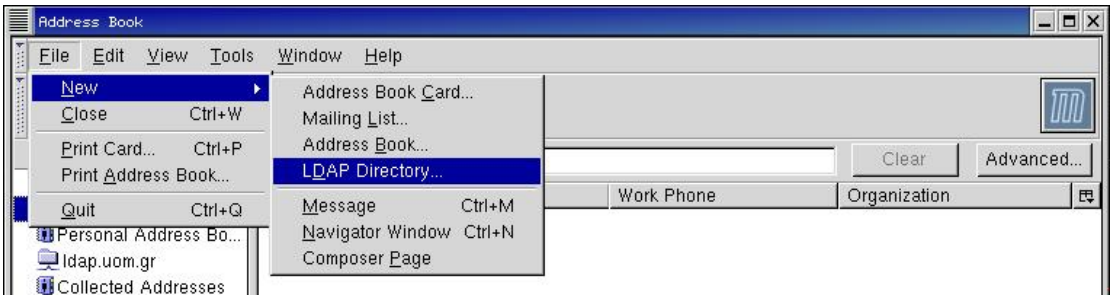
Τ.Ε.Ι. ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ: ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

"ΥΠΗΡΕΣΙΕΣ ΚΑΤΑΛΟΓΟΥ LDAP"



ΕΙΣΗΓΗΤΗΣ :
ΡΙΖΟΣ ΓΕΩΡΓΙΟΣ

ΣΠΟΥΔΑΣΤΗΣ:
ΚΛΑΓΚΟΣ ΣΤΥΛΙΑΝΟΣ

ΑΡΤΑ 2005

ΔΗΛΩΣΗ ΠΕΡΙ ΛΟΓΟΚΛΟΠΗΣ

Όλες οι προτάσεις οι οποίες παρουσιάζονται σ'αυτό το κείμενο και οι οποίες ανήκουν σε άλλους αναγνωρίζονται από τα εισαγωγικά και υπάρχει η σαφής δήλωση του συγγραφέα.Τα υπόλοιπα γραφόμενα είναι επινόηση του γράφοντος ο οποίος φέρει και την καθολική ευθύνη γι'αυτό το κειμενο και δηλώνω υπεύθυνα ότι δεν υπάρχει λογοκλοπή γι'αυτό το κείμεο που παρουσιάζω.

Ονοματεπώνυμο ……

….....

Υπογραφή ……. **Ημερομηνία** ……...

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ 1ο

ΜΕΡΟΣ 2ο

ΜΕΡΟΣ 3ο

ΜΕΡΟΣ 4ο

ΜΕΡΟΣ 5ο

ΜΕΡΟΣ 6ο

ΕΙΣΑΓΩΓΗ – ΕΥΧΑΡΙΣΤΗΡΙΟ

Το δικτυακό περιβάλλον στην σύγχρονη εποχή που ζούμε είναι κάπως πολύπλοκο λόγω της διαρκούς αλλαγής πολλών παραμέτρων(hardware/software) και των νέων τεχνολογιών και ανακαλύψεων πάνω στον τομέα της πληροφορικής,παράλληλα όμως είναι πολύ ενδιαφέρον ακόμα και για χρήστες οι οποίοι δεν έχουν μεγάλη εμπειρία σε διάφορα δίκτυα.

Θα ήθελα να ευχαριστήσω τους καθηγητές:

ΡΙΖΟ ΓΕΩΡΓΙΟ (Διαχείριση Δικτύων)

ΤΣΙΑΝΤΗ ΛΕΩΝΙΔΑ (Διαχείρηση Δικτύων)

ΒΑΣΙΛΕΙΑΔΗ (Προηγμένες Υπηρεσίες Διαδικτύου)

Γιατί χωρίς τη συμβολή τους τίποτα απ'όσα παραθέτω δεν θα είχαν γίνει.Κάποια στοιχεία ίσως να έχουν αλλάξει λόγω των συνεχών αλλαγών στον τομέα της πληροφορικής.

ΜΕΡΟΣ 1ο

ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

Σε ένα πραγματικό περιβάλλον ενός ιδρύματος ή μιας επιχείρησης, είναι συνηθισμένη η ύπαρξη πολλών βάσεων δεδομένων, οι οποίες εξυπηρετούν πολλές φορές κοινές ανάγκες πολλών Καταλόγων. Το πρόβλημα που δημιουργήθηκε με την ύπαρξη πολλών Καταλόγων, ήταν ότι αυτοί οι διαφορετικοί Κατάλογοι δεν μπορούσαν να μοιραστούν άμεσα δεδομένα μεταξύ τους, με αποτέλεσμα μια αναπόφευκτη επιβάρυνση σε hardware και ωρών συντήρησης.

Το πρόβλημα αυτό λύθηκε με την ιδέα μιας κεντρικής Υπηρεσίας Καταλόγου που θα είναι υπεύθυνη για την αποθήκευση της πληροφορίας, η οποία θα αποθηκεύεται μόνο μια φορά ενώ θα μπορούν να την προσπελάσουν όλες οι εφαρμογές που την χρειάζονται.

1.1 Η ΥΠΗΡΕΣΙΑ ΚΑΤΑΛΟΓΟΥ

Ο όρος *Υπηρεσίες Καταλόγου* (*Directory Services*) αναφέρεται στο λογισμικό το οποίο χρησιμοποιείται για την αποθήκευση και την πρόσβαση στις πληροφορίες ενός *Καταλόγου* (*Directory*). Ο Κατάλογος είναι μια βάση δεδομένων η οποία είναι με τέτοιον τρόπο δομημένη ώστε να είναι εύκολη η ανάκτηση, ανάγνωση και αναζήτηση ανάμεσα σε μεγάλο όγκο πληροφοριών που αφορούν ένα ίδρυμα, μια οργάνωση ή μια επιχείρηση. Η κύρια λειτουργία μιας Υπηρεσίας Καταλόγου είναι η αποθήκευση μιας πληροφορίας, έτσι ώστε αυτή να μπορεί να ανακτηθεί είτε με απ' ευθείας αναζήτηση βάσει ενός μοναδικού χαρακτηριστικού, όπως το *user id* ενός χρήστη, είτε με αναζήτηση ανάμεσα σε άλλα σχετικά χαρακτηριστικά, όπως το *πλήρες όνομα* ενός χρήστη.

Οι πληροφορίες που αποθηκεύονται σε έναν Κατάλογο μπορεί να αφορούν:

- Πληροφορίες σχετικά με ένα άτομο, όπως για παράδειγμα πλήρες όνομα, ταχυδρομική διεύθυνση, τηλέφωνο επικοινωνίας, ηλεκτρονική διεύθυνση, αλλά και πιο λεπτομερείς πληροφορίες όπως προϋπηρεσία, αριθμός κοινωνικής ασφάλισης, αριθμός δελτίου ταυτότητας, οικογενειακή κατάσταση κτλ.
- Πληροφορίες σχετικά με ένα ίδρυμα ή μια επιχείρηση, όπως για παράδειγμα περιγραφή αντικειμένου, ταχυδρομική διεύθυνση, ονοματεπώνυμο διευθυντή κτλ.
- Πληροφορίες σχετικά με τις οργανικές μονάδες και τα τμήματα ενός ιδρύματος, μιας οργάνωσης ή μιας επιχείρησης, όπως για παράδειγμα Τμήμα Λογιστηρίου, Τμήμα Μισθοδοσίας κτλ., ή ακαδημαϊκά Τμήματα για ένα Πανεπιστήμιο.
- Πληροφορίες σχετικά με τις φυσικές συσκευές μιας επιχείρησης ή ενός ιδρύματος, όπως για παράδειγμα μάρκα εκτυπωτή, μοντέλο και γραφείο στο οποίο βρίσκεται.
- Πληροφορίες σχετικά με τους διάφορους πόρους του δικτύου μιας επιχείρησης ή ενός ιδρύματος, για παράδειγμα όνομα, τοποθεσία και τρόπος λήψης ενός αρχείου.

Στην πιο συνηθισμένη μορφή τους, οι Υπηρεσίες Καταλόγου στηρίζονται στην αρχιτεκτονική *πελάτη-εξυπηρετητή* (*client/server*). Αυτό σημαίνει ότι μια Υπηρεσία Καταλόγου αποτελείται από τουλάχιστον έναν *Εξυπηρετητή Καταλόγου* (*Directory Server*) και από έναν ή περισσότερους *Πελάτες Καταλόγου* (*Directory Clients*).

Σε ένα δίκτυο, ο Κατάλογος δίνει την πληροφορία για την την θέση που βρίσκονται τα συστατικά του δικτύου. Σε δίκτυα TCP/IP (συμπεριλαμβανόμενου και του Internet), μια πολύ γνωστή client/server Υπηρεσία Καταλόγου είναι ο *DNS* (*Domain Name System*) *Server*. Το DNS συσχετίζει ονομάτα μηχανών με IP διευθύνσεις δικτύου, επιτρέποντας με αυτόν τον τρόπο στους χρήστες να βρίσκουν εύκολα τους πόρους του δικτύου χωρίς να χρειάζεται να θυμούνται τις IP διευθύνσεις τους.

1.2 X.500 ΚΑΙ LDAP

Το πρότυπο *X.500* σχεδιάστηκε από τον οργανισμό *ISO* (*International Standards Organisation*) ήταν αυτό που αρχικά προτάθηκε και χρησιμοποιήθηκε για την καθιέρωση μιας παγκόσμιας ονοματολογίας Καταλόγων. Προσέφερε ένα ανοιχτό πρωτόκολλο επικοινωνίας, το *Directory Access Protocol* (*DAP*) το οποίο μπορούσε να χρησιμοποιηθεί από οποιαδήποτε εφαρμογή για την πρόσβαση στον Κατάλογο. Το X.500 είχε αρκετά πλεονεκτήματα, όπως για παράδειγμα υποστήριζε την αποθήκευση ενός σχήματος στον Κατάλογο το οποίο ήταν επεκτάσιμο ανάλογα με τις ανάγκες, και στο οποίο μπορούσε να αποθηκευτεί οποιαδήποτε μορφή πληροφορίας. Το κύριο μειονέκτημά του όμως, ήταν ότι προσέφερε ένα επικοινωνιακό πρωτόκολλο το οποίο δεν βασιζόταν στο πρωτόκολλο TCP/IP, ενώ επιπλέον παρουσιάζε σημαντική πολυπλοκότητα στη διαχείριση της ονοματολογίας των Καταλόγου.

Το πρωτόκολλο *LDAP* (*Lightweight Directory Access Protocol*) που εμφανίστηκε και καθιερώθηκε στη συνέχεια, διατήρησε τα θετικά στοιχεία του X.500, ενώ ταυτόχρονα παρείχε ένα επικοινωνιακό πρωτόκολλο βασισμένο στο TCP/IP. Προτάθηκε αρχικά το 1996 από την Netscape Communications Corp., το Πανεπιστήμιο του Michigan και περισσότερες από 40 εταιρίες, ως ένα ανοιχτό πρότυπο για τις Υπηρεσίες Καταλόγου στο Internet. Ο όρος *Lightweight* στην ονομασία του, σημαίνει ότι συγκρινόμενο με το DAP περιέχει λιγότερο κώδικα και πιο απλές συναρτήσεις, και συνεπώς είναι για τους κατασκευαστές πιο εύκολα υλοποιήσιμο και μικρότερο σε κόστος.

1.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΚΑΤΑΛΟΓΟΥ

Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά της Υπηρεσίας Καταλόγου:

Global Directory Service

Ένας Κατάλογος επιτρέπει στους χρήστες την πρόσβαση σε ορισμένα δεδομένα τα οποία είναι μοναδικά σε παγκόσμιο επίπεδο. Αυτό σημαίνει ότι οι οντότητες που καταχωρούνται σε έναν κατάλογο είναι μοναδικές με την έννοια ότι δύο οντότητες Καταλόγου οπουδήποτε στον κόσμο έχουν διαφορετικό αναγνωριστικό.

Διασύνδεση ανοιχτού προτύπου (Open Standard Interconnectivity)

Το πρότυπο LDAP είναι ένα ανοιχτό πρότυπο και μπορεί να υιοθετηθεί ελεύθερα από οποιονδήποτε κατασκευαστή λογισμικού Υπηρεσιών Καταλόγου. Επιπλέον, το γεγονός ότι βασίζεται στο TCP/IP προσθέτει το πλεονέκτημα της εύκολης διασύνδεσης μηχανημάτων, ενώ τα μηχανήματα του εξυπηρετητή και του πελάτη είναι ανεξάρτητα κατασκευαστή, αφού η ζήτηση και η αποστολή των δεδομένων γίνεται μέσω του πρωτοκόλλου LDAP.

Προσαρμοστικότητα και Επεκτασιμότητα

Κάθε εφαρμογή μπορεί να έχει το δικό της GUI περιβάλλον, ανάλογα με τις προτιμήσεις και τις απαιτήσεις της επιχείρησης ή του Ιδρύματος. Οι χρήστες βέβαια αγνοούν τους μηχανισμούς των ερωτημάτων και της ανάκτησης των πληροφοριών. Επιπλέον, η υπηρεσία είναι αρκετά ευέλικτη ώστε να υποστηρίζει διαφορετικές σενάρια μιας εφαρμογής αλλά ακόμη και διαφορετικές τοπικές ρυθμίσεις. Οι εφαρμογές της Υπηρεσίας Καταλόγου που βασίζονται στο πρωτόκολλο LDAP έκδοσης 3 (LDAPv3)

μπορούν να υποστηρίξουν πολλές γλώσσες χρησιμοποιώντας το Unicode UTF-8 character set για τις τιμές των χαρακτηριστικών (attributes) αλλά και των αναγνωριστικών (identifiers).

Αποθήκευση ετερογενών δεδομένων

Ο εξυπηρετητής LDAP δεν βασίζεται σε κάποια συγκεκριμένη βάση δεδομένων. Χρησιμοποιεί περισσότερες από μία, κατά τον χρήστη back-end βάση δεδομένων για την αποθήκευση και την ανάκτηση των δεδομένων. Συνεπώς, κάποιος εξυπηρετητής LDAP μπορεί να χρησιμοποιεί μια γνωστή εμπορική βάση δεδομένων, αλλά μπορεί να χρησιμοποιεί και ένα flat αρχείο αποθήκευσης δεδομένων.

Ασφάλεια και έλεγχος πρόσβασης

Το πρωτόκολλο LDAP είναι ένα ασφαλές πρωτόκολλο, το οποίο χρησιμοποιεί τον έλεγχο ταυτότητας για να διασφαλίσει ότι η μεταφορά των δεδομένων είναι ασφαλής. Ο έλεγχος αυτός χρησιμοποιείται από τον εξυπηρετητή ο οποίος ελέγχει την ταυτότητα του πελάτη. Στη έκδοση LDAP 2, αυτό επιτυγχανόταν με την αποστολή ενός αναγνωριστικού χρήστη και ενός κωδικού πρόσβασης, κάτι το οποίο δεν ήταν όμως τόσο ασφαλές. Η τρέχουσα έκδοση v3 του LDAP χρησιμοποιεί το SASL (Simple Authentication and Security Layer -SASL), χαρακτηριστικό το οποίο παρέχει μια ευελιξία στην επιλογή του μηχανισμού ελέγχου ταυτότητας. Το πρωτόκολλο Secure Socket Layer (SSL) protocol, είναι το πιο δημοφιλές για το σκοπό αυτό παρέχοντας ένα υψηλό επίπεδο ασφάλειας. Επιπλέον, το LDAP διαθέτει ένα πλήθος χαρακτηριστικών ελέγχου πρόσβασης, τα οποίο χρησιμοποιούνται για τον έλεγχο στις πληροφορίες του καταλόγου, για παράδειγμα ποιος μπορεί να ανακτήσει συγκεκριμένα δεδομένα.

1.4 ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΚΑΤΑΛΟΓΟΥ

Καταχώρηση (Entry)

Μπορεί να παρομοιαστεί με την γραμμή (row) σε μια βάση δεδομένων. Κάθε καταχώρηση μπορεί να περιέχει διάφορες πληροφορίες που αφορούν ένα μοναδικό άτομο, μια μοναδική συσκευή κτλ.

Χαρακτηριστικό (Attribute)

Μπορεί να παρομοιαστεί με το πεδίο (field) σε μια βάση δεδομένων. Σε μια καταχώρηση που αφορά ένα άτομο, πεδία μπορεί να είναι τα: *user id, full name, postal address* κτλ.

Ανιτικείμενο (Object)

Μπορεί να παρομοιαστεί με τον πίνακα σε μια βάση δεδομένων. Αντικείμενα μπορεί να είναι τα *person, device, department* κτλ. Τα χαρακτηριστικά των αντικειμένων μπορούν να επεκταθούν ή να αλλάξουν σε αντίθεση με τις σχεσιακές βάσεις δεδομένων.

Distinguished Name (DN)

Είναι το όνομα το οποίο καθορίζει μοναδικά αλλά και παγκόσμια μια καταχώρηση σε έναν κατάλογο. Για παράδειγμα, ένα DN μπορεί να είναι το εξής:

uid=bjensen, ou=people, o=airius.com

Το παραπάνω DN αντιστοιχεί στην καταχώρηση *bjensen του* υποκαταλόγου *people* του καταλόγου *airius.com*.Η αριστερότερη τιμή ενός DN ονομάζεται Relative Distinguished Name (RDN).

Directory Information Tree (DIT)

Όλες οι πληροφορίες ενός καταλόγου μπορούν να παρομοιαστούν με ένα δένδρο. Αυτό το δένδρο ονομάζεται Directory Information Tree (DIT).

Σχήμα (Schema)

Το σχήμα ενός Καταλόγου δίνει μια εικόνα των πληροφοριών που περιέχει και του τρόπου με τον οποίο αυτές είναι οργανωμένες. Συνεπώς επιτρέπει στους χρήστες να κατανοήσουν τη διάταξη των πληροφοριών πριν αυτοί αποφασίσουν τον τρόπο με τον οποίο θα προσπελάσουν την πληροφορία που τους ενδιαφέρει.

1.5 ΠΡΟΪΟΝΤΑ ΕΞΥΠΗΡΕΤΗΤΩΝ ΚΑΤΑΛΟΓΟΥ (DIRECTORY SERVERS)

OpenLDAP

Ο OpenLDAP αποτελεί ένα προϊόν μιας συλλογικής προσπάθειας η οποία είχε ως στόχο τη δημιουργία ενός πλήρως λειτουργικού προϊόντος λογισμικού Υπηρεσίας Καταλόγου. Το έργο αυτό διαχειρίζεται από μια παγκόσμια κοινότητα εθελοντών που επικοινωνούν μεταξύ τους με σκοπό την υλοποίηση του λογισμικού και του συνοδευτικού υλικού. Το λογισμικό του OpenLDAP περιλαμβάνει μια πλήρης υλοποίηση του LDAP, όπως server, clients, C SDK, και συμπληρωματικά εργαλεία.

Η τελευταία έκδοση, ο OpenLDAP 2.1 η οποία διατίθεται από τον Ιούνιο του 2002, υποστηρίζει τις περισσότερες πλατφόρμες Unix (ή UNIX-like) όπως: Darwin, FreeBSD, Linux, NetBSD, OpenBSD καθώς και τα περισσότερα εμπορικά UNIX συστήματα. Επίσης, η έκδοση δοκιμάζεται σε άλλες πλατφόρμες όπως Apple MacOS X, IBM zOS, και Microsoft Windows 2000.

Ο Πίνακας 1 περιλαμβάνει μερικά από τα χαρακτηριστικά και τις βελτιώσεις της νέας έκδοσης OpenLDAP 2.1:

- Transaction oriented database backend
- Improved Unicode/DN Handling
- SASL authentication/authorization mapping
- SASL in-directory storage of authentication secrets
- Enhanced administrative limits / access controls
- Enhanced system schema checking
- LDAPv3 extensions:
  - Enhanced Language Tag/Range option support
  - objectClass-based attribute lists
  - LDAP Who ami I? Extended Operation
  - LDAP no-op Control
  - Matched Values Control
  - Misc LDAP Feature Extensions

· LDAP C++ API · Updated LDAP C & TCL APIs · Meta Backend · Monitor Backend · Virtual Context "glue" Backend

Πίνακας 1 – Χαρακτηριστικά και βελτιώσεις του OpenLDAP 2.1

Sun ONE Directory Server

Ο Sun ONE Directory Server αποτελεί μέρος του Sun Open Net Environment (Sun ONE), μια πλατφόρμα που βασίζεται σε ανοιχτά πρότυπα όπως Java και τεχνολογία XML, η οποία παρέχει ένα σημαντικά ευέλικτο περιβάλλον για τη δημιουργία και ανάπτυξη ενός πλήθους υπηρεσιών κατ' απαίτηση (services on demand).

