

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη	2
1. Directories: έννοιες και ορισμοί	4
1.1 Directories & Directory Services	4
1.2 Η ανάγκη δημιουργίας ενός καθολικού Directory	5
1.3 Λειτουργίες και λύσεις μιας καθολικής Directory Service	12
1.4 Διαφορές μεταξύ των Directories και των Βάσεων Δεδομένων	15
1.5 Directory Clients & Servers (Πελάτες και Εξυπηρετητές)	17
2. X.500	18
2.1 Συστατικά μιας X.500 Directory Service	18
2.2 Η δενδρική δομή του X.500	19
2.3 Το λειτουργικό μοντέλο του X.500	21
2.4 Μειονεκτήματα του X.500	24
3. LDAP (Lightweight Directory Access Protocol)	25
3.1 Το LDAP ως ολοκληρωμένη Directory Service	26
3.2 Αρχιτεκτονική του LDAP	28
3.2.1 Το πληροφοριακό μοντέλο	29
3.2.2 Το μοντέλο ονοματολογίας	31
3.2.3 Το λειτουργικό μοντέλο	33
3.2.4 Το μοντέλο ασφάλειας	33
3.3 Το LDAP ως μέρος της λύσης για καθολικές Directory Services	34
4. Το πληροφοριακό μοντέλο των DEN	36
4.1 Κλάσεις των DEN	37

4.1.1 Επιρροές του X.500	37
4.1.2 Επιρροές του CIM	38
4.1.3 Νέες έννοιες των DEN	39

5. Επιχειρησιακές αλλαγές 40

6. Scalable Device Configuration Management, Policy Based Networking 42

6.1 Scalable Device Configuration Management	42
6.2 Policy Based Networking	43

7. Προβλέψεις 46

Αναφορές 47

Περίληψη

Τα directory enabled networks είναι δίκτυα στα οποία ενσωματώνονται οι λεγόμενες directory services. Οι directory services παρέχουν στο χρήστη τη δυνατότητα του εντοπισμού των πόρων του δικτύου. Η ανάγκη για την παροχή της δυνατότητας αυτής έχει αυξηθεί ταυτόχρονα με τη ραγδαία αύξηση του μεγέθους των επιχειρησιακών δικτύων και ενώ στα LANs, τα οποία συνέδεαν μερικές δεκάδες ή εκατοντάδες υπολογιστές, αποτελούσε απλώς μία ευκολία, στα σημερινά intranets που συνδέουν χιλιάδες υπολογιστικών πόρων αποτελεί μία κρισιμότερη υπηρεσία.

Σήμερα, οι τάσεις σε ότι αφορά την εξέλιξη των δικτύων είναι προφανείς. Η ανάγκη της απλοποίησης της επαφής του χρήστη με το δίκτυο καθώς και η διευκόλυνση της διαχείρισης των δικτύων με τεχνικές που περιλαμβάνουν την αποδοτική εκχώρηση εύρους ζώνης και τη λειτουργία τους με βάση συγκεκριμένες πολιτικές, οδηγούν τις εξελίξεις στον διαρκώς εξελισσόμενο αυτό τομέα. Η λύση που φέρεται ως πιθανή να επιτύχει την ικανοποίηση αυτών των αναγκών ακούει στο όνομα directory enabled networks.

Abstract

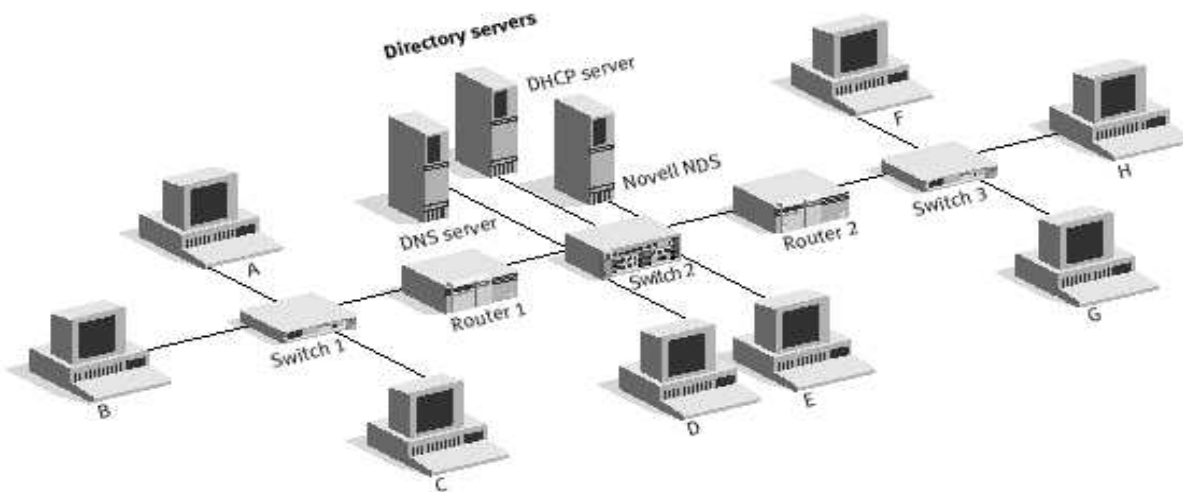
Directory services play the important role of helping users locate resources on a network. The need for this function has grown along with the size of the corporate network. What was only a nicety on LANs that connected tens or hundreds of clients has become a truly critical service on intranets that connect thousands of resources and users.

Two trends are obvious. The need to simplify the user's contact with the network and the need to simplify the technical management of the network, including bandwidth management and the expansion and introduction of new technologies. A cost effective solution to both of these problems is directory enabled networks.

