον οποίο τα δεδομένα χωρίζονται ή αντιγράφονται μπορούν συχνά να ρυθμίζονται για να επηρεάζουν την απόδοση και την διαθεσιμότητα του καταλόγου. Για παράδειγμα, ένας κατανεμημένος και αντιγραμμένος κατάλογος μπορεί να έχει καλύτερη απόδοση επειδή ένα αίτημα ανάγνωσης μπορεί να εξυπηρετηθεί από έναν κοντινό server. Ένας συγκεντρωτικός κατάλογος μπορεί να είναι λιγότερο διαθέσιμος επειδή σε περίπτωση αποτυχίας δεν θα μπορεί να δώσει πληροφορίες δεδομένου ότι είναι μοναδικός και δεν υπάρχει αντίγραφο του. Ωστόσο, ένας κατανεμημένος κατάλογος ίσως να είναι πιο δύσκολο να διατηρηθεί, εξ αιτίας των πολλών θέσεων που πιθανόν βρίσκονται κάτω από τον έλεγχο πολλών διαχειριστών και που πρέπει να παραμένουν ενημερωμένες και σε κατάσταση λειτουργίας. Ο σχεδιασμός και η συντήρηση μιας υπηρεσίας καταλόγου μπορεί να είναι πολύπλοκες διαδικασίες.

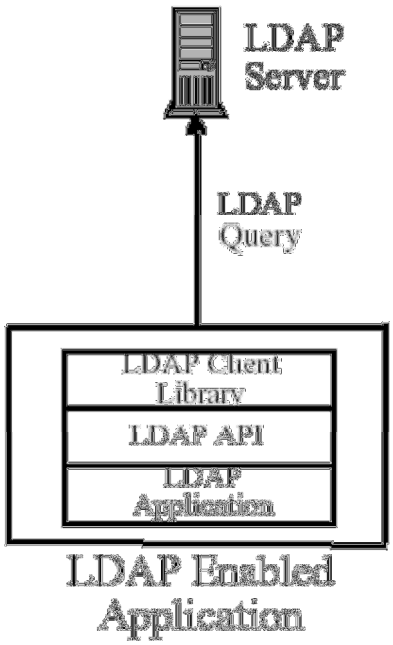
1.2 Ο Κατάλογος ως Υποδομή

Ένας κατάλογος ο οποίος προσπελαύνεται από όλες τις εφαρμογές αποτελεί ένα ζωτικής σημασίας μέρος της υποδομής που υποστηρίζει ένα κατανεμημένο σύστημα. Μια υπηρεσία καταλόγου προσφέρει μια ενιαία λογική όψη των χρηστών, των πόρων, και άλλων αντικειμένων που συνθέτουν ένα κατανεμημένο σύστημα. Αυτό επιτρέπει στους χρήστες και στις εφαρμογές να έχουν πρόσβαση στους δικτυακούς πόρους με τρόπο διαφανή. Δηλαδή, το σύστημα αντιμετωπίζεται σαν ένα σύνολο και όχι σαν μια συλλογή από ανεξάρτητα μέρη. Τα αντικείμενα μπορούν να προσεγγίζονται με το όνομα ή με μια λειτουργία χωρίς την γνώση προσδιοριστικών όπως οι host διευθύνσεις, ονόματα αρχείων εξυπηρετητών και διευθύνσεις ηλεκτρονικού ταχυδρομείου.

1.2.1 Διαθέσιμες Εφαρμογές Καταλόγου

Μια διαθέσιμη εφαρμογή καταλόγου είναι η εφαρμογή που χρησιμοποιεί μια υπηρεσία καταλόγου για να βελτιώσει την λειτουργικότητα της, την χρήση της και την διαχείρισή της. Σήμερα πολλές εφαρμογές κάνουν χρήση των πληροφοριών που θα μπορούσαν να αποθηκευθούν σε ένα κατάλογο. Για παράδειγμα, ας θεωρήσουμε μια εφαρμογή ημερολογίου που χρησιμοποιείται με σκοπό την οργάνωση συνεδριάσεων του προσωπικού μιας εταιρείας σε διαφορετικές αίθουσες διασκέψεων. Στην χειρότερη περίπτωση, η εφαρμογή ημερολογίου δεν χρησιμοποιεί καμία υπηρεσία καταλόγου. Εάν αυτό συνέβαινε, ο χρήστης που θα προσπαθούσε να προγραμματίσει ένα meeting θα έπρεπε να θυμάται τον αριθμό κάθε αίθουσας που θα ήταν κατάλληλη για το meeting. Και ακόμα θα αναρωτιόταν αν η αίθουσα είναι αρκετά μεγάλη, αν διαθέτει τον απαραίτητο ακουστικό και οπτικό εξοπλισμό και ούτω καθεξής. Επίσης ο χρήστης θα έπρεπε να θυμάται τα ονόματα και τις διευθύνσεις e-mail κάθε συμμετέχοντος που χρειάζεται να λάβει μια σημείωση συνεδρίασης. Είναι προφανές ότι μια τέτοια εφαρμογή θα ήταν δύσκολο να χρησιμοποιηθεί.

Εάν οι πληροφορίες για τις αίθουσες διάσκεψης (μέγεθος, τοποθεσία, ειδικός εξοπλισμός) και οι πληροφορίες προσωπικού (ονόματα, διευθύνσεις e-mail, τηλεφωνικοί αριθμοί και λοιπά) μπορούσαν να προσπελάζονται μέσω μιας υπηρεσίας καταλόγου, η εφαρμογή θα ήταν πολύ πιο εύκολο να χρησιμοποιηθεί. Επιπλέον, θα βελτιωνόταν η λειτουργικότητα της εφαρμογής. Παραδείγματος χάριν, θα μπορούσε να παρουσιάζεται στον χρήστη μια λίστα με όλες τις διαθέσιμες αίθουσες συνεδριάσεων καθώς και το μέγεθος και οι απαιτήσεις εξοπλισμού τους. Όμως οι υπεύθυνοι ανάπτυξης των διαθέσιμων εφαρμογών καταλόγου βρίσκονται αντιμέτωποι με ένα πρόβλημα. Τι θα συμβεί εάν δεν λάβουν υπόψη ότι μια υπηρεσία καταλόγου θα υπάρξει σε όλα τα περιβάλλοντα; Εάν υπάρχει μια υπηρεσία καταλόγου, αυτή μπορεί να ειδικεύεται σε ένα συγκεκριμένο λειτουργικό σύστημα δικτύου (NOS), καθιστώντας την εφαρμογή μη εκτελέσιμη. Μπορεί η υπάρχουσα υπηρεσία καταλόγου να διευρυνθεί για να αποθηκεύσειτον τύπο των πληροφοριών που χρειάζονται από την εφαρμογή; Λόγω αυτών των ανησυχιών, οι υπεύθυνοι ανάπτυξης εφαρμογών συχνά υιοθετούν την μέθοδο ανάπτυξης του δικού τους καταλόγου που θα υποστηρίζει μια συγκεκριμένη εφαρμογή.



1.2.2 Τα Πλεονεκτήματα ενός Κοινού Καταλόγου

Ένας κατάλογος που υποστηρίζει μια συγκεκριμένη εφαρμογή αποθηκεύει μόνο την πληροφορία που χρειάζεται αυτή η εφαρμογή και η οποία δεν μπορεί να προσπελαστεί από άλλες εφαρμογές. Επειδή είναι δύσκολο να στηθεί μια πλήρης λειτουργικά υπηρεσία καταλόγου, οι κατάλογοι ειδικών εφαρμογών είναι πολύ λίγοι. Πιθανόν να αποθηκεύουν μόνο ένα συγκεκριμένο τύπο πληροφορίας και ίσως να μην διαθέτουν δυνατότητες αναζήτησης ούτε την υποστήριξη της αντιγραφής και διαμοίρασης της πληροφορίας και να μην έχουν ένα πλήρες σύνολο εργαλείων διαχείρισης. Ένας κατάλογος μιας συγκεκριμένης εφαρμογής μπορεί να είναι τόσο απλός όσο ένα σύνολο αρχείων κειμένου ή θα μπορούσε να αποθηκευθεί και να προσεγγίζεται με έναν ατεκμηρίωτο, ιδιόκτητο τρόπο.
Σε έναν τέτοιο περιβάλλον, κάθε εφαρμογή δημιουργεί και διαχειρίζεται το δικό της κατάλογο. Αυτό γρήγορα γίνεται ένας εφιάλτης διαχείρισης. Η ίδια διεύθυνση e-mail που αποθηκεύεται από την εφαρμογή ημερολογίου μπορεί επίσης να αποθηκευθεί από μια εφαρμογή ταχυδρομείου και από μια εφαρμογή που ειδοποιεί τους χειριστές συστήματος για προβλήματα εξοπλισμού. Η προσπάθεια να διατηρούνται ενήμερα και συγχρονισμένα τα αντίγραφα των πληροφοριών είναι δύσκολη, ειδικά όταν αναμιγνύονται διαφορετικές διεπαφές χρηστών και διαφορετικά συστήματα διαχείρισης. Αυτό που χρειάζεται είναι ένας κοινός, ανεξάρτητος από εφαρμογές, κατάλογος. Αν οι υπεύθυνοι ανάπτυξης εφαρμογών μπορούσαν να βεβαιωθούν για την ύπαρξη μιας υπηρεσίας καταλόγου, τότε οι κατάλογοι ειδικών εφαρμογών δεν θαήταν απαραίτητοι. Ωστόσο, ένας κοινός κατάλογος πρέπει να βασίζεται σε ένα ανοιχτό πρότυπο το οποίο να υποστηρίζεται από πολλούς προμηθευτές σε πολλές πλατφόρμες και που πρέπει να προσεγγίζεται μέσω ενός πρότυπου
API. Είναι απαραίτητο να είναι επεκτάσιμο έτσι ώστε να μπορεί να κρατήσει τους τύπους των δεδομένων που χρειάζονται από τις αυθαίρετες δοκιμές. Και ακόμα πρέπει να παρέχει πλήρη λειτουργικότητα χωρίς να απαιτεί υπερβολικούς πόρους από τα μικρότερα συστήματα. Δεδομένου ότι περισσότεροι χρήστες και εφαρμογές θα έχουν πρόσβαση στον κοινό κατάλογο και θα εξαρτώνται από αυτόν, πρέπει επίσης να είναι εύρωστος, ασφαλής και με δυνατότητες εξέλιξης.
Όταν μια τέτοια υποδομή καταλόγου βρίσκεται σε ισχύ, οι υπεύθυνοι ανάπτυξης εφαρμογών μπορούν να αφιερώσουν τον χρόνο τους στην ανάπτυξη εφαρμογών και όχι στην δημιουργία καταλόγων που υποστηρίζουν συγκεκριμένες εφαρμογές. Με αυτόν τον τρόπο, οι υπεύθυνοι ανάπτυξης εφαρμογών που βασίζονται στην επικοινωνιακή δομή του TCP/IP και στην απομακρυσμένη διαδικασία κλήσης (RPC), θα είναι σε θέση να στηριχτούν σε ισχυρές, πλήρους λειτουργίας υπηρεσίες καταλόγου. Το LDAP είναι το πρωτόκολλο που πρέπει να χρησιμοποιηθεί για την πρόσβαση σε αυτή την κοινή υποδομή καταλόγου. Όπως το HTTP (Hypertext Transfer Protocol) και το FTP (File Transfer Protocol), έτσι και το LDAP είναι ένα απαραίτητο μέρος της ακολουθίας πρωτοκόλλων του Internet.
Όταν οι εφαρμογές έχουν πρόσβαση σε έναν πρότυπο κοινό κατάλογο παρά σε έναν κατάλογο που υποστηρίζει εξειδικευμένες εφαρμογές, τότε η περιττή

και δαπανηρή διαχείριση μπορεί να εξαλειφθεί και οι κίνδυνοι ασφάλειας να είναι περισσότερο ελεγχόμενοι. Οι εφαρμογές ημερολογίου, ταχυδρομείου και ενημερώσεων των χειριστών μπορούν να προσπελαύνουν τον ίδιο κατάλογο για να ανακτήσουν ένα δεδομένο όπως για παράδειγμα μια διεύθυνση e-mail. Θα εμφανιστούν νέες χρήσεις του καταλόγου πληροφοριών και θα αναπτυχθεί μια σύμπραξη καθώς περισσότερες εφαρμογές θα επωφεληθούν από τον κοινό κατάλογο.

1.3 Πρότυπα και Ιστορία του LDAP

Κατά τη δεκαετία του 1970, η ολοκλήρωση των επικοινωνιών και των τεχνολογιών πληροφορικής οδήγησε στην ανάπτυξη νέων τεχνολογιών επικοινωνίας. Πολλά από τα ιδιωτικά συστήματα που αναπτύχθηκαν ήταν μη συμβατά με άλλα συστήματα. Έγινε προφανές ότι χρειάζονταν πρότυπα για να επιτρέψουν στους εξοπλισμούς και στα συστήματα διαφορετικών προμηθευτών να επικοινωνήσουν μεταξύ τους. Για τον καθορισμό τέτοιων προτύπων αναπτύχθηκαν δυο κορυφαίες ανεξάρτητες προσπάθειες τυποποίησης.

1.3.1 ΤΟ OSI και το Internet

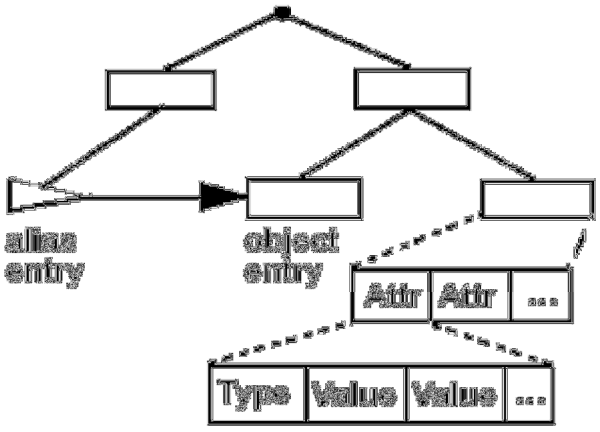
Μια κίνηση προτύπων έγινε από την CCITT (*Comite Consultatif International Telephonique et Telegrafique,* ή *Consultative Committee on International Telephony and Telegraphy*) και τον ISO (*International Standards Organization*). Η CCITT έχει γίνει από τότε η ITU-T (*International Telecommunications Union- Telecommunication Standardization Sector*). Η προσπάθεια αυτή οδήγησε στο πρότυπο αναφοράς (ISO
7498) του
OSI (Open Systems Interconnect), το οποίο καθόρισε ένα μοντέλο δεδομένων επικοινωνίας επτά επιπέδων με φυσική μεταφορά στο χαμηλότερο στρώμα και των πρωτοκόλλων εφαρμογής στα ανώτερα επίπεδα.
Η άλλη κίνηση προτύπων έγινε γύρω από το Internet και αναπτύχθηκε από την έρευνα που υποστηρίχθηκε από το DARPA (*the Defense Advanced Research Projects Agency*) στις Ηνωμένες Πολιτείες. Ο *Internet Architecture*

Board (IAB) και η IETF (*Internet Engineering Task Force*) αναπτύσσουν πρότυπα για το Internet υπό μορφή εγγράφων που ονομάζονται RFCs (Request for Comments) τα οποία αφού πρώτα εγκριθούν, εφαρμοσθούν και χρησιμοποιηθούν για ένα χρονικό διάστημα, τελικά γίνονται πρότυπα (STDs). Πριν μια πρόταση υλοποιηθεί σε RFC καλείται προσχέδιο διαδικτύου (Internet Draft).
Οι δυο διαδικασίες προτύπων προσεγγίζουν την τυποποίηση από δυο διαφορετικές προοπτικές. Η προσέγγιση του OSI άρχισε από μια ξεκάθαρη βάση και καθόρισε πρότυπα χρησιμοποιώντας μια επίσημη διαδικασία επιτροπής χωρίς την απαίτηση εφαρμογών. Το Internet χρησιμοποιεί μια λιγότερο επίσημη προσέγγιση εφαρμοσμένης μηχανικής όπου οποιοσδήποτε μπορεί να προτείνει και να σχολιάσει πάνω στα RFCs ενώ απαιτούνται οι εφαρμογές για να ελεγχθεί ό,τι είναι εφικτό.
Τα πρωτόκολλα OSI αναπτύχθηκαν αργά και επειδή τρέχουν ολόκληρη τη σωρό πρωτοκόλλου δεν έχουν ευρέως επεκταθεί ειδικά στους υπολογιστές γραφείου και στην μικρή αγορά υπολογιστών. Στο μεταξύ, το TCP/IP και το Internet αναπτύσσονταν και εφαρμόζονταν ραγδαία. Επίσης, κάποιοι προμηθευτές δικτύου ανέπτυξαν ιδιωτικά πρωτόκολλα δικτύου και άλλα προϊόντα.

1.3.2 X.500: Το Πρότυπο Υπηρεσίας Καταλόγου

Εντούτοις, τα πρωτόκολλα του OSI αντιμετώπισαν σημαντικά ζητήματα στα μεγάλα κατανεμημένα συστήματα που αναπτύσσονταν για την αγορά των ηλεκτρονικών υπολογιστών και του Internet. Ένα τέτοιο σημαντικό πεδίο ήταν οι υπηρεσίες καταλόγου. Η CCITT δημιούργησε το 1988 το πρότυπο X.500 το οποίο έγινε *ISO 9594, Data Communications Network Directory, Recommendations X.500-X.521* το 1990, αν και ακόμα αναφέρεται συνήθως ως X.500.
Το X.500 οργανώνει τις καταχωρήσεις καταλόγου σε ένα ιεραρχικό namespace που είναι ικανό να υποστηρίζει μεγάλες ποσότητες πληροφορίας. Επίσης προσφέρει ισχυρές δυνατότητες αναζήτησης ώστε να γίνεται ευκολότερη η ανάκτηση πληροφοριών. Λόγω της λειτουργίας του και της ικανοτητάς του να εξελίσσεται, το X.500 συχνά χρησιμοποιείται μαζί με πρόσθετες ενότητες (modules) για την διαλειτουργικότητα ανάμεσα σε υπηρεσίες καταλόγου που δεν είναι συμβατές μεταξύ τους. Το X.500 ορίζει ότι η επικοινωνία ανάμεσα στον πελάτη καταλόγου και στον εξυπηρετητή καταλόγου γίνεται με την χρήση του πρωτοκόλλου DAP (Directory Access Protocol). Ωστόσο, ως ένα πρωτόκολλο στρώματος εφαρμογής, το DAP απαιτεί ολόκληρη τη στοίβα του OSI για να λειτουργήσει. Η υποστήριξη της στοίβας OSI χρειάζεται περισσότερους πόρους από όσους είναι διαθέσιμοι σε πολλά μικρά υπολογιστικά περιβάλλοντα.

Επομένως έγινε επιθυμητή μια διεπαφή σε έναν X.500 server καταλόγου που θα χρησιμοποιεί λιγότερους πόρους ή αλλιώς προέκυψε η ανάγκη για ένα ‘’ελαφρύτερο’’ πρωτόκολλο.



Σχήμα 1.3.2 Πληροφοριακό μοντέλο X.500. Το μοντέλο X.500 βρίσκεται στο κέντρο και περιτριγυρίζεται από καταχωρήσεις οι οποίες απαρτίζονται από χαρακτηριστικά που έχουν συντακτικούς τύπους και μια ή περισσότερες τιμές. Οι καταχωρήσεις είναι οργανωμένες υπό τη μορφή δένδρου. Οι καταχωρήσεις με ψευδώνυμο (alias) χρησιμοποιούνται για την δημιουργία μη- ιεραρχικών σχέσεων.

1.3.3 LDAP: Η «Ελαφριά» Πρόσβαση στο Internet

Το LDAP αναπτύχθηκε ως μια ελαφριά εναλλακτική λύση για το DAP. Το LDAP απαιτεί την ελαφρύτερη και δημοφιλέστερη στοίβα πρωτοκόλλου του TCP/IP από αυτή του OSI. Επίσης απλοποιεί κάποιες λειτουργίες του X.500 και παραλείπει μερικά εσωτερικά χαρακτηριστικά γνωρίσματα του.

Δυο πρόδρομοι του LDAP παρουσιάστηκαν ως RFCs από την IETF, το DAS (Directory Assistance Service) (RFC 1202) και το DIXIE Protocol Specification (RFC 1249). Και τα δυο ήταν ενημερωτικά RFC τα οποία δεν προτάθηκαν ως

πρότυπα. Η Υπηρεσία Βοήθειας Καταλόγου (DAS) καθόρισε μια μέθοδο με την οποία ένας πελάτης καταλόγου μπορούσε να επικοινωνήσει με έναν αντιπρόσωπο (proxy) πάνω σε έναν ενεργό host OSI ο οποίος θέτει αιτήματα X.500 εκ μέρους του πελάτη. Το DIXIE είναι παρόμοιο με το DAS, αλλά προσφέρει μια πιο άμεση μετάφραση του DAP.