Η τελευταία έκδοση είναι η Sun ONE Directory Server 5.1, και υποστηρίζει τις παρακάτω πλατφόρμες:

- Sun Solaris 9 και 8 Operating Environments (SPARC Platform Edition)
- Sun Linux 5.0
- Red Hat Linux 7.2
- Hewlett Packard HP-UX 11.0/11i (PA-RISC 1.1 or 2.0)
- IBM AIX 4.3.3 (PowerPC)
- Microsoft Windows NT Server 4.0 SP6a (Intel Architecture)
- Microsoft Windows 2000 Server and Advanced Server SP2 (Intel Architecture)

Ο Πίνακας 2 περιλαμβάνει τα κυριότερα χαρακτηριστικά του Sun ONE Directory Server 5.1:

Scalability and Performance	§ The multiple database architecture supports distributed naming contexts, providing:
	  § Virtually unlimited scalability to support millions of users on a single system
	  § Improved backup/restore characteristics
	  § Load balancing across multiple servers
	§ The macro Access Control Instruction for composite access control lists provides improved efficiency in the access control mechanism

Enhanced Administration	§ Automatic replication of access control rules and schema information § Editable schema through LDAP or a configuration file § Support for nested roles for users in the directory § Account inactivation - an administrator can inactivate a user account or a domain of accounts

	§ Server-to-server LDAP chaining - provides a method for LDAP servers to forward requests on behalf of clients § Replication from iPlanet Directory Server 4.x supplier to Sun ONE Directory Server 5.x for data migration
Advanced Security	§ Restricts access to directory data down to the attribute level § Controls users ability to perform read, write, search, or compare operations § Offers access control based on either user identity, IP address, or domain name § Supports anonymous access § Provides authenticated and encrypted LDAP operations using SSL encryption § Delivers authenticated and encrypted replication using SSL § Supports PKCS#11 for hardware accelerated SSL § Supports password policy management to control minimum and maximum password lengths and password histories § Enables user authentication through user ID/password, X.509 v3 public-key certificates, or administrator-defined method § Supports DIGEST-MD5 authentication
Superior Reliability and Availability	§ Two-way multimaster for high availability update eliminates single point of write failure § Unlimited number of read-only consumers for high availability searching § Hub suppliers for cascading replication § Compatibility with iPlanet Directory Server 4.x supplier-consumer replication mechanism § Transaction logging enables failure recovery § Support for the Simple Network Management Protocol provides flexible network management and monitoring § Online backups, configuration changes, schema updates, and indexing
Support of Industry Standards	§ LDAP version 2 and version 3 operations § X.509 digital certificates § LDAP search filters, including presence, equality, inequality, substring, approximate ("sounds like"), and the Boolean operators and (&), or (|), and not (!) § LDAP version 3 intelligent referral, which lets a directory refer a query to another directory § Implements relevant LDAP version 2 and 3 RFCs, including RFC 1274, 1558, 1777, 1778, 1959, 2195, 2222, 2247, 2251, 2252, 2253, 2254, 2255, 2256, 2279, 2307, 2377

Πίνακας 2 – Χαρακτηριστικά του Sun ONE Directory Server 5.1

Σε όλες τις πλατφόρμες, για την εγκατάσταση του *Sun ONE Directory Server 5.1* είναι απαραίτητα τα εξής:

- 2 GB χώρος στον σκληρό δίσκο για την ελάχιστη εγκατάσταση. Για συστήματα παραγωγής, χρειάζονται τουλάχιστον 2GB για την υποστήριξη των product binaries, των βάσεων δεδομένων και των log files (τα log files απαιτούν εξ' ορισμού 1 GB). Για πολύ μεγάλους καταλόγους, μπορεί να χρειάζονται 4GB ή περισσότερα.
- 256 MB μνήμης RAM. Για καλύτερη απόδοση στα μεγάλα συστήματα παραγωγής, θα πρέπει να υπάρχουν από 256 MB έως 1 GB RAM.

Επίσης, ο Πίνακας 2 περιλαμβάνει ενδεικτικές απαιτήσεις σε χώρο στο δίσκο και στο μέγεθος της μνήμης RAM, για διάφορες κατηγορίες πλήθους καταχωρήσεων. Οι καταχωρήσεις στο LDIF αρχείο υπολογίζεται ότι είναι μεγέθους περίπου 100 Bytes, ενώ για μεγαλύτερες καταχωρήσεις τα παρακάτω μεγέθη θα πρέπει να τετραπλασιαστούν.

10,000 - 250,000 καταχωρήσεις	Χώρος στο δίσκο: 2 GB	Μέγεθος μνήμης: 256 MB
250,000 - 1,000,000 καταχωρήσεις	Χώρος στο δίσκο: 4 GB	Μέγεθος μνήμης: 512 MB
> 1,000,000 entries	Χώρος στο δίσκο: 8GB	Μέγεθος μνήμης: 1 GB

iPlanet Directory Server -
(Πρόκειται για τις προγενέστερες εκδόσεις του Sun ONE Directory Server)

Novell eDirectory

Το προϊόν Novell eDirectory 8.7 είναι το λογισμικό τις Novell για την ανάπτυξη της Υπηρεσίας Καταλόγου. Υποστηρίζει το πρωτόκολλο LDAP καθώς και πολλά άλλα πρότυπα του Internet, ενώ διαθέτει εκδόσεις για τα περισσότερα λειτουργικά συστήματα. Συγκεκριμένα, υποστηρίζει τις εξής πλατφόρμες:

- IBM AIX
- Linux 8.0
- Microsoft Windows NT 4.0
- Microsoft Windows 2000 Server and Advanced Server
- Novell NetWare 5.x and 6
- Sun Solaris

Ο πίνακας 3 περιλαμβάνει τα σημαντικότερα χαρακτηριστικά της τρέχουσας έκδοσης eDirectory 8.7.

interoperability and compatibility	eDirectory is compatible with hundreds of directories, databases and applications available today.

secure identity-management solution	With such a solution you can deliver or revoke a user's access to resources with a single change to one data source. This real-time control over your resources simultaneously improves user productivity and increases network security, both of which save you money.
easier management	With Novell iManager, an included utility that supports secure directory administration through a Web browser and many wireless devices. eDirectory also incorporates SNMP management support and event publishing via LDAP to facilitate directory management and monitoring.
support for dynamic group functionality persistent searches and live continuous backup	Administrative overhead is significantly reduced. In addition, enhancements to LDAP performance and partition-replication functions improve your network's scalability and speed in an Internet environment.
eDirectory features role-based administration	This feature ensures that users can only access those resources permitted by their roles and relationships with your organization. eDirectory also includes Novell Modular Authentication Services (NMAS) Standard Edition to provide support for advanced password and certificate login methods. Other superior security features include Novell International Cryptographic Infrastructure, passwords encrypted over Secure Sockets Layer (SSL), RSA private key/public key encryption, Secure Authentication Services, smart cards and X.509v3 certificates.

Πίνακας 3 – Χαρακτηριστικά του Novell eDirectory 8.7

Ο Πίνακας 4 περιλαμβάνει τις απαιτήσεις συστήματος του Novell eDirectory 8.7 για τις διάφορες πλατφόρμες που υποστηρίζει.

NetWare	· NetWare 6 with Support Pack 2 or later · NetWare 5.1 with Support Pack 5 or later and JVM 1.3.1 IMPORTANT: Novell eDirectory 8.7 does not support NetWare 5.0 To use RCONSOLE, you need a ConsoleOne® administrator workstation that meets the following requirements: · A 200 MHZ or faster processor · A minimum of 64 MB RAM (128 MB recommended) · Novell Client™ software that shipped with NetWare 5.1 SP5 or later
Windows NT/2000	· Windows NT Server 4.0 with Service Pack 6 or later, or Windows 2000 Server with Service Pack 2 or later IMPORTANT: Windows XP is not a supported Novell eDirectory 8.7 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 3.0 or later —Novell Client for Windows NT 4.5 or later · Administrative rights to the Windows 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 Tree object so that you can extend the schema and create objects.
Linux	· Redhat* Linux 7.2 or 7.3 NOTE: Ensure that the latest glibc patches are applied from Redhat Errata on Redhat 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 ConsoleOne requirements for Linux: · ConsoleOne® 1.3.4 · 64 MB RAM minimum (128 MB recommended) · 200 MHz or faster processor (a faster one is recommended)
Solaris	· All recommended Solaris OS patches: available at the SunSolve* Web page. · Solaris 7 on Sun SPARC (with patch 106327-13 or later for 32-bit systems) · Solaris 7 on Sun SPARC (with patch 106300-07 or later for 64-bit systems) · Solaris 8 on Sun SPARC (with patch 108827-20 or later) · 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 ConsoleOne requirements for Solaris: · ConsoleOne 1.3.4

	· 64 MB RAM minimum (128 MB recommended)
AIX	· AIX 4.3.3 with Maintenance Level 10, JVM 1.3.1, and the latest AIX V5.0 Runtime Libraries · AIX 5L with Maintenance Level 2, JVM 1.3.1, and the latest AIX V6.0 Runtime Libraries · All recommended AIX OS patches, which are available at the IBM Tech Support Web site · A minimum of 128 MB RAM · 190 MB of disk space for the eDirectory server · 12 MB of disk space for the eDirectory administration utilities · 74 MB of disk space for every 50,000 users NOTE: ConsoleOne is not supported on AIX. You can use other platforms, such as Windows, for ConsoleOne

Πίνακας 4– Πλατφόρμες / Απαιτήσεις Novell eDirectory

IBM Directory Server

Ο IBM Directory Server αποτελεί τη λύση της IBM στα προϊόντα λογισμικού Υπηρεσιών Καταλόγου. Η τελευταία έκδοση του προϊόντος, ο IBM Directory Server 5.1, είναι χτισμένη στην τεχνολογία DB2 της IBM και χρησιμοποιεί το πρότυπο LDAP, προσφέροντας μια αξιόπιστη και ευέλικτη πλατφόρμα η οποία είναι συμβατή με αρκετά λειτουργικά συστήματα και εφαρμογές. Η έκδοση 5.1 προσφέρει περισσότερα χαρακτηριστικά ασφάλειας και δυνατότητες replication καθώς και περισσότερη ευκολία στη διαχείριση.

Ο Πίνακας 5 περιλαμβάνει τις υποστηριζόμενες πλατφόρμες και τις απαιτήσεις του IBM Directory Server 5.1.

AIX	Version 4.3.3 (with Maintenance Level 8 or higher), 5.1 (with Maintenance Level 1 or higher) or 5.2; IBM DB2 Universal Database v7.2 with FixPak 5 or higher or V8.1. The Korn Shell is required. Web Administration Tool: embedded version of WebSphere Application Server - Express, V5.0; Netscape V7.0	A minimum of 256 MB RAM (512 MB or more is strongly recommended).
HP-UX	HP-UX 11i (with December 2001 GOLDBASE11i bundle, December 2001 GOLDAPPS11i bundle, and patch PHSS_26560). IBM DB2 Universal Database v7.2 with FixPak 5 or higher or V8.1. The Korn shell is required. Web Administration Tool: Apache	A minimum of 256 MB RAM (512 MB or more is strongly recommended).

	Tomcat 4.0.3, plus one of the following versions of Java. IBM v 1.3.1, Service release 2 or higher, but not v1.4; Sun version 1.3.1_4; or HP-UX v1.3.1.06; Netscape v6.2.3, v7.0 or Microsoft Internet Explorer v5.0	
Linux	Linux Operating System for Intel based systems: Red Hat Version 7.2 or 7.3, Red Hat Linux Advanced Server v2.1, UnitedLinux, or SuSE Version 7.2, 7.3, or 8.0. IBM DB2 Universal Database v7.2 with FixPak 5 or higher or V8.1. The Korn shell is required. Linux for eServer zSeries systems: Linux Operating System from Red Hat Version 7.1, SuSE Version 7.0, Turbolinux 6.5, or UnitedLinux. IBM DB2 Universal Database v7.2 with FixPak 5 or higher or V8.1. The Korn shell is required. Web Administration Tool: embedded version of WebSphere Application Server - Express, V5.0; Netscape v6.2.3, v7.0	A minimum of 256 MB RAM (512 MB or more is strongly recommended).
Solaris	Solaris Operating Environment Software versions 7, 8, or 9. IBM DB2 Universal Database v7.2 with FixPak 5 or higher or V8.1. The Korn shell is required. Web Administration Tool: embedded version of WebSphere Application Server - Express, V5.0; Netscape v6.2.3, v7.0 or Microsoft Internet Explorer v5.0	A minimum of 256 MB RAM (512 MB or more is strongly recommended).
Windows 2000, Windows NT	Microsoft Windows 2000, Windows XP, or Windows NT ® 4.0 with Service Pack 6 or higher. IBM DB2 Universal Database v7.2 with FixPak 5 or higher or V8.1. IBM DB2 Universal Database v7.2 or V8.1. Web Administration Tool: embedded version of WebSphere Application Server - Express, V5.0; Netscape v6.2.3, v7.0 or Microsoft Internet Explorer v5.5	A minimum of 256 MB RAM (512 MB or more is strongly recommended).

Πίνακας 5 – Πλατφόρμες / Απαιτήσεις IBM Directory Server 5.1

Microsoft's Active Directory

Το Active Directory περιλαμβάνεται στο λειτουργικό σύστημα Windows 2000 της Microsoft, και αποτελεί την πρόταση της Microsoft στα προϊόντα λογισμικού Υπηρεσιών Καταλόγου.

Ο Πίνακας 6 περιλαμβάνει τα κυριότερα χαρακτηριστικά του Active Directory της Microsoft:

Manageability	· Centralized Management · Group Policy · Global Catalog · IntelliMirror Desktop Management · Automated Software Distribution · Active Directory Service Interfaces (ADSI) · Backward Compatibility · Delegated Administration · Multi-Master Replication
Security	· Kerberos Authentication · Smart Card Support · Transitive Domain Trust · PKI/x.509 · LDAP over SSL · Required Authentication Mechanism · Attribute-Level Security · Spanning Security Groups · LDAP ACL Support
Interoperability	· DirSync Support · Active Directory Connectors (ADC) · Open APIs · Native LDAP · DNS Naming · Open Change History · DEA Platform · DEN Platform · Extensible Schema

Πίνακας 6 – Χαρακτηριστικά του Active Directory της Microsoft

1.6 ΟΦΕΛΗ ΑΠΟ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΥΠΗΡΕΣΙΑΣ ΚΑΤΑΛΟΓΟΥ

Το κυριότερο πλεονέκτημα της κεντρικής χρήσης LDAP σε ένα ίδρυμα είναι το γεγονός ότι όλες οι υπηρεσίες μπορούν να βασιστούν σε μία κεντρική αποθήκη δεδομένων και να αποφευχθούν οι πολλαπλές εγγραφές χρηστών για κάθε υπηρεσία. Παράλληλα η διαχείριση των εγγραφών των χρηστών μπορούν να γίνουν από εξελιγμένα εργαλεία διαχείρισης LDAP εγγραφών ενώ επίσης είναι δυνατόν και να εφαρμοστούν περιορισμοί στη διαχείριση των χρηστών και των υπηρεσιών ανά διαχειριστή με βάση διάφορα περίπλοκα κριτήρια. Πιο αναλυτικά οι ακόλουθες υπηρεσίες μπορούν να βασιστούν σε LDAP:

1.6.1 **EMAIL**

Η κυριότερη υπηρεσία που παρέχεται από τα ιδρύματα στους χρήστες τους είναι πάντα η υπηρεσία ηλεκτρονικού ταχυδρομείου. Σαν υπηρεσία ηλεκτρονικού ταχυδρομείου εννοούμε το σύνολο των SMTP,POP3 και IMAP servers που παρέχουν πρόσβαση σε λογαριασμούς email στα μέλη των ιδρυμάτων. Η υποστήριξη LDAP από την υπηρεσία αυτή είναι ιδιαίτερα σημαντική καθώς έτσι αποφεύγεται η δημιουργία τοπικών χρηστών στους εξυπηρετητές ηλεκτρονικού ταχυδρομείου με ότι αυτό συνεπάγεται από πλευράς διαχείρισης και ασφάλειας. Πιο συγκεκριμένα η υποστήριξη LDAP επιτρέπει τα εξής:

- Ταυτοποίηση των χρηστών της υπηρεσίας (ιδιαίτερα στις περιπτώσεις του POP3 και IMAP).
- Καθορισμό του mailhost και του maildir του χρήστη. Κατά αυτόν τον τρόπο είναι αρκετά εύκολη η υλοποίηση της υπηρεσίας mail με πολλούς mail servers κάτι που δίνει μεγάλες δυνατότητες επέκτασης.
- Καθορισμό και εφαρμογή quotas ανά χρήστη τόσο σε επίπεδο αριθμού αρχείων όσο και συνολικού μεγέθους.
- Δυνατότητα καθορισμού mail forwarding address και mail aliases ανά χρήστη
- Υλοποίηση υπηρεσίας mailing lists βασισμένης εξ ολοκλήρου σε LDAP
- Εφαρμογή ποικιλίας ACLs και ορίων στα μηνύματα (όπως πχ στο μέγιστο επιτρεπόμενο μέγεθος μηυμάτων) κάτι πολύ σημαντικό ιδιαίτερα για τις περιπτώσεις των mailing lists.

1.6.2 **DNS**

Άλλη μία από τις βασικές υπηρεσίες που παρέχεται σε όλα τα ιδρύματα είναι η υπηρεσία DNS. Η υποστήριξη LDAP από την υπηρεσία αυτή επιτρέπει το delegation της διαχείρισης του DNS χωρίς την εγκατάσταση αντίστοιχων εξυπηρετητών DNS καθώς και τη υλοποίηση της διαχείρισης αυτής μέσα από αυτοματοποιημένα περιβάλλοντα διαχείρισης. Στον τομέα αυτό το κυριότερο πακέτο είναι το LDAP-SDB module.

1.6.3 **FTP**

Η υποστήριξη του LDAP από την υπηρεσία FTP είναι ιδιαίτερα σημαντική για την παροχή χώρου προσωπικών web σελίδων στα μέλη της ακαδημαικής κοινότητας των ιδρυμάτων. Η υποστήριξη LDAP από αυτή την υπηρεσία επιτρέπει την:

- Ταυτοποίηση των χρηστών της υπηρεσίας
- Ορισμό per user quotas για τον επιτρεπόμενο χώρο που έχουν δικαίωμα να χρησιμοποιήσουν οι χρήστες καθώς και για τον μέγιστο αριθμό αρχείων που μπορούν να δημιουργήσουν
- Ορισμό του home directory και εξυπηρετητή στον οποίο θα βρίσκονται αποθηκευμένα τα αρχεία των χρηστών της υπηρεσίας

Στον τομέα αυτό τα κυριότερα πακέτα με υποστήριξη για LDAP είναι το ανοικτό πακέτο proftpd και το εμπορικό αλλά ελεύθερο για εκπαδευτικούς σκοπούς πακέτο ncftpd). Το proftpd έχει ιδιαίτερα ώριμο ldap module αλλά δεν επιτρέπει στη φάση αυτή την εφαρμογή user quotas. Το πακέτο αυτό χρησιμοποιείται αυτή τη στιγμή με επιτυχία στο ΠΣΔ για την παροχή περιοχής web σελίδων στα σχολεία. Το πακέτο NcFTPd χρησιμοποιείται με επιτυχία το τελευταίο διάστημα στο ΕΜΠ για την παροχή υπηρεσίας προσωπικών σελίδων στα μέλη της ακαδημαικής κοινότητας.

1.6.4 **DIALUP**

Θεωρείται ότι για την υποστήριξη της υπηρεσίας απομακρυσμένης πρόσβασης (dialup) θα χρησιμοποιηθεί τεχνολογία RADIUS. Η υποστήριξη LDAP από αυτή την υπηρεσία επιτρέπει την:

- Ταυτοποίηση των χρηστών της υπηρεσίας. Στον τομέα αυτόν μπορεί να χρησιμοποιηθεί η κλασσική μέθοδος με login/password αλλά και νέες μέθοδοι ταυτοποίησης όπως Certificate Authentication (EAP-TLS).

- Ορισμό των dialup settings των χρηστών (αριθμός επιτρεπόμενων καναλιών σε χρήση, εφαρμογή session και idle timeouts).
- Εφαρμογή ημερήσιων/εβδομαδιαίων/μηνιαίων quotas ανά χρήστη για περιορισμό της χρησιμοποίησης των περιορισμένων πόρων της υπηρεσίας dialup των ιδρυμάτων.
- Εφαρμογή περιορισμών στη σύνδεση των χρηστών όπως για παράδεγμα caller-id authentication

Στον τομέα αυτό υπάρχει ένας σεβαστός αριθμός από εμπορικά και ανοικτά πακέτα λογισμικού με υποστήριξη για αποθήκευση των χρηστών και της διαμόρφωσης των λογαριασμών τους σε βάση LDAP. Το πλέον ώριμο ανοικτό πακέτο λογισμικού που παρέχει αυτή τη λειτουργικότητα είναι το πακέτο freeradius . Αυτή τη στιγμή το πακέτο αυτό βρίσκεται στην έκδοση 0.8.1 και αναμένεται ότι στο πρώτο τρίμηνο του 2003 θα είναι διαθέσιμη η εκδοση τελική έκδοση 1.0.