1. Directories: έννοιες και ορισμοί

1.1 Directories & Directory Services

Directory, ή στα Ελληνικά κατάλογος, είναι μία ειδικής χρήσης βάση δεδομένων η οποία περιέχει πληροφορίες σχετικές με τους διάφορους πόρους που είναι διαθέσιμοι σε ένα δίκτυο και οι οποίες χρησιμοποιούνται για τη διαχείριση του δικτύου [5]. Η διαφορά μεταξύ ενός directory και ενός κλασσικού Συστήματος Διαχείρισης Βάσεων Δεδομένων (DataBase Management System – DBMS) έγκειται στο γεγονός ότι οι directories είναι βελτιστοποιημένοι για διαχείριση δεδομένων, οι λειτουργίες ανάγνωσης των οποίων είναι πολύ πιο συχνές από τις λειτουργίες εγγραφής ή τροποποίησής τους. Επομένως, οι directories παρέχουν εξαιρετικούς χρόνους απόκρισης σε διαδικασίες αναζήτησης δεδομένων, αλλά μειονεκτούν σε ότι αφορά τους χρόνους απόκρισης σε διαδικασίες εγγραφής και ενημέρωσης δεδομένων. Η εικόνα 1.1 δείχνει ένα δίκτυο μιας επιχείρησης και μερικούς από τους directories που απαιτούνται για την υποστήριξή του.



Εικόνα 1.1: Directories για υποστήριξη δικτύου επιχείρησης.

Συγκρινόμενοι με κλασσικά DBMSs, οι directories είναι σχετικά ανώριμοι αναφορικά με την ικανότητά τους να εκτελούν ορισμένες από τις πιο πολύπλοκες

διαδικασίες οι οποίες επιτρέπουν τη διαχείριση μεγάλου όγκου πληροφοριών. Τυποποιημένα χαρακτηριστικά ενός εμπορικού DBMS αποτελούν η διαδοχή διαγραφών (cascading deletes), τα σύνολα αποτελεσμάτων (result sets) και η οπισθοχώρηση συναλλαγών (transaction rollback). Τα χαρακτηριστικά αυτά δεν υποστηρίζονται, προς το παρόν, από τους directories.

Τέλος, μία directory service (υπηρεσία καταλόγου), μπορεί να λαμβάνει χώρα σε έναν μοναδικό server ή να είναι κατανεμημένη σε περισσότερους. Σε έναν κατανεμημένο directory όλοι οι servers συνεργάζονται έτσι ώστε να παρέχουν μία ενοποιημένη directory service, η οποία θα πρέπει ταυτόχρονα να μην παρουσιάζει σφάλματα. Μία τέτοια directory service παρέχει, μέσω αντιγραφής, μία κοινή όψη των δεδομένων ανεξάρτητη από τη θέση του client.

1.2 Η ανάγκη δημιουργίας ενός καθολικού Directory

Μία ‘παραδοσιακή’ directory service παρέχει ένα μέσο για τον εντοπισμό και την αναγνώριση χρηστών και διαθέσιμων πόρων σε ένα κατανεμημένο σύστημα. Δίνει επίσης τη δυνατότητα πρόσθεσης, τροποποίησης, αφαίρεσης, μετονομασίας και γενικά διαχείρισης των μερών του συστήματος χωρίς να διακόπτεται η λειτουργία των υπόλοιπων των μερών του. Επομένως, μία directory service επιτελεί τις παρακάτω λειτουργίες [18]:

- ο Αποθηκεύει πληροφορίες σχετικές με τα συστατικά του συστήματος με κατανεμημένο τρόπο. Οι πληροφορίες αυτές αντιγράφονται σε διάφορους servers έτσι ώστε ένας χρήστης ή μία υπηρεσία που χρειάζεται πρόσβαση σε μία συγκεκριμένη πληροφορία να έχει τη δυνατότητα να την αντλήσει από έναν τοπικό server.
- ο Υποστηρίζει υπηρεσίες ‘λευκών σελίδων’ (white pages) για αναζήτηση με βάση κάποιο χαρακτηριστικό (π.χ. ‘Ποιος είναι ο αριθμός τηλεφώνου του Γιάννη Παπαδόπουλου;’) καθώς και ‘κίτρινων σελίδων’ (yellow pages) για αναζήτηση με βάση κάποια κατηγοριοποίηση (π.χ. ‘Σε ποια σημεία του τέταρτου ορόφου υπάρχουν έγχρωμοι εκτυπωτές;’).

- ο Επιτρέπει απλό έλεγχο πρόσβασης των χρηστών στις δικτυακές υπηρεσίες έτσι ώστε να είναι πλήρως εκμεταλλεύσιμοι τόσο οι δικτυακοί πόροι όσο και οι υπηρεσίες.
- ο Παρέχει ένα ανεξάρτητο από τοποθεσία σημείο διοίκησης και διαχείρισης.
- ο Δημιουργεί αντίγραφα των δεδομένων για την παροχή αξιόπιστων πληροφοριών. Οι τροποποιήσεις που επιφέρονται σε οποιοδήποτε αντίγραφο των δεδομένων διαδίδονται σε όλα τα αντίγραφα μέσω του δικτύου έτσι ώστε οι πληροφορίες που ζητά κάθε εφαρμογή η οποία έχει πρόσβαση στον directory να είναι συνεπείς.