Η πρώτη έκδοση του LDAP ορίσθηκε ως το Ελαφρύ Πρωτόκολλο Πρόσβασης X.500 (RFC 1487) το οποίο αντικαταστάθηκε από το Ελαφρύ Πρωτόκολλο Πρόσβασης Καταλόγου LDAP (RFC 1777). Το LDAP βελτιώνει περαιτέρω τις ιδέες και τα πρωτόκολλα των DAS και DIXIE. Είναι πιο ουδέτερη εφαρμογή και μειώνει την δυσκολία των πελατών να ενθαρρύνουν την επέκταση των εφαρμογών καταλόγου. Ένα μεγάλο μέρος της εργασίας για το DIXIE και για το LDAP εκτελέσθηκε στο πανεπιστήμιο του Μίσιγκαν το οποίο παρέχει εφαρμογές αναφοράς του LDAP και διατηρεί ιστοσελίδες σχετικές με το LDAP και καταλόγους διευθύνσεων.

Το RFC 1777 καθορίζει το ίδιο το πρωτόκολλο LDAP το οποίο μαζί με

• την αναπαράσταση στοιχειοσειράς των τυποποιημένων συντακτικών των χαρακτηριστικών (The String Representation of Standard Attribute Syntaxes)

• μια αναπαράσταση στοιχειοσειράς των διακριτών ονομάτων *(A String Representation of Distinguished Names, RFC 1779)*
• ένα LDAP URL Format *(RFC 1959)*
• μια αναπαράσταση στοιχειοσειράς των φίλτρων αναζήτησης LDAP *(A String Representation of LDAP Search Filters, RFC 1960)*
καθορίζει την έκδοση 2 του LDAP (LDAP v. 2).
Η δεύτερη έκδοση έχει φθάσει στην κατάσταση προσχεδίου σύμφωνα με την διαδικασία τυποποίησης της IETF, δηλαδή ένα βήμα πριν να γίνει πρότυπο. Αν και θα μπορούσαν να γίνουν αλλαγές σε ένα προσχέδιο προτύπου, επιδιώκεται πρώτα μια ουσιώδης δοκιμή του. Πολλοί προμηθευτές έχουν εφαρμόσει προϊόντα τα οποία υποστηρίζουν την έκδοση 2 του LDAP. Άλλοι εφαρμόζουν προϊόντα που υποστηρίζουν εξ ολοκλήρου ή μερικώς την έκδοση 3.
Η έκδοση 3 έχει καθοριστεί από το Lightweight Directory Access Protocol (v3) (RFC 2251). Σχετικά RFCs που είναι πρόσφατα ή ενημερωμένα για την έκδοση 3 είναι:
• *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions (RFC 2252)*
• *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names (RFC 2253)*
• *The String Representation of LDAP Search Filters (RFC 2254)*
• *The LDAP URL Format (RFC 2255)*
• *A Summary of the X.500 (96) User Schema for use with LDAPv3 (RFC 2256)*
Το RFC 2251 είναι προτεινόμενο πρότυπο, ένα βήμα πριν γίνει προσχέδιο. Είναι πιθανόν να γίνουν κάποιες μικρές αναθεωρήσεις αλλά επιδιώκεται η δοκιμή από διάφορες ομάδες. Το LDAPv3 επεκτείνει το LDAPv2 στα ακόλουθα σημεία:

Παραπομπές Ένας server ο οποίος δεν αποθηκεύει τα ζητούμενα δεδομένα μπορεί να παραπέμψει τον client σε έναν άλλο server.
Ασφάλεια Επικύρωση με την χρησιμοποίηση του μηχανισμού Simple Authentication and Security Layer (SASL).
Διεθνοποίηση Υποστήριξη UTF-8 για τους διεθνείς χαρακτήρες.
Επεκτασιμότητα Νέοι τύποι αντικειμένων και λειτουργιών μπορούν να καθορίζονται δυναμικά και το σχήμα (schema) να δημοσιεύεται με τυποποιημένο τρόπο.

Το LDAP ορίζει το πρωτόκολλο επικοινωνίας μεταξύ του πελάτη καταλόγου και του server καταλόγου, όμως δεν καθορίζει μια διεπαφή προγραμματισμού για τον πελάτη. Το LDAP Application Program Interface (RFC 1823) καθορίζει ένα API γλώσσας C για να υπάρχει πρόσβαση σε έναν κατάλογο που χρησιμοποιεί το LDAP έκδοσης 2. Αυτό είναι ένα ενημερωτικό RFC, το οποίο σημαίνει ότι δεν είναι ένα επίσημο πρότυπο. Ωστόσο, έχει γίνει ένα de facto πρότυπο. Ένα τυποποιημένο πρωτόκολλο και η διάθεση ενός κοινού API για διαφορετικές πλατφόρμες είναι οι κυριότεροι λόγοι που κάνουν ευρέως αποδεκτό το LDAP.

1.3.4 Σύγκριση DAP- LDAP

Η απόδοση του LDAP είναι ικανοποιητική στις περισσότερες εφαρμογές. Στην ενότητα αυτή γίνεται σύγκριση των DAP και LDAP σε τέσσερις τομείς: στον απαιτούμενο χρόνο απόκρισης των ερωτημάτων, στο μέγεθος των ερωτημάτων, στην ταχύτητα κωδικοποίησης PDU και στο μέγεθος και την πολυπλοκότητα των εφαρμογών που συντελούνται από την μεριά του client. Για τις συγκρίσεις αυτές χρησιμοποιήθηκε η εφαρμογή LDAP του Πανεπιστημίου Μίσιγκαν και η εφαρμογή DAP του ISODE. Στο X.500, ο κατάλογος είναι κατανεμημένος μεταξύ πολλών servers και ονομάζεται DSA (Directory System Agent). Ανεξάρτητα με ποιον server είναι συνδεδεμένος ο client, βλέπει την ίδια άποψη του καταλόγου. Εάν ένας server δεν είναι σε θέση να απαντήσει σε ένα αίτημα του client, τότε μπορεί να δρομολογήσει το αίτημα σε έναν άλλο server (διαδικασία αλυσίδας) ή να παραπέμψει τον client σε άλλον server (βλ. 2.2.2.2). Έτσι χρησιμοποιήθηκε ο ίδιος DSA για όλες τις

μετρήσεις των ερωτημάτων αποκτώντας με αυτό τον τρόπο μια βασική γραμμή σύγκρισης. Ο πίνακας 1.3.4.α' δείχνει την απόδοση μιας σειράς τυπικών ερωτημάτων των DAP και LDAP. Τα τεστ διεξήχθησαν σε ένα μηχάνημα στο οποίο έτρεχαν οι clients των DAP και LDAP, ο LDAP server και ο DSA. Όπως φαίνεται στον πίνακα, η καθυστέρηση που σημείωσε το LDAP είναι ελάχιστη. Η καθυστέρηση αυτή θα μπορούσε να εξαλειφθεί συνολικά από μια εγγενή εφαρμογή DSA που αποβάλλει την ενδιάμεση μετάφραση κωδικοποίησης, αποκωδικοποίησης και την μετάφραση πρωτοκόλλου.

Query	DAP	LDAP
Unauthenticated bind	30	68
Authenticated bind	34	56
Simple search (one entry)	32	41
Simple search (50 entries)	293	353

Πίνακας 1.3.4.α'. Σύγκριση των χρόνων των ερωτημάτων των DAP και LDAP. Οι αναζητήσεις εκτελέσθηκαν με την χρήση του ίδιου DSA. Οι χρόνοι είναι σε ms.

Πίνακας 1.3.4.α'. Σύγκριση των χρόνων των ερωτημάτων των DAP και LDAP. Οι αναζητήσεις εκτελέσθηκαν με την χρήση του ίδιου DSA. Οι χρόνοι είναι σε ms.

Ο πίνακας 1.3.4.β' δείχνει το μέγεθος των ερωτημάτων. Όπως φαίνεται, τα ερωτήματα LDAP είναι ουσιαστικά μικρότερα από τα ισοδύναμα DAP. Οι εξοικονομήσεις οφείλονται στο απλουστευμένο DN και στις κωδικοποιήσεις των τιμών. Τα μεγέθη των ερωτημάτων είναι επίσης μειωμένα λόγω της απουσίας των ελέγχων υπηρεσίας σε κάθε λειτουργία.

Query	DAP	LDAP
Unauthenticated bind	192	14
Authenticated bind	409	138
Simple search request	237	105
Single search result	547	355

Πίνακας 1.3.4.β'. Σύγκριση των μεγεθών των ερωτημάτων DAP και LDAP. Τα ερωτήματα LDAP είναι σημαντικά μικρότερα από τα αντίστοιχα DAP. Τα μεγέθη των ερωτημάτων είναι σε bytes.

Οι πίνακες 1.3.4.γ' και 1.3.4.δ' παρουσιάζουν τον χρόνο αποκωδικοποίησης και κωδικοποίησης τυπικών DAP και LDAP PDUs. Δείχνουν ότι το LDAP έχει ένα μέτριο πλεονέκτημα απόδοσης για απλά PDUs και ένα ουσιαστικό πλεονέκτημα για σύνθετα PDUs, ειδικά για εκείνα που περιέχουν πολλά διακριτά ονόματα (DNs) όπου η αντιπροσώπευση της στοιχειοσειράς LDAP είναι ένα μεγάλο κέρδος.

PDU Complexity	DAP	LDAP
Simple	550	110
Medium	7,925	714
Complex	38,393	2,702

Πίνακας 1.3.4.γ'. Σύγκριση των χρόνων αποκωδικοποίησης των DAP και LDAP. Τα στοιχεία πρωτοκόλλου LDAP είναι ευκολότερο να αποκωδικοποιηθούν ειδικά για σύνθετα PDUs. Το σύνθετο PDU περιείχε ένα χαρακτηριστικό με περισσότερα από 600 DNs. Περίπου μισός από τον χρόνο αποκωδικοποίησης DAP ξοδεύτηκε σε έναν διπλό έλεγχο για να εξασφαλισθεί ότι μια ιδιότητα διαθέτει μόνο μια από κάθε τιμή.

PDU Complexity	DAP	LDAP
Simple	24	6
Medium	1,084	324
Complex	2656	989

Πίνακας 1.3.4.δ' Σύγκριση των χρόνων κωδικοποίησης DAP και LDAP. Τα στοιχεία πρωτοκόλλου LDAP είναι κωδικοποιημένα πιο αποτελεσματικά, ειδικά για πολύπλοκα PDUs.

Τέλος, έγινε σύγκριση του μεγέθους της εφαρμογής και της πολυπλοκότητας του κώδικα. Μια τέτοια σύγκριση είναι δύσκολο να γίνει διότι πρέπει να αξιολογηθεί το ευρύ φάσμα των δεξιοτήτων και των στόχων των προγραμματιστών που εργάζονται για την παραγωγή των εφαρμογών. Ωστόσο μερικά ευνοϊκά συμπεράσματα για το LDAP μπορούν να προέλθουν από το συντριπτικό πλεονέκτημα που έχει σε αυτόν τον τομέα, όπως φαίνεται στον πίνακα 1.3.4.ε'.

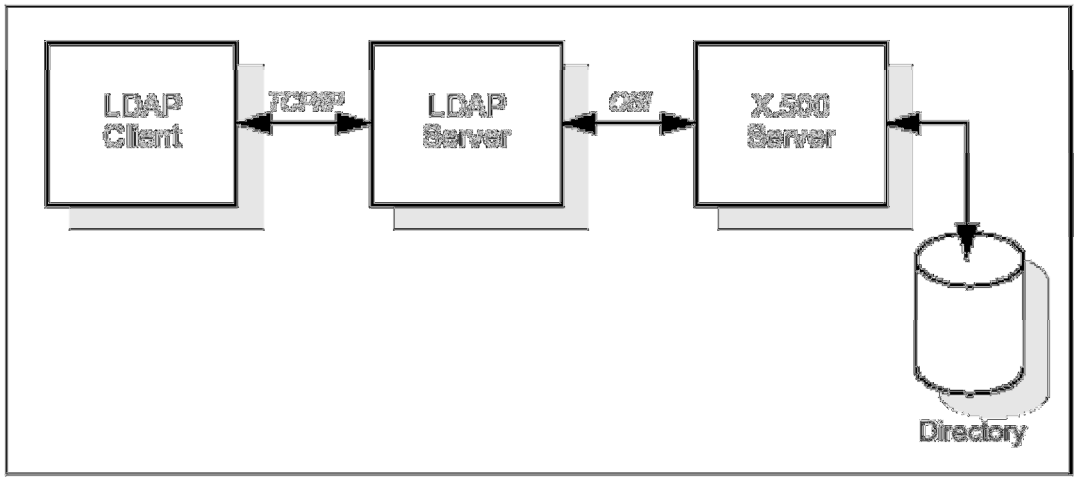
Metric	DAP	LDAP
Total size (DE)	1,484,568	334,552
Text	958,464	221,184
Data	385,024	73,728
BSS	141,080	39,640
Semicolon count	46,746	1,989
If count	9369	568

Πίνακας 1.3.4.ε' Σύγκριση της πολυπλοκότητας εφαρμογής των DAP και LDAP. Ο DE client, ο οποίος μπορεί να δημιουργηθεί είτε με τη χρήση του DAP είτε του LDAP, χρησιμοποιείται για να συγκρίνει το μέγεθος εφαρμογής. Ο semicolon count που προσεγγίζει τον αριθμό προτάσεων και ο αριθμός των προτάσεων «if» που προσεγγίζει τον αριθμό των paths του κώδικα αποτελούν τα δυο μέτρα πολυπλοκότητας. Η σύγκριση έγινε μεταξύ του ISODE- 8.0 και της εφαρμογής LDAP του Πανεπιστημίου Μίσιγκαν.

Για την σύγκριση μεγέθους επιλέχθηκε ο πελάτης ερευνών καταλόγου (Directory Enquiries Client) ο οποίος μπορεί να μεταγλωττισθεί ώστε να χρησιμοποιήσει είτε το DAP είτε το LDAP για την επικοινωνία X.500. Συγκρίθηκε επίσης η πολυπλοκότητα κώδικα του ISODE DAP και των βιβλιοθηκών των LDAP clients. Χρησιμοποιήθηκαν δύο μέτρα πολυπλοκότητας. Το πρώτο, ο συνολικός αριθμός του χαρακτήρα '' ; '' που προσεγγίζει τον αριθμό των προτάσεων και το δεύτερο, ο συνολικός αριθμός των προτάσεων «if» που προσεγγίζει τον αριθμό των paths της κωδικοποίησης. Στον υπολογισμό των συγκεκριμένων μέτρων, καταβλήθηκε προσπάθεια να συμπεριληφθούν μόνο οι μερίδες του κώδικα που απαιτούνται για να υπάρχει πρόσβαση στον X.500.

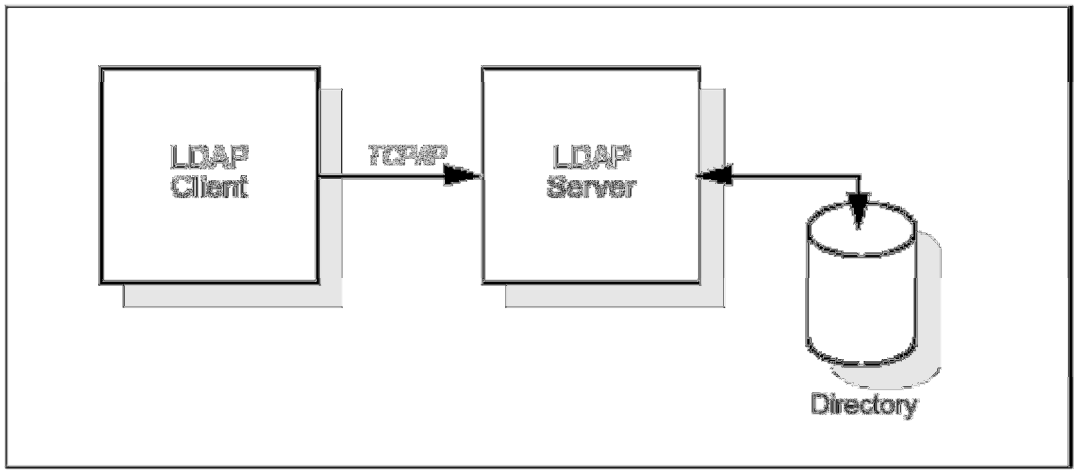
1.4 LDAP: Πρωτόκολλο ή Κατάλογος;

Το LDAP ορίζει ένα πρωτόκολλο επικοινωνίας, δηλαδή, καθορίζει την μεταφορά και το format των μηνυμάτων που χρησιμοποιούνται από έναν πελάτη για να έχει πρόσβαση στα δεδομένα ενός καταλόγου της μορφής του X.500. Το LDAP δεν καθορίζει από μόνο του την υπηρεσία καταλόγου. Πολλοί άνθρωποι μιλούν για τους καταλόγους LDAP. Άλλοι λένε ότι το LDAP είναι απλώς ένα πρωτόκολλο και όχι ένας κατάλογος. Τι είναι όμως κατάλογος LDAP;
Ένα πρόγραμμα εφαρμογής πελάτη εισάγει ένα μήνυμα LDAP μέσω της κλήσης ενός LDAP API. Αλλά ένας εξυπηρετητής καταλόγου X.500 δεν καταλαβαίνει τα μηνύματα LDAP. Στην πραγματικότητα, ο πελάτης LDAP και ο εξυπηρετητής X.500 χρησιμοποιούν διαφορετικά πρωτόκολλα επικοινωνίας (TCP/IP εν αντιθέσει με το OSI). Ο πελάτης LDAP επικοινωνεί με μια διαδικασία πύλης (gateway) που διαβιβάζει αιτήματα στον εξυπηρετητή καταλόγου X.500. Η πύλη αυτή είναι γνωστή ως εξυπηρετητής LDAP (LDAP server). Ο LDAP server εξυπηρετεί τα αιτήματα του LDAP client. Το επιτυγχάνει αυτό με το να γίνεται ο ίδιος πελάτης στον X.500 server. Ο LDAP server πρέπει να επικοινωνεί χρησιμοποιώντας και το TCP/IP και το OSI.



Σχήμα 1.4.α' Ο LDAP Server ως πύλη σε έναν X.500 Server

Καθώς μεγαλώνει η χρήση του LDAP και τα οφέλη του είναι προφανή, τα άτομα τα οποία δεν διέθεταν εξυπηρετητές X.500 ή που δεν είχαν τα κατάλληλα περιβάλλοντα για να τους υποστηρίξουν, θέλησαν να στήσουν καταλόγους που θα είχαν πρόσβαση σε αυτούς πελάτες LDAP. Έτσι λοιπόν γιατί να μην υπάρχει ο LDAP server αποθηκευμένος με δυνατότητα πρόσβασης στον κατάλογο από μόνος του (βλ. σχήμα 1.4.β') αντί να συμπεριφέρεται ως πύλη στους X.500 servers; Αυτό εξαλείφει οποιαδήποτε ανάγκη για το OSI. Βέβαια αυτό κάνει τον LDAP server πολύπλοκο αφού πρέπει να αποθηκεύει και να ανακτά τις καταχωρήσεις καταλόγου. Οι συγκεκριμένοι LDAP servers συχνά αποκαλούνται αυτόνομοι servers επειδή δεν εξαρτώνται από τον server καταλόγου X.500. Από την στιγμή που το LDAP δεν υποστηρίζει όλες τις δυνατότητες του X.500, ένας αυτόνομος LDAP server χρειάζεται μόνο να υποστηρίζει τις δυνατότητες που απαιτούνται από το LDAP.



Σχήμα 1.4.β' Αυτόνομος LDAP Server

Το RFC 1777 (LDAPv2) αναφέρει την παροχή πρόσβασης στον κατάλογο X.500. Το RFC 2251 (LDAPv3) συζητά την πρόσβαση σε καταλόγους που υποστηρίζουν το μοντέλο X.500. Αυτή η αλλαγή στη γλώσσα απεικονίζει την ιδέα ότιένας LDAP server μπορεί να εφαρμόσει ο ίδιος τον κατάλογο ή να αποτελέσει πύλη για έναν X.500 κατάλογο.
Από την πλευρά του πελάτη, οποιοσδήποτε server που εφαρμόζει το πρωτόκολλο LDAP είναι ένας LDAP server καταλόγου, εφόσον ο server εφαρμόζει τον κατάλογο ή είναι πύλη σε έναν server X.500. Ο κατάλογος ο οποίος προσεγγίζεται μπορεί να αποκαλείται LDAP κατάλογος, εφόσον ο κατάλογος εφαρμόζεται από έναν αυτόνομο LDAP server ή από έναν X.500 server.