Το πακέτο αυτό υποστηρίζει χρήστες σε LDAP με τα dialup settings να είναι αποθηκευμένα στις εγγραφές των χρηστών. Παράλληλα υποστηρίζεται accounting σε SQL βάση (υποστηρίζονται MySQL,PostgreSQL,DB2,Oracle και ODBC) και παρέχονται δυνατότητες πολλαπλών εξυπηρετητών, attribute rewriting και πολλές άλλες λειτουργικότητες καθώς και ένα ιδιαίτερα εξελιγμένο web based εργαλείο διαχείρισης (dialup_admin). Το πακέτο αυτό χρησιμοποιείται εδώ και αρκετό καιρό σε μεγάλα installations στην ελληνική ακαδημαική κοινότητα, όπως στο ΕΜΠ, Πανελλήνιο Σχολικό Δίκτυο , Πολυτεχνείο Κρήτης κα.

1.6.5 **WEB**

Στον τομέα αυτό η βασικη απαίτηση είναι το web authentication των χρηστών σε web σελίδες να γίνεται με βάση την πληροφορία που περιέχεται στον LDAP server. Η απαίτηση αυτή μπορεί να ικανοποιηθεί με αντίστοιχα authentication modules για τον apache. Πιο συγκεκριμένα μπορεί να χρησιμοποιηθεί είτε το auth_ldap module που παρέχει απευθείας σύνδεση με LDAP server είτε το auth_radius module που παρέχει σύνδεση με RADIUS server ο οποίος στη συνέχεια μπορεί να κάνει το authentication μέσω LDAP.

1.7 ΥΛΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΑΣ ΚΑΤΑΛΟΓΟΥ

1.7.1 **ΔΟΜΗ DIT**

Το DIT (Directory Information Tree) αποτελεί τη λογική δομή και κατηγοριοποίηση των δεδομένων της υπηρεσίας καταλόγου. Η δομή ενός DIT με βάση την οποία θα οργανωθούν τα δεδομένα μιας υπηρεσίας καταλόγου μπορεί να είναι είτε ιεραρχική (hierarchical DIT) είτε επίπεδη (flat DIT).

Κάθε μια από τις δύο παραπάνω προσεγγίσεις παρουσιάζει μειονεκτήματα και πλεονεκτήματα.

Hierarchical DITs

Τα σημαντικότερα χαρακτηριστικά της ιεραρχικής δομής ενός DIT είναι ότι:

- οδηγούν σε μεγαλύτερα DNs (Distinguished Names)
- απεικονίζουν με μεγαλύτερη ακρίβεια την πραγματική δομή του συστήματος το οποίο αναπαριστούν
- μπορούν να προκαλέσουν περισσότερα διαχειριστικά προβλήματα στην περίπτωση που τα δεδομένα του οργανισμού μεταβάλλονται συχνά
- ελαχιστοποιούν την πιθανότητα του ενδεχομένου να προκύψουν δύο κοινά DNs.

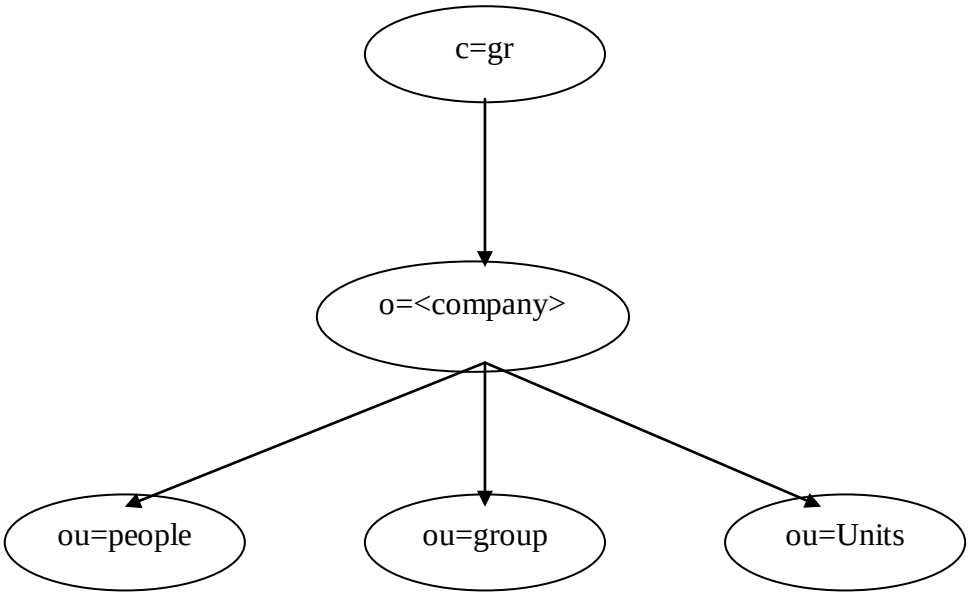
Flat DITs

Τα σημαντικότερα χαρακτηριστικά ενός flat DIT είναι ότι:

- δεν υπάρχει ανάγκη εκτενούς κατηγοριοποίησης
- τα DNs που προκύπτουν είναι σύντομα και ευκολομνημόνευτα
- το δέντρο είναι πιο σταθερό από την άποψη ότι είναι πιο εύκολα διαχειρίσιμες οι αλλάγες και οι μετακινήσεις των χρηστών καθώς αρκούν αλλαγές στα attributes της εγγραφής και δεν απαιτείται κάποια αλλαγή στο DN της εγγραφής.

Για την ευκολότερη διαχείριση της υπηρεσίας προτείνουμε την επίπεδη δομή του δένδρου (flat DIT). Ιδιαίτερα σε περιπτώσεις που ο όγκος των δεδομένων δεν είναι μεγάλος ώστε να απαιτείται η σύνθετη οργάνωση του στα πλαίσια του ιεραρχικού δέντρου, η επίπεδη δομή φαίνεται να δίνει συγκριτικά περισσότερα πλεονεκτήματα σε σχέση με την ιεραρχική.

Το παρακάτω σχήμα παρουσιάζει ένα παράδειγμα προτεινόμενης επίπεδης μορφή δέντρου.



1.7.2 **ΣΧΗΜΑ (Schema)**

Το σχήμα που προτείνουμε προς υλοποίηση βασίζεται στην ιεραρχία της παρακάτω εικόνας:

Η παραπάνω ιεραρχία περιέχει τις κλάσεις και τα χαρακτηριστικά που περιγράφονται στη συνέχεια του κειμένου.

1.7.3 **RFC-defined objectclasses**

top (rfc 2256)

- Η κλάση **top** βρίσκεται στην κορυφή της ιεραρχίας. Όλες οι υπόλοιπες κλάσεις που δεν ορίζονται έτσι ώστε να έχουν κάποια ανώτερη κλάση στην ιεραρχία, θα πρέπει να βρίσκονται κάτω από την top.

person (rfc 2256)

- Η κλάση person ακολουθεί στην ιεραρχία. Τα απαραίτητα attributes που θα πρέπει να οριστούν είναι τα εξής:

ATTRIBUTE	ΠΕΡΙΓΡΑΦΗ
sn	Το επώνυμο του χρήστη
cn	Το ονοματεπώνυμο του χρήστη

Τα attributes που ορίζονται προαιρετικά είναι τα εξής:

ATTRIBUTE	ΠΕΡΙΓΡΑΦΗ
description	Περιγραφή
seeAlso	Το DN μιας εγγραφής που περιέχει επιπλέον στοιχεία.
telephoneNumber	Τηλέφωνο
userPassword	Ο μυστικός κωδικός του χρήστη

organizationalPerson (rfc 2256)

- Η κλάση **organizationalPerson** κληρονομεί από την κλάση person.

Τα attributes που ορίζονται για αυτή την κλάση είναι τα εξής:

ATTRIBUTE	ΠΕΡΙΓΡΑΦΗ
title	Ο τίτλος του χρήστη πχ Project Leader
X121Address	
registeredAddress	Η διεύθυνση του χρήστη
ou	Το locality του χρήστη
preferredDeliveryMethod	Ο τρόπος με τον οποίο γίνεται η επικοινωνία μεταξύ των χρηστών
teletexTerminalIdentifier	teletex terminal identifier
st	Ο νομός στον οποίο ανήκει ο χρήστης
telexNumber	Telex number
l	Το locality του χρήστη
telephonenumber	Το τηλέφωνο εργασίας του χρήστη σε σύνταξη τηλεφωνικού αριθμού (πχ +30 10 7723010)

physicalDeliveryOfficeName	Διεύθυνση του χρήστη
postalCode	Ταχυδρομικός κώδικας
postalAddress	Διεύθυνση
facsimileTelephoneNumber	Fax
street	Η φυσική διεύθυνση του χρήστη

inetOrgPerson (rfc 2798)

- Η κλάση **inetOrgPerson** κληρονομεί από την κλάση organizationalPerson.

Τα attributes που ορίζονται για την κλάση αυτή είναι τα εξής:

ATTRIBUTE	ΠΕΡΙΓΡΑΦΗ
audio	Αρχεία ήχου
departmentNumber	Ο κωδικός του τμήματος στο οποίο ανήκει ο χρήστης
displayName	Το όνομα που επιθυμεί ο χρήστης να εμφανίζεται
employeeNumber	Αναγνωριστικός κωδικός του χρήστη. Παίρνει μοναδικές τιμές (single valued).
employeeType	Η κατηγορία στην οποία ανήκει ο χρήστης
homePhone	Το τηλέφωνο σπιτιού
homePostalAddress	Η διεύθυνση σπιτιού
labeledURI	Uniform Resource Identifier
manager	Ορίζει το manager του χρήστη. Είναι τύπου DN
mobile	Το κινητό τηλέφωνο του χρήστη
userCertificate	Το πιστοποιητικό ασφαλείας του χρήστη
uid	Το username του χρήστη
mail	Το mail του χρήστη όπως χρησιμοποιείται από την υπηρεσία mail
businessCategory	Η κατηγορία στην οποία ανήκει ο χρήστης πχ μέλος ΔΕΠ, Μεταπτυχιακός φοιτητής, Διοικητικός κτλ.
o	Το πλήρες όνομα του οργανισμού στον οποίο είναι μέλος ο χρήστης (πχ Εθνικό Μετσόβιο Πολυτεχνείο)
jpegPhoto	JPEG φωτογραφία του χρήστη
givenName	Το όνομα του χρήστη
photo	Φωτογραφία
x500uniqueIdentifier	Χρησιμοποιείται στον ορισμό του αντικειμένου στην περίπτωση που το DN έχει ξαναχρησιμοποιηθεί. Πρόκειται για διαφορετικό attribute σε σχέση τόσο με το uid όσο και με uniqueIdentifier
userSMIMECertificate	Ορίζει το προσωπικό πιστοποιητικό του χρήστη, πληροφορίες σχετικά με ολόκληρη την αλυσίδα των Αρχών Πιστοποίησης και με τον αλγόριθμο κρυπτογράφησης
userPKCS12	Ορίζει το πρότυπο διακίνησης προσωπικών δεδομένων

eduPerson

- Η κλάση **eduPerson** που ακολουθεί στην ιεραρχία είναι προϊόν της ομάδας εργασίας EDUCAUSE/Internet2, στόχος της οποίας ήταν η δημιουργία μιας κλάσης που θα ενσωματώνει το σύνολο των κοινών χαρακτηριστικών των εκπαιδευτικών ιδρυμάτων. Η κλάση **eduPerson** κληρονομεί τα attributes όλων των κλάσεων που προαναφέρθηκαν.

Τα attributes που ορίζονται για την κλάση αυτή είναι τα εξής:

ATTRIBUTE	ΠΕΡΙΓΡΑΦΗ
eduPersonAffiliation	Ορίζει την κατηγορία στην οποία ανήκει ο χρήστης. Οι κατηγορίες είναι οι εξής: faculty, student, staff, alum, member, affiliate, employee
eduPersonNickname	Ανεπίσημο όνομα χρήστη
eduPersonOrgDN	Το DN του εκπαιδευτικού ιδρύματος στον οποίο ανήκει ο χρήστης
eduPersonOrgUnitDN	Το DN του κατώτερου τμήματος στο οποίο ανήκει ο χρήστης
eduPersonPrimaryAffiliation	Περιγράφει τη σχέση του χρήστη με το εκπαιδευτικό ίδρυμα στο οποίο ανήκει. Πιθανές τιμές του attribute είναι οι εξής: faculty, student, staff, alum, member, affiliate, employee
eduPersonEntitlement	URI (URN ή URL) που ορίζει το σύνολο των δικαιωμάτων σε συγκεκριμένους πόρους
eduPersonPrimaryOrgUnitDN	Το DN των εγγραφών που ορίζει την μονάδα (Organizational Unit(s)) στην οποία ανήκει ο χρήστης.

1.7.4 **Application objectclasses**

Στο σχήμα του LDAP θα πρέπει να προστεθούν κλάσεις για να υποστηρίξουν υπηρεσίες όπως οι Qmail και radius authentication.

qmailuser

- Η κλάση qmailuser χρησιμοποιείται για LDAP υποστήριξη του Qmail.

Τα attributes που ορίζονται σε αυτή την κλάση είναι τα εξής:

ATTRIBUTE	ΠΕΡΙΓΡΑΦΗ
qmailDotMode	Ο τρόπος με τον οποίο θα βλέπει ο χρήστης τα αρχεία του qmail. Οι τιμές που μπορεί να πάρει το qmailDotMode είναι οι εξής: both, dotonly, ldaponly, ldapwithprog, none
deliveryMode	Ο τρόπος με τον οποίο παραδίδονται τα μηνύματα. . Οι τιμές που μπορεί να πάρει το deliveryMode είναι οι εξής: : normal, forwardonly, nombox, localdelivery, reply
qmailGID	Το GID του χρήστη
mailReplyText	Η απάντηση που θα αποστέλλεται σε κάθε εισερχόμενο μήνυμα

deliveryProgramPath	Πρόγραμμα που εκτελείται με κάθε εισερχόμενο μήνυμα
accountStatus	Η κατάσταση του λογαριασμού
qmailUID	Το UID του χρήστη
mailAlternateAddress	Εναλλακτική διεύθυνση του χρήστη
mailQuota	Η χωρητικότητα της θυρίδας του χρήστη
mailHost	Ο server στον οποίο αποθηκεύονται τα μηνύματα
mailForwardingAddress	Η email διεύθυνση στην οποία θα προωθούνται τα μηνύματα προς το χρήστη

radiusprofile

- Η κλάση radiusprofile χρησιμοποιείται για LDAP υποστήριξη του radius.

Κάποια από τα attributes που ορίζονται σε αυτή την κλάση και σχετίζονται με το authorization του χρήστη είναι τα παρακάτω:

radiusLoginTCPPort
radiusLoginTime
radiusarapfeatures
radiusarapsecurity
radiusarapzoneaccess
radiuscallbackid
radiuscallbacknumber
radiuscalledstationid
radiuscallingstationid
radiusclass

posixAccount

- Η κλάση posixAccount χρησιμοποιείται στις περιπτώσεις του PAM ή NSS ldap authentication και ορίζει τα παρακάτω Attributes

ATTRIBUTE	ΠΕΡΙΓΡΑΦΗ
uidNumber	Το uid του χρήστη
gidNumber	Το gid του χρήστη
homeDirectory	Το homeDirectory του χρήστη
userPassword	Το password του χρήστη
loginShell	Το loginShell του χρήστη
gecos	Το cn του χρήστη

1.8 ΠΡΟΤΕΙΝΟΜΕΝΑ INDEXES

Ένας από τους σημαντικότερους παράγοντες που επηρεάζουν την απόδοση του συστήματος ιδιαίτερα όσο αφορά το χρόνο απόκρισης στα ερωτήματα που γίνονται προς τον server, είναι η δημιουργία των κατάλληλων indexes.

Τα indexes που μπορούν να δημιουργηθούν είναι τα: mail clients Netscape messenger, Outlook express και Mozilla.

ΜΕΡΟΣ 2ο

2.1 ΑΣΦΑΛΕΙΑ ΤΟΥ SERVER

Η ασφάλεια του server και η ελεγχόμενη πρόσβαση σε αυτόν είναι ένα από τα σπουδαιότερα θέματα που χρήζουν ιδιαίτερης προσοχής. Ο μηχανισμός προστασίας και ασφαλούς πρόσβασης υλοποιείται με τον ορισμό των ACIs (access control instructions). Κάθε φορά που ο server δέχεται ένα αίτημα, το αν θα το εξυπηρετήσει ή όχι εξαρτάται από τα ACIs που έχουν οριστεί για τον χρήστη που προσπαθεί να συνδεθεί (bind). Ένα ACI μπορεί να επιτρέπει ή όχι λειτουργίες όπως η ανάγνωση, η αναζήτηση, η σύγκριση και η μεταβολή του περιεχομένου του server.

Ένα ACI μπορεί να οριστεί για ολόκληρο το δέντρο, για ένα κομμάτι του ή για συγκεκριμένες εγγραφές και να αφορά την πρόσβαση ενός χρήστη ή μιας ομάδας χρηστών από μια συγκεκριμένη IP διεύθυνση ή DNS όνομα.

Παραδείγματα τυπικών ACIs ενός ldap server είναι τα εξής:

- Οι χρήστες μπορούν να μεταβάλλουν το περιεχόμενο της εγγραφής τους αλλά όχι και να σβήσουν την ίδια την εγγραφή

```
aci: (targetattr = "*")(version 3.0;acl "Allow all except write to self";allow
(read,compare,search,selfwrite,add)(userdn = "ldap:///self");)
```

- Επιτρέπεται στους χρήστες ανώνυμη πρόσβαση με περιορισμένα δικαιώματα (search, compare, read) και για συγκεκριμένα attributes.

```
aci: (targetattr != "userPassword || radius* || dialupaccess || chappassword |
 | creatorsName ||modifiersName") (version 3.0;acl "Anonymous access";allow
(read,compare,search)(userdn = "ldap:///anyone");)
```

- Ο administrator (uid=admin, ou=TopologyManagement, o=NetscapeRoot) έχει όλα τα δικαιώματα

```
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrator"; allow
 (all) userdn = "ldap:///uid=admin, ou=Administrators,
ou=TopologyManagement,
  o=NetscapeRoot";)
```

- Όλα τα μέλη της ομάδας Configuration Administrators έχουν όλα τα δικαιώματα

```
aci: (targetattr="*")(version 3.0; acl "Enable Configuration Administrator Gro
 up modification"; allow (all) groupdn = "ldap:///cn=Configuration Administrat
 ors, ou=Groups, ou=TopologyManagement, o=NetscapeRoot";)
```

- Τα μέλη του group Directory Administrators έχουν όλα τα δικαιώματα

```
aci: (target="ldap:///o=auth,c=gr")(targetattr="*")(version 3.0; acl "Director
 y Administrators Group"; allow (all) groupdn = "ldap:///ou=Directory Administ
 rators,o=auth,c=gr"; )
```

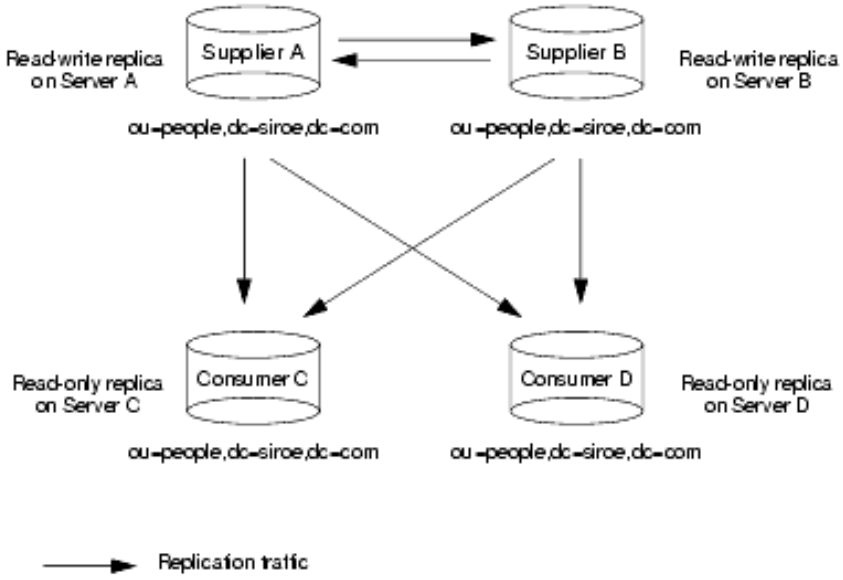
2.2 MULTIMASTER REPLICATION

Ένας άλλος παράγοντας που εξασφαλίζει την καλή απόδοση και την αξιοπιστία του συστήματος είναι η δυνατότητα να διατηρούμε μηχανισμούς που από τη μία θα βελτιώνουν συνολικά την επίδοση του συστήματος και από την άλλη θα εξασφαλίζουν την άμεση και αποτελεσματική αντιμετώπιση τυχόν προβλημάτων.