Όλες αυτές οι υπηρεσίες είναι, φυσικά, χρήσιμες, καθώς διευκολύνουν τη διαχείριση του δικτύου αλλά και προσφέρουν τη δυνατότητα της όσο το δυνατόν καλύτερης εκμετάλλευσης των πόρων και των υπηρεσιών του από τους χρήστες και τις δικτυακές εφαρμογές. Παρόλα αυτά ο ρόλος των directory services έχει αναβαθμιστεί τα τελευταία χρόνια έτσι ώστε να μπορούν να επιτελούν περισσότερες και πιο πολύπλοκες λειτουργίες από τις προαναφερθείσες. Οι κυριότεροι λόγοι που δημιούργησαν την ανάγκη αναβάθμισης του ρόλου των directories είναι οι εξής [6]:

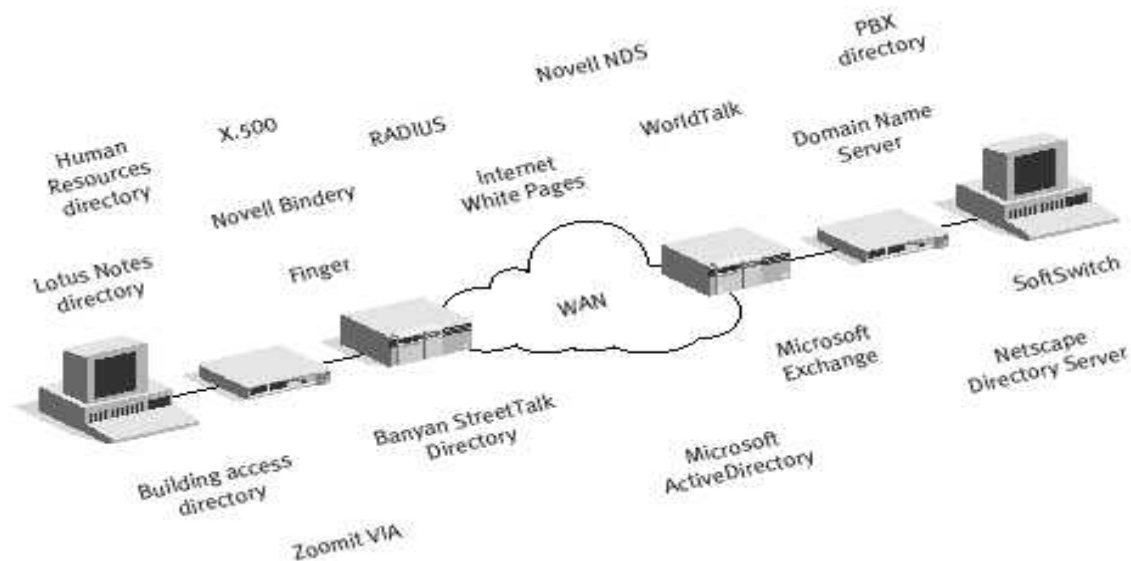
- ο **Η 'έκρηξη' του αριθμού των υπολογιστών που είναι συνδεδεμένοι σε δίκτυο.** Το 1993 το ποσοστό των υπολογιστών που ανήκουν σε εταιρείες και είναι συνδεδεμένοι σε δίκτυο ήταν μόλις 23%. Το 1998 το ποσοστό αυτό αυξήθηκε σε 50%. Επίσης, ο συνολικός αριθμός υπολογιστών συνδεδεμένων σε δίκτυο ήταν περίπου 150.000.000 το 1997, ενώ υπολογίζεται ότι το 2001 ο αριθμός αυτός θα ξεπεράσει τα 269.000.000. Με τον διαρκώς αυξανόμενο αριθμό υπολογιστών που έχουν πρόσβαση σε δίκτυο κάθε άλλο παρά έκπληξη προκαλεί το γεγονός ότι η εξεύρεση πόρων στο δίκτυο είναι πλέον από δύσκολη έως προβληματική.
- ο **Η αναζήτηση δεδομένων αφορά πλέον και τις εφαρμογές εκτός από τους χρήστες.** Η αναζήτηση μιας διεύθυνσης e-mail από ένα χρήστη είναι παράδειγμα μιας συνηθισμένης ερώτησης προς έναν directory. Ωστόσο, είναι οι εφαρμογές αυτές που ολοένα και περισσότερο αναζητούν πληροφορίες στους directories. Για παράδειγμα, οι web servers πρέπει να αναζητήσουν τα δικαιώματα πρόσβασης ενός χρήστη πριν δώσουν πρόσβαση σε μία web page

στο συγκεκριμένο χρήστη. Επίσης οι mail servers χρειάζεται να γνωρίζουν που βρίσκεται το mailbox ενός χρήστη ώστε να δρομολογούν σωστά τα mail που απευθύνονται σ'αυτόν.