1.5 Η Πορεία του LDAP

Το LDAP έχει εξελιχθεί για να ικανοποιήσει την ανάγκη παροχής πρόσβασης σε μια υποδομή ενός κοινού καταλόγου. Το LDAP είναι μια ανοιχτή βιομηχανία προτύπου που υποστηρίζεται από πολλούς προμηθευτές συστήματος σε πολλές πλατφόρμες. Ενσωματώνεται σε προϊόντα λογισμικού και γρήγορα γίνεται επιλογή ως πρωτόκολλο πρόσβασης καταλόγου. Επιτρέπει στα προϊόντα διαφορετικών προμηθευτών και πλατφόρμων να επικοινωνούν και να παρέχουν μια παγκόσμια υποδομή καταλόγου, όπως έγινε με το HTTP που συνέβαλε στην ανάπτυξη του Παγκόσμιου Ιστού. Τα πρόσφατα προϊόντα LDAP υποστηρίζουν τουλάχιστον την έκδοση 2. Ήδη, πολλά υποστηρίζουν μέρη της έκδοσης 3 ή και ολόκληρη.
Οι υπεύθυνοι ανάπτυξης εφαρμογών μπορούν να επωφεληθούν από το LDAP για να δημιουργήσουν εφαρμογές καταλόγου επόμενης γενιάς. Ενώ ο X.500 έχει παραδοσιακά αναπτυχθεί μόνο σε μεγάλους οργανισμούς όπου μπορεί να δεσμεύσει τους απαραίτητους πόρους για να τον υποστηρίξουν, το LDAP είναι επίσης κατάλληλο για μικρούς οργανισμούς. Για παράδειγμα, μια μικρή εταιρεία μπορεί να θέλει να ανταλλάξει έγγραφα με τους πελάτες και τους προμηθευτές της χρησιμοποιώντας ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange). Η EDI απαιτεί και οι δυο πλευρές να συμφωνούν ως προς τον τύπο των εγγράφων που θα ανταλλαγούν, τις ιδιαιτερότητες της επικοινωνίας και ούτω καθεξής. Οι εταιρείες θα μπορούσαν να εκδώσουν τα χαρακτηριστικά της δικής τους EDI σε -δημόσιας πρόσβασης- LDAP καταλόγους για να διευκολύνουν την ηλεκτρονική ανταλλαγή. Μια κοινή υποδομή καταλόγου ενθαρρύνει νέες χρήσεις. Τα DEN (Directory Enabled Networks) παίρνουν την πρωτοβουλία και προτείνουν οι πληροφορίες για την κατασκευή δικτύων, για τα πρωτόκολλα, για τα χαρακτηριστικά των routers και ούτω καθεξής, να αποθηκεύονται σε κατάλογο LDAP. Η διαθεσιμότητα αυτής της πληροφορίας με ένα κοινό format από πολλούς προμηθευτές εξοπλισμού θα οδηγήσει στην έξυπνη διαχείριση και στην παροχή των δικτυακών πόρων. Τα παραδείγματα αυτά δείχνουν τις ποικίλες χρήσεις των εφαρμογών καταλόγου που υποστηρίζονται από μια κοινή υποδομή καταλόγου στην οποία πετυχαίνουμε πρόσβαση μέσω του LDAP.

1.6 Προϊόντα Εξυπηρετητών Καταλόγου (Directory Servers)

OpenLDAP 2.3

Ο OpenLDAP αποτελεί ένα προϊόν μιας συλλογικής προσπάθειας για την ανάπτυξη ενός ισχυρού και ανοιχτού κώδικα LDAP το οποίο είναι κατάλληλο για εφαρμογές και εργαλεία ανάπτυξης εφαρμογών. Το έργο αυτό διαχειρίζεται μια παγκόσμια κοινότητα εθελοντών που χρησιμοποιεί το Internet με σκοπό την επικοινωνία, τον σχεδιασμό και την ανάπτυξη του OpenLDAP Suite και της πρόσφατης τεκμηρίωσής του.

Το OpenLDAP Project πρόσφατα ανακοίνωσε την κυκλοφορία του OpenLDAP 2.3 (Ιούνιος 2005). Το λογισμικό OpenLDAP 2.3 αποτελεί μια ακολουθία του LDAP v3 που υποστηρίζει servers, χρησιμότητες και εργαλεία ανάπτυξης εφαρμογών.

Η έκδοση αυτή υποστηρίζει τις περισσότερες πλατφόρμες UNIX (και UNIX-like) όπως Darwin, FreeBSD, Linux, NetBSD καθώς και τα πιο εμπορικά UNIX συστήματα. Η έκδοση αυτή δοκιμάζεται επίσης (μερικώς ή εξ' ολοκλήρου) και σε άλλες πλατφόρμες όπως στις Apple MacOS X, IBM zOS, και Microsoft Windows 2000.

Ο OpenLDAP 2.3 περιέχει τις εξής σημαντικές επαυξήσεις:

-Slapd(8) enhancements

- Updated slapd "overlay" interface, and several example (and mostly experimental) overlays.
- Updated LDAP "sync" Engine with replication support, provider now an "overlay"
- Numerous access control enhancements, including experimental "don't disclose on error" capability
- Configuration Backend

- LDAPv3 extensions, including:
  - LDAP Password Policy
  - LDAP Component Matching (requires OpenLDAP-snacc)
  - LDAP Modify Increment

Επίσης περιλαμβάνει τα εξής συστατικά:

- slapd - a stand-alone LDAP directory server
- slurpd - a stand-alone LDAP replication server
- -lldap - a LDAP client library
- -llber - a lightweight BER/DER encoding/decoding library
- LDIF tools - data conversion tools for use with slapd
- LDAP tools - A collection of command line LDAP utilities
- Admin Guide, Manual Pages - associated documentation
- SNACC - ASN.1 development tools for OpenLDAP

Επιπροσθέτως, υπάρχουν μερικά συμβαλλόμενα συστατικά:

- LDAPC++ - a LDAP C++ SDK
- Various slapd modules and slapi plugins

ONE Directory Server 5.2 Sun

Ο Sun ONE Directory Server 5.2 είναι ένας ισχυρός και με δυνατότητες εξέλιξης κατανεμημένος server ο οποίος βασίζεται στο LDAP. Το λογισμικό του είναι μέρος του Sun Open Net Environment (Sun ONE) το οποίο βασίζεται σε ανοιχτά πρότυπα όπως Java και παρέχει ένα σημαντικά ευέλικτο περιβάλλον για την δημιουργία ενός πλήθους υπηρεσιών κατ' απαίτηση (services on demand). Ο συγκεκριμένος server προσφέρει πληροφορίες για έναν μεγάλο αριθμό εφαρμογών υποστηρίζοντας δυο πρωτόκολλα για την πρόσβαση στον παγκόσμιο κατάλογο: το LDAP και το DSML (Directory Services Markup Language).

IBM Tivoli Directory Server

Ο IBM Tivoli Directory Server παρέχει μια ισχυρή υποδομή ταυτότητας LDAP όπου αποτελεί το ίδρυμα για την ανάπτυξη περιεκτικών εφαρμογών διαχείρισης ταυτότητας και προηγμένων αρχιτεκτονικών λογισμικού όπως οι υπηρεσίες Ιστού. Οι πλατφόρμες που υποστηρίζει ο IBM Tivoli Directory Server είναι: AIX, Solaris, Microsoft, IBM eServer iSeries, pSeries και zSeries.

eDirectory 8.7.3 Novell

Ο Novell eDirectory είναι μια υψηλής απόδοσης και ασφαλής υπηρεσία καταλόγου. Μπορεί να αποθηκεύσει και να διαχειρισθεί εκατομμύρια αντικείμενα, όπως χρήστες, εφαρμογές, συσκευές δικτύου και δεδομένα. Παρέχει συγκεντρωτική διαχείριση ταυτότητας, υποδομή, ασφάλεια διαδικτύου και δυνατότητες εξέλιξης σε όλους τους τύπους εφαρμογών που τρέχουν πίσω και πέρα από το firewall. Ο Novell eDirectory 8.7.3 παρέχει διαδικτυακές και ασύρματες δυνατότητες διαχείρισης, επιτρέποντας την πρόσβαση και διαχείριση του καταλόγου, των χρηστών, των δικαιωμάτων πρόσβασης και των δικτυακών πόρων.

Ο Novell eDirectory υποστηρίζει το πρότυπο κατάλογου LDAPv3 και παρέχει υποστήριξη για υπηρεσίες TLS/SSL που βασίζονται στον πηγαίο κώδικα OpenSSL. Τρέχει σε Linux, NetWare, Windows, Solaris, AIX και HP-UX.

Οι απαιτήσεις συστήματος για τον Novell eDirectory 8.7.3 είναι:

NetWare

- NetWare 5.1 Support Pack 6 or later
- NetWare 6 Support Pack 3 or later
- NetWare 6.5 Support Pack 1 (eDirectory 8.7.3 is only supported through the NetWare 6.5 Support Pack 1 installation)

If you are using RCONSOLE, you will need a ConsoleOne® administrator workstation with the following:

- 200 MHZ or faster processor
- 64 MB RAM (128 recommended)
- Novell Client™ for Windows NT/2000/XP version 4.9 or later or Novell Client for Windows 95/98 version 3.4 or later

Windows

One of the following:

- Windows NT Server 4.0 with Service Pack 6 or later
- Windows 2000 Server with

Important**:** Windows XP is not a supported Novell eDirectory 8.7.3 platform.

- An assigned IP address
- A Pentium 200 with a minimum of 64 MB RAM (128 MB recommended) and a monitor color palette set to a number higher than 16

(Optional) One or more workstations running one of the following:

- Novell Client for Windows 95/98 version 3.4 or later
- Novell Client for Windows NT/2000/XP version 4.9 or later
- Administrative rights to the NT/2000 server and to all portions of the eDirectory tree that contain domain-enabled User objects. For an installation into an existing tree, you need administrative rights to the root of the tree so that you can extend the schema and create objects.

Linux

One of the following:

- SUSE LINUX Enterprise Server 9 (IR3 required)
- SUSE LINUX Enterprise Server 8
- Red Hat Linux 7.3, 8.0, 9.0, or Red Hat Advanced Server 2.1 **Note:** Ensure that the latest glibc patches are applied from Red Hat Errata on Red Hat systems.
- 128 MB RAM minimum
- 90 MB of disk space for the eDirectory server
- 25 MB of disk space for the eDirectory administration utilities
- 74 MB of disk space for every 50,000 users

Ensure that gettext is installed

Solaris

One of the following:

- Solaris 8 on Sun SPARC (with patch 108827-20 or later)
- Solaris 9 on Sun SPARC
- All of the latest recommended sets of patches are available on the SunSolve webpage. If you do not update your system with the latest patches before installing eDirectory, you will get the patchadd error.
- 128 MB RAM minimum
- 120 MB of disk space for the eDirectory server
- 32 MB of disk space for the eDirectory administration utilities
- 74 MB of disk space for every 50,000 users

ΚΕΦΑΛΑΙΟ 2

ΑΡΧΙΤΕΚΤΟΝΙΚΗ LDAP:

Το LDAP είναι βασισμένο στο μοντέλο client/server και έχει εξελιχθεί ως ένα ελαφρύ πρωτόκολλο για την πρόσβαση στις πληροφορίες των υπηρεσιών καταλόγου X.500. Από τότε έχει γίνει πιο ανεξάρτητο από το X.500 και οι servers που υποστηρίζουν αποκλειστικά το LDAP και όχι το DAP, είναι πλέον κοινοί. Η επιτυχία του LDAP έχει αυξηθεί και αυτό οφείλεται στα ακόλουθα χαρακτηριστικά που το καθιστούν απλούστερο στην εφαρμογή σε σχέση με το X.500 και το DAP:

- Το LDAP τρέχει στο TCP/IP και όχι στη στοίβα του πρωτοκόλλου OSI. Το TCP/IP είναι λιγότερο απαιτητικό σε πόρους και είναι ευρέως διαθέσιμο, ειδικά στα υπολογιστικά συστήματα γραφείου.
- Το λειτουργικό μοντέλο του LDAP είναι πιο απλό. Παραλείπει τα αντίγραφα και τα σπανίως χρησιμοποιούμενα εσωτερικά χαρακτηριστικά γνωρίσματα. Όλα αυτά καθιστούν το LDAP ευκολότερο στην κατανοησή και στην εφαρμογή του.
- Το LDAP χρησιμοποιεί στοιχειοσειρές (strings) για να αναπαραστήσει τα δεδομένα και όχι πολύπλοκα δομημένα συντακτικά όπως η ASN.1 (Abstract Syntax Notation One).

2.1 Επισκόπηση Αρχιτεκτονικής LDAP

Το LDAP καθορίζει το περιεχόμενο των μηνυμάτων που ανταλλάσσονται μεταξύ του LDAP client και του LDAP server. Τα μηνύματα διευκρινίζουν τις λειτουργίες που ζητούνται από τον πελάτη (αναζήτηση, τροποποίηση, διαγραφή κ.λ.π.), τις απαντήσεις από την μεριά του server, και το format των δεδομένων που μεταφέρονται στα μηνύματα. Τα μηνύματα LDAP μεταφέρονται πάνω στο TCP/IP. Επειδή το TCP/IP είναι πρωτόκολλο που προσανατολίζεται με σύνδεση, υπάρχουν λειτουργίες που γίνονται για να καθιερώσουν και να διακόψουν μια σύνοδο μεταξύ του πελάτη και του εξυπηρετητή.

Ωστόσο, για τον σχεδιαστή του καταλόγου LDAP, δεν έχει τόσο σημασία η δομή των μηνυμάτων που στέλνονται και λαμβάνονται. Αυτό που έχει σημασία είναι το λογικό μοντέλο το οποίο καθορίζεται από αυτά τα μηνύματα και από τους τύπους των δεδομένων π.χ. πώς οργανώνεται ο κατάλογος, ποιες λειτουργίες μπορούν να γίνουν, με ποιο τρόπο προστατεύονται οι πληροφορίες και ούτω καθεξής.

Η γενική αλληλεπίδραση μεταξύ των LDAP server και client παίρνει την ακόλουθη μορφή:

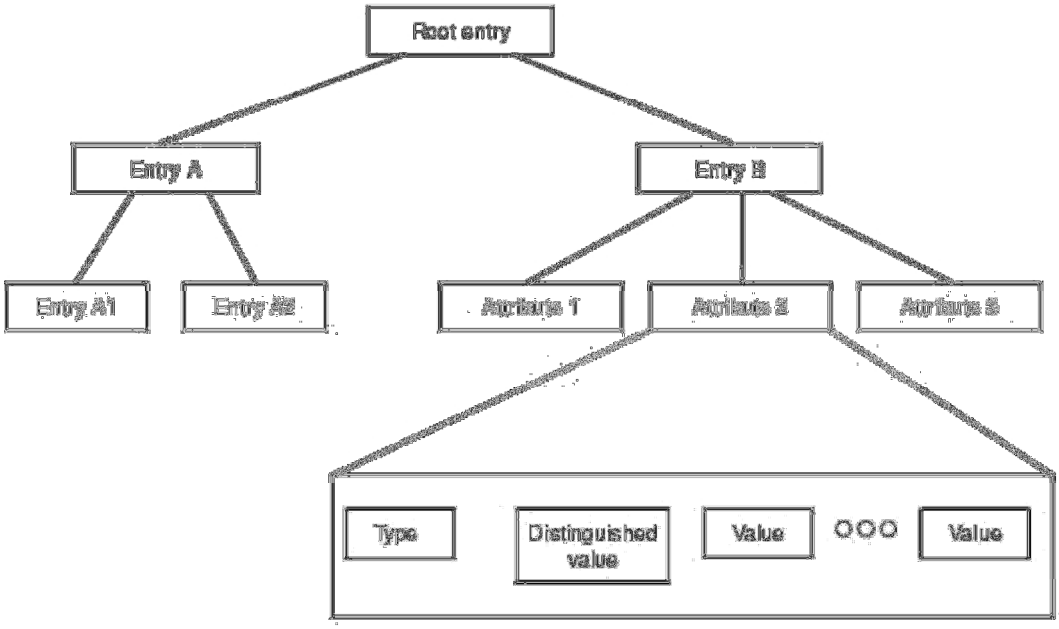
- Ο client καθιερώνει μια σύνοδο με έναν LDAP server που είναι γνωστή ως *δέσμευση* του server. Ο client διευκρινίζει το host name ή την IP διεύθυνση και τον port number του TCP/IP όπου σε αυτόν ‘’ακούει’’ ο LDAP server. Ο client μπορεί να παρέχει ένα user name και ένα κωδικό πρόσβασης για να επικυρώνεται κατάλληλα με τον server. Ή μπορεί να καθιερώσει μια ανώνυμη σύνοδο με προεπιλεγμένα δικαιώματα πρόσβασης (by default). Επίσης ο client και ο server μπορούν να καθιερώσουν μια σύνοδο που να εφαρμόζει ισχυρές μεθόδους κρυπτογράφησης δεδομένων.

• Έπειτα ο client εκτελεί λειτουργίες πάνω στα δεδομένα του καταλόγου. Αυτό επιτρέπει στις πληροφορίες καταλόγου να διαχειρίζονται και να ερωτώνται. Επίσης το LDAP υποστηρίζει την αναζήτηση δεδομένων που ικανοποιούν αυθαίρετα κριτήρια τα οποία έχουν καθοριστεί από τον χρήστη. Η διαδικασία αναζήτησης είναι πολύ συνηθισμένη για τον LDAP. Ένας χρήστης μπορεί να διευκρινίσει ποιο μέρος του καταλόγου θέλει να αναζητηθεί και ποια πληροφορία να επιστραφεί. Ένα φίλτρο αναζήτησης που χρησιμοποιεί όρους BOOLEAN διευκρινίζει ποιο στοιχείο του καταλόγου ταιριάζει με το κριτήριο αναζήτησης.

• Όταν ο client ολοκληρώσει την υποβολή ερωτημάτων κλείνει την σύνοδο με τον server. Αυτό είναι γνωστό ως *αποδέσμευση* (unbinding).

Αν και δεν καθορίζεται από το πρωτόκολλο LDAP ούτε από την αρχιτεκτονική του, υπάρχει ένα γνωστό LDAP API που επιτρέπει στις εφαρμογές να αλληλεπιδρούν εύκολα με τους LDAP servers. Το API μπορεί να θεωρηθεί ως μια προέκταση της αρχιτεκτονικής του LDAP. Παρόλο που το LDAP API της γλώσσας C είναι μόνο ένα ενημερωτικό RFC και η πιο πρόσφατη ενημερωσή του είναι ένα προσχέδιο Internet, έχει καταφέρει de facto να φθάσει σε κατάσταση προτύπου επειδή υποστηρίζεται από όλους τους σημαντικούς προμηθευτές LDAP. Η φιλοσοφία του LDAP API είναι να διατηρεί τα πράγματα απλά. Αυτό σημαίνει ότι μπορεί, με χαμηλό γενικά κόστος, να προστεθεί υποστήριξη καταλόγου στις υπάρχουσες εφαρμογές.

Επειδή το LDAP προορίστηκε αρχικά ως μια ελαφριά εναλλακτική λύση του DAP για την πρόσβαση σε καταλόγους X.500, ακολουθεί το μοντέλο X.500. Ο κατάλογος αποθηκεύει και οργανώνει δομές δεδομένων γνωστές ως ***καταχωρήσεις*** (*entries*). Μια καταχώρηση καταλόγου συνήθως περιγράφει ένα **αντικείμενο** όπως ένα άτομο, έναν εκτυπωτή, έναν server και τα λοιπά. Κάθε καταχώρηση έχει ένα όνομα γνωστό ως ***διακριτό όνομα*** (*Distinguished Name(DN))* που την προσδιορίζει μοναδικά. Το DN αποτελείται από μια ακολουθία μερών που ονομάζονται *σχετικά διακριτά ονόματα* (*RDNs*) τα οποία μοιάζουν κατά πολύ με το όνομα αρχείου που περιέχει τα paths ονομάτων καταλόγου σε πολλά λειτουργικά συστήματα όπως των UNIX και WINDOWS. Οι καταχωρήσεις μπορούν να ταξινομούνται σε μια ιεραρχική μορφή δέντρου βασισμένη στα διακριτά ονοματά τους. Το δέντρο των καταχωρήσεων καταλόγου ονομάζεται Δέντρο Πληροφοριών Καταλόγου (Directory Information Tree (**DIT**)).



Σχήμα 2.1 Δομή DIT

Κάθε καταχώρηση περιέχει ένα ή περισσότερα ***χαρακτηριστικά*** (*attributes*) τα οποία περιγράφουν την καταχώρηση. Κάθε χαρακτηριστικό έχει έναν τύπο και μια τιμή. Για παράδειγμα, η καταχώρηση καταλόγου ενός ατόμου μπορεί να έχει το χαρακτηριστικό telephoneNumber. Το συντακτικό του χαρακτηριστικού telephoneNumber διευκρινίζει ότι ο τηλεφωνικός αριθμός πρέπει να είναι μια ακολουθία από αριθμούς που μπορεί να περιέχουν διαστήματα και παύλες. Η τιμή του χαρακτηριστικού θα είναι ο τηλεφωνικός αριθμός του ατόμου π.χ 512-555-1212.

Μια καταχώρηση καταλόγου περιγράφει κάποιο **αντικείμενο** (*object*). Μια *κατηγορία αντικειμένου* είναι μια γενική περιγραφή που συχνά αναφέρεται ως *φόρμα* αντικειμένου σε αντιδιαστολή με την περιγραφή ενός συγκεκριμένου αντικειμένου. Παραδείγματος χάριν, η κατηγορία (**class**) αντικειμένου *person* έχει ένα χαρακτηριστικό surname ενώ το αντικείμενο που περιγράφει το John Smith έχει ένα χαρακτηριστικό surname με την τιμή Smith.