Τη δυνατότητα αυτή μας την παρέχουν οι ldap servers μέσω των μηχανισμών αντιγραφής (replication). Το κύριο πλεονέκτημα του replication είναι ότι μπορούμε να διατηρούμε αντίγραφα ενός server για να εξασφαλίσουμε την ανεκτικότητα σε σφάλματα, το διαμοιρασμό του φόρτου μέσω της κατανομής των λειτουργιών σε διαφορετικούς servers και τη μεγαλύτερη ασφάλεια των δεδομένων.

Η πιο απλή μορφή replication είναι το single-master replication όπου ένας κύριος server αποτελεί τον supplier που προωθεί τις αλλαγές σε servers-αντίγραφα του, τους consumers.

Ο iPlanet Directory Server 5.0 υποστηρίζει multimaster replication κατά το οποίο ένας server μπορεί να είναι ταυτόχρονα supplier και consumer και κατά συνέπεια το ίδιο υποδένδρο (subtree) υπάρχει και μεταβάλλεται από 2 servers. Το παρακάτω σχήμα απεικονίζει μια περίπτωση multimaster replication.



Το υποδένδρο αποτελεί ξεχωριστό read-write replica σε καθέναν από τους servers. Αυτό σημαίνει ότι ο κάθε server διατηρεί το δικό του change log αρχείο για κάθε replica. Το αρχείο αυτό περιγράφει τις αλλαγές που πρέπει να προωθηθούν στους consumers αλλά και στους υπόλοιπους masters στην περίπτωση του multimaster replication.

Στο συγκεκριμένο σχήμα replication ο αριθμός των consumers που μπορούν να συμμετέχουν μπορεί να είναι οποιοσδήποτε. Ο κάθε consumer διατηρεί το δικό του read-only replica. Οι consumers δέχονται αλλαγές από τους δύο suppliers και μπορούν να έχουν ορισμένα referrals σχετικά και με τους δύο suppliers ώστε να ανακατευθύνουν τα αιτήματα που προέρχονται από αυτούς.

Τα σημαντικότερα πλεονεκτήματα που παρουσιάζονται με την υλοποίηση του multimaster replication είναι η υποστήριξη (fault tolerance) που μπορεί να παρέχει ο καθένας από τους δύο servers στην περίπτωση που υπάρχει κάποιο πρόβλημα με τον άλλο, καθώς επίσης και το γεγονός ότι οι αλλαγές θα γίνονται στον τοπικό server του κατανεμημένου συστήματος.

Πρόβλημα μπορεί να δημιουργηθεί όταν στους δύο masters μεταβάλλεται ταυτόχρονα το περιεχόμενο της ίδιας εγγραφής. Οι μηχανισμοί επίλυσης αυτών των συγκρούσεων βασίζονται στην ύπαρξη timestamps και ανάλογα με τη λειτουργία που πρόκειται να επιτελεστεί δίδεται και η κατά περίπτωση λύση.

ΜΕΡΟΣ 3ο

3.1 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΚΑΤΑΛΟΓΟΥ

Στα πλαίσια της δράσης ενός καταλόγου οι απαιτήσεις από την υπηρεσία καταλόγου είναι οι ακόλουθες:

- Να είναι ιδιαίτερα γρήγορη στις αναζητήσεις σε ένα μεγάλο αριθμό από εξυπηρετητές καταλόγου ιδρυμάτων
- Να υπάρχει δυνατότητα να γίνει scaling της υπηρεσίας και να μην υπάρχει υποβάθμιση της ποιότητας της ανεξαρτήτως του μεγέθους των βάσεων χρηστών που διατηρούν τα ιδρύματα
- Να μην δημιουργεί επιπλέον φόρτο στους εξυπηρετητές καταλόγου των ιδρυμάτων καθώς και να μην δημιουργεί προβλήματα ασφάλειας

Κάποιες αρχιτεκτονικές καταλόγου είναι οι ακόλουθες:

- **Referral Architecture:**

Υπηρεσία καταλόγου που απλώς επιστρέφει ldap referrals προς τον τελικό χρήστη ο οποίος είναι υπεύθυνος να πραγματοποιήσει στη συνέχεια τις απαραίτητες αναζητήσεις ldap στους αντίστοιχους εξυπηρετητές καταλόγου. Η λύση αυτή παρουσιάζει το μεγάλο πλεονέκτημα της ευκολίας διαχείρισης και μηδενικού κόστους ανάπτυξης (απαιτείται απλώς η εγκατάσταση ενός εξυπηρετητή ldap που θα περιέχει μία εγγραφή c=gr η οποία και θα περιέχει τα αντίστοιχα referrals).

Η λύση όμως αυτή στηρίζεται στην συνεχή καλή λειτουργία των εξυπηρετητών καταλόγου στους οποίους δείχνει καθώς η δυσλειτουργία ενός από αυτούς θα γίνει αντιληπτή από όλους τους χρήστες της υπηρεσίας και θα οδηγήσει σε υποβάθμιση της ποιότητας της. Επιπλέον δεν επιτρέπει την πραγματοποίηση έξυπνων κλήσεων (rewrites κτλ), την παρουσίαση ενός σχετικά ενιαίου Directory Information Tree (αντίθετα απλώς παρουσιάζονται ξεχωριστά τα DITs των ιδρυμάτων) και τέλος δεν επιτρέπει κανενός είδους έλεγχο στα queries που τελικά πραγματοποιούνται στους εξυπηρετητές των ιδρυμάτων από την υπηρεσία (κάτι που τελικά μπορεί να δημιουργήσει πρόβλημα ασφάλειας και προστασίας των δεδομένων των χρηστών). Πρέπει επίσης να προστεθεί ότι η υλοποίηση της λύσης αυτής απαιτεί από τους διαχειριστές των αντίστοιχων εξυπηρετητών καταλόγου να επιτρέπουν ανώνυμη πρόσβαση σε αυτούς από όλο τον κόσμο κάτι το οποίο δημιουργεί σαφή προβλήματα ασφάλειας και δεν είναι κάτι που όλοι οι διαχειριστές είναι έτοιμοι να κάνουν.

- **Main Index Architecture:**

Υπηρεσία ευρετηρίου που με κάποιο μηχανισμό αντλεί από τους εξυπηρετήτες καταλόγου των ιδρυμάτων πληροφοριακά attributes για όλες τις εγγραφές τις οποίες περιέχουν. Τα δεδομένα αυτά στη συνέχεια αποθηκεύονται σε μία δομή τύπου LDAP από όπου μπορούν να γίνουν αναζητήσεις οι οποίες στο τέλος επιστρέφουν referrals στις πλήρεις εγγραφές των

χρηστών στους εξυπηρετητές των ιδρυμάτων. Η λύση αυτή παρουσιάζει το πλεονέκτημα της μεγάλης ταχύτητας (καθώς οι αναζητήσεις γίνονται τοπικά) καθώς και του πλήρη ελέγχου στα δεδομένα πάνω στα οποία γίνονται οι αναζητήσεις αλλά και στις ίδιες τις αναζητήσεις (εφαρμογή access lists, time/size limits κτλ). Επιπλέον από τους διαχειριστές των εξυπηρετητών καταλόγου των ιδρυμάτων απαιτείται απλώς η παραχώρηση ενός λογαριασμού στους εξυπηρετητές αυτούς (εφόσον δεν επιτρέπεται ανώνυμη πρόσβαση) μέ τη χρήση του οποίου θα γίνεται η άντληση των δεδομένων.

Το μεγάλο μειονέκτημα της λύσης αυτής είναι ότι παρουσιάζει μεγάλο χρόνο ανάπτυξης, μεγάλο διαχειριστικό κόστος, το κόστος της υπηρεσίας μεγαλώνει καθώς μεγαλώνουν τα δεδομένα των ιδρυμάτων και τέλος απαιτεί από όλα τα ιδρύματα να κάνουν προσβάσιμα τα αντίστοιχα πληροφοριακά attributes για την άντληση και χρήση τους από την υπηρεσία ευρετηρίου κάτι το οποίο μπορεί να αντιβαίνει στην πολιτική ασφάλειας τους. Επιπλέον συνεχίζει να υπάρχει η απαίτηση οι εξυπηρετητές καταλόγου των ιδρυμάτων να συνεχίζουν να είναι προσβάσιμοι από όλο τον κόσμο.

- **Meta Directory Architecture:**

Υπηρεσία ευρετηρίου που αναλαμβάνει να πραγματοποιήσει τις αναζητήσεις εκ μέρους των χρηστών στους εξυπηρετητές καταλόγου των ιδρυμάτων. Στη συνέχεια τα δεδομένα που επιστρέφονται από τους εξυπηρετήτες υπόκεινται σε τοπική επεξεργασία και ακολούθως επιστρέφονται στον χρήστη. Κατά αυτόν τον τρόπο χωρίς να απαιτείται η διατήρηση τοπικών δεδομένων διατηρείται πλήρης έλεγχος στις αναζητήσεις που πραγματοποιούνται μέσω της υπηρεσίας ενώ παράλληλα υπάρχει η δυνατότητα για πραγματοποίηση εξελιγμένων μετατροπών τόσο στα queries όσο και στις απαντήσεις (rewrites, attribute mapping κτλ). Επιπλέον δεν απαιτείται οι εξυπηρετητές καταλόγου να επιτρέπουν ανώνυμη πρόσβαση καθώς η υπηρεσία ευρετηρίου μπορεί να συνδεθεί στους εξυπηρετητές (LDAP BIND) με συγκεκριμένο BIND DN/password.

Από τις παραπάνω υλοποιήσεις καλύτερη είναι η τελευταία λόγω των σαφών πλεονεκτημάτων που παρουσιάζει και της ευκολίας εγκατάστασης και διαχείρισης που παρουσίαζει.

Για τους σκοπούς της υλοποίησης και στα πλαισια της υποστήριξης του ελεύθερου λογισμικού χρησιμοποιήθηκε η πλατφόρμα λογισμικού Openldap και συγκεκριμένα η έκδοση 2.1.12 (η πλέον πρόσφατη κατά τη στιγμή εγκατάστασης της υπηρεσίας) με ενεργοποίηση του meta backend για την πραγματοποίηση των αναζητήσεων στους εξυπηρετητές καταλόγου των ιδρυμάτων. Το meta backend αναλαμβάνει να προωθήσει κάθε request που φτάνει στον εξυπηρετητή καταλόγου σε όλους τους εξυπηρετητές καταλόγου των ιδρυμάτων και να επιστρέψει στη συνέχεια στο χρήστη τις απαντήσεις. Παράλληλα αν απαιτείται γίνεται και rewrite στα επιστρεφόμενα DNs. Κατά αυτόν τον τρόπο ενώ η ρίζα του Directory Tree ενός ιδρύματος μπορεί να είναι o=ntua,c=gr αυτή γίνεται rewrite σε dc=ntua,dc=gr.

Με βάση τα παραπάνω δημιουργήθηκαν δύο διαφορετικά Directory Trees:

- **dc=gr** και
- **c=gr**

Επιπλέον το meta backend έχει αυξημένες δυνατότητες attribute mapping. Κατά αυτόν τον τρόπο μπορεί κάποιο ίδρυμα για τους δικούς του λόγους να χρησιμοποιεί διαφορετικό attribute για μία συγκεκριμένη πληροφορία από τα υπόλοιπα ιδρύματα αλλά αυτό να μη φαίνεται στην τελική πληροφορία που είναι διαθέσιμη από την κεντρική υπηρεσία καταλόγου καθώς αυτό γίνεται mapped στο attribute που χρησιμοποιείται από τα υπόλοιπα ιδρύματα.

3.2 ΑΛΛΑΓΕΣ ΣΤΟΝ ΠΗΓΑΙΟ ΚΩΔΙΚΑ

Κατά τους αρχικούς ελέγχους της υπηρεσίας παρατηρήθηκε το ακόλουθο πρόβλημα:

Αν κάποιος από τους εξυπηρετητές καταλόγου των ιδρυμάτων δεν ήταν διαθέσιμος το meta backend έμενε σε connecting state μέχρι να λήξει το TCP connection timeout (συνήθως 2 λεπτά). Αυτό προφανώς δημιουργούσε σημαντικά προβλήματα στην υπηρεσία. Για τον σκοπό αυτό πραγματοποιήθηκαν αλλαγές στον κώδικα του meta backend προκειμένου να προστεθεί μία επιπλεόν μεταβλητή διαμόρφωσης *network-timeout* με την οποία ορίζεται σε δευτερόλεπτα ο χρόνος που θα πρέπει να αναμένει η βιβλιοθήκη LDAP μέχρι να θεωρήσει ότι η σύνδεση στον εξυπηρετητή καταλόγου απέτυχε. Με την εφαρμογή της αλλαγής αυτής ο χρόνος απόκρισης της υπηρεσίας μειώθηκε σημαντικά.

3.3 ΕΓΚΑΤΑΣΤΑΣΗ ΥΠΗΡΕΣΙΑΣ

Η εγκατάσταση της υπηρεσίας ακολούθησε τα εξής βήματα:

- Μεταφόρτωση της τελευταίας έκδοσης του λογισμικού openldap από το ftp://ftp.openldap.org/ ή τα mirrors του.
- Εφαρμογή του patch με τις απαιτούμενες αλλαγές. Το patch αυτό έχει υποβληθεί στην κοινότητα του openldap με νούμερο ITS #2413.
- ./configure --prefix=/home/dsgunet/local --enable-rewrite --enable-dnssrv --enable-meta --disable-bdb --enable-ldap
- make depend
- make
- make install

Μετά από τα παραπάνω βήματα η εγκατάσταση θα πρέπει να έχει ολοκληρωθεί πλήρως. Στη συνέχεια θα πρέπει να γίνουν οι αναγκαίες μετατροπές στο αρχείο local/etc/openldap/slapd.conf. Το αρχείο αυτό παρατίθεται στο τέλος τους παρούσας τεκμηρίωσης.

3.4 ΑΡΧΕΙΟ ΔΙΑΜΟΡΦΩΣΗΣ

Οι κυριότερες μεταβλητές διαμόρφωσης που μας ενδιαφέρουν είναι οι εξής:

- **include:** Ορίζει συνήθως τα schma αρχεία τα οποία θα περιλαμβάνει ο εξυπηρετητής. Πέραν του default core.schema προκειμένου να λειτουργεί ικανοποιητικά η υπηρεσία θα πρέπει να προστεθούν και τα παρακάτω αρχεία:

- cosine.schema
- inetorgperson.schema

Γενικώς η υπηρεσία θα επιστρέφει μόνο εκείνα τα attributes τα οποία γνωρίζει μέσα από το LDAP schema. Επομένως, απαιτείεται να έχουν προστεθεί τα αντίστοιχα schema files στο αρχείο διαμόρφωσης της υπηρεσίας.

- **sizelimit**: Ορίζει το γενικό sizelimit όριο που θα εφαρμόζεται σε όλες τις αναζητήσεις. Στην περίπτωση μας προκειμένου να μειωθεί ο φόρτος για τους εξυπηρετητες των ιδρυμάτων έχει αποδωθεί η τιμή 90.
- **threads:** Ορίζει τον αριθμό από threads τα οποία θα χρησιμοποιεί ο εξυπηρετητής.
- **timelimit:** Ορίζει το timelimit όριο το οποίο θα εφαρμοστεί σε όλες τις αναζητήσεις. Στην περίπτωση μας προκειμένου να μειωθεί ο φόρτος για τους εξυπηρετητές των ιδρυμάτων έχει αποδωθεί η τιμή 60 (1 λεπτό).
- **idletime:** Ορίζει το χρονικό όριο για το οποίο μία σύνδεση προς τον εξυπηρετητή μπορεί να παραμείνει ανενεργή. Στην περίπτωση μας έχει επιλεγεί ως τιμή το 600 (10 λεπτά).
- **binddn:** Ορίζει το DN με το οποίο θα κάνει LDAP BIND η υπηρεσία στον συγκεκριμένο εξυπηρετητή καταλόγου. Η μεταβλητή αυτή δεν χρησιμοποιείται στις περιπτώσεις εξυπηρετητών που επιτρέπουν ανώνυμη πρόσβαση.
- **bindpw:** Ορίζει το password με το οποίο θα κάνει LDAP BIND η υπηρεσία στον συγκεκριμένο εξυπηρετητή καταλόγου. Όπως και παραπάνω η μεταβλητή αυτή δεν χρησιμοποιείται στις περιπτώσεις εξυπηρετητών που επιτρέπουν ανώνυμη πρόσβαση.
- **database:** Ορίζει το backend το οποίο θα χρησιμοποιηθεί. Στην περίπτωση μας είναι το meta backend και η μεταβλητή αυτή εμφανίζεται δύο φορές στο αρχείο διαμόρφωσης καθώς διατηρούμε δύο δέντρα πληροφορίας το dc=gr και το c=gr
- **lastmod:** Ορίζει αν το backend θα διατηρεί για κάθε εγγραφή πληροφορία για την τελευταία αλλαγή. Στην περίπτωση μας κάτι τέτοιο δεν έχει νόημα για αυτό και απενεργοποιήθηκε.
- **suffix:** Η ρίζα του δέντρου. Στην περίπτωση μας υπάρχουν δύο δέντρα το dc=gr και c=gr
- **readonly:** Ορίζει αν η βάση θα βρίσκεται σε κατάσταση μόνο ανάγνωσης. Στην περίπτωση μας έχει ενεργοποιηθεί (επιτρέπονται δηλαδή μόνο αναζητήσεις μέσω της υπηρεσίας).
- **network-timeout:** Η νέα μεταβλητή που προσθέσαμε στον κώδικα με την οποία ορίζουμε τον μέγιστο χρόνο (σε δευτερόλεπτα) για τον οποίο θα περιμένουνμε για την επιτυχή σύνδεση σε έναν από τους εξυπηρετητές καταλόγου των ιδρυμάτων. Στην περίπτωση μας έχει επιλεγεί η τιμή του ενός δευτερολέπτου προκειμένου να μην δημιουργείται οποιοδήποτε πρόβλημα στην ποιότητα της υπηρεσίας προς τον τελικό χρήστη.
- **uri:** Το LDAP URL του εξυπηρετητή καταλόγου στον οποίο θα πραγματοποιήσουμε αναζητήσεις. Ένα παράδειγμα είναι το παρακάτω:
  uri "ldap://ldap.ntua.gr:389/dc=ntua,dc=gr"
- **suffixmassage:** Εάν η ρίζα του δέντρου πληροφοριών του ιδρύματος δεν ταιριάζει με το root με το οποίο θέλουμε εμείς να εμφανίζεται τότε κάνουμε rewrite όπως παρακάτω:
  suffixmassage "dc=ntua,dc=gr" "o=ntua,c=gr"
- **map:** Εάν απαιτείται μπορούμε να κάνουμε mapping κάποιο attribute που περιέχεται σε έναν από τους εξυπηρετητές καταλόγου των ιδρυμάτων σε κάποιο άλλο όπως παρακάτω:
  map attribute mail ntuapersonmail

3.5 ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΗΣ

Η πολιτική πρόσβασης που ορίστηκε καθορίζει ότι η πρόσβαση στην υπηρεσία επιτρέπεται μόνο από ένα μηχάνημα στο οποίο και λειτουργεί η web based υπηρεσία αναζήτησης. Κατά αυτόν τον τρόπο υπάρχει πλήρης έλεγχος στις αναζητήσεις που πραγματοποιούνται μέσω της υπηρεσίας και δεν επιτρέπονται περιπτώσεις ldap crawling. Η πολιτική πρόσβασης υλοποιείται όπως φαίνεται παρακάτω:

```
access to *
    by peername=www.gunet.gr read stop
    by peername=* none stop
```

Πέραν των παραπάνω έχει υλοποιηθεί μηχανισμός αποτροπής συγκεκριμένων αναζητήσεων που μπορούν να δημιουργήσουν πρόβλημα στους εξυπηρετητές των ιδρυμάτων. Πιο συγκεκριμένα απαγορεύονται οι αναζητήσεις που περιέχουν λιγότερους από 4 χαρακτήρες στο φίλτρο αναζήτησης. Η υλοποίηση του μηχανισμού αυτού φαίνεται παρακάτω:

```
rewriteEngine   on

rewriteContext  searchFilter
rewriteRule     "=\\*?.{3}\\*?)" "failed" "#"
```

ΜΕΡΟΣ 4ο

4.1 ΣΥΝΔΕΣΗ ΥΠΗΡΕΣΙΑΣ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ ΜΕ FREERADIUS

Ο εξυπηρετητής τις ανήκει στην κατηγορία του ελεύθερου λογισμικού και παρέχει πολύ μεγάλες δυνατότητες, ευελιξία και ταχύτητα και μπορεί ικανοποιήσει με τον καλύτερο τρόπο και τις μεγαλύτερες απαιτήσεις μεγέθους.