- ο **Οι νέες δικτυακές υπηρεσίες.** Όταν τα Λειτουργικά Συστήματα Δικτύου (Network Operating Systems – NOS) παρείχαν μόνο τη δυνατότητα διαμοιρασμού αρχείων και υπηρεσίες εκτύπωσης, ο ρόλος ενός directory ήταν να παρέχει βοήθεια στους χρήστες να εντοπίσουν τους file servers και τους εκτυπωτές. Καθώς, όμως, νέοι τύποι υπηρεσιών εμφανίζονται στα δίκτυα και οι δικτυακές εφαρμογές αποτελούν τον κανόνα και όχι την εξαίρεση, οι directory services αναλαμβάνουν πλέον το ρόλο της οργάνωσης των πόρων του δικτύου έτσι ώστε αυτοί να είναι όσο το δυνατόν πιο εύχρηστοι.
- ο **Τα επιχειρησιακά intranets.** Η μετατροπή των τοπικών δικτύων (Local Area Networks - LANs) των επιχειρήσεων σε επιχειρησιακά intranets έφερε τα θέματα ασφάλειας στην κορυφή της λίστας των προβλημάτων που έχουν να αντιμετωπίσουν οι διαχειριστές δικτύων. Όταν τα LANs απομόνωναν τις διάφορες ομάδες εργασίας σε μία επιχείρηση τα θέματα ασφάλειας δεν ήταν τόσο κρίσιμα όσο σήμερα που τα intranets έχουν καταστήσει επιτακτική την ανάγκη ελέγχου πρόσβασης για κάθε χρήστη. Ο directory είναι η προφανής τοποθεσία στην οποία αποθηκεύονται τα usernames, passwords, certificates και public keys τα οποία παρέχουν το πλαίσιο ανάπτυξης τεχνολογιών για πιστοποίηση ταυτότητας και κρυπτογράφηση. Οι τεχνολογίες αυτές χρησιμοποιούνται τόσο σε intranets επιχειρήσεων όσο και στο Internet.
- ο **Τα extranets.** Τα δίκτυα που συνδέουν συνεργαζόμενες επιχειρήσεις ή επιχειρήσεις με προμηθευτές και πελάτες απαιτούν directory services για την παροχή ασφάλειας, αλλά και για την παροχή ενός κοινού χώρου αποθήκευσης πληροφοριών όπως οι προδιαγραφές προϊόντων, οι διαδικασίες τιμολόγησης και τα λογιστικά. Οι συγκεκριμένοι directories επικοινωνούν με πολλαπλές βάσεις δεδομένων που περιέχουν επιχειρησιακές πληροφορίες.
- ο **Το ηλεκτρονικό εμπόριο (e-commerce).** Το ηλεκτρονικό εμπόριο, που διεξάγεται κυρίως μέσω του Internet, απαιτεί τη χρήση directory services για δύο κυρίως λόγους. Ο πρώτος είναι να επιτρέπει στους πελάτες να εντοπίζουν

τους πωλητές. Ο δεύτερος λόγος είναι το γεγονός ότι ο directory παίζει σημαντικό ρόλο στη δημιουργία υποδομής δημοσίου κλειδιού (Public Key Infrastructure – PKI), η οποία είναι απαραίτητη για την ασφάλεια των ηλεκτρονικών συναλλαγών. Το ηλεκτρονικό εμπόριο μέσω του Internet απαιτεί κρυπτογράφηση των ανταλλασσόμενων δεδομένων και τεχνολογίες ψηφιακής υπογραφής τα οποία επιτυγχάνονται με τη βοήθεια των directories.

Το πρόβλημα που αντιμετωπίζουν πολλές επιχειρήσεις είναι το γεγονός ότι στο δίκτυο που υποστηρίζει τις λειτουργίες της επιχείρησης υπάρχει συνήθως ένας μεγάλος αριθμός directories η διαχείριση των οποίων αποτελεί μία επίπονη και πολλές φορές εφιαλτική διαδικασία. Σύμφωνα με έρευνα της εταιρείας Forrester Research Inc., μία τυπική επιχείρηση μπορεί να έχει έως και 181 ξεχωριστούς directories καθώς και αρχεία με πληροφορίες σχετικές με τους χρήστες του δικτύου. Η προσέγγιση αυτή δημιουργεί ‘πληροφοριακές νησίδες’ (information islands) με αποτέλεσμα η εκτέλεση απλών λειτουργιών όπως η προσθήκη ή η αφαίρεση ενός χρήστη και η αλλαγή των δικαιωμάτων του, καθώς και η δημιουργία νέων δικτυακών εφαρμογών να αποτελεί μία πολύπλοκη διαδικασία που πρέπει να εκτελεστεί από το διαχειριστή του δικτύου [4]. Στην εικόνα 2 απεικονίζεται το γεγονός της ύπαρξης ενός μεγάλου αριθμού directories σε ένα επιχειρησιακό δίκτυο.



Εικόνα 1.2: Πολλαπλοί directories σε ένα επιχειρησιακό δίκτυο.

Παραδείγματα directories που μπορεί να υπάρχουν σε ένα δίκτυο μιάς επιχείρησης αποτελούν οι directories αρχείων που υπάρχουν σε κάθε σκληρό δίσκο, PBX directories για αριθμούς τηλεφώνου, directories ανθρωπίνων πόρων (human resources) για στοιχεία σχετικά με τους υπαλλήλους, e-mail directories, directories για απομακρυσμένη πρόσβαση (remote access), directories λειτουργικού συστήματος δικτύου (Network Operating System - NOS), και Internet directories (Finger, Domain Name Server – DNS, Internet White Pages).