Οι κατηγορίες αντικειμένου που μπορεί να αποθηκεύσει ένας server καταλόγου καθώς και τα χαρακτηριστικά που περιέχονται σ' αυτές, περιγράφονται στο **σχήμα** (*schema*). Το σχήμα καθορίζει το είδος των κατηγοριών αντικειμένου που επιτρέπεται να αποθηκευθούν στον κατάλογο, ποια χαρακτηριστικά πρέπει να έχουν, ποια από αυτά είναι προαιρετικά και τον συντακτικό τύπο αυτών. Για παράδειγμα, θεωρούμε ένα σχήμα που ορίζει μια κατηγορία αντικειμένου με το όνομα person. Το σχήμα της κατηγορίας person απαιτεί ότι ένα άτομο θα έχει το χαρακτηριστικό surname το οποίο θα είναι ένα string χαρακτήρων, διευκρινίζοντας ότι η καταχώρηση ενός ατόμου μπορεί προαιρετικά να έχει και το χαρακτηριστικό telephoneNumber όπου είναι ένα string αριθμών, κενών και παυλών.

Το LDAP ορίζει λειτουργίες για την προσπέλαση και τροποποίηση καταχωρήσεων καταλόγου όπως:

- Αναζήτηση για καταχωρήσεις που ικανοποιούν τα κριτήρια που καθορίζονται από τον χρήστη
- Προσθήκη καταχώρησης
- Διαγραφή καταχώρησης

- Τροποποίηση καταχώρησης

- Τροποποίηση του διακριτού ή του σχετικού διακριτού ονόματος μιας καταχώρησης
- Σύγκριση καταχώρησης

Το LDAP είναι τεκμηριωμένο σε πολλά IETF RFCs. Παρατίθενται τα RFCs της έκδοσης 3 με μια μικρή περιγραφή για να γίνει μια επισκόπηση των εγγράφων που καθορίζουν την αρχιτεκτονική του LDAP.

1. RFC 2251 Lightweight Directory Access Protocol (v3)

Περιγράφει το πρωτόκολλο LDAP που είναι σχεδιασμένο ώστε να παρέχει ελαφριά πρόσβαση σε καταλόγους που υποστηρίζουν το μοντέλο X.500. Το ελαφρύ πρωτόκολλο προορίστηκε για εφαρμογή σε περιβάλλοντα περιορισμένων πόρων όπως οι browsers και τα μικρά υπολογιστικά συστήματα γραφείου. Αυτό το RFC αποτελεί τον πυρήνα της οικογένειας των LDAP RFCs. Περιγράφει το πώς ονομάζονται οι καταχωρήσεις με τα διακριτά ονόματα, καθορίζει το format των μηνυμάτων που ανταλλάσσονται μεταξύ του πελάτη και του server, απαριθμεί τις λειτουργίες που μπορούν να εκτελεσθούν από την μεριά του πελάτη και διευκρινίζει ότι τα δεδομένα αναπαριστώνται με την χρησιμοποίηση της κωδικοποίησης χαρακτήρα UTF-8. Το RFC 2251 διευκρινίζει ότι οι καταχωρήσεις καταλόγου που περιγράφονται στο σχήμα πρέπει να είναι οι ίδιες αναγνώσιμες έτσι ώστε ένας πελάτης να μπορεί να προσδιορίσει τον τύπο των αντικειμένων που αποθηκεύει ο κατάλογος. Καθορίζει τον τρόπο με τον οποίο ένας πελάτης μπορεί να προσφύγει σε έναν άλλον LDAP server εάν ένας server δεν περιέχει την ζητούμενη πληροφορία. Περιγράφει το πώς οι μεμονωμένες λειτουργίες με τις κατάλληλες ρυθμίσεις μπορούν να επεκταθούν και πώς οι πρόσθετες λειτουργίες μπορούν να προσδιοριστούν χρησιμοποιώντας επεκτάσεις. Επίσης συζητάει για το πώς οι πελάτες μπορούν να ζητήσουν επικύρωση από τους servers και προαιρετικά να χρησιμοποιήσουν το Simple Authentication and Security Layer (SASL) για να επιτρέψουν πρόσθετους μηχανισμούς επικύρωσης.

2. RFC 2252 Lightweight Directory Access Protocol (v3): *Attribute Syntax Definitions*

Το LDAP χρησιμοποιεί οκταδικά strings για να αναπαραστήσει τις τιμές των χαρακτηριστικών για τη μεταφορά στο πρωτόκολλο LDAP. Αυτό το RFC καθορίζει το πώς αναπαριστώνται τιμές όπως οι ακέραιοι αριθμοί, διευθύνσεις e-mail και τα λοιπά. Για παράδειγμα, ο ακέραιος 123 αναπαριστάται από το string ‘’123’’. Οι ορισμοί αυτοί ονομάζονται συντακτικά χαρακτηριστικών (attribute syntaxes). Το συγκεκριμένο RFC περιγράφει το πώς κωδικοποιείται ένα χαρακτηριστικό με ένα συγκεκριμένο συντακτικό τύπο όπως ‘’τηλεφωνικός αριθμός’’. Επίσης καθορίζει τους κανόνες που χρειάζονται για να καθορισθεί αν οι τιμές ικανοποιούν τα κριτήρια αναζήτησης.
Αυτοί οι τύποι χαρακτηριστικών και ο συντακτική τους μορφή χρησιμοποιούνται για να χτίσουν το σχήμα που περιγράφει τις κατηγορίες αντικειμένων. Ένα σχήμα αναφέρει τα χαρακτηριστικά που πρέπει να έχει μια καταχώρηση καταλόγου. Κάθε καταχώρηση καταλόγου έχει ένα objectclass χαρακτηριστικό το οποίο απαριθμεί το σχήμα (ένα ή περισσότερα) που

περιγράφει την καταχώρηση. Παραδείγματος χάριν, μια καταχώρηση καταλόγου μπορεί να περιγραφθεί από τις κατηγορίες αντικειμένου residentialPerson και organizationalPerson. Αν ένα χαρακτηριστικό objectclass περιλαμβάνει την τιμή extensibleObject, τότε μπορεί να περιέχει οποιοδήποτε χαρακτηριστικό.

3. RFC 2253 Lightweight Directory Access Protocol (v3): *UTF-8 String Representation of Distinguished Names*

Τα διακριτά ονόματα (DNs) είναι τα μοναδικά αναγνωριστικά των καταχωρήσεων καταλόγου τα οποία μερικές φορές καλούνται πρωτεύοντα κλειδιά (primary keys). Το X.500 χρησιμοποιεί την ASN.1 για να κωδικοποιήσει τα διακριτά ονόματα. Το LDAP κωδικοποιεί τα διακριτά ονόματα ως strings. Αυτό το RFC ορίζει τον τρόπο με τον οποίο αναπαριστώνται τα DNs με την μορφή strings. Μια αναπαράσταση string είναι εύκολο να κωδικοποιηθεί και να αποκωδικοποιηθεί και επιπλέον είναι ανθρωπίνως αναγνώσιμη. Ένα DN αποτελείται από μια ακολουθία σχετικών διακριτών ονομάτων (RDNs) που χωρίζονται με κόμματα. Η ακολουθία των RDNs κάνουν τα DN ονόματα να είναι οι πρόγονοι μιας καταχώρησης καταλόγου στην ρίζα ενός DIT. Κάθε RDN έχει συγκροτηθεί από την τιμή ενός χαρακτηριστικού που ανήκει σε μια καταχώρηση. Για παράδειγμα, το DN cn=John Smith, ou=Austin, o=IBM, c=US αντιπροσωπεύει μια καταχώρηση που αφορά ένα άτομο με το όνομα (cn: common name) John Smith που ανήκει στην οργανωτική μονάδα (ou: organizational unit) Austin στον οργανισμό (o: organization) IBM στην χώρα (c: country) US.

4. RFC 2254 *The String Representation of LDAP Search Filters*

Τα φίλτρα αναζήτησης του LDAP παρέχουν έναν ισχυρό μηχανισμό αναζήτησης καταχωρήσεων καταλόγου που ικανοποιούν ορισμένα κριτήρια. Το πρωτόκολλο LDAP ορίζει την δικτυακή αναπαράσταση ενός φίλτρου αναζήτησης. Μια τέτοια αναπαράσταση μπορεί να χρησιμοποιηθεί σε πολλές εφαρμογές ή στον πηγαίο κώδικα ενός προγράμματος για να ορίσει τα κριτήρια αναζήτησης. Οι τιμές των χαρακτηριστικών συγκρίνονται με την χρησιμοποίηση τελεστών όπως ‘’=’’, ‘’>’’. Οι Boolean τελεστές μπορούν να χρησιμεύσουν στην κατασκευή πιο σύνθετων φίλτρων. Παραδείγματος χάριν, το φίλτρο αναζήτησης (| (sn=Smith) (cn=Jo*)) ψάχνει για εγγραφές που είτε έχουν ένα χαρακτηριστικό surname Smith είτε ένα common name που αρχίζει από Jo.

5. RFC 2255 *The LDAP URL Format*

Οι URLs (Uniform Resource Locators) χρησιμοποιούνται για να αναγνωρίζουν ιστοσελίδες, αρχεία και άλλες πηγές στο Internet. Ένα LDAP URL διευκρινίζει ότι μια αναζήτηση LDAP θα εκτελεσθεί σε συγκεκριμένο LDAP server. Ένα LDAP URL αντιπροσωπεύει με σταθερό και τυποποιημένο τρόπο την επιστρεφόμενη πληροφορία ως το αποτέλεσμα της αναζήτησης.

6. RFC 2256 *A Summary of the X.500 (96) User Schema for use with LDAPv3*

Πολλά σχήματα και χαρακτηριστικά που συνήθως προσεγγίζονται από τους πελάτες καταλόγου είναι ήδη καθορισμένα από το X.500. Αυτό το RFC κάνει μια επισκόπηση των χαρακτηριστικών και των κατηγοριών αντικειμένου που πρέπει οι LDAP servers να αναγνωρίζουν. Για παράδειγμα, καθορίζονται χαρακτηριστικά όπως cn (common name), description και postalAddress.

Επίσης καθορίζονται κατηγορίες αντικειμένου όπως country, organizationalUnit, groupOfNames και applicationEntity.

Τα RFCs που αναφέρθηκαν παραπάνω διαμορφώνουν τον πυρήνα του LDAP προδιαγραφής έκδοσης 3. Εκτός από αυτά τα RFCs, η IETF διαθέτει έναν αριθμό προτεινόμενων επεκτάσεων του LDAPv3 που μπορούν να εφαρμοσθούν από τους προμηθευτές. Εντούτοις, οι επεκτάσεις αυτές βρίσκονται ακόμα σε κατάσταση προσχεδίων αλλά μπορεί να αλλάξουν. Η ακόλουθη λίστα συνοψίζει κάποιες από τις προτεινόμενες επεκτάσεις:

- Υποχρεωτική εφαρμογή επικύρωσης

  Μια προσπάθεια ώστε να υπάρξει μια τουλάχιστον πρότυπη, ασφαλής μέθοδο επικύρωσης σε όλους τους servers και clients (όχι μόνο στο LDAP), παρά ξεχωριστές μέθοδοι για κάθε πρωτόκολλο που τρέχει πάνω στο TCP/IP.
- Επεκτάσεις για Δυναμικές Υπηρεσίες Καταλόγου

  Αυτή είναι μια επέκταση πρωτοκόλλου που επιτρέπει στους πελάτες να αλληλεπιδρούν πιο αξιόπιστα με τους servers όταν τα περιεχόμενα του καταλόγου αλλάζουν.
- LDAP Χρήση των Κωδικών Γλώσσας στο

  Περιγράφει την προσθήκη των κωδικών φυσικής γλώσσας στα χαρακτηριστικά που αποθηκεύονται στον κατάλογο LDAP.
- LDAPv3 για την ασφάλεια του στρώματος μεταφοράς Επέκταση του

  Καθορίζει την ενσωμάτωση του μηχανισμού ασφάλειας στρώματος μεταφοράς (TLS) μέσα στο LDAP.
- LDAP για τον χειρισμό σελιδοποιημένων αποτελεσμάτων Επέκταση ελέγχου

  Περιγράφει μια επέκταση ελέγχου για σελιδοποίηση των αποτελεσμάτων αναζήτησης. Αυτό αποτελεί ειδική αξία για τους απλούς, -περιορισμένης λειτουργίας- πελάτες έτσι ώστε να μπορούν να ζητούν τα αποτελέσματα αναζήτησης να επιστρέφονται σε μικρότερα τμήματα (σελίδες) κάθε φορά.
- LDAP Παραπομπές και αναφορές πληροφορίας σε καταλόγους

  Καθορίζει το πώς οι παραπομπές και οι αναφορές πληροφορίας μπορούν να αποθηκευθούν ως χαρακτηριστικά και πώς μπορούν να χρησιμοποιηθούν.
- LDAP για την ταξινόμηση των αποτελεσμάτων αναζήτησης στον server. Επέκταση ελέγχου

  Επιτρέπει την ταξινόμηση των αποτελεσμάτων αναζήτησης στον server απ' ότι στον client. Αυτό μπορεί να είναι επιθυμητό για την κατασκευή απλούστερων -περιορισμένης λειτουργίας- πελατών.
- LDAP Η διεπαφή προγραμματισμού του

Καθορίζει το API της γλώσσας C στο LDAP. Οι περισσότεροι προμηθευτές ήδη ενσωματώνουν αυτή την επέκταση ή τουλάχιστον ένα μέρος αυτής.

2.2 Τα Πρότυπα LDAP

Το LDAP μπορεί να γίνει καλύτερα κατανοητό αν εξετάσουμε τα τέσσερα μοντέλα στα οποία είναι βασισμένο:

- **Πληροφορία**

  Περιγράφει την δομή των πληροφοριών που αποθηκεύονται σε έναν κατάλογο LDAP.

- **Ονομασία**

  Περιγράφει τον τρόπο με τον οποίο η πληροφορία οργανώνεται και αναγνωρίζεται στον κατάλογο LDAP.

- **Λειτουργικότητα**

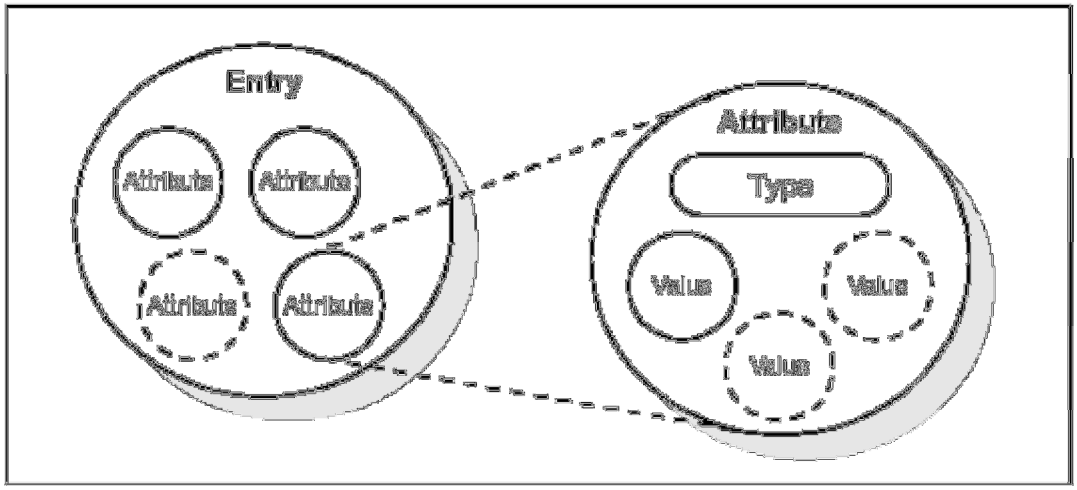
  Περιγράφει τις λειτουργίες που μπορούν να εκτελεσθούν πάνω στις αποθηκευμένες πληροφορίες καταλόγου LDAP.

- **Ασφάλεια**

  Περιγράφει το πώς η αποθηκευμένη πληροφορία καταλόγου LDAP μπορεί να προστατεύεται από μη επικυρωμένες προσβάσεις.

2.2.1 Το Πληροφοριακό Μοντέλο

Η βασική μονάδα αποθηκευμένων πληροφοριών καταλόγου ονομάζεται *καταχώρηση*. Οι καταχωρήσεις αναπαριστούν αντικείμενα όπως άτομα, servers, οργανισμούς και ούτω καθεξής. Αποτελούνται από μια συλλογή χαρακτηριστικών που περιέχουν πληροφορίες για τα αντικείμενα. Κάθε χαρακτηριστικό έχει έναν τύπο και μια ή περισσότερες τιμές. Ο τύπος του χαρακτηριστικού συνδέεται με έναν συντακτικό τύπο. Ο συντακτικός τύπος διευκρινίζει τα είδη των τιμών που μπορούν να αποθηκευθούν. Για παράδειγμα, μια καταχώρηση μπορεί να έχει το χαρακτηριστικό facsimileTelephoneNumber. Ο συντακτικός τύπος μαζί με αυτόν τον τύπο του χαρακτηριστικού διευκρινίζει ότι οι τιμές είναι τηλεφωνικοί αριθμοί οι οποίοι αναπαρίστανται από εκτυπώσιμα strings. Είναι πιθανό μια καταχώρηση καταλόγου ενός οργανισμού να περιέχει διαφορετικές τιμές για το παραπάνω χαρακτηριστικό. Αυτό σημαίνει ότι ένας οργανισμός ή άτομο που αντιπροσωπεύεται από την οντότητα θα έχει πολλούς αριθμούς fax. Η σχέση μεταξύ καταχώρησης καταλόγου, των χαρακτηριστικών και των τιμών της φαίνεται στο σχήμα 2.2.1.



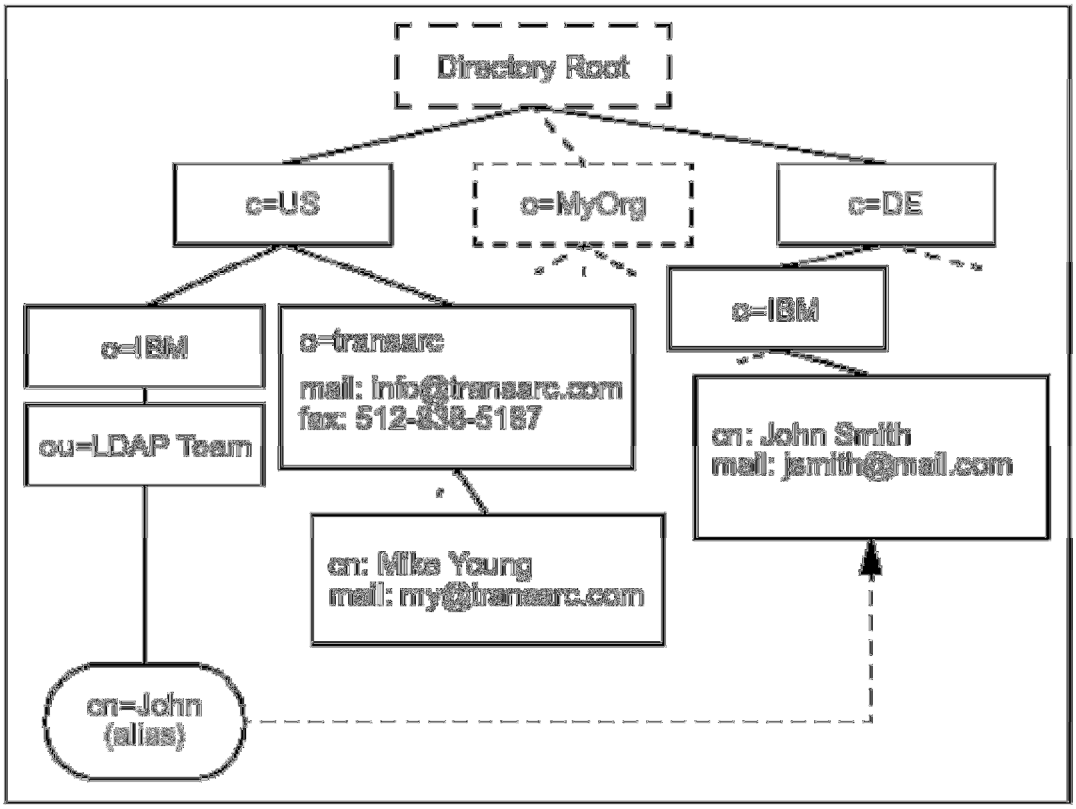
Σχήμα 2.2.1 Καταχωρήσεις, χαρακτηριστικά και τιμές

Εκτός από τον καθορισμό των δεδομένων που αποθηκεύονται ως τιμή σε ένα χαρακτηριστικό, ένας συντακτικός τύπος καθορίζει επίσης το πώς αυτές οι τιμές συμπεριφέρονται κατά την διάρκεια των διαδικασιών αναζήτησης και άλλων λειτουργιών καταλόγου. Παραδείγματος χάριν, το χαρακτηριστικό telephoneNumber έχει έναν συντακτικό τύπο ο οποίος καθορίζει:
• την λεξικογραφική σειρά
• ότι τα κενά και οι παύλες αγνοούνται κατά την διάρκεια των συγκρίσεων
• ότι οι τιμές πρέπει να είναι strings χαρακτήρων.