4.1.1 **Δυνατότητες**

- **Authentication μέσω LDAP:** Η πιστοποίηση των χρηστών γίνεται με τη χρήση κατάλληλων LDAP ερώτησεων.
- **Authorization LDAP**: Το authorization των χρηστών γίνεται και αυτό μέσω LDAP πρωτοκόλλου. Μέσω ενός attribute στον LDAP καθορίζεται η δυνατότητα πρόσβασης στην υπηρεσία τηλεφωνικής πρόσβασης.
- **Reply-Items στον LDAP:** οι παράμετροι σύνδεσης των χρηστών προσδιορίζονται από attributes που περιέχονται στο entry του χρήστη στον διακομιστή LDAP.
- **Ημερήσια, Εβδομαδιαία Όρια:** Μετρητές χρησιμοποιούνται για τον έλεγχο και επιβολή ημερήσιων και εβδομαδιαίων ορίων χρήσης του dial-up.
- **Υποστήριξη των μηχανισμών PAP, CHAP, MS-CHAP και EAP (EAP-MD5 και EAP-TLS):** Υποστηρίζονται όλες οι παραπάνω μέθοδοι αποστολής του συνθηματικού του χρήστη. Στην περίπτωση του PAP υποστηρίζεται πλήθος δυνατών μεθόδων κωδικοποίησης του συνθηματικού του χρήστη όπως cleartext, crypt, MD5 καθώς και SHA1.
- **Login-Time:** Καθορισμός του επιτρεπόμενου χρόνου σύνδεσης των χρηστών
- **Expiration Date:** Καθορισμός του χρόνου λήξης της ισχύος ενός συγκεκριμένου κωδικού χρήστη.
- **Double logins:** Ανίχνευση double-login (πολλαπλή πρόσβαση) των χρηστών
- **Authorization** με βάση τα Caller-Ids των χρηστών και τα IP addresses του access server στον οποίο συνδέονται (τοπική πρόσβαση)
- **Multi-threaded :** Ο ίδιος ο server καθώς και τα βασικά modules (LDAP,SQL κτλ) είναι πλήρως multithreaded με αποτέλεσμα τη δυνατότητα υποστήριξης σχεδόν απεριόριστου αριθμού αιτήσεων
- **Accounting σε mySQL βάση (όπως επίσης και σε πολλές άλλες βάσεις δεδομένων όπως Orcale, DB2, MSSQL κτλ).**
- **Web-based σύστημα διαχείρισης** (dialup-admin)

4.2 LDAP

4.2.1 **Authentication**

Η πιστοποίηση των χρηστών γίνεται μέσω ενός bind request στον διακομιστή LDAP με το login/password που παρέχει ο χρήστης κατά την σύνδεση. Κατά αυτόν τον τρόπο υποστηρίζονται όλοι οι τρόποι κρυπτογράφησης του password του χρήστη τους οποίους υποστηρίζει ο διακομιστής LDAP. Επιπλέον παρέχεται η δυνατότητα η αποστολή του login και του password στον ldap server να γίνει μέσω ασφαλούς σύνδεσης SSL.

4.2.2 **Authorization**

Για το authorization των χρηστών χρησιμοποιείται το objectclass **radiusprofile**, το οποίο παρέχει τα διάφορα attributes που σχετίζονται με το authorization. Ένα τέτοιο attribute για παράδειγμα είναι το dialupaccess, το οποίο εάν είναι FALSE ο χρήστης δεν επιτρέπεται να χρησιμοποιήσει την υπηρεσία. Το objectclass επίσης περιέχει και άλλα attributes, τα οποία είναι είτε check items τα οποία ελέγχονται κατά το authorization του χρήστη, είτε reply items με παραμέτρους σύνδεσης που επιστρέφονται στον access server εάν το authentication επιτύχει (π.χ., session-timeout, idle-timeout).

Ο αναλυτικός ορισμός του radiusprofile παρουσιάζεται παρακάτω:

LDAP Attribute	Περιγραφή	Τύπος (check/reply item
radiusSimultaneousUse	Ορίζει τον μέγιστό αριθμό από ταυτόχρονες συνδέσεις (όχι multilink) που μπορούν να γίνουν από ένα συγκεκριμένο χρήστη. Συνήθως λαμβάνει την τιμή 1 προκειμένου να αποκλείονται περιπτώσεις double login	check
radiusAuthType	Ορίζει τον τύπο του authentication που θα εκτελεστεί από τον radius server	check
radiusExpiration	Ορίζει την ημερομηνία κατά την οποία θα λήξει η πρόσβαση του χρήστη (είναι της μορφής 20 May 2002)	check
dialupaccess	Ορίζει το κατα πόσο ο χρήστης έχει πρόσβαση στην υπηρεσία dialup. Αν έχει την τιμή FALSE τότε η πρόσβαση του χρήστη στην υπηρεσία δεν επιτρέπεται. Αν έχει οποιαδήποτε άλλη τιμή τότε η πρόσβαση επιτρέπεται	check
radiusHint		check
radiusLoginTime	Ορίζει το χρονικό διάστημα (σε UUCP format) κατά το οποίο μπορεί να συνδεθεί ο αντίστοιχος χρήστης στην υπηρεσία	check
radiusarapfeatures		
radiusarapsecurity		
radiusarapzoneaccess		
radiuscallbackid		
radiuscallbacknumber		
radiuscalledstationid	Το τηλέφωνο στο οποίο καλεί ο χρήστης (DNIS)	check
radiuscallingstationid	Το τηλέφωνο από το οποίο γίνεται η κλήση (CLID)	check

radiusclass		
radiusfilterid		
radiusframedappletalklink		
radiusframedappletalknetwork		
radiusframedappletalkzone		
radiusframedcompression	Το πρωτόκολλο συμπίεσης το οποίο θα εφαρμοστεί στη σύνδεση. Το πλέον διαδεδομένο και συνηθισμένο πρστόκολλο είναι το Van-Jacobson-TCP-IP	reply
radiusframedipaddress	Η διεύθυνση IP η οποία θα αποδωθεί στον χρήστη	reply
radiusframedipnetmask	Η IP netmask που θα αποδωθεί στο χρήστη	reply
radiusframedipxnetwork		reply
radiusframedmtu	Το MTU της σύνδεσης	reply
radiusframedprotocol	Το πρωτόκολλο της σύνδεσης (συνήθως είναι PPP)	reply
radiusframedroute		reply
radiusframedrouting		reply
radiusidletimeout	Ο μέγιστος χρόνος για τον οποίο επιτρέπεται η σύνδεση του χρήστη να μείνει ανενεργή (idle)	reply
radiusloginiphost		reply
radiusloginlatgroup		reply
radiusloginlatnode		reply
radiusloginlatport		reply
radiusloginlatservice		reply
radiusloginservice		reply
radiuslogintcpport		reply
radiuspasswordretry		reply
radiusportlimit	Ο μέγιστος αριθμός απο διαθέσιμα κανάλια στον access server τα οποία μπορεί να ανοίξει ταυτόχρονα ο χρήστης σε μία mutlink σύνδεση	reply
radiusprompt		reply
radiusservicetype	Ο τύπος της σύνδεσης του χρήστη. Συνηθισμένες τιμές είναι Framed-User εφόσον η σύνδεση είναι τύπου Framed, Outbound-User για εξερχόμενες (από την πλευρά του access server) συνδέσεις και Login-User για συνδέσεις telnet	reply
radiussessiontimeout	Ο μέγιστος χρόνος που μπορεί να διαρκέσει η σύνδεση	reply
radiusterminationaction		reply
radiustunnelassignmentid		reply
radiustunnelclientendpoint		reply
radiustunnelmediumtype		reply
radiustunnelpassword		reply
radiustunnelpreference		reply
radiustunnelprivategroupid		reply
radiustunnelserverendpoint		reply
radiustunneltype		reply
radiusvsa		reply
radiuscheckitem	Γενικής φύσης attribute το οποίο μπορεί να χρησιμοποιηθεί για την αποθήκευση οποιουδήποτε check item. Η τιμή του πρέπει να είναι της μορφής <RADIUS attribute> <operator> <value> (πχ NAS-IP-Address := "194.63.239.238")	check
radiusreplyitem	Γενικής φύσης attribute το οποίο μπορεί να χρησιμοποιηθεί για την αποθήκευση οποιουδήποτε reply item. Η τιμή του πρέπει να είναι της μορφής <RADIUS attribute> <operator> <value> (πχ Cisco-AVPair := "lcp:send-secret=XXXXXX")	reply

Οι ρυθμίσεις που αφορούν τον κάθε χρήστη ορίζονται με τον συνδυασμό τεσσάρων προφίλ, του **User-Profile**, του **Default-Profile**, του **Regular-Profile** και του **προσωπικού προφίλ** του κάθε χρήστη. Το User-Profile συνήθως ορίζεται μέσα στο αρχείο users με βάση ελέγχους στα radius attributes που περιέχονται στο Access-Request πακέτο. Ορίζει το DN ενός entry το οποίο περιέχει ρυθμίσεις για μία συγκεκριμένη κατηγορία χρηστών. Αν είναι ορισμένο τότε το Default-Profile δεν λαμβάνεται υπόψη. Κατά αυτό τον τρόπο μπορεί να επιλέγεται ένα γενικό profile για τους χρήστες αναλόγως με τον τύπο της αιτούμενης σύνδεσης ή με βάση άλλα κριτήρια τα οποία μπορεί να ορίσει ο διαχειριστής της υπηρεσίας. Έτσι αιτήσεις με Service-Type=Framed-User θα έχουν διαφορετικές ρυθμίσεις (profiles) από τις αιτήσεις με Service-Type=Login-User. Το Default-Profile είναι ένα ξεχωριστό DN που ορίζεται στο αρχείο διαμόρφωσης του radius server και το οποίο (το default-profile entryt) περιέχει attributes που προσδιορίζουν τις προκαθορισμένες (default) ρυθμίσεις των χρηστών. Το Regular-Profile είναι ένα attribute που περιέχεται στα entries των χρηστών και το οποίο δείχνει σε κάποιο DN με ρυθμίσεις που αφορούν την ομάδα χρηστών στην οποία ανήκει ο χρήστης. Τέλος, το entry του κάθε χρήστη μπορεί να περιέχει attributes που διαφοροποιούν το προφίλ του συγκεκριμένου χρήστη από τις default ρυθμίσεις ή τις ρυθμίσεις ομάδας. Προφανώς, κατά το authorization του κάθε χρήστη οι παράμετροι της σύνδεσης προσδιορίζονται από τα τρία αυτά προφίλ, με σειρά φθίνουσας προτεραιότητας: προφίλ χρήστη, Regular-Profile, Default-Profile.

4.2.3 **Accounting**

Για το accounting συνήθως χρησιμοποιείται μία βάση mysql η οποία αποθηκεύει την σχετική πληροφορία. Πιο συγκεκριμένα, για τον σκοπό αυτό χρησιμοποιείται ο πίνακας **radacct** ο οποίος αποθηκεύει ένα row πληροφορίας για κάθε dial-up session.

Αμέσως μετά την επιτυχή πιστοποίηση του χρήστη ο access server στέλνει ένα Accounting-Start πακέτο στο radius server το οποίο περιέχει βασικές πληροφορίες για τη σύνδεση (την πόρτα στην οποία συνδέθηκε ο χρήστης, ο αριθμός τηλεφώνου απο τον οποίο συνδέθηκε κτλ) το οποίο και χρησιμοποιείται για τη δημιουργία ενός νέου row στον πίνακα radacct το οποίο και περιέχει τις πληροφορίες αυτές. Μετά την αποσύνδεση του χρήστη ο access server στέλνει ένα Accounting-Stop πακέτο το οποίο περιέχει πλήθος πληροφοριών για τη σύνδεση όπως την ip address, τα bytes που παραλήφθηκαν και στάλθηκαν κτλ.

Οι πληροφορίες αυτές χρησιμοποιούνται για να ανανεωθεί η αντίστοιχη εγγραφή στον πίνακα radacct. Σε περίπτωση που έχει ενεργοποιηθεί κάτι τέτοιο στον access server μετά την επιτυχή σύνδεση του χρήστη ο access server μπορεί να στείλει ένα Accounting-Update το οποίο να περιέχει πληροφορίες για το χρήστη οι οποίες δεν ήταν διαθέσιμες κατά την πιστοποίηση του (όπως πχ η IP address που του παραχωρήθηκε).

Σημειώνεται ότι εάν το session-time μιας σύνδεσης είναι 0, το session δεν θεωρείται επιτυχές και το αντίστοιχο row δεν αποθηκεύεται από την accounting διαδικασία στον πίνακα. Αυτό τυπικά συμβαίνει σε περιπτώσεις ανεπιτυχούς authentication. Πάντως, ο πίνακας (όπως αναφέρεται παρακάτω) μπορεί να περιέχει rows με session-time=0, τα οποία εισάγονται από άλλες διαδικασίες (bad login)

Η δομή του πίνακα radacct φαίνεται παρακάτω:

Πεδίο	Τύπος	Περιγραφή
RadAcctId	bigint(21)	Το ID του κάθε row
AcctSessionId	varchar(32)	Το Session ID της κάθε σύνδεσης
AcctUniqueId	varchar(32)	Αν έχει ενεργοποιηθεί το acct_unique module του freeradius το πεδίο αυτό θα περιέχει ένα μοναδικό id για τη σύνδεση αυτή
UserName	varchar(64)	Το username του χρήστη
Realm	varchar(64)	Το realm στο οποίο ανήκει ο χρήστης. Αν δεν ανήκει σε κάποιο τότε το πεδίο αυτό παραμένει κενό
NASIPAddress	varchar(15)	Η IP Address του access server στον οποίο συνδέθηκε ο χρήστης
NASPortId	int(12)	Η πόρτα του access server στην οποία συνδέθηκε ο χρήστης
NASPortType	varchar(32)	Ο τύπος της πόρτας στην οποία έγινε η σύνδεση
AcctStartTime	datetime	Ο χρόνος έναρξης της σύνδεσης
AcctStopTime	datetime	Ο χρόνος λήξης της σύνδεσης
AcctSessionTime	int(12)	Ο συνολικός χρόνος της σύνδεσης
AcctAuthentic	varchar(32)	
ConnectInfo_start	varchar(32)	
ConnectInfo_stop	varchar(32)	
AcctInputOctets	bigint(12)	Ο συνολικός αριθμός των bytes που εισήλθαν στον access server στη σύνδεση
AcctOutputOctets	bigint(12)	Ο συνολικός αριθμος των bytes που αποστάλθηκαν προς τον χρήστη
CalledStationId	varchar(30)	Ο αριθμός τηλεφώνου τον οποίο κάλεσε ο χρήστης
CallingStationId	varchar(30)	Ο αριθμός τηλεφώνου από τον οποίο έγινε η κλήση για την πραγματοποίηση της σύνδεσης
AcctTerminateCause	varchar(32)	Ο λόγος λήξης της σύνδεσης (πχ User-Request, Session-Timeout κτλ)
ServiceType	varchar(32)	Ο τύπος της σύνδεσης (px Framed-User, Outbound-User)
FramedProtocol	varchar(32)	Ο τύπος του πρωτοκόλλου που χρησιμοποιήθηκε εφόσον η σύνδεση ήταν τύπου Framed (συνήθως είναι PPP)
FramedIPAddress	varchar(15)	Η IP Address που αποδώθηκε στο χρήστη
AcctStartDelay	int(12)	Η καθυστέρηση που παρουσιάστηκε κατά την αποθήκευση του Accounting-Start

AcctStopDelay	int(12)	Η καθυστέρηση που παρουσιάστηκε κατά την αποθήκευση του Accounting-Stop

4.2.4 **Μετρητές**

Το σύστημα παρέχει δυνατότητα μετρητών για authorization και accounting χρήση σε ωριαία, ημερήσια, εβδομαδιαία και μηνιαία βάση. Αυτή την στιγμή χρησιμοποιούνται μόνο ημερήσιοι και εβδομαδιαίοι μετρητές. Ο κάθε ένας από αυτούς τους μετρητές χρησιμοποιεί ένα attribute (**Max-Daily-Session, Max-Weekly-Session** αντίστοιχα) που ορίζει το μέγιστο όριο ημερισίου/εβδομαδιαίου χρόνου που δικαιούται ο κάθε χρήστης, το οποίο και περιέχεται στο entry του χρήστη στον LDAP. Το attribute αυτό θα πρέπει να γίνεται map σε αντίστοιχο attribute στον LDAP το οποίο να έχει προστεθεί και στο LDAP schema του LDAP server.

Οι ημερήσιοι και εβδομαδιαίοι μετρητές χρησιμοποιούνται κατά το authorization για να επιστρέψουν το υπόλοιπο του ημερησίου/εβδομαδιαίου χρόνου του χρήστη. Κατά το authorization, η τιμή του ημερησίου/εβδομδιαίου μετρητή αφαιρείται από το ημερήσιο/εβδομαδιαίο όριο. Με τον τρόπο αυτό υπολογίζεται και επιστρέφεται το Session-Timeout της σύνδεσης, που δηλώνει το μέγιστο χρόνο που επιτρέπεται να μείνει συνδεδεμένος ο χρήστης. Η τιμή του μετρητή ενημερώνεται όταν ο χρήστης κάνει logout προσθέτοντας στην προηγούμενη τιμή την χρονική διάρκεια του νέου session.

Ειδικές περιπτώσεις αποτελούν οι περιπτώσεις αλλαγής ημέρας/εβδομάδας. Συγκεκριμένα:

- Εάν ένας χρήστης κάνει login κάποια στιγμή πριν τις 00:00 και ο χρόνος που του απομένει είναι πέραν τις αλλαγής μέρας, το Session-Timeout υπολογίζεται ως ο χρόνος που απομένει ως τις 00:00 συν το Max-Daily-Session.
- Εάν ο χρήστης κάνει logout μετά την αλλαγή της ημέρας/εβδομάδας, ο μετρητής της μέρας/εβδομάδας τίθεται στο χρονικό διάστημα από την αλλαγή ως την στιγμή της αποσύνδεσης.
- Στις υπόλοιπες περιπτώσεις, οι μετρητές μηδενίζονται στην αλλαγή της ημέρας/εβδομάδας (στις 00:00 κάθε μέρας και στις 00:00 της Κυριακής αντίστοιχα).

Οι ημερήσιοι και εβδομαδιαίοι μετρητές κρατιούνται σε ξεχωριστό DBM αρχείο. Ουσιαστικά πρόκειται για διαφορετικά instances του ίδιου module με διαφορετικό configuration προκειμένου το ένα να κάνει reset ανά μήνα και το άλλο ανά εβδομάδα.

4.3 ΕΓΚΑΤΑΣΤΑΗ-ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ

Η εγκατάσταση της υπηρεσίας περιλαμβάνει δύο σκέλη: το compilation του distribution με ενεργοποίηση των απαραίτητων επιλογών για υποστήριξη ldap authentication/authorization και mysql accounting και την παραμετροποίηση των αρχείων διαμόρφωσης του server.

4.3.1 **Compilation**

Η διαδικασία compilation του radius server είναι σχετικά απλή. Αφού γίνει μεταφόρτωση του distribution του radius server στον αρχικό κατάλογο εκτελούμε το αρχείο configure ως εξής:

./configure --prefix=/usr/local/radiusd –with-localstatedir=/var/radiusd --with-rlm-ldap-lib-dir=/usr/local/openldap/lib --with-rlm-ldap-include-dir=/usr/local/openldap/include --with-mysql-lib-dir=/usr/local/mysql/lib/mysql --with-mysql-include-dir=/usr/local/mysql/include –enable-snmp

Η αποστολή των παραμέτρων που δίνονται ως ορίσματα προς το configure είναι προφανής. Στη συνέχεια τρέχουμε τις εντολές make και make install. Εφόσον δεν υπήρξε πρόβλημα ο radius server θα έχει εγκατασταθεί κάτω από τον κατάλογο /usr/local/radiusd με τα log files να περιέχονται στον κατάλογο /var/radiusd.

Στη συνέχεια από τον κατάλογο src/modules/rlm_sql/drivers/rlm_sql/mysql χρησιμοποιούμε το αρχείο db_mysql.sql για να προσθέσουμε τους ορισμούς των πινάκων της SQL βάσης του radius server στον mysql server. Προηγουμένως θα πρέπει να έχει προφανώς δημιουργηθεί η βάση radius στον SQL server.

4.3.2 **Δομή Εγκατάστασης**

radiusd/:
radiusd/bin: Περιέχει τα διάφορα προγράμματα αλληλεπίδρασης με το radius server
radiusd/etc:
radiusd/etc/raddb: Περιέχει όλα τα αρχεία διαμόρφωσης του radius server
radiusd/lib: Περιέχει τα modules του radius server με τη μορφή DLLs.
radiusd/man: Περιέχει τις man pages για το radius server καθώς και για τα προγράμματα που περιέχονται στον κατάλογο bin
radiusd/man/man1:
radiusd/man/man5:
radiusd/man/man8:
radiusd/sbin: Στον κατάλογο αυτό περιέχεται το εκτελέσιμο του radius server.
/var/radiusd: Στον κατάλογο αυτό καταγράφονται τα log files της υπηρεσίας.