Το πρόβλημα της ύπαρξης πολλαπλών directories εντείνεται καθώς το μέγεθος της πληροφοριακής υποδομής των επιχειρήσεων (enterprise's information infrastructure) αυξάνεται. Το αποτέλεσμα είναι ότι οι πληροφορίες που θα έπρεπε να περιέχονται σε έναν και μόνο directory, πολλές φορές περιέχονται σε περισσότερους. Έτσι, το όνομα ενός υπαλλήλου, ο αριθμός τηλεφώνου του και η ηλεκτρονική διεύθυνσή του είναι δυνατόν να περιλαμβάνονται στον directory ανθρωπίνων πόρων, στον e-mail directory και στον NOS directory. Το πρόβλημα γίνεται ακόμη μεγαλύτερο λόγω του γεγονότος ότι κάθε directory έχει τις δικές του λειτουργίες (authenticate, read, write, search κ.τ.λ.), το δικό του πρωτόκολλο πρόσβασης (access protocol) και τη δική του σύμβαση ονομασίας των καταχωρήσεων. Είναι, λοιπόν, δυνατόν το όνομα ενός χρήστη να καταχωρείται σε έναν directory ως 'Γιάννης Παπαδόπουλος', σε έναν δεύτερο ως 'Γιάννης Κ. Παπαδόπουλος' και σε έναν τρίτο ως 'Γ. Παπαδόπουλος'. Επομένως, είναι φανερή η δυσκολία της επικοινωνίας και της ανταλλαγής δεδομένων μεταξύ των directories κάτι που δημιουργεί δυσκολίες στην τροποποίηση των καταχωρήσεών τους. Όταν λαμβάνει χώρα μία μεταβολή μιας καταχώρησης σε έναν directory, η αλλαγή αυτή πρέπει να μεταδοθεί και σε όλους τους υπόλοιπους directories από το διαχειριστή του δικτύου. Για παράδειγμα, αν κάποιος υπάλληλος φύγει από την επιχείρηση, οι πληροφορίες που τον αφορούν διαγράφονται από τον directory ανθρωπίνων πόρων, αλλά μπορεί να υπάρξει καθυστέρηση μέχρι να διαγραφούν και από τους υπόλοιπους directories. Το πρόβλημα που δημιουργείται έχει να κάνει με την ασφάλεια του δικτύου, καθώς ο συγκεκριμένος υπάλληλος, παρότι έχει φύγει από την επιχείρηση, διατηρεί το δικαίωμα της απομακρυσμένης πρόσβασης στο δίκτυό της.

Συνοψίζοντας, θα πρέπει να αναφερθεί ότι, με τη χρήση των directories, οι επιχειρήσεις προσπαθούν να προσφέρουν δύο ειδών υπηρεσίες: Απλοποίηση της

πρόσβασης στο δίκτυο για τους χρήστες και παροχή πληροφοριών στους σωστούς ανθρώπους, στη σωστή τοποθεσία και στην κατάλληλη χρονική στιγμή με ταυτόχρονη ελαχιστοποίηση του κόστους για την επιχείρηση. Όταν, όμως, αντί για έναν καθολικό directory, υπάρχουν πολλαπλοί, δημιουργούνται τα παρακάτω προβλήματα που σχετίζονται με την αδυναμία του δικτύου να διαχειριστεί και να συσχετίσει τα δεδομένα που βρίσκονται αποθηκευμένα σε διαφορετικούς directories [13]:

- ο **Απουσία ελέγχου της κατανομής εύρους ζώνης (bandwidth allocation).** Οι διάφορες εφαρμογές χρειάζονται διαφορετικό εύρος ζώνης, ανάλογα με τη φύση τους. Για παράδειγμα, μία εφαρμογή μπορεί να χρειαστεί να μεταδώσει video σε μία συγκεκριμένη αλλά απρόβλεπτη στιγμή. Αν το δίκτυο δεν μπορεί να διαθέσει άμεσα στην εφαρμογή αυτή το απαιτούμενο εύρος ζώνης, τότε η εφαρμογή δεν θα μπορέσει να επιτύχει το σκοπό της. Αντίθετα, αν το δίκτυο έχει τη δυνατότητα της άμεσης, δυναμικής κατανομής του εύρους ζώνης, οι δικτυακές εφαρμογές εκτελούνται αποτελεσματικά και το συνολικό κόστος λειτουργίας του δικτύου μειώνεται δραματικά.
- ο **Απουσία ελέγχου καθυστέρησης.** Ορισμένες εφαρμογές μπορεί να έχουν συγκεκριμένες απαιτήσεις καθυστέρησης. Έτσι, ενώ η αποστολή e-mail δε χρειάζεται ιδιαίτερη μεταχείριση, η μετάδοση φωνής πρέπει να έχει υψηλή προτεραιότητα καθώς υπάρχει ένα άνω όριο καθυστέρησης. Τα δίκτυα, λοιπόν, θα πρέπει να έχουν τη δυνατότητα απόδοσης προτεραιότητας σε συγκεκριμένες εφαρμογές.
- ο **Αργή και δαπανηρή διαχείριση του δικτύου.** Αν η διαχείριση του δικτύου είναι αποκεντροποιημένη, η διόρθωση προβλημάτων γίνεται με αργό ρυθμό, αυξάνοντας το κόστος της μη λειτουργίας του δικτύου. Χαρακτηριστικό είναι το πρόβλημα της αναβάθμισης του λογισμικού των εκατοντάδων υπολογιστών ενός δικτύου. Αν η διαδικασία αυτή δεν είναι αυτοματοποιημένη, το κόστος της αναβάθμισης του λογισμικού για κάθε υπολογιστή ξεχωριστά φτάνει σε αστρονομικά επίπεδα.
- ο **Έλλειψη ασφάλειας.** Κάθε επιχειρησιακό δίκτυο θα πρέπει να έχει μία συγκεκριμένη πολιτική ασφάλειας. Για παράδειγμα, θα πρέπει να υπάρχει ένα μόνο password για κάθε οντότητα, μέσω του οποίου θα ελέγχεται η πρόσβαση

σε όλους τους πόρους του δικτύου. Λαμβάνοντας υπόψη το πρόβλημα που μπορεί να δημιουργηθεί αν κάποιος συνεργάτης της επιχείρησης μεταβληθεί σε ανταγωνιστή και εξακολουθεί να έχει πρόσβαση στο επιχειρησιακό δίκτυο, γίνεται φανερό η σημασία που αποκτά η ύπαρξη συγκεκριμένης πολιτικής ασφάλειας η οποία μπορεί να υλοποιηθεί άμεσα σε ολόκληρο το δίκτυο.