2.2.2 Το Μοντέλο Ονομασίας

Το μοντέλο ονομασίας LDAP καθορίζει τον τρόπο με τον οποίο οι καταχωρήσεις αναγνωρίζονται και οργανώνονται. Οι καταχωρήσεις είναι οργανωμένες υπό μορφή δέντρου που ονομάζεται Directory Information Tree (DIT) και τακτοποιούνται μέσα στο DIT με βάση το DN τους. Ένα DN είναι ένα μοναδικό όνομα που σαφώς προσδιορίζει μια μοναδική καταχώρηση. Τα DN είναι δημιουργημένα από μια ακολουθία σχετικών διακριτών ονομάτων (RDNs). Κάθε RDN που βρίσκεται σε ένα DN αντιστοιχεί σε ένα κλαδί του DIT που ξεκινάει από τη ρίζα του δέντρου ως την καταχώρηση του καταλόγου. Κάθε RDN προέρχεται από τα χαρακτηριστικά της καταχώρησης καταλόγου. Στην απλή και συνηθισμένη περίπτωση, ένα RDN έχει την μορφή <όνομα χαρακτηριστικού> = <τιμή>. Ένα DN αποτελείται από την ακολουθία των RDNs που χωρίζονται με κόμματα.
Ένα παράδειγμα ενός DIT φαίνεται στο σχήμα 2.2.2.α'. Το παράδειγμα είναι πολύ απλό αλλά μπορεί να χρησιμοποιηθεί και για την επεξήγηση μερικών βασικών εννοιών. Κάθε πλαίσιο αντιπροσωπεύει μια καταχώρηση καταλόγου.

Η καταχώρηση ρίζας είναι εννοιολογική και στην πραγματικότητα δεν υπάρχει. Τα χαρακτηριστικά παρατίθενται μέσα σε κάθε καταχώρηση. Η λίστα των χαρακτηριστικών που παρουσιάζεται δεν είναι ολοκληρωμένη. Για παράδειγμα, η καταχώρηση για την χώρα DE (c=DE) θα μπορούσε να έχει το χαρακτηριστικό description (περιγραφή) με την τιμή Germany (Γερμανία).



Σχήμα 2.2.2.α'. Παράδειγμα ενός DIT

Η οργάνωση των καταχωρήσεων στο DIT περιορίζεται από τους αντίστοιχους ορισμούς των κατηγοριών αντικειμένου. Είναι συνηθισμένο να ακολουθούμε ένα γεωγραφικό ή οργανωτικό σχήμα. Παραδείγματος χάριν, οι καταχωρήσεις που αντιπροσωπεύουν χώρες θα τοποθετούνταν στην κορυφή του DIT. Κάτω από τις χώρες θα βρίσκονταν διεθνείς οργανισμοί, πόλεις, επαρχίες και ούτω καθεξής. Κάτω από αυτό το επίπεδο, οι καταχωρήσεις μπορεί να αφορούν άτομα που βρίσκονται σε αυτούς τους οργανισμούς ή περαιτέρω υποδιαιρέσεις του οργανισμού. Τα χαμηλότερα επίπεδα των καταχωρήσεων του DIT μπορούν να αναπαριστούν οποιοδήποτε αντικείμενο όπως άτομα, εκτυπωτές, εξυπηρετητές εφαρμογών και τα λοιπά. Το βάθος ή το εύρος του DIT δεν είναι απαγορευτικό και μπορεί να σχεδιαστεί ώστε να ταιριάζει με τις απαιτήσεις των εφαρμογών.

Οι καταχωρήσεις ονομάζονται σύμφωνα με τη θέση τους στο DIT. Η καταχώρηση που βρίσκεται χαμηλά δεξιά στο Σχήμα 2.2.2.α' έχει το DN cn=John Smith, o=IBM, c=DE. Σημειώνεται ότι συνήθως τα DNs διαβάζονται από τα φύλλα προς τη ρίζα σε αντίθεση με τα ονόματα αρχείου συστήματος που συνήθως διαβάζονται από την ρίζα προς τα φύλλα. Όπως αναφέρθηκε, τα DNs αποτελούνται από την ακολουθία των RDNs. Κάθε RDN είναι κατασκευασμένο από ένα

χαρακτηριστικό (ή χαρακτηριστικά) της καταχώρησης που ονομάζει. Παραδείγματος χάριν, το DN cn=John Smith, o=IBM, c=DE έχει κατασκευαστεί από την πρόσθεση του RDN cn=John Smith στο DN o=IBM, c=DE της προηγούμενης καταχώρησης. Σημειώνεται το cn=John Smith είναι χαρακτηριστικό στην καταχώρηση cn=John Smith, o=IBM, c=DE. Το DN μιας καταχώρησης προσδιορίζεται όταν δημιουργείται. Επίσης θα ήταν νόμιμο να έχει δημιουργηθεί μια καταχώρηση με το DN mail=jsmith@mail.com, o=IBM, c=DE.
Το DIT περιγράφεται ως μια μορφή δέντρου αλλά δεν είναι δέντρο. Αυτό συμβαίνει εξ αιτίας των ψευδωνύμων (aliases). Τα ψευδώνυμα επιτρέπουν στη δομή δένδρου να είναι παρακάμψιμη. Αυτό μπορεί να είναι χρήσιμο αν μια καταχώρηση ανήκει σε περισσότερους από έναν οργανισμούς ή αν ένα χρησιμοποιούμενο
DN είναι πολύπλοκο. Μια άλλη συνηθισμένη χρήση των ψευδωνύμων είναι όταν οι καταχωρήσεις μετακινούνται μέσα στο DIT και επιθυμούμε πρόσβαση για να συνεχίσουμε να εργαζόμαστε όπως πριν. Στο Σχήμα 2.2.2.α' το cn=John, ou=LDAP Team, o=IBM, c=US είναι ένα alias για το cn= John Smith, o= IBM, c=DE. Τα ψευδώνυμα δεν χρειάζεται να δείχνουν στις καταχωρήσεις φύλλων στο DIT. Για παράδειγμα, το o=Book, c=US θα μπορούσε να ήταν ψευδώνυμο για το ou=ITSO, o=IBM, c=US.

2.2.2.1 Το Συντακτικό των DNs

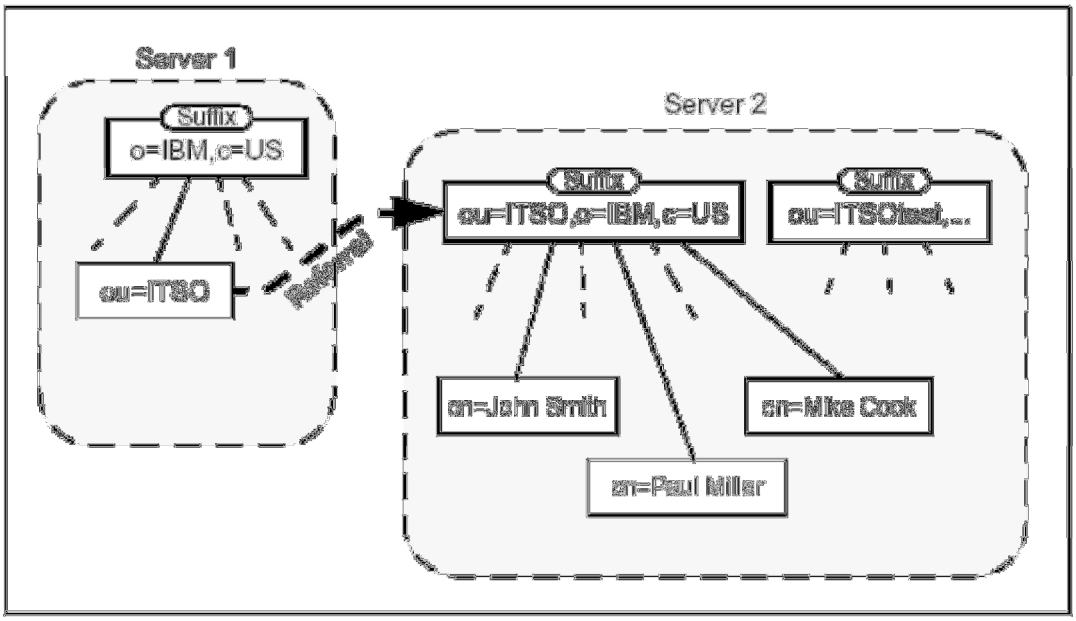
Τα DNs χρησιμοποιούνται ως πρωτεύοντα κλειδιά στις καταχωρήσεις καταλόγου. Το LDAP ορίζει μια string αναπαράσταση των DNs. Το Σχήμα 2.2.2.1.α' δείχνει την επίσημη γραμματική των DNs. Σημειώνεται ότι τα RDNs μπορεί να γίνουν πιο πολύπλοκα σε αντίθεση με τα παραδείγματα που περιγράφηκαν παραπάνω. Ένα RDN μπορεί να αποτελείται από ποικίλα χαρακτηριστικά συνοδευόμενα από το ''+'' όπως στο DN cn=John Smith+1=Stuttgart, o=IBM, c=DE. Εάν οι τιμές των χαρακτηριστικών περιέχουν ειδικούς χαρακτήρες πρέπει να γίνεται διαφυγή αυτών με την χρήση του χαρακτήρα ''\'' πριν από αυτούς. Το ακόλουθο DN περιέχει ένα κόμμα

o=Transarc\, Inc., c=US.

Τα DNs στην έκδοση 3 του LDAP είναι περισσότερο περιοριστικά απ' ότι στην έκδοση 2. Παραδείγματος χάριν, στο LDAPv2 ο ειδικός χαρακτήρας '' ; '' μπορεί επίσης να χωρίζει τα RDNs. Στο LDAPv3 πρέπει να είναι αποδεκτή η παλαιότερη σύνταξη αλλά όμως δεν πρέπει να δημιουργούνται DNs που δεν προσαρμόζονται με το νεότερο συντακτικό τύπο.

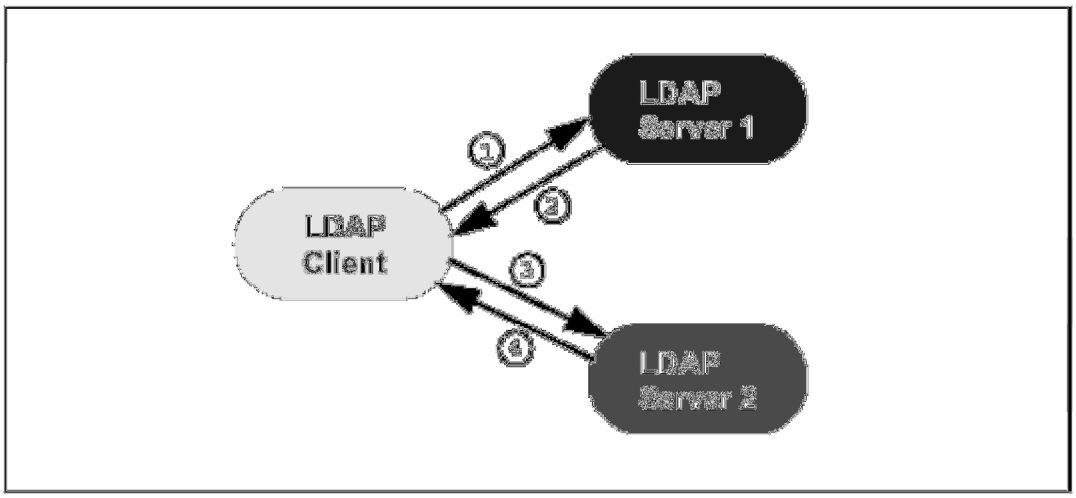
2.2.2.2 Επιθέματα και Παραπομπές

Ένας αυτόνομος LDAP server ίσως να μην αποθηκεύει ολόκληρο το DIT. Ένας server μπορεί να αποθηκεύει τις καταχωρήσεις ενός συγκεκριμένου τμήματος και όχι τις καταχωρήσεις για αυτούς που προηγούνταν του τμήματος. Παραδείγματος χάριν, ένας server μπορεί να αποθηκεύσει τις καταχωρήσεις για το τμήμα
ITSO της IBM. Ο ανώτερος κόμβος του DIT που αποθηκεύεται από τον server θα είναι το ou=ITSO, o=IBM, c=US. Ο server δεν θα αποθηκεύσει καταχωρήσεις για το c=US ή για o=IBM, c=US. Η ανώτατη καταχώρηση που αποθηκεύεται από έναν server ονομάζεται *επίθεμα*. Κάθε καταχώρηση λήγει σε ένα επίθεμα (σημειώνεται ότι στην σύνταξη των DNs οι –ανωτέρου επιπέδου- καταχωρήσεις βρίσκονται στο τέλος).
Ένας server μπορεί να υποστηρίξει ποικίλα επιθέματα. Για παράδειγμα, εκτός από την αποθήκευση πληροφοριών για το ITSO τμήμα, ο ίδιος server θα μπορούσε να αποθηκεύσει πληροφορίες για το τμήμα πωλήσεων στο Transarc. Σε αυτή την περίπτωση ο server θα είχε τα επιθέματα ou=ITSO, o=IBM, c=US και ou=sales, o=Transarc, c=US.
Από την στιγμή που ο server δεν αποθηκεύει ολόκληρο το δένδρο, οι servers θα πρέπει να συνδέονται με κάποιον τρόπο μεταξύ τους ώστε να σχηματίσουν ένα κατανεμημένο κατάλογο που θα περιέχει ολόκληρο το DIT. Αυτό κατορθώνεται με τις *παραπομπές*. Συνεχίζοντας το παράδειγμα, ένας άλλος server ίσως να αποθηκεύσει την καταχώρηση o=IBM, c=US αλλά όχι πληροφορίες για το τμήμα ITSO. Εάν κάποιος αναζητήσει πληροφορία σε αυτόν τον κατάλογο για το τμήμα ITSO, δεν θα βρει καμία. Ωστόσο ο server μπορεί να αποθηκεύσει μια παραπομπή στον LDAP server που θα περιέχει την πληροφορία. Η παραπομπή αυτή συμπεριφέρεται ως δείκτης ο οποίος ακολουθεί την επιθυμητή πληροφορία όπου αυτή βρίσκεται. Ένα τέτοιο παράδειγμα φαίνεται στο Σχήμα 2.2.2.2.α’ όπου το βέλος της παραπομπής δείχνει την λογική σύνδεση της παραπομπής και όχι την τεχνική εφαρμογή. Μια παραπομπή είναι μια καταχώρηση της παραπομπής objectClass. Έχει ένα χαρακτηριστικό, το ref, του οποίου η τιμή είναι το LDAP URL της καταχώρησης που παραπέμπεται σε έναν άλλο LDAP server.



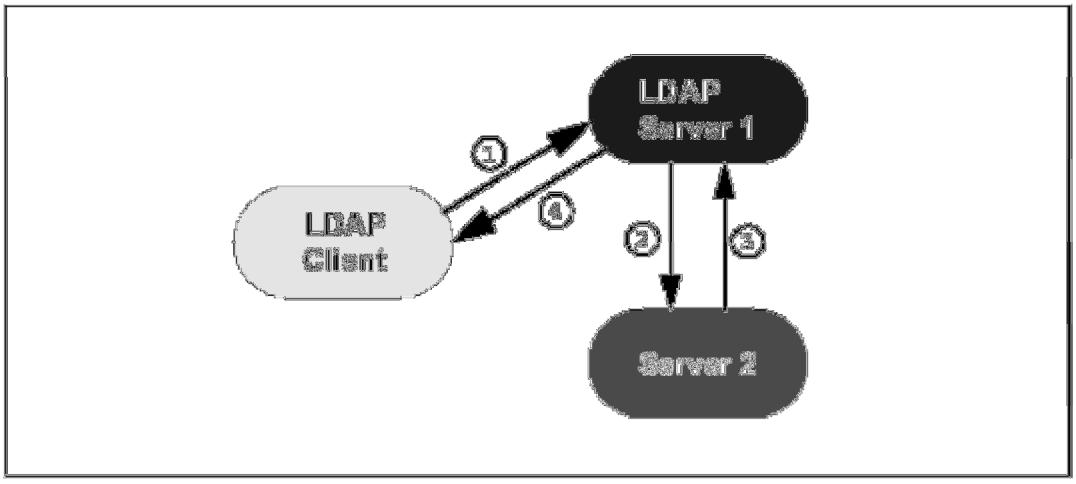
Σχήμα 2.2.2.2.α' Παράδειγμα DIT με παραπομπές και επιθέματα

Όταν ένας client στέλνει ένα αίτημα στον LDAP server, η απόκριση στον client μπορεί να είναι μια παραπομπή. Έπειτα ο client μπορεί να επιλέξει να ακολουθήσει την παραπομπή με το να ρωτήσει τον άλλον server ο οποίος περιέχεται στην παραπομπή που επιστρέφεται από τον πρώτο LDAP server. Οι παραπομπές δεν ακολουθούνται από τους
servers. Αυτό μπορεί να βελτιώσει την απόδοση του server με το να τεθεί εκτός φόρτωσης η διαδικασία σύνδεσης άλλων servers με τον client.
Το Σχήμα 2.2.2.2.β' απεικονίζει έναν client που ακολουθεί μια παραπομπή. Ένας LDAP client ζητάει πληροφορία από τον LDAP server 1 (1). Το αίτημα απαντάται με μια παραπομπή στον LDAP server 2 (2). Έπειτα ο client συνδέεται με τον LDAP server 2 (3). Ο LDAP server 2 παρέχει τα δεδομένα που έχουν ζητηθεί στον client (4).



Σχήμα 2.2.2.2.β' Παραπομπή που ακολουθείται από τον client

Στο Σχήμα 2.2.2.2.γ' απεικονίζεται η διαδικασία *αλυσίδας*. Ένας LDAP client ζητάει πληροφορία από τον LDAP server 1 (1). Ο LDAP server 1 βρίσκει μια παραπομπή στον server 2 και προωθεί το αίτημα (2).Ο server 2 δίνει τα ζητούμενα δεδομένα στον LDAP server 1 (3). Κατόπιν ο LDAP server 1 επιστρέφει τα αποτελέσματα στον client (4). Σημειώνεται ότι η συγκεκριμένη εξήγηση και το Σχήμα 2.2.2.2.γ' υπάρχουν για την επεξήγηση περιπτώσεων στις οποίες δεν συμπεριλαμβάνεται η διαδικασία αλυσίδας στις προδιαγραφές της έκδοσης 2 ή 3 του LDAP.



Σχήμα 2.2.2.2.γ' Διαδικασία αλυσίδας των server

Το LDAP API επιτρέπει στον προγραμματιστή να διευκρινίζει πότε πρέπει οι παραπομπές να ακολουθούνται αυτόματα ή να επιστρέφονται στο πρόγραμμα. Εάν αυτές ακολουθούνται αυτόματα τότε η βιβλιοθήκη του LDAP client (ούτε ο server ούτε το πρόγραμμα εφαρμογής) ακολουθεί την παραπομπή. Το γεγονός αυτό δεν απαιτεί επιπλέον κωδικοποίηση και είναι διαφανές στον προγραμματιστή. Για να αποφευχθούν οι μεγάλου μήκους αναζητήσεις ή παραπομπές που (λανθασμένα) σχηματίζουν ένα βρόχο, ο προγραμματιστής μπορεί να μειώσει τον αριθμό των παραπομπών που ακολουθούν ένα αίτημα.

Εάν η παραπομπή επιστρέφεται στο πρόγραμμα, τότε πρέπει να συμπεριλαμβάνεται η κωδικοποίηση για να φαίνεται ότι η παραπομπή έχει επιστρέψει. Η παραπομπή μπορεί να αξιολογηθεί και να αποφασισθεί αν θα ακολουθηθεί ή όχι. Αυτό είναι αρκετά πολύπλοκο αλλά δίνει στον προγραμματιστή καλύτερη δυνατότητα επιλογής για το ποιες παραπομπές πρέπει να ακολουθούνται και ποιες όχι.

Οι παραπομπές επιτρέπουν σε ένα DIT να μοιρασθεί και να κατανεμηθεί σε πολλούς servers. Επίσης τα μέρη του DIT μπορούν να αντιγραφούν. Αυτό μπορεί να βελτιώσει την απόδοση και την διαθεσιμότητα.

Η έκδοση 2 του LDAP δεν καθορίζει επίσημα τις παραπομπές αλλά η έκδοση 3 τις συμπεριλαμβάνει. Ούτε η έκδοση 2 ούτε η 3 καθορίζουν την αλυσίδα, όμως δεν είναι απαγορευτική αν οι προμηθευτές επιθυμήσουν να την εφαρμόσουν. Οι προμηθευτές, για παράδειγμα, μπορούν να επιλέξουν να εφαρμόσουν έναν μηχανισμό αλυσίδας τύπου X.500 ή να παρέχουν λειτουργικότητα μέσω κατανεμημένων Βάσεων Δεδομένων.

2.2.2.3 Πληροφορία του Server

Ένας LDAP server έκδοσης 3 πρέπει να παρέχει πληροφορίες για τον εαυτό του. Η ειδική καταχώρηση που ονομάζεται ρίζα DSE με ένα –μηδενικού μήκους (κενό)- DN περιέχει χαρακτηριστικά που περιγράφουν τον server. Τα χαρακτηριστικά αυτά μπορούν να ανακτηθούν για να αποκαλυφθούν βασικές πληροφορίες για τον server και το DIT που αποθηκεύει. Η πληροφορία για τον server περιλαμβάνει:

- Τα επιθέματα που αποθηκεύει ο server
- Το DN μιας ειδικής καταχώρησης που περιέχει μια λίστα όλων των objectClass και του σχήματος των χαρακτηριστικών που είναι γνωστά στον server.
- Την έκδοση ή τις εκδόσεις του LDAP που υποστηρίζονται
- Μια λίστα με επιπλέον λειτουργίες και ελέγχους
- Μια λίστα των υποστηριζόμενων μηχανισμών ελέγχου SASL
- Μια λίστα των εναλλακτικών LDAP servers

Καθώς το LDAP επεκτείνεται, οι επιπρόσθετες πληροφορίες για τον server θα αποθηκεύονται στην ρίζα DSE.