4.3.3 **Παραμετροποίηση**

Η παραμετροποίηση των αρχείων διαμόρφωσης της υπηρεσίας περιλαμβάνει την διαμόρφωση των εξής σημείων στα παρακάτω αρχεία:

clients.conf: Στο αρχείο αυτό προστίθενται εγγραφές για κάθε radius client ο οποίος απαιτείται να κάνει ερωτήσεις στο radius server. Κάθε εγγραφή είναι της μορφής:

```
client 147.102.220.5 {
      secret = mysecret
      shortname = client1
     nastype = other
}
```

Το nastype περιέχει τον τύπο του access server. Η παράμετρος αυτή είναι απαραίτητη κατά τον έλεγχο πολλαπλής πρόσβασης (double login detection) καθώς αυτή προσδιορίζει τον τύπο του

access server και άρα την μέθοδο με την οποία θα ερωτηθεί προκειμένου να προσδιοριστεί κατά πόσον ο χρήστης είναι ήδη συνδεδεμένος. Σε περίπτωση που ο access server είναι cisco μπορεί να δωθεί η τιμή cisco στην παράμετρο nastype. Αν ο access server είναι άλλου τύπου ο διαχειριστής θα πρέπει να συμβουλευτεί τα σχόλια που περιλαμβάνονται στο αρχείο προκειμένου να βρεί τον τύπο που πρέπει να χρησιμοποιήσει.

Είναι απαραίτητο να υπάρχει τουλάχιστον μία εγγραφή για κάθε access server ο οποίος θα χρησιμοποιεί το radius server για AAA. Επιπλέον καλό είναι να προστεθεί ένα entry για το localhost για την εύκολη πραγματοποίηση πειραμάτων καθώς και ένα entry για τον υπολογιστή στον οποίο είναι εγκατεστημένη η εφαρμογή web διαχείρισης dialup_admin προκειμένου να είναι δυνατή η λειτουργία των σελίδων 'Check Server' και 'Test User'.

snmp.conf: Στο αρχείο αυτό γίνεται η παραμετροποίηση του snmp interface που παρέχει ο radius server. Ουσιαστικά απαιτείται μόνο η προσθήκη μίας εγγραφής για το smux server στον οποίο θα συνδεθεί ο radius server ως εξής:

smux_password = sec

sql.conf: Στο αρχείο αυτό γίνεται η παραμετροποίηση του sql module του radius server. Παρακάτω παρατίθενται οι παράμετροι οι οποίοι θα πρέπει να αλλαχθούν για τη σωστή λειτουργία του sql module:

```
# Database type
# Current supported are: rlm_sql_mysql, rlm_sql_postgresql, rlm_sql_iodbc, rlm_sql_oracle
driver = "rlm_sql_mysql"

# Connect info
server = "localhost"
login = "root"
password = ""

# Database table configuration
radius_db = "radius"

# If you want both stop and start records logged to the
# same SQL table, leave this as is.  If you want them in
# different tables, put the start table in acct_table1
# and stop table in acct_table2
acct_table1 = "radacct"
acct_table2 = "radacct"

authcheck_table = "radcheck"
authreply_table = "radreply"

groupcheck_table = "radgroupcheck"
groupreply_table = "radgroupreply"

usergroup_table = "usergroup"

# Remove stale session if checkrad does not see a double login
deletestalesessions = yes
```

 # Print all SQL statements when in debug mode (-x)
sqltrace = yes
sqltracefile = ${logdir}/sqltrace.sql

 # number of sql connections to make to server
num_sql_socks = 5

Οι κύριες παράμετροι οι οποίες θα πρέπει να αλλαχθούν είναι το *server* το οποίο ορίζει τον SQL server στον οποίο θα συνδεθεί το module, το *login,password* που ορίζει το login και το password με το οποίο θα γίνει η σύνδεση στον SQL server, το *radius_db* που ορίζει το όνομα της βάσης του radius server (κανονικά θα πρέπει να παραμείνει το όνομα radius) και το *num_sql_socks* που ορίζει τον αριθμό των συνδέσεων τις οποίες θα διατηρεί το sql module με τον SQL server. Όσο μεγαλύτερη κίνηση προβλέπεται να έχει ο radius server τόσο μεγαλύτερη θα πρέπει να τεθεί η μεταβλητή αυτή. Θα πρέπει να είναι κατ ελάχιστο ίση με τον αριθμό των radius server threads που έχουν οριστεί στο radiusd.conf.

naspasswd: Στο αρχείο αυτό προστίθεται μία γραμμή για κάθε access server. Το αρχείο αυτό επίσης χρησιμοποιείται κατά τον έλεγχο των double logins και η μορφή του είναι ως εξής:

server- name SNMP community

όπου *server-name* είναι η IP ή το domain name του access server και *community* είναι το SNMP community για RO SNMP κλήσεις στον access server αυτόν.

radiusd.conf: Το βασικό αρχείο διαμόρφωσης του radius server. Το αρχείο περιέχει ένα μεγάλο όγκο από χρήσιμα σχόλια τα οποία βοηθούν στην κατανόηση του προορισμού της κάθε παραμέτρου. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στα εξής σημεία στο αρχείο:

```
ldap ldap1{
        server = "nic450.att.sch.gr"
        identity = "cn=Directory Manager"
        password = "XXXXXX"
        basedn = "dc=sch,dc=gr"
        filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
        default_profile = "uid=default-dialup,ou=people,dc=sch,dc=gr"
        access_attr = "dialupAccess"
        profile_attribute = "dialupRegularProfile"
        dictionary_mapping = ${raddbdir}/ldap.attrmap
        timeout = 4
        timelimit = 3
        net_timeout = 1
        ldap_debug = 0x0000
        ldap_connections_number = 5
       #password_header = "{clear}"
        #password_attribute = userPassword
        #groupname_attribute= cn
       #groupmembership_filter="(|(&(objectClass=GroupOfNames)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))"
        #groupmembership_attribute = radiusGroupName
      }
```

Στο σημείο αυτό γίνεται η διαμόρφωση του ldap module. Η χρήση των παραπάνω παραμέτρων είναι η εξής:

- *server:* Ο ldap server στον οποίο θα συνδεθεί το ldap module
- *identity,password:* Το DN/Password με το οποίο θα κάνει bind το ldap module στον ldap server.
- *basedn:* Το DN το οποίο θα χρησιμοποιηθεί ως base στις αναζητήσεις που πραγματοποιούνται στον ldap.
- *filter:* Το φίλτρο με το οποίο γίνονται οι αναζητήσεις. Η παράμετρος '%{Stripped-User-Name:-%{User-Name}}' αντικαθίσταται κάθε φορά απο το username του χρήστη.
- *default_profile:* Το DN του Default-Profile entry που περιγράφηκε παραπάνω.
- *access_attr:* Το attribute το οποίο ορίζει την δυνατότητα του χρήστη να χρησιμοποιήσει την υπηρεσία dialup. Στην περίπτωση που το attribute αυτό δεν υπάρχει στο entry του χρήστη η πρόσβαση δεν επιτρέπεται.
- *profile_attribute:* Το attribute στο entry του κάθε χρήστη το οποίο και δείχνει στο DN του Regular-Profile entry το οποίο περιγράφηκε παραπάνω. Δεν είναι απαραίτητο το attribute αυτό να υπάρχει στο entry του χρήστη.
- *dictionary_mapping:* Ορίζει που βρίσκεται το αρχείο στο οποίο γίνονται map τα RADIUS attributes σε LDAP attributes. Το αρχείο αυτό είναι της μορφής:
- *ldap_connections_number:* Ο αριθμός των συνδέσεων οι οποίες θα γίνουν με τον εξυπηρετητή LDAP. Θα πρέπει κανονικά να είναι ίσο με τον αριθμό των server threads που έχει οριστεί πιο πριν στο radiusd.conf
- *password_attribute:* Το LDAP attribute το οποίο περιέχει το password του user entry. Αν δεν είναι κενό τότε γίνεται extraction του password προκειμένου να χρησιμοποιηθεί κατά τη φάση του authentication (για παράδειγμα από τα chap και pap modules).
- *password_header:* Αν δεν είναι κενό τότε ορίζει το password header το οποίο θα πρέπει να παραληφθεί κατά το extraction του password.

```
counter daily{
        filename = ${localstatedir}/db.day
        key = User-Name
        count-attribute = Acct-Session-Time
        reset = daily
        counter-name = Daily-Session-Time
        check-name = Max-Daily-Session
        allowed-servicetype = Framed-User
}
```

Στο σημείο αυτό γίνεται η διαμόρφωση του counter module το οποίο και εφαρμόζει τα ημερήσια και εβδομαδιαία όρια χρήσης. Παραπάνω φαίνεται η διαμόρφωση του module για ημερήσια όρια χρήσης. Η χρήση των παραπάνω παραμέτρων έχει ως εξής:

- *filename:* Το αρχείο στο οποίο διατηρούνται οι μετρητές για κάθε χρήστη.
- *reset:* Κάθε πότε γίνεται η αρχικοποίηση των μετρητών. Μπορεί να πάρει τις τιμές 'daily','weekly' και 'monthly'.
- *check-name:* Το attribute το οποίο ορίζει το όριο χρήσης. Μπορεί να πάρει τις τιμές 'Max-Daily-Session','Max-Weekly-Session','Max-Monthly-Session'.

```
# PAP module to authenticate users based on their stored password
#
#  Supports multiple encryption schemes
#  clear: Clear text
#  crypt: Unix crypt
#    md5: MD5 ecnryption
#   sha1: SHA1 encryption.
#  DEFAULT: crypt
pap {
      encryption_scheme = crypt
}
```

Στο σημείο αυτό γίνεται η διαμόρφωση του pap module το οποίο και επιτρέπει τον έλεγχο του password του χρήστη με ένα ήδη διαθέσιμο κρυπτογραφημένο password (το οποίο έχει εξαχθεί για παράδειγμα μέσω του ldap module από την εγγραφή του χρήστη). Υποστηρίζεται μόνο μία παράμετρος:

- *encryption_scheme:* Το σχήμα κρυπτογράφησης που χρησιμοποιείται. Μπορεί να είναι *clear* για απουσία κρυπτογράφησης, *crypt* για τη *unix* crypt, *md5* για MD5 και *sha1* για SHA1.

```
chap {
}
```

Στο σημείο αυτό γίνεται η διαμόρφωση του chap module το οποίο και επιτρέπει την πιστοποίηση χρηστών που συνδέονται με χρήση του πρωτοκόλλου CHAP εφόσον είναι διαθέσιμο το password του χρήστη σε clear text μορφή (έχει εξαχθεί για παράδειγμα μέσω του ldap module από την εγγραφή του χρήστη).

```
checkval nas-check{
      item-name = "NAS-IP-Address"
      check-name = "NAS-IP-Address"
      data-type = "ipaddr"
}
```

Στο σημείο αυτό γίνεται η διαμόρφωση του checkval module το οποίο και επιτρέπει την εξουσιοδότηση ενός χρήστη μόνο αν ένα attribute στο Access-Request απο τον access server περιέχει μία συγκεκριμένη τιμή. Κατά αυτόν τον τρόπο είναι δυνατή η εξουσιοδότηση ενός χρήστη μόνο στην περίπτωση που καλεί από ένα συγκεκριμένο τηλέφωνο ή προσπαθεί να συνδεθεί σε ένα συγκεκριμένο access server. Η χρήση των παραμέτρων έχει ώς εξής:

item-name: Το attribute το οποίο θα αναζητηθεί για να γίνει η σύγκριση. Εάν το attribute αυτό δεν περιέχεται στο Access-Request τότε επιτρέπεται η σύνδεση.
check-name: Το attribute με την τιμή του οποίου θα γίνει η σύγκριση. Το attribute αυτό θα πρέπει να περιέχεται στο entry του χρήστη στο ldap και γίνεται διαθέσιμο αυτόματα από το ldap module. Αν το attribute αυτό είναι διαθέσιμο πολλές φορές, ο έλεγχος γίνεται για κάθε τιμή που είναι διαθέσιμη.
data-type: Ο τύπος των δεδομένων. Μπορεί να είναι ‘string’ για κείμενο, ‘integer’ για νούμερο, ‘ipaddr’ για IP address, ‘date’ για ημερομηνία και ‘octets’ για binary πληροφορία.

Πιθανές περιπτώσεις όπου μπορεί να χρησιμοποιηθεί το module αυτό είναι οι παρακάτω:

- Την εξουσιοδότηση ενός χρήστη μόνο αν συνδέεται από ένα (ή περισσότερους) τηλεφωνικό αριθμό. Για τον σκοπό αυτό κάθε user entry θα πρέπει να περιέχει ένα ή περισσότερα attributes radiuscallingstationid τα οποία περιέχουν τα νούμερα από τα οποία επιτρέπεται να συνδέεται ο χρήστης.
- Την εξουσιοδότηση ενός χρήστη μόνο αν συνδέεται σε ένα συγκεκριμένο access server. Για κάθε χρήστη προστίθενται δύο attributes στο entry του:
  radiusCheckItem=NAS-IP-Address := "194.63.239.238"
  radiusCheckItem=NAS-IP-Address := "255.255.255.255"

  Το πρώτο attribute περιέχει την IP διεύθυνση του access server από τον οποίο μπορεί να συνδέεται ο χρήστης ενώ το δεύτερο χρησιμοποιείται για να μπορεί να λειτουργεί η σελίδα 'Test User' στο περιβάλλον dialup_admin.

Πιο συγκεκριμένα οι λειτουργίες του radius server είναι οι εξής:

- *instantiate:* Η αρχικοποίηση των modules. Στο section αυτό θα πρέπει να προστεθούν modules τα οποία θα πρέπει να αρχικοποιηθούν πριν από τα υπόλοιπα όπως για παράδειγμα το counter module που πρέπει να κάνει register το check-name attribute.
- *authenticate:* Ο έλεγχος του password του χρήστη. Στην παραπάνω περίπτωση για τον έλγχο αυτό χρησιμοποιείται το ldap module. Αντί του ldap module είναι δυνατόν να χρησιμοποιείται το pap module εφόσον έχει διαμορφωθεί το ldap module να κάνει εξαγωγή του password του χρήστη κατά την φάση του authorization.
- *authorize:* Στο σημείο αυτό γίνεται ο έλεγχος της πρόσβασης του χρήστη (η πρόσβαση επιτρέπεται από το dialupaccess attribute, ο χρήστης δεν έχει υπερβεί το μέγιστο ημερήσιο/εβδομαδιαίο χρόνο χρήσης κτλ) καθώς και η προσθήκη των απαραίτητων radius attributes που θα περιέχονται στην απάντηση στον access server (session-timeout, service-type κτλ).
- *accounting:* Η καταγραφή πληροφοριών για τα sessions των χρηστών με βάση τις πληροφορίες που περιέχονται στα Accounting-Start και Accounting-Stop πακέτα.
- *session:* Στο σημείο αυτό γίνεται ο έλεγχος αν απαιτείται για πολλαπλή πρόσβαση του χρήστη (ο έλεγχος γίνεται μόνο αν είναι ορισμένο το Simultaneous-Use attribute για το χρήστη).
- *postauth:* Η λειτουργία αυτή εκτελείται μετά την επιτυχή πιστοποίηση του χρήστη. Εδώ προστίθενται modules όπως το ippool module το οποίο χρησιμοποιείται για server side ip pool management.

Το keyword redundant είναι ειδικό και χρησιμοποιείται προκειμένου να υλοποιείται μηχανισμός fallback. Όσα modules περιέχονται σε ένα redundant section θα δοκιμάζονται το ένα μετά το άλλο μέχρι ένα από αυτά να μην αποτύχει.

users: Το αρχείο στο οποίο ορίζονται οι γενικές περιπτώσεις authentication. Προκειμένου να γίνεται επεξεργασία του αρχείου αυτού θα πρέπει να είναι ενεργοποιημένο το module files και να έχει προστεθεί στο authorization section. Περισσότερες πληροφορίες για τη διαμόρφωση του αρχείου υπάρχουν στο αντίστοιχο manpage καθώς και στο sample αρχείο που περιέχεται στο distribution. Σε γενικές γραμμές το αρχείο θα πρέπει να είναι της μορφής:

DEFAULT Auth-Type = FailOver, Simultaneous-Use := 1

Fall-Through = 1

DEFAULT Service-Type == NAS-Prompt-User
Fall-Through = 1

DEFAULT Service-Type == Framed-User, Framed-Protocol == PPP, User-Profile := "uid=default-dialup,ou=people,dc=sch,dc=gr"
Port-Limit = 1,
Session-Timeout = 14400,
Idle-Timeout = 600,
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-Compression = Van-Jacobson-TCP-IP,
Framed-IP-Address = 255.255.255.254,
Framed-IP-Netmask = 255.255.255.255,
Framed-MTU = 1500

DEFAULT Service-Type == Framed-User, Framed-Protocol == SLIP
Framed-Protocol = SLIP

DEFAULT Service-Type == Outbound-User, User-Profile := ""

4.3.4 **Προληπτικός και Κατασταλτικός Έλεγχος**

Ο έλεγχος της καλής λειτουργίας της υπηρεσίας ουσιαστικά περιλαμβάνει την πιστοποίηση ότι οι radius servers τρέχουν κανονικά και ότι επιστρέφουν τα σωστά attributes για τους χρήστες. Εφόσον η υπηρεσία στηρίζεται για την πιστοποίηση των χρηστών και για την καταγραφή του accounting σε εξωτερικές υπηρεσίες (όπως η υπηρεσία ldap και οι διακομιστές mysql) είναι απαραίτητο αν εμφανίζονται προβλήματα να ερευνάται η πιθανότητα να υπάρχει πρόβλημα με κάποια από αυτές τις υπηρεσίες.

Σε περίπτωση που οι υπηρεσίες αυτές λειτουργούν κανονικά κα συνεχίζει να παρουσιάζεται πρόβλημα στη λειτουργία της υπηρεσίας μπορεί να χρησιμοποιηθεί η λειτουργία ‘Check Server’ που παρέχεται από το εργαλείο web διαχείρισης (dialup_admin). Η λειτουργία αυτή θα πρέπει να είναι επιτυχής και να επιστρέψει τις σωστές τιμές για τα διάφορα radius attributes.

Σε περίπτωση που είναι ανεπιτυχής θα πρέπει να ελεγχθεί ότι η διεργασία του radius server τρέχει κανονικά και αν απαιτηθεί να γίνει επανεκκίνηση της

Σε περίπτωση που η λειτουργία επιστρέφει λάθος radius attributes θα πρέπει να ελεγχθεί εάν λειτουργεί κανονικά η υπηρεσία καταλόγου και ότι δεν έχει γίνει κάποια αλλαγή στη διαμόρφωση της υπηρεσίας που δεν έχει ανακοινωθεί. Πέραν των παραπάνω καλό είναι να γίνεται έλεγχος της διαθέσιμης χωρητικότητας στους δίσκους στους οποίους κρατούνται τα logs της υπηρεσίας καθώς και στους δίσκους στους οποίους αποθηκεύονται οι πίνακες της mysql βάσης.

4.3.5 **FAQ Υπηρεσίας**

Ο χρήστης αναφέρει πρόβλημα με το password του

Αρχικά μέσα από την κεντρική σελίδα διαχείρισης του χρήστη στο περιβάλλον dialup_admin μπορούν να αντληθούν χρήσιμες πληροφορίες για το χρήστη. Θα πρέπει να δοθεί ιδιαίτερη

προσοχή στο πεδίο'Useful User Description' το οποίο εάν ο κωδικός του χρήστη έχει ξεπεράσει τα όρια χρήσης ή είναι κλειδωμένος θα είναι κόκκινο και θα περιέχει ανάλογο κείμενο περιγραφής.
Σε περίπτωση που το πεδίο αυτό δεν περιέχει κάποια χρήσιμη πληροφορία θα πρέπει να ελέγχεται η σελίδα που περιέχει το accounting του χρήστη. Εάν υπήρξε πρόβλημα στις τελευταίες συνδέσεις του χρήστη τότε οι αντίστοιχες εγγραφές θα εμφανίζονται με κόκκινο χρώμα ενώ ο λόγος της αποτυχίας θα εμφανίζεται στο πεδίο 'terminate cause'. Συνήθεις περιπτώσεις προβλημάτων είναι:

- Αποτυχημένο password
- Υπέρβαση ορίου χρήσης (ημερήσιου, εβδομαδιαίου κτλ)
- Πολλαπλή πρόσβαση
- Κλήση έξω από επιτρεπόμενο διάστημα

Στην περίπτωση που το πρόβλημα έχει να κάνει με το password του χρήστη από την κεντρική σελίδα διαχείρισης μπορεί να γίνει επαλήθευση του password, ενώ από τη σελίδα δοκιμών ('Test User') μπορεί να γίνει επαλήθευση της διαδικασίας login όπως αυτή λαμβάνει χώρα στον radius server.