- **Έλλειψη συνεπούς δικτυακής πολιτικής (network policy).** Η έλλειψη ενός κεντρικού χώρου αποθήκευσης της πολιτικής του δικτύου οδηγεί στην αυθαίρετη απόδοση εύρους ζώνης και προτεραιοτήτων από τους τοπικούς διαχειριστές του δικτύου. Έτσι δεν είναι δυνατή η απόδοση εγγύησης ότι μία εφαρμογή θα εκτελεστεί επιτυχώς.
- **Απουσία ελέγχου των χρηστών.** Τα επιχειρησιακά δίκτυα δεν μπορούν να περιορίσουν την πρόσβαση των χρηστών σε κρίσιμες περιόδους. Κατά τη διάρκεια μίας τηλεδιάσκεψης θα ήταν λογική η απαγόρευση αποστολής e-mail ή αναζητήσεων στο web κάτι το οποίο δεν μπορεί να επιτευχθεί με αποκεντροποιημένη διαχείριση του δικτύου.
- **Αργή απόκριση της επιχείρησης στις ανάγκες της αγοράς.** Καθώς οι εμπορικές δραστηριότητες στον 21^ο αιώνα περιστρέφονται όλο και περισσότερο γύρω από το Internet, κάθε επιχείρηση πρέπει να αντιδρά γρήγορα και αποτελεσματικά στις αλλαγές που συμβαίνουν. Αν το δίκτυο της επιχείρησης δεν υποστηρίζει τις γρήγορες αλλαγές το αποτέλεσμα είναι η απώλεια επιχειρηματικών ευκαιριών.
- **Ανακριβή δεδομένα.** Λόγω του γεγονότος ότι τα δεδομένα της επιχείρησης είναι εξαπλωμένα σε μεγάλο αριθμό directories, μία μικρή αλλαγή είναι δυνατόν να μη διαδοθεί σε όλους. Έτσι, αν η διεύθυνση ενός πελάτη αλλάξει και η αλλαγή αυτή δεν διαδοθεί σε ολόκληρο το δίκτυο, η επικοινωνία με το συγκεκριμένο πελάτη πιθανότατα θα διακοπεί.
- **Μη χρήσιμη αναπαραγωγή δεδομένων.** Εφόσον η αποθήκευση δεδομένων προσδίδει επιπλέον κόστος στη λειτουργία του δικτύου, η ύπαρξη ενός κεντρικοποιημένου directory μπορεί να μειώσει σημαντικά το κόστος αυτό.
- **Ασύμβατες μορφές αποθήκευσης δεδομένων.** Εξαιτίας του γεγονότος ότι τα δεδομένα αποθηκεύονται με διαφορετικές μορφές στους διάφορους directories,

οι εφαρμογές που είναι σχεδιασμένες ώστε να εκτελούνται χρησιμοποιώντας δεδομένα ενός συγκεκριμένου directory πρέπει να ανασχεδιαστούν ώστε να είναι δυνατή η εκτέλεσή τους λαμβάνοντας δεδομένα και από τους υπόλοιπους directories του δικτύου.

Από τα παραπάνω γίνεται φανερό ότι η ζωή των διαχειριστών δικτύων θα γινόταν πολύ πιο εύκολη αν υπήρχε ένας καθολικός directory για ολόκληρο το επιχειρησιακό δίκτυο. Με τη λέξη ‘καθολικός’ εννοείται ένας directory που θα ενοποιεί την αποθήκευση όλων των πληροφοριών που πρέπει να αποθηκεύονται σ’ αυτόν.

1.3 Λειτουργίες και λύσεις μιας καθολικής Directory Service

Μέχρι τώρα, οι directories εξετάστηκαν υπό την υπόθεση ο αριθμός τους σε ένα επιχειρησιακό δίκτυο είναι πολλαπλός. Ωστόσο, τα πραγματικά οφέλη που μπορεί να αποκομίσει μία επιχείρηση από τη χρήση των directory services γίνονται πραγματικότητα με την ενοποίηση όλων των directories σε έναν καθολικό ο οποίος πλέον παίζει το ρόλο ενός κοινού πόρου του δικτύου. Ο κοινός αυτός πόρος επιτρέπει στους χρήστες αλλά και στις εφαρμογές που εκτελούνται στο δίκτυο να εντοπίζουν άμεσα τους πόρους που απαιτούνται για την εκτέλεση συγκεκριμένων λειτουργιών [11]. Με την ενοποίηση, λοιπόν, των directories ενός δικτύου επιλύονται τα περισσότερα από τα προαναφερθέντα προβλήματα.

Καταρχάς, μία νέα λειτουργία του δικτύου καθίσταται δυνατή με τη χρήση των directories. Ένα δίκτυο βασισμένο σε πολιτικές (Policy Based Network – PBN) επιτρέπει στο διαχειριστή του δικτύου την παροχή υψηλής ποιότητας υπηρεσιών σε συγκεκριμένους χρήστες και εφαρμογές αλλά και την παροχή υπηρεσιών χαμηλότερης ποιότητας σε λιγότερο κρίσιμες εφαρμογές. Οι επιχειρήσεις χρησιμοποιούν την τεχνολογία των PBNs για τη βελτιστοποίηση της χρήσης του υπάρχοντος εύρους ζώνης, αποφεύγοντας, έτσι, τη δαπανηρή εγκατάσταση υψηλότερης ταχύτητας αγωγών αλλά και επιτυγχάνοντας την επιθυμητή απόδοση του δικτύου. Ο directory αποτελεί το κρισιμότερο συστατικό ενός PBN, εφόσον οι πολιτικές (policies) που καθορίζουν τον

τρόπο λειτουργίας του δικτύου βρίσκονται αποθηκευμένες σ' αυτόν και με τον τρόπο αυτό γίνονται διαθέσιμες σε συσκευές όπως hubs, routers και switches.