2.2.3 Το Λειτουργικό Μοντέλο

Το LDAP ορίζει τις λειτουργίες προσπέλασης και τροποιήσης των καταχωρήσεων καταλόγου. Η ενότητα αυτή παρουσιάζει τις λειτουργίες του LDAP με τρόπο ανεξάρτητο από γλώσσες προγραμματισμού. Οι λειτουργίες του LDAP μπορούν να χωρισθούν στις παρακάτω κατηγορίες:

Query: Περιλαμβάνει την αναζήτηση και την σύγκριση λειτουργιών που χρησιμοποιούνται για την ανάκτηση πληροφοριών από τον κατάλογο

Update: Περιλαμβάνει την πρόσθεση, την διαγραφή, την τροποποίηση και την τροποποίηση των RDN που χρησιμοποιούνται για να ενημερώσουν την αποθηκευμένη πληροφορία καταλόγου

Authentication: Περιλαμβάνει τις διαδικασίες σύνδεσης, αποσύνδεσης και ματαίωσης που γίνονται για να συνδεθούμε με έναν LDAP server ή να αποσυνδεθούμε από αυτόν, κατοχυρώνοντας έτσι τα δικαιώματα προσπέλασης και την προστασία των πληροφοριών.Η πιο συνηθισμένη ενέργεια είναι η αναζήτηση. Η διαδικασία της αναζήτησης είναι πολύ ευέλικτη και έχει μερικές από τις πιο περίπλοκες επιλογές.

2.2.3.1 Αναζήτηση (search)

Η λειτουργία της αναζήτησης επιτρέπει σε έναν client να ζητήσει από έναν LDAP server να ψάξει σε κάποια τμήματα του DIT για πληροφορίες που θα ικανοποιούν τα κριτήρια αναζήτησης του χρήστη με σκοπό να διαβάσει και να απαριθμήσει τα αποτελέσματα. Δεν υπάρχουν ξεχωριστές διαδικασίες για την ανάγνωση και την εμφάνιση αποτελεσμάτων. Και οι δύο είναι συνδεδεμένες με την αναζήτηση. Η αναζήτηση μπορεί να είναι γενική ή πολύ ειδική. Αυτή επιτρέπει σε κάποιον να διευκρινίσει το σημείο από όπου ξεκινάει η αναζήτηση μέσα στο DIT, τί βάθος θα έχει η αναζήτηση στο DIT, ποια χαρακτηριστικά πρέπει να έχει μια καταχώρηση για να θεωρηθεί ότι ταιριάζει με τα κριτήρια και ποια χαρακτηριστικά πρέπει να επιστραφούν για τις ταιριασμένες καταχωρήσεις.

Μερικά παραδείγματα αναζητήσεων είναι:

- Βρες την διεύθυνση ταχυδρομείου για το cn=John Smith, o=IBM, c=DE.
- Βρες όλες τις καταχωρήσεις που είναι απόγονοι της καταχώρησης ou=ITSO, o=IBM, c=US.
- Βρες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου και τους τηλεφωνικούς αριθμούς όλων όσων εργάζονται στην IBM που το επιθετό τους περιέχει τους χαρακτήρες ‘’miller’’ και διαθέτουν επίσης αριθμό fax.

Για να εκτελεστεί μια αναζήτηση πρέπει να καθορισθούν οι παρακάτω παράμετροι:

• **Βάση**

Ένα DN που ορίζει το σημείο εκκίνησης- το οποίο αποκαλείται αντικείμενο βάσης- της αναζήτησης. Το αντικείμενο βάσης είναι ένας κόμβος μέσα στο DIT.

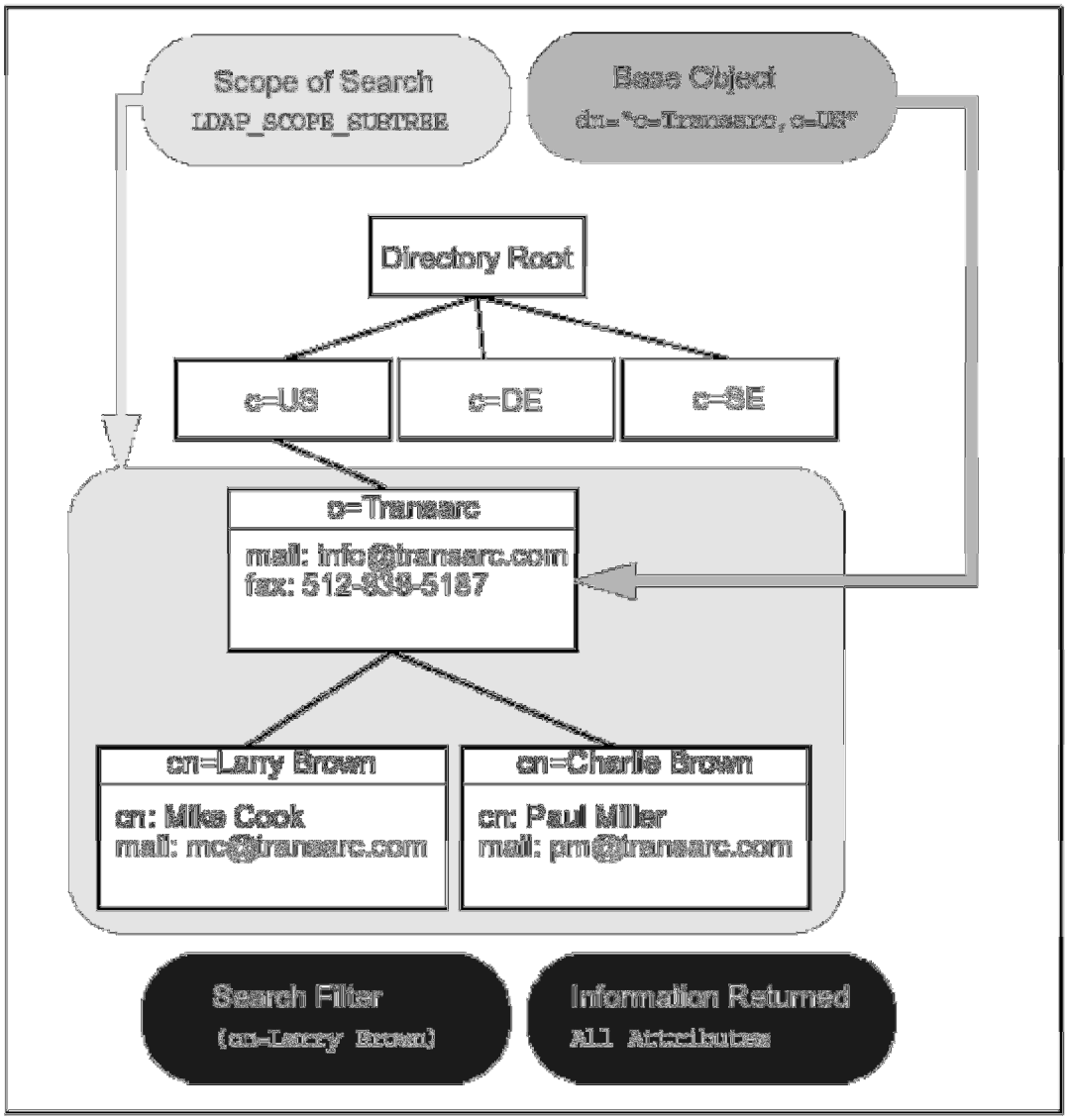
• **Πεδίο**

Καθορίζει την τοποθεσία μέσα στο δέντρο που θα γίνει η αναζήτηση με αφετηρία το αντικείμενο βάσης. Υπάρχουν τρεις επιλογές: baseObject, singleLevel
και wholeSubtree. Εάν είναι καθορισμένη η baseObject, εξετάζεται μόνο το αντικείμενο βάσης. Εάν καθορίζεται η singleLevel εξετάζονται μόνο τα άμεσα ‘’παιδιά’’ του αντικειμένου βάσης. Το ίδιο το αντικείμενο βάσης δεν εξετάζεται. Στην περίπτωση της wholeSubtree, εξετάζεται το αντικείμενο βάσης και όλοι οι απογονοί του.

• **Φίλτρα αναζήτησης**
Ορίζει τα κριτήρια που πρέπει να ταιριάξει μια καταχώρηση για να επιστραφεί από την αναζήτηση. Το φίλτρο αναζήτησης είναι ένας Boolean συνδυασμός των διεκδικούμενων τιμών χαρακτηριστικού. Μια τιμή που πρόκειται να γίνει τιμή χαρακτηριστικού εξετάζει την υπάρχουσα τιμή για το αν είναι μεγαλύτερη, μικρότερη, ίση και ούτω καθεξής. Παραδείγματος χάριν, ένα φίλτρο αναζήτησης μπορεί να ψάχνει για καταχωρήσεις που να περιέχουν τη λέξη ‘’printer’’ ή να ανήκουν στον οργανισμό ITSO.

• **Καταχωρήσεις επιστροφής**
Διευκρινίζει ποια χαρακτηριστικά ανακτώνται από τις καταχωρήσεις που ταιριάζουν με τα κριτήρια αναζήτησης. Από τη στιγμή που μια καταχώρηση έχει πολλά χαρακτηριστικά, αυτό επιτρέπει στον χρήστη να βλέπει μόνο αυτά που τον ενδιαφέρουν. Φυσιολογικά, ο χρήστης ενδιαφέρεται για την τιμή των χαρακτηριστικών. Ωστόσο, είναι δυνατόν να επιστρέφονται μόνο οι τύποι των χαρακτηριστικών και όχι οι τιμές τους.

• **Όρια**
Οι αναζητήσεις μπορεί να είναι πολύ γενικές, εξετάζοντας μεγάλα υπόδεντρα και προκαλώντας την επιστροφή πολλών καταχωρήσεων ως αποτελέσματα. Ο χρήστης μπορεί να θέσει όρια μεγέθους και χρόνου για να αποφύγει την δύστροπη αναζήτηση καταναλώνοντας πολλές πηγές. Το όριο μεγέθους περιορίζει των αριθμό καταχωρήσεων που επιστρέφονται από την αναζήτηση. Το χρονικό όριο περιορίζει τον συνολικό χρόνο αναζήτησης. Οι servers είναι ελεύθεροι να επιβάλλουν πιο περιοριστικά όρια ακόμα και αν δεν έχουν ζητηθεί από την πλευρά του client.



Σχήμα 2.2.3.1 Παράμετροι αναζήτησης

2.2.3.2 Παραπομπές και Αναφορές Συνέχειας

Εάν ο server δεν περιέχει το αντικείμενο βάσης, θα επιστρέψει μια παραπομπή στον server που το έχει, εάν αυτό είναι δυνατόν. Από την στιγμή που θα βρεθεί το αντικείμενο βάσης οι αναζητήσεις singleLevel και wholeSubtree ίσως συναντήσουν άλλες παραπομπές. Αυτές οι παραπομπές επιστέφονται στα αποτελέσματα της αναζήτησης μαζί με άλλες παρόμοιες καταχωρήσεις. Οι συγκεκριμένες παραπομπές ονομάζονται αναφορές συνέχειας επειδή δείχνουν πού μπορεί να συνεχιστεί μια αναζήτηση.

Παραδείγματος χάριν, όταν αναζητάμε σε ένα υπόδεντρο οποιονδήποτε που ονομάζεται Smith, μπορεί να επιστραφεί μια αναφορά συνέχειας σε έναν άλλο server πιθανώς μαζί με πολλές άλλες ταιριαστές καταχωρήσεις. Δεν εγγυάται ότι υπάρχει καταχώρηση με το όνομα Smith στον άλλο server, αλλά ότι η αναφορά συνέχειας δείχνει σε ένα υπόδενδρο που θα μπορούσε να περιέχει μια τέτοια καταχώρηση. Εξαρτάται από τον client να ακολουθήσει την αναφορά αν το επιθυμεί. Αφού μόνο η έκδοση 3 του LDAP καθορίζει τις παραπομπές, οι αναφορές συνέχειας δεν υποστηρίζονται από τις προηγούμενες εκδόσεις.

2.2.3.3 Φίλτρο Αναζήτησης

Το φίλτρο αναζήτησης ορίζει τα κριτήρια που πρέπει να ταιριάξει μια καταχώρηση για να επιστραφεί από μια αναζήτηση. Το βασικό συστατικό ενός φίλτρου αναζήτησης είναι η διεκδίκηση τιμής χαρακτηριστικού της μορφής:

attribute operator value

2.2.3.4 Σύγκριση

Όπως φανερώνει και το όνομά της, η λειτουργία της σύγκρισης συγκρίνει μια καταχώρηση για μια τιμή χαρακτηριστικού. Αν η καταχώρηση έχει αυτή την τιμή, η σύγκριση επιστρέφει την τιμή TRUE. Αλλιώς επιστρέφει την FALSE. Αν και η σύγκριση είναι απλούστερη από μια αναζήτηση, είναι περίπου η ίδια με την αναζήτηση πεδίου βάσης με ένα φίλτρο αναζήτησης χαρακτηριστικού που είναι ίσο με την τιμή (attribute=value). Η διαφορά βρίσκεται στο ότι αν η καταχώρηση δεν έχει καθόλου το χαρακτηριστικό (το χαρακτηριστικό δεν εμφανίζεται), η αναζήτηση θα επιστρέψει ότι δεν βρήκε κάτι. Από την άλλη πλευρά, η σύγκριση θα επιστρέψει FALSE. Αυτό δείχνει ότι η καταχώρηση υπάρχει αλλά δεν διαθέτει χαρακτηριστικά που ταιριάζουν με τα κριτήρια της καθορισμένης τιμής.

2.2.3.5 Διαδικασίες Ενημέρωσης (UPDATE)

Add
Εισάγει νέες καταχωρήσεις μέσα στον κατάλογο

Delete
Διαγράφει υπάρχουσες καταχωρήσεις από τον κατάλογο. Μόνο οι κόμβοι των φύλλων μπορούν να διαγραφούν.

Modify

Αλλάζει τα χαρακτηριστικά και τις τιμές που περιέχονται σε μια υπάρχουσα καταχώρηση. Επιτρέπει να προστεθούν νέα χαρακτηριστικά και να διαγραφούν ή να τροποποιηθούν ισχύοντα χαρακτηριστικά.

2.2.3.6 Λειτουργίες Επικύρωσης (AUTHENTICATION)

Οι λειτουργίες επικύρωσης χρησιμοποιούνται για να ξεκινήσουν ή να ολοκληρώσουν μια σύνοδο ανάμεσα σε έναν LDAP client και σε έναν LDAP server. Η σύνοδος μπορεί να διασφαλισθεί σε πολλά επίπεδα αρχίζοντας από μια επισφαλή ανώνυμη σύνοδο, δηλαδή μια ανεπικύρωτη σύνοδο κατά την οποία ο client γνωστοποιεί τον εαυτό του μέσω ενός password και, καταλήγοντας σε μια ασφαλή, κρυπτογραφημένη σύνοδο χρησιμοποιώντας μηχανισμούς SASL. Το SASL προστέθηκε στην έκδοση 3 του LDAP για να υπερνικήσει την αδύναμη επικύρωση του LDAPv2 (κάποιοι προμηθευτές, ωστόσο, έχουν προσθέσει ισχυρότερες μεθόδους επικύρωσης όπως το Kerberos στην LDAPv2).

2.2.3.7 Έλεγχοι και Εκτεταμένες Λειτουργίες

Οι έλεγχοι και οι εκτεταμένες λειτουργίες επιτρέπουν στο πρωτόκολλο LDAP να επεκταθεί χωρίς να αλλάξει το ίδιο το πρωτόκολλο. Οι έλεγχοι τροποποιούν τη συμπεριφορά μιας λειτουργίας και οι εκτεταμένες λειτουργίες προσθέτουν νέες λειτουργίες στο πρωτόκολλο LDAP. Η λίστα των ελέγχων και των επεκτάσεων που υποστηρίζονται από έναν LDAP server μπορούν να προμηθευτούν από την εξέταση του κενού DN στον server.

Οι έλεγχοι μπορούν να καθορισθούν για την επέκταση κάθε λειτουργίας και προστίθενται στο τέλος του μηνύματος της λειτουργίας του πρωτοκόλλου. Παρέχονται ως παράμετροι στις συναρτήσεις του API. Στο μέλλον, οι τυποποιημένοι έλεγχοι ίσως να καθορίζονται στα σχετικά LDAP RFCs.

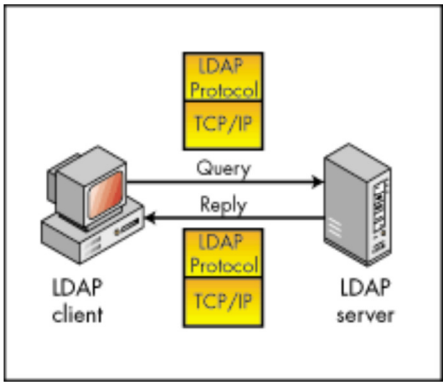
Ένας έλεγχος έχει μια -δεκαδικής στοιχειοσειράς- ταυτότητα αντικειμένου που χρησιμεύει για την αναγνωρισή του, μια αυθαίρετη τιμή ελέγχου που φυλάσσει παραμέτρους για τον έλεγχο, και ένα επίπεδο κρισιμότητας. Όταν το επίπεδο κρισιμότητας είναι TRUE ο server πρέπει να υποστηρίζει τον έλεγχο ή αν δεν τον υποστηρίξει τότε πρέπει να απορρίψει ολόκληρη την λειτουργία. Εάν το επίπεδο κρισιμότητας είναι FALSE, ο server που δεν υποστηρίζει τον έλεγχο πρέπει να εκτελέσει την λειτουργία όπως θα γινόταν αν δεν είχε καθορισθεί έλεγχος.
Για παράδειγμα, ένας έλεγχος μπορεί να παρατείνει την διαδικασία διαγραφής προκαλώντας μια εγγραφή λογιστικού ελέγχου η οποία θα καταγράφεται σε ένα αρχείο που προσδιορίζεται από την πληροφορία της τιμής του ελέγχου.
Μια εκτεταμένη λειτουργία επιτρέπει να καθορισθεί μια εντελώς νέα λειτουργία. Το μήνυμα του πρωτοκόλλου της εκτενούς λειτουργίας περιέχει μια ταυτότητα αντικειμένου δεκαδικού string που χρησιμοποιείται για την αναγνώριση της εκτενούς λειτουργίας και ένα αυθαίρετο string των δεδομένων της συγκεκριμένης λειτουργίας.

2.2.4 Το Μοντέλο Ασφάλειας

Η ασφάλεια των πληροφοριών που αποθηκεύονται στον κατάλογο είναι αντικείμενο σημαντικής μελέτης. Μερικοί κατάλογοι προορίστηκαν να προσεγγίζονται δημόσια μέσω του Internet αλλά ο κάθε χρήστης δεν θα πρέπει απαραίτητα να εκτελέσει κάποια λειτουργία. Ο κατάλογος μιας εταιρείας που εξυπηρετεί το δικό της Intranet μπορεί να αποθηκευθεί πίσω από ένα firewall ώστε να κρατά μακριά το ευρύ κοινό από την πρόσβασή του σε αυτόν, όμως απαιτείται περισσότερος έλεγχος ασφάλειας μέσα στο ίδιο το Intranet. Για παράδειγμα, καθένας θα ήταν σε θέση να αναζητήσει το e-mail ενός υπαλλήλου αλλά μόνο ο υπάλληλος ή ο διαχειριστής συστήματος θα μπορούσε να το αλλάξει. Ίσως τα μέλη του τμήματος προσωπικού να έχουν την άδεια να αναζητήσουν τον τηλεφωνικό αριθμό ενός υπαλλήλου αλλά οι συνεργάτες τους να μην έχουν την άδεια αυτή. Μπορεί η πληροφορία να χρειασθεί να κρυπτογραφηθεί πριν διατεθεί σε όλο το δίκτυο. Μια πολιτική ασφάλειας καθορίζει ποιος και τί είδους πρόσβαση έχει και σε ποια πληροφορία. Η πολιτική ασφάλειας είναι καθορισμένη από τον οργανισμό ο οποίος διατηρεί τον κατάλογο. Ένας κατάλογος θα πρέπει να υποστηρίζει τις βασικές προϋποθέσεις που χρειάζονται για να εφαρμοσθεί μια πολιτική ασφάλειας. Ο κατάλογος μπορεί να μην είναι σε θέση να παρέχει άμεσα τις συγκεκριμένες δυνατότητες ασφάλειας, αλλά μπορεί να συνεργασθεί με μια έμπιστη υπηρεσία ασφάλειας δικτύου η οποία θα παρέχει τις βασικές υπηρεσίες ασφάλειας. Πρώτον, χρειάζεται μια μέθοδος επικύρωσης των χρηστών. Η επικύρωση επιβεβαιώνει ότι οι χρήστες είναι πράγματι αυτοί που δηλώνουν ότι είναι. Ένα όνομα χρήστη (user name) και ένας κωδικός (password) αποτελούν ένα βασικό σχέδιο επικύρωσης. Μόλις οι χρήστες

επικυρώνονται πρέπει να διευκρινισθεί αν έχουν την έγκριση ή την άδεια να εκτελέσουν την αιτούμενη ενέργεια πάνω στο συγκεκριμένο αντικείμενο.
Η επικύρωση συχνά βασίζεται στους καταλόγους ελέγχου πρόσβασης (ACLs). Ένα ACL είναι μια λίστα των εγκρίσεων που ίσως συνδέονται με τα αντικείμενα και τις ιδιότητες στον κατάλογο. Ένα ACL απαριθμεί τον τύπο πρόσβασης που επιτρέπεται σε κάθε χρήστη. Προκειμένου να γίνουν οι ACLs μικρότεροι και πιο εύχρηστοι, οι χρήστες που έχουν τα ίδια δικαιώματα πρόσβασης συχνά τοποθετούνται σε ομάδες ασφάλειας.