4.3.6 **Πολιτική Ασφάλειας**

Το RADIUS πρωτόκολλο εκ φύσεως προσφέρει ασφαλή τρόπο μεταφοράς των ευαίσθητων δεδομένων των χρηστών (passwords) καθώς γίνεται κρυπτογράφηση στα δεδομένα αυτά με χρήση του secret key επικοινωνίας radius server <-> access server (NAS). Επιπλέον κατά την πιστοποίηση του χρήστη απο τον LDAP είναι δυνατόν να δημιουργείται ασφαλές κανάλι επικοινωνίας SSL μέσω του οποίου να γίνεται η αποστολή του username/password του χρήστη για την πιστοποίηση του.

Επιπλέον είναι απαραίτητο να επιτρέπονται αιτήσεις μόνο από συγκεκριμένους πελάτες οι οποίοι και θα είναι καταγραμμένοι στο αρχείο clients.conf όπως αναφέρθηκε παραπάνω. Οι πελάτες αυτοί θα πρέπει να είναι μόνο οι access servers οι οποίοι χρησιμοποιούν το RADIUS server για λειτουργίες AAA, το localhost καθώς και όποιοι άλλοι πελάτες είναι δυνατόν να κάνουν ερωτήσεις στο RADIUS server όπως για παράδειγμα ο υπολογιστής στον οποίο είναι εγκατεστημένη η εφαρμογή web based διαχείρισης dialup_admin.

Καλό θα ήταν να αποκλειστεί μέσω ACIs στους αντίστοιχους δρομολογητές η δυνατότητα αποστολής RADIUS πακέτων στο διακομιστή από πελάτες πέραν των ήδη γνωστών.

4.3.7 **Αντίγραφα ασφαλείας**

Η πολιτική αντιγράφων ασφαλείας θα πρέπει να είναι η εξής:

- Δημιουργία αντίγραφου ασφαλείας της αρχικής εγκατάστασης, αμέσως μετά το πέρας της εγκατάστασης.
- Διατήρηση αντιγράφων ασφαλείας του καταλόγου που περιέχει τα αρχεία διαμόρφωσης της υπηρεσίας (etc/raddb) κάθε εβδομάδα σε βάθος ενός μήνα.

4.4 ΕΙΔΙΚΑ ΘΕΜΑΤΑ

4.4.1 Large Scale Dialout

Το Large Scale Dialout υλοποιείται με τη χρήση του RADIUS πρωτοκόλλου και κατάλληλων ερωτήσεων από την πλευρά των access servers. Πιο συγκεκριμένα για κάθε access server (NAS) διατηρούνται entries με όνομα NAS-1,NAS-2 κτλ τα οποία και περιέχουν routes προς κάθε προορισμό που είναι προσπελάσιμος από τον access server αυτόν. Κάθε entry μπορεί να περιέχει μέχρι 50 τέτοια routes. Η μορφή του κάθε entry είναι όπως παρακάτω:

NAS-1 Password = “cisco”, Service-Type = Outbound-User
Cisco-AVPair = “ip:route=20.1.3.0 255.255.255.0 172.31.229.41 200”,
Cisco-AVPair = “ip:route=20.1.2.0 255.255.255.0 172.31.229.31 200”,
Cisco-AVPair = “ip:route=20.1.1.0 255.255.255.0 172.31.229.41 200”,
Cisco-AVPair = “ip:route=172.31.229.41 255.255.255.255 Dialer1 200 name echo-8.cisco.com”

Για κάθε προορισμό διατηρείται επίσης ένα entry το οποίο περιέχει τον αριθμό τηλεφώνου που θα πρέπει να κληθεί, το συνθηματικό εισόδου καθώς και την IP για το interface το οποίο θα δημιουργηθεί. Το όνομα των entries αυτών πρέπει πάντα να λήγει σε ‘-out’ και η μορφή τους είναι όπως παρακάτω:

Echo-8.cisco.com-out Password=”cisco”, Service-Type = Outbound-User
Cisco-AVPair = “outbound:addr*172.31.229.41”
Cisco-AVPair = “outbound:dial-number=60039”
Cisco-AVPair = “outbound:send-secret=secret"

Το password για τα entries του LSD πρέπει να είναι πάντα ‘cisco’.

4.4.2 Multilink

Δύο attributes ορίζουν τις Multilink δυνατότητες του κάθε χρήστη: Το Port-Limit και το Simultaneous-Use. Το πρώτο ορίζει πόσα κανάλια μπορεί να ανοίξει ο χρήστης. Το δεύτερο ορίζει τον αριθμό των logins που μπορεί να κάνει συγχρόνως ο κάθε χρήστης. Εάν ο χρήστης συνδέεται με multilink και αιτεί αριθμό καναλιών μικρότερο ή ίσο απο το Port-Limit που αντιστοιχεί στο χρήστη τότε η αίτηση του γίνεται αποδεκτή.

4.4.3 RADIUS Server Fail Over

Είναι δυνατόν να εγκατασταθούν παραπάνω από ένας RADIUS servers προκειμένου να επιτευχθεί μεγαλύτερη διαθεσιμότητα από την υπηρεσία. Πέραν των ίδιων των εξυπηρετητών RADIUS είναι απαραίτητο να υπάρχει υψηλη διαθεσιμότητα και στις χρησιμοποιούμενες βάσεις, δηλαδή στη βάση του RADIUS καί στη βάση της MySQL. Αναφορικά με τη βάση LDAP μπορεί να υλοποιηθεί replication στην υπηρεσία χρησιμοποιώντας τις δυνατοτήτες που προσφερουν τα

αντίστοιχα πακέτα λογισμικού. Ως αναφορά την MySQL (δηλαδή το accounting) είναι δυνατόν να χρησιμοποιηθούν οι δυνατότητες που προσφέρει ο ίδιος ο freeradius για αυτή τη λειτουργία. Πιο συγκεκριμένα στο distribution του freeradius περιλαμβάνεται και το utility radrelay. Η λειτουργία του παραπάνω προγράμματος είναι να διαβάζει συνεχώς ένα accounting detail αρχείο και να στέλνει τα δεδομένα που περιλαμβάνονται σε αυτό σε έναν απομακρυσμένο RADIUS server. Αν ληφθεί επιβεβαίωση για τα δεδομένα τότε αυτά διαγράφονται από το αντίστοιχο detail αρχείο. Κατά αυτόν τον τρόπο εφόσον ο απομακρυσμένος εξυπηρετητής αποκρίνεται κανονικά το detail αρχείο θα έχει μηδενικό μέγεθος. Αν σταματήσει να αποκρίνεται τότε το πρόγραμμα απλώς προσπαθεί συνεχώς να στείλει τα αντίστοιχα δεδομένα ενώ το detail αρχείο αυξάνει σε μέγεθος καθώς προστίθενται νέα accounting δεδομένα. Με άλλα λόγια ακόμα και αν ένας απομακρυσμένος εξυπηρετητής δεν είναι διαθέσιμος και πάλι το accounting θα είναι συγχρονισμένο. Αν καί στους δύο εξυπηρετητές λειτουργεί ένα αντίστοιχο πρόγραμμα τότε όποιος εξυπηρετητής και αν εξυπηρετεί την υπηρεσία το accounting θα παραμένει συγχρονισμένο μεταξύ τους. Το πρόγραμμα αυτό είναι αρκετά έξυπνο για να αποφεύγει ατέρμονα loops.
Ουσιαστικά λοιπόν θα πρέπει σε κάθε RADIUS server να προστεθέι ένα instance του detail module ώς εξής:

```
    detail {
        detailfile = ${radacctdir}/detail
        locking = yes
        detailperm = 0600
    }

accounting {
    .......
    detail
}
```

Επιπλέον θα πρέπει να εκτελεστεί το radrelay utility ως εξής:

/usr/local/radiusd/bin/radrelay -a /var/radiusd/log/radacct –S /usr/local/radiusd/etc/raddb/radrelay.secret -r <remote_radius_server> detail"

Το αρχείο radrelay.secret θα πρέπει να περιέχει το secret του RADIUS server.

4.4.4 MySQL Tuning Guidelines

Συνιστάται ιδιαίτερα αν το accounting που θα διατηρείται στην MySQL είναι μεγαλύτερο από μερικές χιλιάδες rows να χρησιμοποιούνται InnoDB tables αντί για MyISAM tables καθώς το table level locking των τελευταίων μπορεί να δημιουργήσει μεγάλα προβλήματα απόδοσης ιδιαίτερα αν παράλληλα με την λειτουργία του RADIUS server εκτελούνται μεγάλα queries στη βάση μέσα από εργαλεία όπως το dialup admin.

Επιπλεόν συνίσταται η δημιουργία ενός πρόσθετου multi column index που να περιλαμβάνει τα attributes UserName και AcctStopTime. Αυτό μπορεί να αυξήσει την απόδοση αν χρησιμοποιειται το sql module στο session section καθώς και στα queries που εκτελούνται από το dialup admin.

4.5 ΑΠΑΙΤΗΣΕΙΣ ΑΠΟ ΤΗΝ ΥΠΗΡΕΣΙΑ ΚΑΤΑΛΟΓΟΥ

Το λογισμικό δε θέτει ιδιαίτερες από την υπηρεσία καταλόγου. Βασική απαίτηση είναι να έχει προστεθεί η κλάση radiusprofile με τα αντίστοιχα attributes στο LDAP schema. Επιπλέον είναι προτεινόμενο το attribute uid να είναι indexed προκειμένου να γίνονται γρήγορα οι αναζητήσεις για χρήστες ενώ επιπλέον αν χρησιμοποιούνται και LDAP groups προτείνεται να είναι indexed το αντίστοιχο attribute που περιέχει το όνομα του group (συνήθως το cn).

Κατά την εκκίνηση του radius server το ldap module δημιουργεί ένα connection pool από συνδέσεις προς τον ldap server (όπως αυτές έχουν οριστεί με το directive ldap_connections_num). Αυτές οι συνδέσεις χρησιμοποιούνται στη συνέχεια σε κάθε access-request. Για κάθε αίτηση πραγματοποιείται μία αναζήτηση στον ldap προκειμένου με βάση το username του χρήστη να προσδιοριστεί το DN της εγγραφής του στον ldap και να εξαχθούν τα αντίστοιχα radius attributes που μπορεί να περιέχονται σε αυτή. Σε περίπτωση που έχουν ενεργοποιηθεί οι αντίστοιχες δυνατότητες πραγματοποιούνται επιπλέον αναζητήσεις για τα *Default/User/Regular Profiles*. Κατά συνέπεια κάθε access-request συνεπάγεται το λιγότερο μία αναζήτηση στον εξυπηρετητή ldap ενώ μπορεί τελικά να πραγματοποιηθούν μέχρι και άλλες δύο επιπλέον αναζητήσεις. Το ldap module δεν λαμβάνει μέρος στην επεξεργασία των accounting-requests και έτσι δεν δημιουργεί κανένα επιπλέον φόρτο στην επεξεργασία του accounting.

Τέλος, εφόσον έχει ενεργοποιηθεί το authentication μέσω ldap, το ldap module θα ανοίξει μία νέα ldap σύνδεση για κάθε αίτηση προκειμένου να γίνει η ταυτοποίηση του password του χρήστη. Κάτι τέτοιο προφανώς συνεπάγεται αύξηση του χρόνου εξυπηρέτησης κάθε αίτησης καθώς στο χρόνο εξυπηρέτησης προστίθεται το connection overhead. Εναλλακτικά ο διαχειριστής μπορεί να ενεργοποιήσει την εξαγωγή των passwords του χρήστη από το ldap module και να χρησιμοποιήσει το PAP module για τη φάση του authentication.

4.6 BAD-LOGIN LOG

Το σύστημα κρατάει εγγραφές με τα bad logins του συστήματος στο αρχείο radius.log. Στο αρχείο αυτό αποθηκεύονται οι περιπτώσεις:

- Αποτυχημένης πιστοποίησης του χρήστη (login incorrect).
- Πολλαπλής πρόσβασης (multiple login).
- Υπέρβασης του ημερήσιου/εβδομαδιαίου διαθέσιμου χρόνου.
- Κλήσεις έξω από το επιτρεπτό χρονικό διάστημα.

Στις περιπτώσεις αυτές είναι δυνατόν παράλληλα να γίνεται και αντίστοιχη εγγραφή στον πίνακα radacct. Αυτό μπορεί να επιτευχθεί με τη χρήση του utility log_badlogins που περιλαμβάνεται στο πακέτο dialup_admin. Το utility αυτό είναι γραμμένο σε perl και απαιτεί το module Date::Manip. Επιπλέον στο ίδιο το script θα πρέπει να έχουν ενημερωθεί οι εξής μεταβλητές:

- *$domain*: Η μεταβλητή αυτή περιέχει το domain στο οποίο βρίσκονται οι access servers. Επειδή στο radius.log οι access servers καταγράφονται με το shortname είναι απαραίτητο να είανι γνωστό και το domain στο οποίο ανήκουν προκειμένου στη συνέχεια να μπορεί να προσδιοριστεί η IP τους. Με άλλα λόγια θα πρέπει για κάθε access server το $shortname . $domain να αντιστοιχεί σε μία IP.

- *$mysql*: Το path του mysql utility της MySQL.
- *$tmpfile*: Το path στο οποίο θα καταγράφεται το sql script με το οποίο γίνεται η ενημέρωση του MySQL server. Για κάθε MySQL server προστίθεται το hostname του στο τέλος του ονομάτος του αρχείου. Κατά αυτόν τον τρόπο ακόμα και αν ένας MySQL server δεν αποκρίνεται το log_badlogins θα συνεχίσει να καταγράφει τα δεδομένα στους υπολοιπους servers ενώ μόλις ο server επανέλθει θα του αποσταλούν όλα τα δεδομένα.

Πέραν των παραπάνω είναι απαραίτητο να έχουν οριστεί συγκεκριμένες τιμές σε διάφορες μεταβλητές στο αρχείο admin.conf του dialup_admin αλλά αυτό δεν περιλαμβάνεται στην παρούσα τεκμηρίωση. Η μορφή που θα έχουν τα αντίστοιχα accounting records είναι StartTime = StopTime, SessionTime=0 και terminateCause την αιτία του bad login. Οι εγγραφές αυτές είναι προσβάσιμες από την εφαρμογή web διαχείρισης dialup_admin όπως περιγράφεται στην τεκμηρίωση της εφαρμογής.

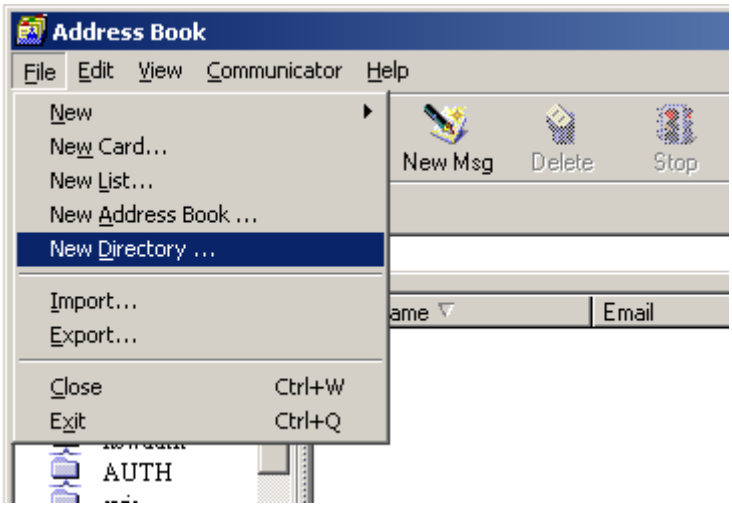
ΜΕΡΟΣ 5ο

5.1 Ερωτήματα στον ldap.gunet.gr, χρησιμοποιώντας Netscape/ Outlook Express/Mozilla

5.1.1 Netscape

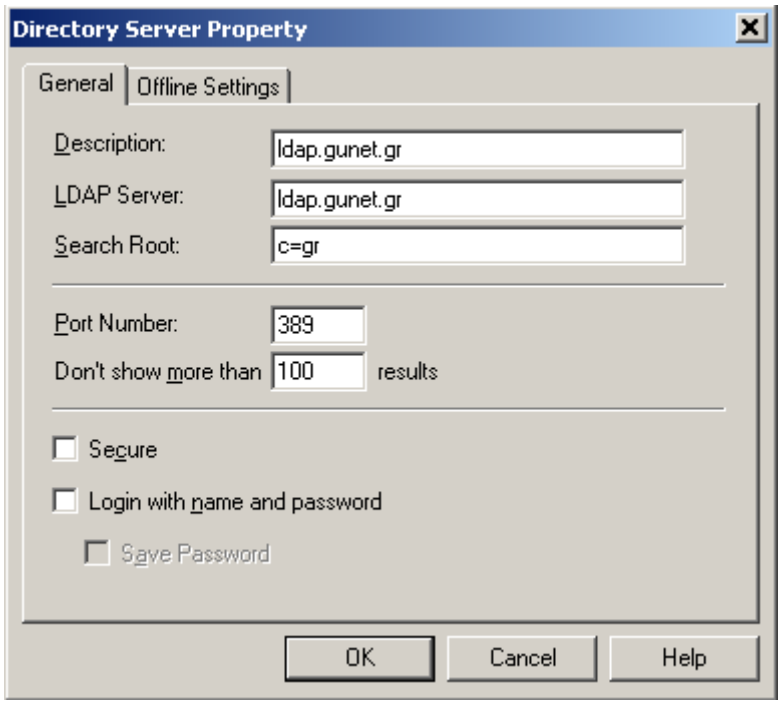
Για να πραγματοποιήσουμε μια αναζήτηση στον ldap του gunet χρησιμοποιώντας το Netscape, θα πρέπει αρχικά να κάνουμε τις απαραίτητες ρυθμίσεις.

Πηγαίνουμε στο address book και επιλέγουμε File και στη συνέχεια New Directory, όπως φαίνεται στο Σχήμα 1.



Σχήμα 1: Δημιουργία καταλόγου

Στη συνέχεια συμπληρώνουμε τα στοιχεία στο πλαίσιο διαλόγου που εμφανίζεται, όπως φαίνεται στο Σχήμα 2.



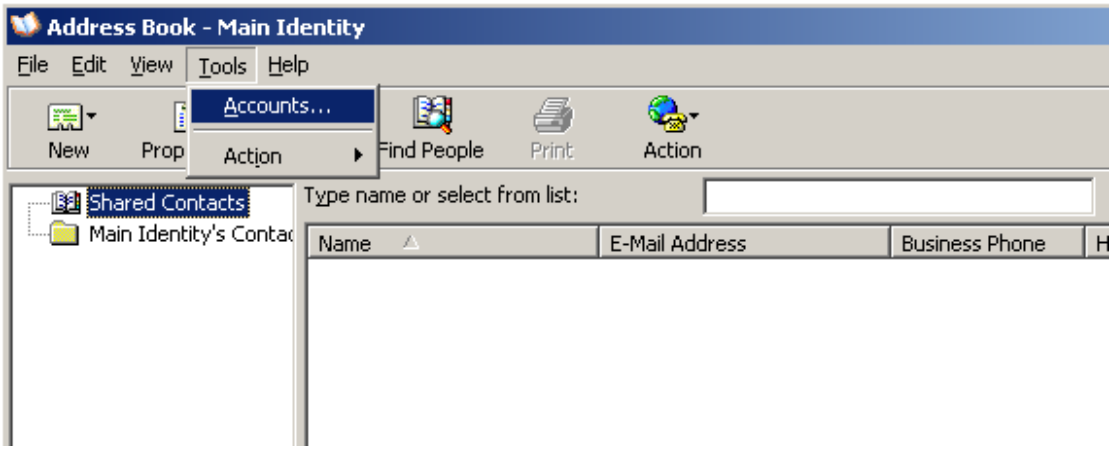
Σχήμα 2: Directory Server Properties

Αφού συμπληρώσουμε τα παραπάνω στοιχεία παρατηρούμε ότι το νέο directory με το όνομα ldap.gunet.gr έχει προστεθεί στα ήδη υπάρχοντα.

5.1.2 **Outlook Express**

Για να πραγματοποιήσουμε αναζητήσεις στον ldap χρησιμοποιώντας το address book του outlook express θα πρέπει αρχικά να ορίσουμε τις ιδιότητες του Directory Service.