Οι directories αποτελούν το πλέον κατάλληλο σημείο για την αποθήκευση των πληροφοριών διαμόρφωσης των συσκευών που περιλαμβάνονται σε ένα δίκτυο. Η υποστήριξη που παρέχουν για την αυτόματη διαχείριση διαμόρφωσης (device configuration management) επιτρέπει στις δικτυακές συσκευές να λαμβάνουν τις παραμέτρους διαμόρφωσής τους απευθείας από τον directory. Τα οφέλη μιας τέτοιας προσέγγισης είναι προφανή, καθώς αν σε ένα δίκτυο υπάρχουν ήδη δέκα διαμορφωμένοι routers, ο διαχειριστής του δικτύου δεν θα πρέπει να ανησυχεί για τη διαμόρφωση του ενδέκατου. Προφανώς ο νέος router θα αυτοδιαμορφωθεί λαμβάνοντας τις κατάλληλες παραμέτρους από τον directory και αυτόματα θα αρχίσει να λειτουργεί κάνοντας έτσι δυνατή τη δημιουργία ενός plug n' play δικτύου.

Η υποστήριξη της ασφάλειας του δικτύου αποτελεί μία ακόμη προφανή λειτουργία των directories. Οι απαραίτητες για την ασφάλεια του δικτύου πληροφορίες, όπως usernames, passwords και certificates αποθηκεύονται στον directory ο οποίος επιτρέπει πλέον στους χρήστες το απλό login, κάτι που απαιτεί από αυτούς να πιστοποιήσουν μία και μόνο φορά την ταυτότητά τους στον directory. Όλοι οι υπόλοιποι servers και οι εφαρμογές χρησιμοποιούν τις πληροφορίες ελέγχου πρόσβασης που βρίσκονται αποθηκευμένες στον directory για να επιτρέψουν ή όχι την πρόσβαση στις υπηρεσίες τους ενός συγκεκριμένου χρήστη.

Οι υπηρεσίες 'κίτρινων σελίδων' (yellow pages) βρίσκονται, επίσης, στο πεδίο δράσης των directories. Είναι πολλές οι εφαρμογές που απευθύνουν ερωτήσεις προς έναν directory αναζητώντας όλες τις οντότητες των οποίων τα χαρακτηριστικά ικανοποιούν συγκεκριμένα κριτήρια. Για παράδειγμα, μία εφαρμογή ηλεκτρονικού εμπορίου μπορεί να αναζητά όλες τις εταιρείες που κατασκευάζουν προϊόντα ψηφιακού ήχου. Οι υπηρεσίες κίτρινων σελίδων είναι ιδιαίτερα χρήσιμες στο πεδίο του ηλεκτρονικού εμπορίου και καθώς αυτό επεκτείνεται ολοένα και σε περισσότερες επιχειρήσεις, είναι προφανής η χρησιμότητα των directories στις επιχειρήσεις αυτές και η αύξηση της ζήτησης των directory services.

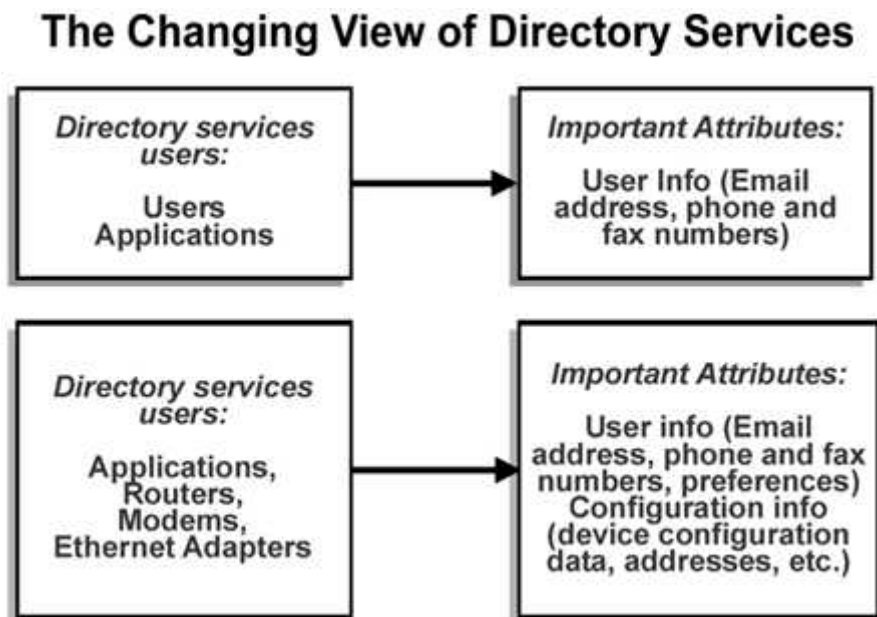
Οι υπηρεσίες αυτές, που παρέχονται από τους directories έχουν θετικό αντίκτυπο τόσο στη λειτουργία του επιχειρησιακού δικτύου όσο και γενικότερα στη λειτουργία