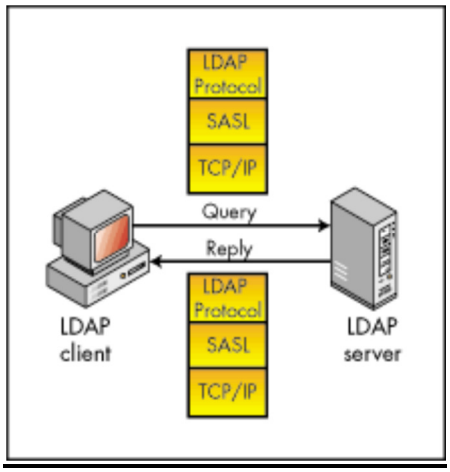
Όπως περιγράφηκε παραπάνω, το μοντέλο ασφάλειας είναι βασισμένο στην λειτουργία **bind**. Υπάρχουν πολλές διαφορετικές λειτουργίες bind και επομένως ο μηχανισμός ασφάλειας που εφαρμόζεται είναι επίσης διαφορετικός. Μια περίπτωση είναι όταν ο client ζητεί πρόσβαση δίνοντας το δικό του αναγνωριστικό DN και έναν κωδικό. Εάν δεν δηλωθούν ο κωδικός και το DN τότε θεωρείται ως ανώνυμη σύνοδος από την πλευρά του LDAP server.



Σχήμα 2.2.4.α' Επικοινωνία client/server χωρίς SASL

Η χρήση των κωδικών αποθαρρύνεται δυναμικά όταν η βαθύτερη υπηρεσία μεταφοράς δεν μπορεί να εγγυηθεί εμπιστευτικότητα και επομένως τα αποτελέσματα των αναζητήσεων κοινοποιούνται σε μη επικυρωμένα μέλη.

Επιπροσθέτως, είναι πιθανή η εντολή bind του Kerberos στην έκδοση 2 του LDAP, αλλά αυτό αποδοκιμάζεται στην έκδοση 3. Αντί για αυτό, το LDAPv3 συνοδεύεται με την εντολή bind του SASL (Simple Authentication and Security Layer) μηχανισμού.



Σχήμα 2.2.4.β' Επικοινωνία client/server με SASL

Αυτό είναι ένα γενικό πλαίσιο επικύρωσης, όπου πολλές μέθοδοι επικύρωσης είναι διαθέσιμες για την επικύρωση του client στον server. Μια από αυτές είναι και το Kerberos.

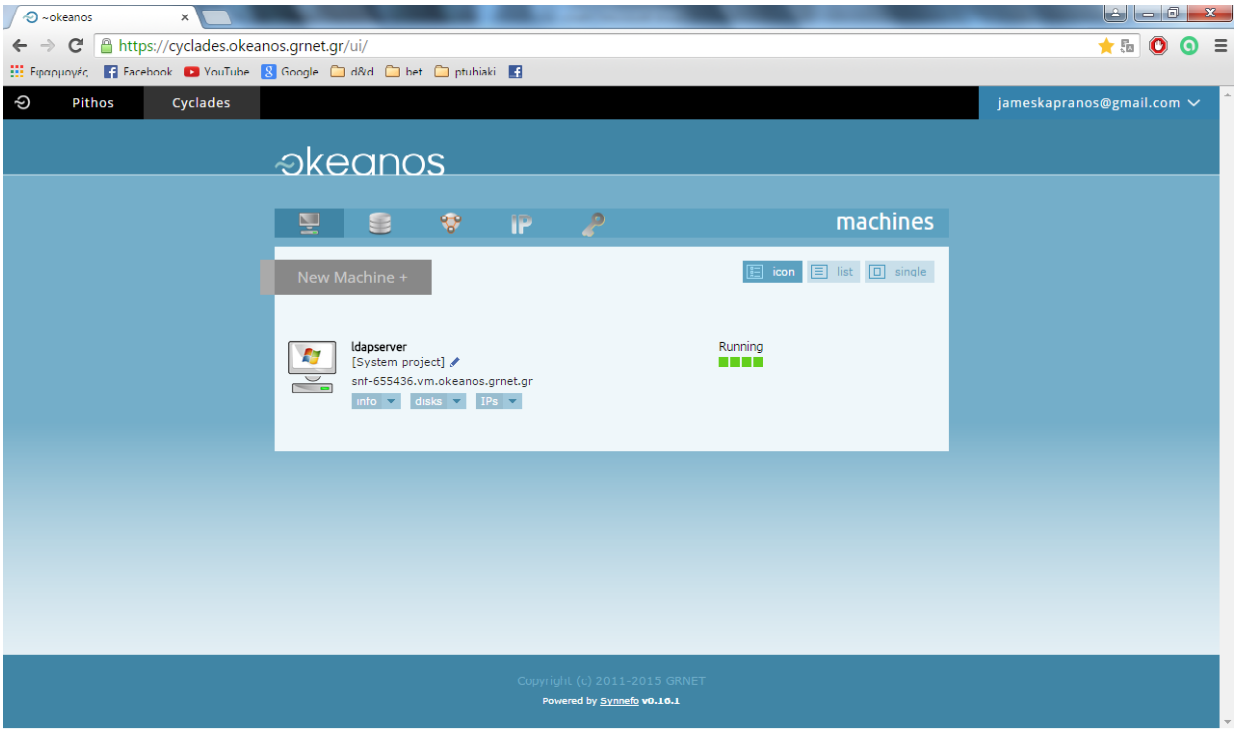
Επιπλέον, οι εκτενείς λειτουργίες πρωτοκόλλου διατίθενται στο LDAPv3. Μια επέκταση σχετική με την ασφάλεια είναι η ''Επέκταση για την Ασφάλεια του Επιπέδου Μεταφοράς'' (TLS) για το LDAPv3. Αυτή καθορίζει λειτουργίες που χρησιμοποιούν την TLS ως μέσο για την κρυπτογράφηση της συνόδου LDAP και προστατεύοντάς την από την παραποίηση δεδομένων. Βασίζεται στο Secure Socket Layer (SSL) Protocol 3.0, το οποίο έχει επινοηθεί από την Netscape Communications Corporation. Η TLS έχει έναν μηχανισμό που της επιτρέπει να επικοινωνεί με έναν SSL server. Μερικοί προμηθευτές όπως ο Netscape και η IBM έχουν ήδη επεκτείνει το πρωτόκολλο LDAP και έχουν προσθέσει κάποιες συγκεκριμένες SSL εντολές έτσι ώστε να είναι δυνατή η κρυπτογράφηση μιας TCP/IP σύνδεσης και κατά συνέπεια παρέχονται μέσα που περιορίζουν την ανάγκη αποστολής απροστάτευτων DN και κωδικών πρόσβασης σε όλο το δίκτυο. Από την στιγμή που ένας client θα αναγνωριστεί, οι πληροφορίες ελέγχου πρόσβασης θα ενημερώσουν για το αν ο client έχει επαρκείς άδειες προσπέλασης για να πραγματοποιήσει αυτό που ζητεί.

ΚΕΦΑΛΑΙΟ 3 (ΕΡΓΑΣΤΗΡΙΑΚΟ ΜΕΡΟΣ)

Στο εργαστηριακό μέρος της πτυχιακής μας εργασίας μας ζητήθηκε να εγκαταστήσουμε έναν LDAP server και μέσω αυτού να πραγματοποιήσουμε μια εξομοίωση του authentication που κάνουν οι φοιτητές στο τμήμα μας ώστε να μπορούν να μπουν στο προσωπικό τους domain με την χρήση ενός username και ενός password (α.μ).

3.1 Τι κάναμε:

Για αρχή φτιάξαμε έναν τοπικό server στον ωκεανό:



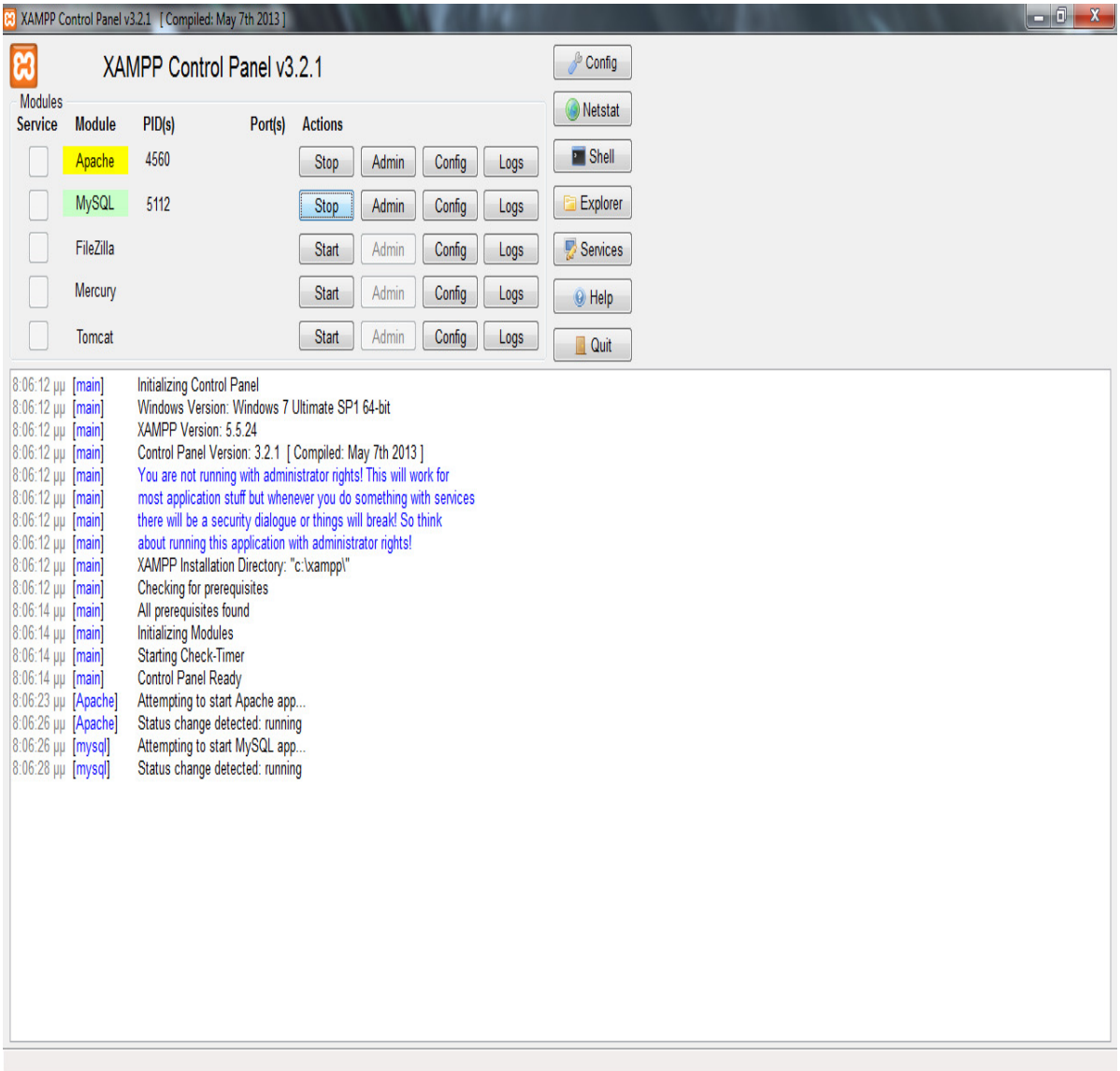
Επίσης χρησιμοποιήσαμε το πρόγραμμα ***XAMPP*** ώστε να μπορουμε να συνδεθούμε με τον σέρβερ και την βάση δεδομένων μας .

3.1.1 XAMPP:

Το XAMPP είναι ένα πακέτο προγραμμάτων ελεύθερου λογισμικού, λογισμικού ανοικτού κώδικα και ανεξαρτήτου πλατφόρμας το οποίο περιέχει το εξυπηρετητή ιστοσελίδων http Apache, την βάση δεδομένων MySQL και ένα διερμηνέα για κώδικα γραμμένο σε γλώσσες προγραμματισμού PHP και Perl.

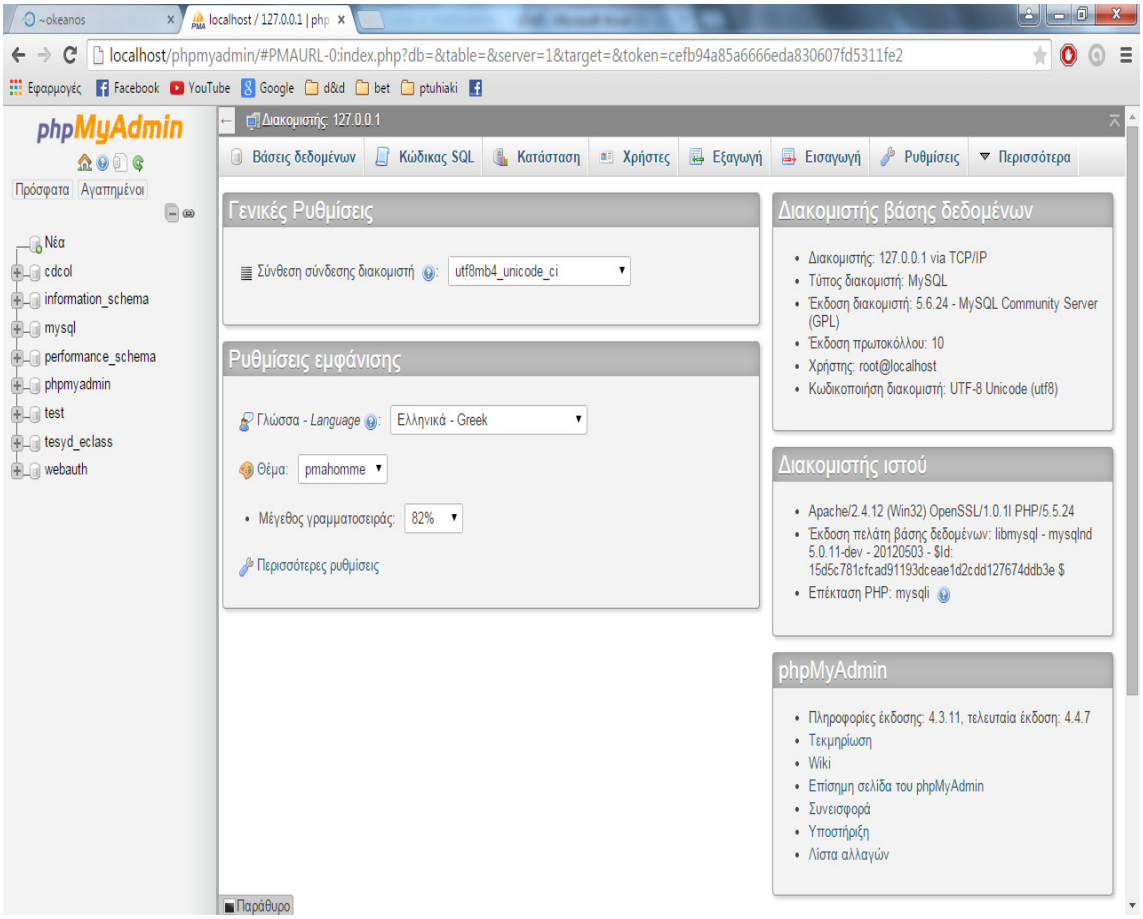
Επίσημα οι σχεδιαστές του XAMPP προόριζαν το λογισμικό ως εργαλείο ανάπτυξης και δοκιμής ιστοσελίδων τοπικά στον υπολογιστή χωρίς να είναι απαραίτητη η σύνδεση στο διαδίκτυο. Για να είναι δυνατή η χρήση του, πολλές σημαντικές λειτουργίες ασφάλειας έχουν απενεργοποιηθεί [3]. Στην πράξη το XAMPP ορισμένες φορές χρησιμοποιείται και για την φιλοξενία ιστοσελίδων. Υπάρχει ειδικό εργαλείο το οποίο περιέχεται στο XAMPP για την προστασία με κωδικό των σημαντικών μερών. Το XAMPP υποστηρίζει την δημιουργία και διαχείριση βάσεων δεδομένων τύπου MySQL και SQLite.

Όταν το XAMPP εγκατασταθεί στον τοπικό υπολογιστή διαχειρίζεται τον localhost ως ένα απομακρυσμένο κόμβο, ο οποίος συνδέεται με το πρωτόκολλο μεταφοράς αρχείων FTP. Η σύνδεση στον localhost μέσω του FTP μπορεί να γίνει με το όνομα χρήστη «newuser» και το κωδικό «wampp». Για την βάση δεδομένων MySQL υπάρχει ο χρήστης «root» χωρίς κωδικό πρόσβασης.

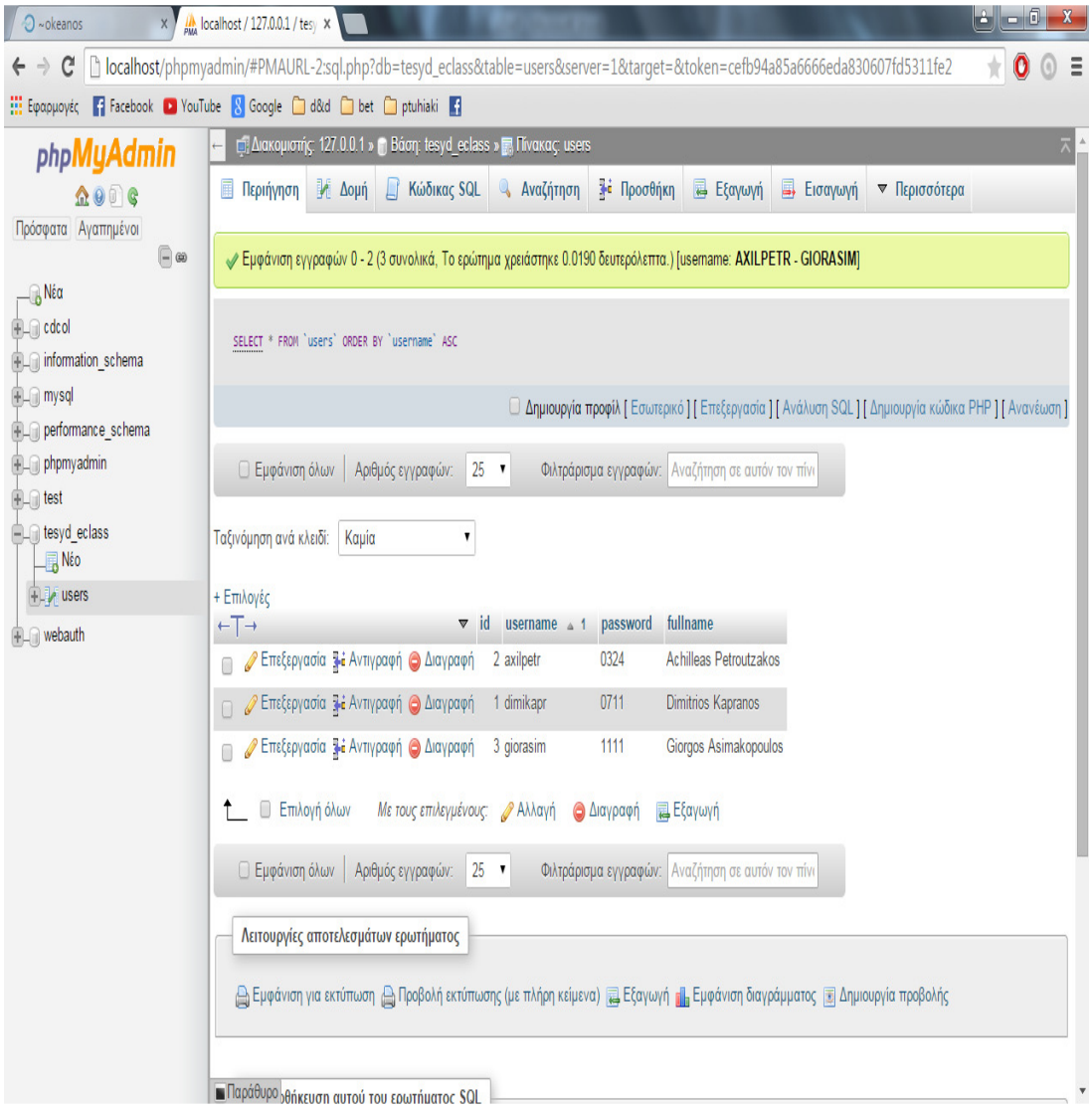

XAMPP Control Panel v3.2.1 [Compiled: May 7th 2013]
XAMPP Control Panel v3.2.1
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
4560
Stop
Admin
Config
Logs
MySQL
5112
Stop
Admin
Config
Logs
FileZilla
Start
Admin
Config
Logs
Mercury
Start
Admin
Config
Logs
Tomcat
Start
Admin
Config
Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
8:06:12 µµ [main] Initializing Control Panel
8:06:12 µµ [main] Windows Version: Windows 7 Ultimate SP1 64-bit
8:06:12 µµ [main] XAMPP Version: 5.5.24
8:06:12 µµ [main] Control Panel Version: 3.2.1 [Compiled: May 7th 2013]
8:06:12 µµ [main] You are not running with administrator rights! This will work for
8:06:12 µµ [main] most application stuff but whenever you do something with services
8:06:12 µµ [main] there will be a security dialogue or things will break! So think
8:06:12 µµ [main] about running this application with administrator rights!
8:06:12 µµ [main] XAMPP Installation Directory: "c:\xampp\"
8:06:12 µµ [main] Checking for prerequisites
8:06:14 µµ [main] All prerequisites found
8:06:14 µµ [main] Initializing Modules
8:06:14 µµ [main] Starting Check-Timer
8:06:14 µµ [main] Control Panel Ready
8:06:23 µµ [Apache] Attempting to start Apache app...
8:06:26 µµ [Apache] Status change detected: running
8:06:26 µµ [mysql] Attempting to start MySQL app...
8:06:28 µµ [mysql] Status change detected: running

3.1.2 phpMyAdmin

Για την βάση δεδομένων του LDAP server μας χρησιμοποιήσαμε το phpMyAdmin. Το phpMyAdmin είναι ένα δωρεάν εργαλείο λογισμικού γραμμένο σε PHP που προορίζεται για να χειριστεί την διαχείριση της MySQL μέσω του World Wide Web. το phpMyAdmin υποστηρίζει ένα ευρύ φάσμα δραστηριοτήτων με την MySQL. Οι πιο συχνά χρησιμοποιούμενες λειτουργίες που υποστηρίζονται από το περιβάλλον εργασίας χρήστη (διαχείριση βάσεων δεδομένων, πίνακες, πεδία, σχέσεις, ευρετήρια, οι χρήστες, άδειες, κλπ), ενώ εξακολουθείτε να έχετε τη δυνατότητα να εκτελέσετε άμεσα οποιαδήποτε δήλωση SQL.