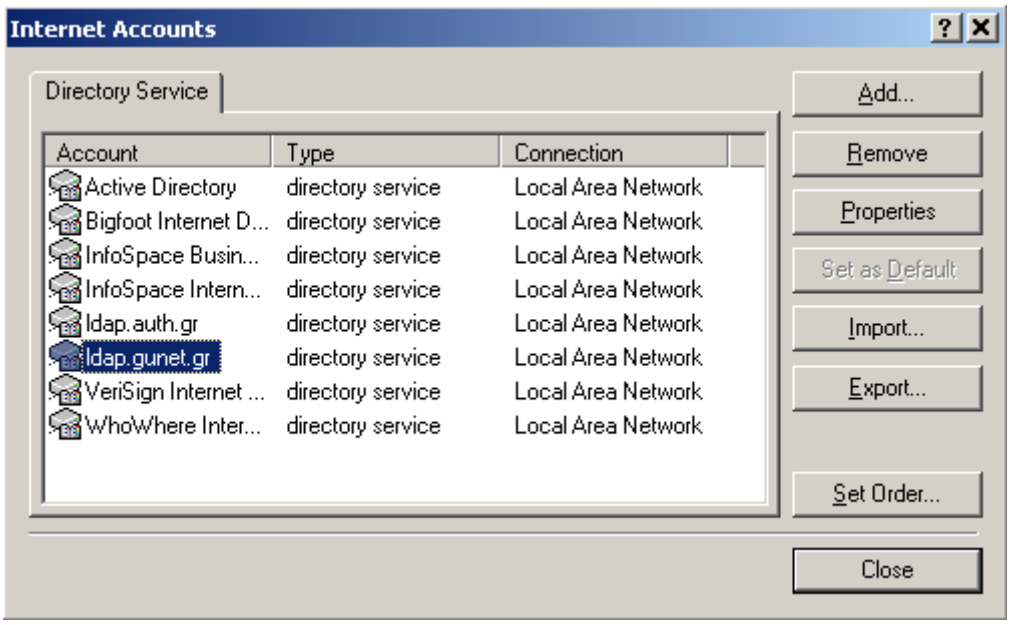
Αρχικά επιλέγουμε Tools -> Accounts, όπως φαίνεται στο σχήμα 8.



Σχήμα 8: Δημιουργία νέου Directory Service

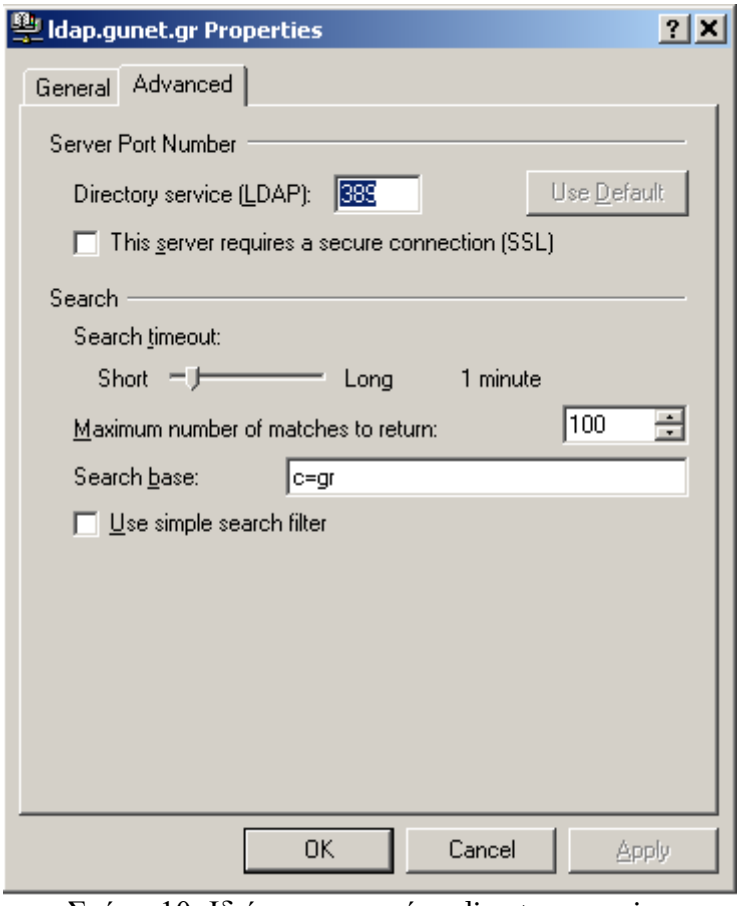
Στη συνέχεια εμφανίζεται ο κατάλογος των Directory Services όποτε επιλέγουμε Add για τη δημιουργία νέου. Στον οδηγό που εμφανίζεται συμπληρώνουμε σαν Internet directory (LDAP) server τον ldap.gunet.gr και στη συνέχεια μπορούμε να επιλέξουμε ή όχι τον έλεγχο των email

διευθύνσεων με βάση τη συγκεκριμένη υπηρεσία. Αφού τελειώσει η διαδικασία έχει προστεθεί το νέο directory service με το όνομα ldap.gunet.gr όπως φαίνεται στο σχήμα 9.



Σχήμα 9: Δημιουργία νέου Directory Service

Πηγαίνοντας στις ιδιότητες του ldap.gunet.gr συμπληρώνουμε τα στοιχεία όπως φαίνεται στο σχήμα 10

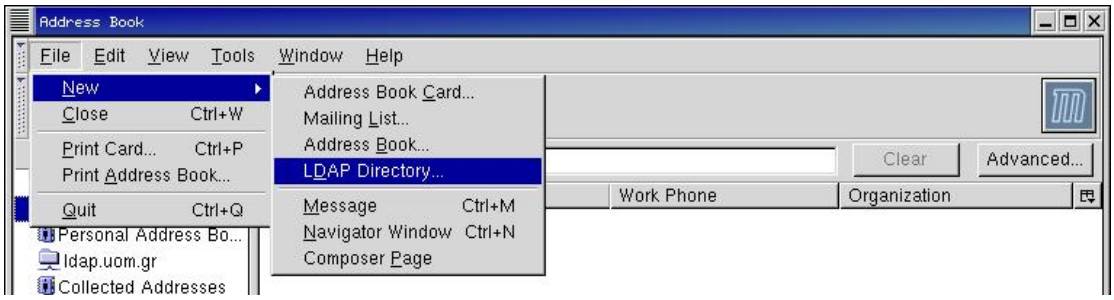


Σχήμα 10: Ιδιότητες του νέου directory service

5.1.3 **Mozilla**

Για να πραγματοποιήσουμε μια αναζήτηση στον ldap του gunet χρησιμοποιώντας το Mozilla, θα πρέπει αρχικά να κάνουμε τις απαραίτητες ρυθμίσεις.

Πηγαίνουμε στο address book και επιλέγουμε File και στη συνέχεια New LDAP Directory όπως φαίνεται στο Σχήμα 14.



Σχήμα 14: Δημιουργία καταλόγου

Στη συνέχεια συμπληρώνουμε τα στοιχεία στο πλαίσιο διαλόγου που εμφανίζεται, όπως φαίνεται στο Σχήμα 15.

Σχήμα 15: Directory Server Properties

Αφού συμπληρώσουμε τα παραπάνω στοιχεία παρατηρούμε ότι το νέο directory με το όνομα ldap.gunet.gr έχει προστεθεί στα ήδη υπάρχοντα.

ΜΕΡΟΣ 6ο

6.1 ΟΛΟΚΛΗΡΩΣΗ DIRECTORY SERVER ΜΕ QMAIL

Η *qmail* μπορεί να εγκατασταθεί και να τρέξει στα περισσότερα UNIX και UNIX-like συστήματα τα οποία όμως πρέπει να πληρούν κάποιες απαιτήσεις:

- Γύρω στα 10 megabytes ελεύθερου χώρου εκεί που θα γίνει το compilation και όσο διαρκεί αυτό. Μετά μπορούν να ελευθερωθούν γύρω στα 4 megabytes σβήνοντας τα object files.
- Ένα πλήρες λειτουργικό σύστμα C το οποίο περιλαμβάνει compiler, system header files και βιβλιοθήκες.
- Μερικά megabytes για τα εκτελέσιμα, την τεκμηρίωση και τα αρχεία ρυθμίσεων.
- Ένα *ασφαλές* filesystem για την ουρά. Για να είναι εγκυημένα αξιόπιστη η qmail απαιτεί η ουρά της να είναι σε filesystem με traditional BSD FFS semantics. Τα περισσότερα τοπικά filesystems πληρούν τα κριτήρια με μια σημαντική εξαίρεση: η link() είναι συχνά *ασύγχρονη*, το οποίο σημαίνει ότι τα αποτελέσματα της link() operation μπορεί να μην έχουν γραφτεί στο δίσκο όταν το link() call επιστρέφει. Η βιβλιοθήκη syncdir του Bruce Guenter μπορεί να χρησιμοποιηθεί ως work around σε αυτό το πρόβλημα.
- Επαρκής αποθηκευτικός χόρος για την ουρά. Μικρά single-user συστήματα χρειάζονται μόνο μερικά megabytes. Μεγάλοι servers μπορούν να χρειάζονται αρκετά gigabytes.
- Ένα συμβατό λειτουργικό σύστημα. Οι περισσότερες εκδόσεις Unix είναι δεκτές. Δείτε το αρχείο README στο source tree για μια πλήρη λίστα.
- Πρόσβαση σε DNS server συνίσταται ισχυρά. Χωρίς αυτόν η qmail μπορεί να στείλει μόνο σε απομακρυσμένα συστήματα τα οποία έχουν γίνει configure στο αρχείο ρύθμισης smtproutes.

6.2 ΟΛΟΚΛΗΡΩΣΗ DIRECTORY SERVER ΜΕ SENDMAIL

Δεδομένου του μεγέθους και της πολυχρηστικότητας του εν λόγο προγράμματος η διαδικασία που προτείνεται ξεκινάει με την διαδικασία του «κτισίματος» από source γιατί το μεγαλύτερο τμήμα των παρεχόμενων πακέτων δεν έχει ενσωματωμένη τη συγκεκριμένη δυνατότητα, επιπλέον είναι καλή πρακτική για κάποια τόσο σημαντικά εργαλεία η εγκατάσταση να πληρει τις απολύτως αναγκαίες απαιτήσεις.

Η sendmail μπορεί να εγκατασταθεί και να τρέξει σε όλα τα UNIX και UNIX-based συστήματα τα οποία όμως πρέπει να πληρούν κάποιες απαιτήσεις:

- Γύρω στα 10 megabytes ελεύθερου χώρου εκεί που θα γίνει το compilation και όσο διαρκεί αυτό. Μετά μπορούν να ελευθερωθούν γύρω στα 8 megabytes σβήνοντας τα object files kai m4 processors και macro definitions.
- Ένα πλήρες λειτουργικό σύστημα C το οποίο περιλαμβάνει compiler, system header files και βιβλιοθήκες.
- Περίπου 2 με 3 megabytes για τα εκτελέσιμα, τα αρχεία ρυθμίσεων και επιπλέον για την τεκμηρίωση.
- Ένα *ασφαλές* file system για την ουρά. Για να είναι εγκυημένα αξιόπιστη η sendmail απαιτεί η ουρά της να είναι σε file system με traditional BSD FFS semantics.

Τα περισσότερα σύγχρονα τοπικά file systems ειδικά όσα έχουν την δυνατότητα logging ή journaling πληρούν τα κριτήρια αυτά. Μερικά από είναι:

Για το Λειτουργικό Σύστημα Linux: Ext3, jfs, reiserfs, xfs.

Για το Λειτουργικό Σύστημα Solaris (έκδοση 7 ή νεώτερη): UFS with logging support, SUN QFS.

Για τα Λειτουργικά Συστήματα BSD: FFS with soft Dependencies, LFS

- Επαρκής αποθηκευτικός χώρος για την ουρά. Μικρά single-user συστήματα χρειάζονται μόνο μερικά megabytes. Μεγάλοι servers μπορούν να χρειάζονται αρκετά gigabytes.
- Ένα συμβατό λειτουργικό σύστημα. Σχεδόν όλες εκδόσεις Unix είναι δεκτές. Δείτε το αρχείο sendmail/README στο source tree για μια πλήρη λίστα με κάποιες από τις ιδιαιτερότητες τους.
- Η ύπαρξη DNS server και η σωστή ρύθμιση θεωρείται ως απαραίτητη. Χωρίς αυτόν είναι πρακτικά αδύνατη η σωστή λειτουργία της υπηρεσίας ηλεκτρονικού ταχυδρομείου.

6.3 IMAP/POP3 AUTHENTICATION ΜΕΣΩ LDAP

Το IMAP (INTERNET MAIL ACCESS PROTOCOL) όπως λέει και το όνομά του, είναι ένα πρωτόκολλο πρόσβασης σε αποθηκευμένα e-mail. Δεν πρέπει να συγχέεται με το SENDMAIL ή το QMAIL καθώς τα δύο τελευταία είναι MTA (MAIL TRANSPORT AGENTS). Το IMAP συγγενεύει με το POP (POST OFFICE PROTOCOL) αλλά έχει πολύ μεγαλύτερες δυνατότητες από το τελευταίο.

6.4 ΣΥΝΔΕΣΗ ΕΞΥΠΗΡΕΤΗΤΩΝ ΟΝΟΜΑΤΟΛΟΓΙΑΣ ΜΕ ΥΠΗΡΕΣΙΑ ΚΑΤΑΛΟΓΟΥ (BIND LDAP-SDB)

Η υπηρεσία DNS είναι μία από τις βασικές υπηρεσίες που παρέχουν όλα τα ιδρύματα στους χρήστες τους. Ένα από τα βασικά προβλήματα είναι το delegation της διαχειρίσης του naming space στα τμήματα και στους τομείς των ιδρυμάτων. Το delegation αυτό προυποθέτει ότι είτε οι delegated διαχειριστές θα διατηρούν δικούς τους DNS εξυπηρετητές για τα domains τα οποία διαχειρίζονται είτε ότι θα πρέπει να τους παραχωρηθεί πρόσβαση στους κεντρικούς DNS εξυπηρετητές των ιδρυμάτων.

Η λύση σε αυτό το πρόβλημα είναι η αποθήκευση των DNS εγγραφών για αυτά τα domains σε LDAP database και η παροχή ενός interface διαχείρισης για τη διαχείριση των εγγραφών από τους ίδιους τους διαχειριστές. Αυτό έχει το πλεονέκτημα ότι είναι δυνατόν να χρησιμοποιηθούν LDAP access lists που επιτρέπουν στον διαχειριστή της υπηρεσίας DNS να ορίσει διαχειριστές και δικαιώματα ανά domain όπως αυτός επιθυμεί και η διαχείριση όλων των παραπάνω να γίνεται από ένα αυτοματοποιημένο και εύκολο στη χρήση του περιβάλλον διαχείρισης.

Το ανοικτό πακέτο λογισμικού BIND είναι αυτό το οποίο χρησιμοποιείται στην πλειονότητα των εγκαταστάσεων DNS εξυπηρετητών. Για το πακέτο αυτό παρέχεται το module LDAP SDB το οποίο επιτρέπει την αποθήκευση των DNS zones σε LDAP server. Με τη χρήση του είναι δυνατόν συγκεκριμένα zones να είναι αποθηκευμένα σε βάση LDAP και να εξυπηρετούνται απευθείας με ερωτήσεις στη βάση.

Η κεντρική web σελίδα για το module αυτό μπορεί να βρεθεί στη διεύθυνση (*http://www.venaas.no/ldap/bind-sdb/*). Στη σελίδα αυτή περιέχεται πάντα η τελευταία έκδοση του αντίστοιχου πακέτου. Στη συνέχεια θα πρέπει να ενημερωθεί το ldap schema του LDAP server με το objectclass dnszone που μπορεί να βρεθεί στη διεύθυνση του sdb module.

6.4.1 **dnsZone objectclass**

Τα DNS δεδομένα αποθηκεύονται στον LDAP με χρήση της dnsZone objectclass όπως αυτή περιγράφεται παρακάτω:

LDAP attribute	**Περιγραφή**
dNSTTL	Το TTL της εγγραφής
dNSClass	Η Class του resource Record
zoneName	Το όνομα της ζώνης στην οποία ανήκει η εγγραφή
relativeDomainName	
pTRRecord	PTR Record
hInfoRecord	Host Info Record
mInfoRecord	Mail Box Info Record
tXTRecord	Text String Record
SigRecord	Signature Record
KeyRecord	
aAAARecord	IPv6 IP Address Record
LocRecord	Location Record
nXTRecord	non-Existent
SRVRecord	Service Location (SRV) Record
nAPTRRecord	Naming Authority Pointer Record
kXRecord	Key Exchange Delegation
certRecord	Certificate
a6Record	A6 Record Type
dNameRecord	Non-Terminal DNS Name Redirection

6.4.2 **Διαμόρφωση**

Πριν από οποιαδήποτε αλλαγή στον ίδιο τον DNS server θα πρέπει να έχει ενημερωθεί το schema του LDAP server με την objectclass dnsZone καθώς επίσης και να έχουν προστεθεί τα αντίστοιχα δεδομένα.
Στη συνέχεια θα πρέπει για κάθε ζώνη που θέλουμε να εξυπηρετείται από τον ldap server να προστεθεί το ακόλουθο στο αρχείο διαμόρφωσης του BIND:

```
zone "myzone.com" {
      type master;
      database "ldap ldap://ldap.host/dc=myzone,dc=zone,o=DNS,dc=myzone,dc=com  172800";
};
```

Όπου αντί για myzone.com τοποθετούμε τη δική μας ζώνη, αντί για ldap.host τον ldap server όπου περιέχονται πληροφορίες για τη ζώνη και το DN κάτω από το οποίο βρίσκονται τοποθετημένα τα δεδομένα της ζώνης. Αν απαιτείται μπορεί να προστεθεί και ldap filter στο παραπάνω LDAP URL όπως φαίνεται παρακάτω:

ldap://host/base???(o=internal)

6.4.3 **Προτεινόμενη βασική δομή των εξυπηρετητών DNS**

Ένας ή περισσότεροι DNS master εξυπηρετούν τα zone files μέσω του LDAP-SDB module οι οποίοι όμως δεν είναι δηλωμένοι σαν NS servers για τα αντίστοιχα domains. Στο επόμενο επίπεδο βρίσκονται οι NS servers για τα αντίστοιχα domains οι οποίοι ανά τακτά χρονικά διαστήματα (όπως αυτά ορίζονται στα αντίστοιχα SOA records των domains) κάνουν zone transfers για αυτά τα domains από τους κεντρικούς DNS masters. Όλα τα DNS requests για αυτά τα domains γίνονται μόνο σε αυτούς τους εξυπηρετητές. Κατά αυτόν τον τρόπο οι LDAP εξυπηρετητές με την πρωτογενή πληροφορία δεν χρησιμοποιούνται παρά μόνο για τα DNS zone transfers και κατά συνέπεια δεν δημιουργείται κανένα πρόβλημα απόδοσης από την λειτουργία της υπηρεσίας DNS με χρήση LDAP.

6.4.4 **Απαιτήσεις από την υπηρεσία καταλόγου**

Οι απαιτήσεις του λογισμικού από την υπηρεσία καταλόγου είναι κατ αρχήν να έχει προστεθεί η objectclass dnsZone και τα αντίστοιχα attributes στο LDAP schema. Παράλληλα προκειμένου να εκτελούνται με ταχύτητα οι αντίστοιχες αναζητήσεις στην υπηρεσία θα πρέπει να είναι indexed τα attributes zoneName και relativeDomainName.

Με βάση την προτεινόμενη διαμόρφωση οι απαιτήσεις απο πλευράς ισχύος από την υπηρεσία καταλόγου είναι ουσιαστικά μηδαμινές καθώς απαιτείται απλώς ένα LDAP Search Operation κάθε φορά που λαμβάνει χώρα ένα DNS zone transfer.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ(3η ΕΚΔΟΣΗ).
ΔΙΚΤΥΑ ΘΕΩΡΙΑ ΚΑΙ ΠΡΑΞΗ.
ΣΗΜΕΙΩΣΕΙΣ ΠΡΩΤΟΚΟΛΛΩΝ ΔΙΑΔΙΚΤΥΩΝ.
DNS And Bind 4th Edition, by Paul Albitz and Cricket Liu O' Reilly.
RADIUS Securing Public Access to Private Resources Jonathan Hassell O' Reilly.

ΣΥΝΔΕΣΜΟΙ

- Bind DNS Server: http://www.isc.org/products/BIND/
- qmail: http://www.qmail.org
- sendmail: http://www.sendmail.org
- imap: http://www.imap.org
- pop3: http://www.ietf.org/rfc/rfc1939.txt
- MySQL Database: http://www.mysql.com/
- http://www.openldap.org
- The Freeradius Project: http://www.freeradius.org/
- http://www.openldap.org

ΟΡΟΛΟΓΙΑ

SDB	Simplified Database Interface
DNS	Domain Name Service
RADIUS	Remote Authentication Dial In User Service
LDAP	Lightweight Directory Access Protocol
EAP	Extensible Authentication Protocol
PPP	Point-to-Point Protocol
TLS	Transport Layer Security
ACI	Access Control Instruction
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
SNMP	Simple Network Management Protocol
MTU	Maximum Transmission Unit
IP	Internet Protocol
NAS	Network Access Server
SHA1	Secure Hash Algorithm Ver1
MD5	Message Digest5