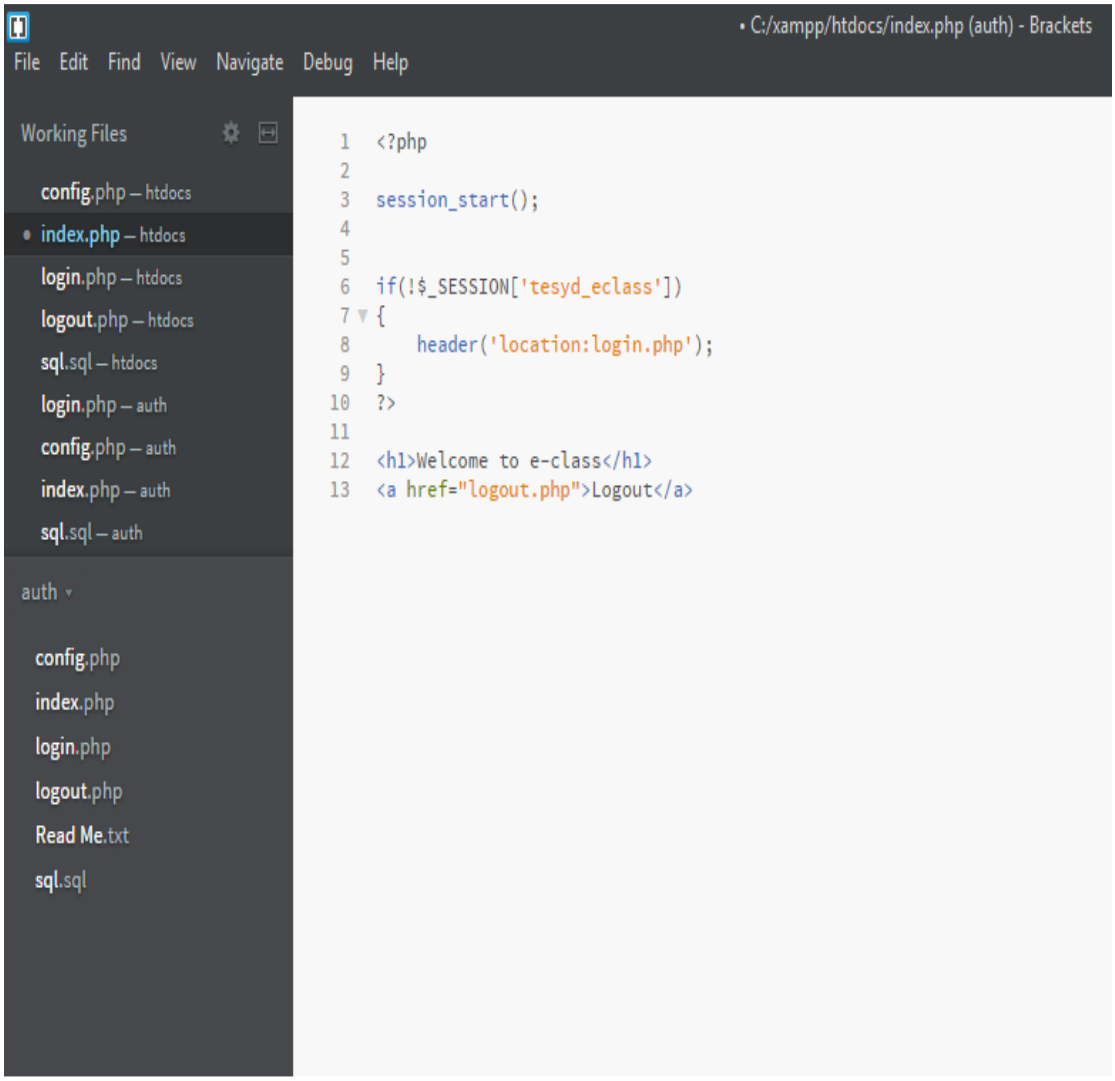


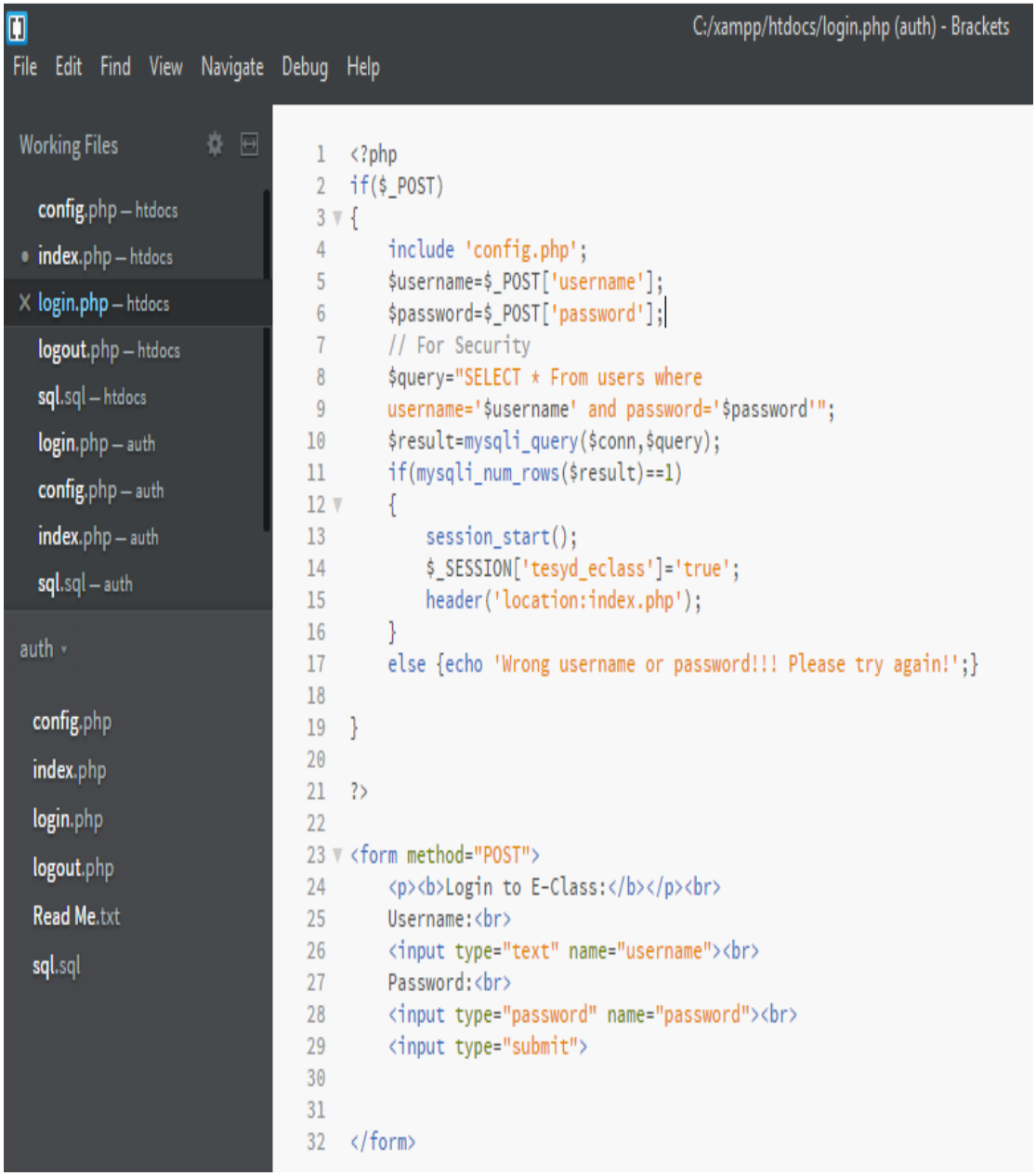
Δημιουργήσαμε την βάση δεδομένων μας μαζί με τις εγγραφές της:

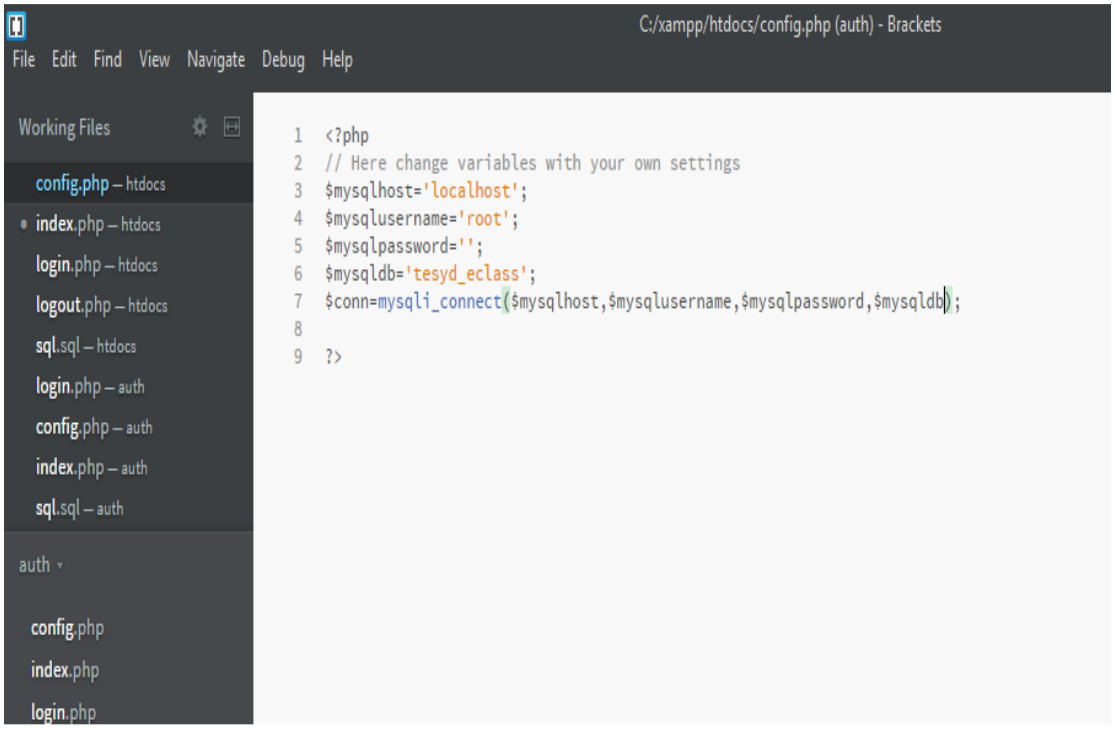


3.1.2 BRACKETS

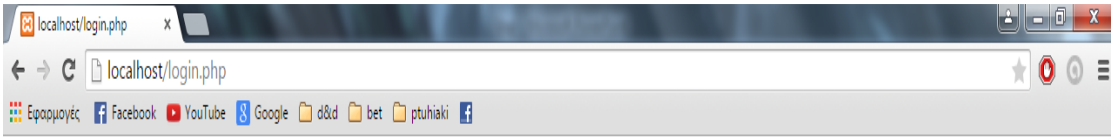
Για να μπορέσουμε να χρησιμοποιήσουμε την βάση μας και να κανουμε το configuration μέσω του LDAP server μας χρησιμοποιήσαμε το BRACKETS. Το Brackets είναι ένας open source text editor που πραγματικά μας έλυσε τα χέρια… Σε αυτόν μπορείς να γράψεις html, sgl, php ενώ ταυτόχρονα να βλέπεις την πρόοδο σου αφού κάνει live preview της εργασίας σου…




C:/xampp/htdocs/login.php (auth) - Brackets
File Edit Find View Navigate Debug Help
Working Files
config.php – htdocs
index.php – htdocs
login.php – htdocs
logout.php – htdocs
sql.sql – htdocs
login.php – auth
config.php – auth
index.php – auth
sql.sql – auth
auth
config.php
index.php
login.php
logout.php
Read Me.txt
sql.sql
1 <?php
2 if($_POST)
3 {
4 include 'config.php';
5 $username=$_POST['username'];
6 $password=$_POST['password'];
7 // For Security
8 $query="SELECT * From users where
9 username='$username' and password='$password'";
10 $result=mysqli_query($conn,$query);
11 if(mysqli_num_rows($result)==1)
12 {
13 session_start();
14 $_SESSION['tesyd_eclass']='true';
15 header('location:index.php');
16 }
17 else {echo 'Wrong username or password!!! Please try again!';}
18
19 }
20
21 ?>
22
23 <form method="POST">
24 Login to E-Class:
25 Username:
26 <input type="text" name="username">
27 Password:
28 <input type="password" name="password">
29 <input type="submit">
30
31
32 </form>


C:/xampp/htdocs/config.php (auth) - Brackets
File Edit Find View Navigate Debug Help
Working Files
config.php – htdocs
index.php – htdocs
login.php – htdocs
logout.php – htdocs
sql.sql – htdocs
login.php – auth
config.php – auth
index.php – auth
sql.sql – auth
auth
config.php
index.php
login.php
1 <?php
2 // Here change variables with your own settings
3 $mysqlhost='localhost';
4 $mysqlusername='root';
5 $mysqlpassword='';
6 $mysqldb='tesyd_eclass';
7 $conn=mysqli_connect($mysqlhost,$mysqlusername,$mysqlpassword,$mysqldb);
8
9 ?>


C:/xampp/htdocs/logout.php (auth) - Brackets
File Edit Find View Navigate Debug Help
Working Files
config.php – htdocs
index.php – htdocs
login.php – htdocs
logout.php – htdocs
sql.sql – htdocs
1 <?php
2 session_start();
3 session_unset();
4 session_destroy();
5 header('location:login.php');
6 ?>



Login to E-Class:

Username:

Password:

Υποβολή

ΕΠΙΛΟΓΟΣ

Το LDAP (Lightweight Directory Access Protocol) είναι ένα προτεινόμενο ανοιχτό πρότυπο για τοπικές ή παγκόσμιες υπηρεσίες καταλόγου που βρίσκονται σε ένα τοπικό δίκτυο ή στο Internet. Με αυτήν την έννοια ένας κατάλογος μοιάζει κατά πολύ με έναν τηλεφωνικό κατάλογο. Το LDAP μπορεί να χειρισθεί πολλών ειδών πληροφορίες αλλά προς το παρόν χρησιμοποιείται για τον συσχετισμό ονομάτων με τηλεφωνικούς αριθμούς και διευθύνσεις ηλεκτρονικού ταχυδρομείου. Οι κατάλογοι είναι σχεδιασμένοι να υποστηρίζουν μεγάλο όγκο ερωτημάτων, αλλά τα δεδομένα που είναι αποθηκευμένα στους καταλόγους δεν αλλάζουν συχνά.

Το LDAP είναι περισσότερο χρήσιμο σε αντίθεση με έναν τηλεφωνικό κατάλογο επειδή ο σχεδιασμός του είναι προορισμένος να υποστηρίζει την μετάδοση διαμέσου των LDAP servers σε όλο το Internet, όπως γίνεται περίπου με το DNS (Domain Name Service). Το σύστημα DNS συμπεριφέρεται σαν το βιβλίο διευθύνσεων του Internet με την παρακολούθηση των domain names και των IP διευθύνσεων. Στο μέλλον, το LDAP θα παρέχει τον ίδιο τύπο πρόσβασης για πολλά είδη πληροφοριών καταλόγου. Προς το παρόν, το LDAP χρησιμοποιείται για μικρούς οργανισμούς π.χ για ένα πανεπιστήμιο ή σε μεγάλες εταιρείες, για λογαριασμό των υπηρεσιών καταλόγου.

Το LDAP είναι ένα σύστημα client-server. Ένας LDAP client συνδέεται με έναν LDAP server και είτε ζητάει πληροφορίες είτε παρέχει πληροφορία που χρειάζεται να ενσωματωθεί στον server. Με την σειρά του ο server απαντάει στο ερώτημα παραπέμποντας το ερώτημα σε άλλον LDAP server, ή δέχεται τις πληροφορίες προς ενσωμάτωση στον κατάλογο.

Μερικές φορές το LDAP αναφέρεται ως X.500 Lite. Το X.500 είναι ένα διεθνές πρότυπο για καταλόγους. Διαθέτει πλήρη χαρακτηριστικά γνωρίσματα, αλλά είναι πολύπλοκο και απαιτεί πολλούς πόρους και ολόκληρη την στοίβα OSI. Από την άλλη μεριά, το LDAP μπορεί να τρέχει σε ένα PC εύκολα και χρησιμοποιεί το TCP/IP. Το LDAP προσπελάζει τους καταλόγους X.500 αλλά δεν υποστηρίζει κάθε δυνατότητα του X.500.

Το κύριο πλεονέκτημα του LDAP είναι η ενοποίηση ορισμένων τύπων πληροφορίας σε έναν οργανισμό. Για παράδειγμα, όλοι οι χρήστες μιας επιχείρησης συγχωνεύονται σε έναν κατάλογο LDAP. Ο κατάλογος αυτός μπορεί να ερωτηθεί από οποιαδήποτε εφαρμογή LDAP που χρειάζεται πληροφορίες καταλόγου.

Άλλα πλεονεκτήματα του LDAP περιλαμβάνουν την ευκολία εφαρμογής του (σε σύγκριση με το X.500) και το –καλά ορισμένο- API (Application Programming Interface), που σημαίνει ότι θα αυξηθεί στο μέλλον ο αριθμός των εφαρμογών που σχετίζονται με το LDAP καθώς και οι LDAP gateways.

Μειονέκτημα είναι το γεγονός ότι η χρήση του LDAP απαιτεί εφαρμογές που υποστηρίζουν το πρωτόκολλο. Επιπλέον το LDAP δεν υποστηρίζει μεγάλο αριθμό εσωτερικών γνωρισμάτων ασφάλειας όπως συμβαίνει με το X.500.

Το LDAP συνήθως χρησιμοποιείται ως ο κεντρικός εξυπηρετητής επικύρωσης έτσι ώστε οι χρήστες να έχουν μια ενοποιημένη σύνδεση που καλύπτει τους POP servers, IMAP servers, τα μηχανήματα που συνδέονται στο δίκτυο χρησιμοποιώντας το Samba και ακόμα τα Windows NT. Όλες αυτές οι καταστάσεις σύνδεσης μπορούν να βασίζονται στον ίδιο κωδικό χρήστη χρησιμοποιώντας το LDAP.

ΠΗΓΕΣ:

ΒΙΒΛΙΑ:

***LDAP System Administration*. by Gerald Carter**

Mastering OpenLDAP
Configuring, Securing and
***Integrating Directory Services*. by Matt Butcher**

Internet:

Wikipaidia
Google
Gracion
Youtube