ολόκληρης της επιχείρησης. Παρόλο που η χρήση των συγκεκριμένων υπηρεσιών είναι σε ορισμένες περιπτώσεις δαπανηρή, το κόστος αυτό υποσκελίζεται από το γεγονός ότι οι directories παρέχουν στις επιχειρήσεις τις παρακάτω δυνατότητες [13]:

- ο **Άμεση απόκριση της επιχείρησης στις ανάγκες της αγοράς.** Η δυνατότητα μιας επιχείρησης να ενσωματώσει άμεσα μία νέα τεχνολογία στις δικτυακές της εφαρμογές και η δυνατότητα κλιμάκωσης του δικτύου της αυξάνει τις επιχειρηματικές της ευκαιρίες λόγω της μεγάλης σημασίας που έχει αποκτήσει η χρήση των δικτύων στον σημερινό επιχειρηματικό κόσμο τόσο όσον αφορά τη μεταξύ των εταιρειών επικοινωνία όσο και την επικοινωνία μεταξύ των εταιρειών και των προμηθευτών ή των πελατών τους.
- ο **Γρήγορη και αποδοτική, όσον αφορά το κόστος, διαχείριση του δικτύου.** Εφόσον η διαχείριση του δικτύου είναι κεντροκοποιημένη, τα σφάλματα στη λειτουργία του δικτύου μπορούν εύκολα να απομονωθούν και να διορθωθούν. Το αποτέλεσμα είναι η μείωση του κόστους λειτουργίας του δικτύου.
- ο **Ακρίβεια δεδομένων.** Τα συνολικά έξοδα μιας επιχείρησης μειώνονται σημαντικά αν τα δεδομένα που χρειάζεται για τη λειτουργία της είναι ακριβή, κατεύθυνση προς την οποία οδηγούν οι directory services. Παράδειγμα ελάττωσης των εξόδων αποτελεί η απουσία λαθών σε λογαριασμούς και σε τιμολόγια.
- ο **Συμβατότητα των αποθηκευμένων δεδομένων.** Η συμβατότητα των αποθηκευμένων δεδομένων, όσον αφορά τη μορφή τους, δίνει τη δυνατότητα σε όλες τις εφαρμογές που τα χρησιμοποιούν να έχουν ενιαία όψη των δεδομένων της επιχείρησης. Με τον τρόπο αυτό δεν χρειάζεται η τροποποίηση των δικτυακών εφαρμογών ανάλογα με τα χρησιμοποιούμενα δεδομένα για την εκτέλεσή τους.

Το συμπέρασμα που μπορεί να εξαχθεί λαμβάνοντας υπόψη τις πιο πάνω εφαρμογές μιας directory service είναι ότι η χρήση των directories ως απλά ευρετήρια πληροφοριών από χρήστες και εφαρμογές έχει πάψει να υφίσταται. Οι directories, πλέον, αποθηκεύουν όλες τις πληροφορίες που αφορούν συγκεκριμένες οντότητες που υπάρχουν σε ένα δίκτυο. Τέτοιες οντότητες είναι οι χρήστες, οι εφαρμογές, οι συσκευές και οι διάφορες υπηρεσίες. Οι πληροφορίες αυτές χρησιμοποιούνται είτε από τις ίδιες

τις οντότητες, είτε από άλλους χρήστες ή προγράμματα που χρειάζονται την πρόσβαση σ' αυτές.



Εικόνα 1.3: Η αλλαγή του ρόλου των directory services.

Στην εικόνα 1.3 φαίνεται η αλλαγή του ρόλου των directory services σε σχέση τόσο με τα χαρακτηριστικά των οντοτήτων τα οποία αποθηκεύουν όσο και με τις οντότητες που κάνουν χρήση των αποθηκευμένων πληροφοριών.

1.4 Διαφορές μεταξύ των Directories και των Βάσεων Δεδομένων

Ο ορισμός των directories αναφέρει ότι πρόκειται για βάσεις δεδομένων (data bases) με αποτέλεσμα να δημιουργείται σύγχυση ανάμεσα στις δύο αυτές έννοιες. Οι directories αποτελούν εξειδικευμένες βάσεις δεδομένων με συγκεκριμένα χαρακτηριστικά που τους διαφοροποιούν από αυτές.

Το πρώτο από τα χαρακτηριστικά αυτά είναι το γεγονός ότι ένας directory προσπελάζεται πολύ συχνά για λειτουργίες αναζήτησης και πολύ σπάνια για λειτουργίες εγγραφής. Για το λόγο αυτό οι directories είναι βελτιστοποιημένοι για

προσπελάσεις ανάγνωσης. Οι προσπελάσεις εγγραφής περιορίζονται στους διαχειριστές συστημάτων και στους ιδιοκτήτες των συγκεκριμένων πληροφοριών. Αντίθετα, μία βάση δεδομένων γενικού σκοπού υποστηρίζει προσπελάσεις ανάγνωσης και εγγραφής με την ίδια βαρύτητα.

Το γεγονός ότι οι directories είναι βελτιστοποιημένοι για την αποθήκευση στατικών πληροφοριών τους κάνει ακατάλληλους για αποθήκευση πληροφοριών που αλλάζουν ταχύτατα. Για παράδειγμα, ο αριθμός των εργασιών που βρίσκονται στην ουρά ενός εκτυπωτή δεν θα πρέπει να αποθηκεύεται σε κάποιον directory, επειδή μία τέτοια πληροφορία θα πρέπει να ανανεώνεται συχνότατα ώστε να είναι ακριβής. Αντίθετα, η διεύθυνση ενός print server αποτελεί χαρακτηριστικό παράδειγμα πληροφορίας που αποθηκεύεται σε έναν directory.

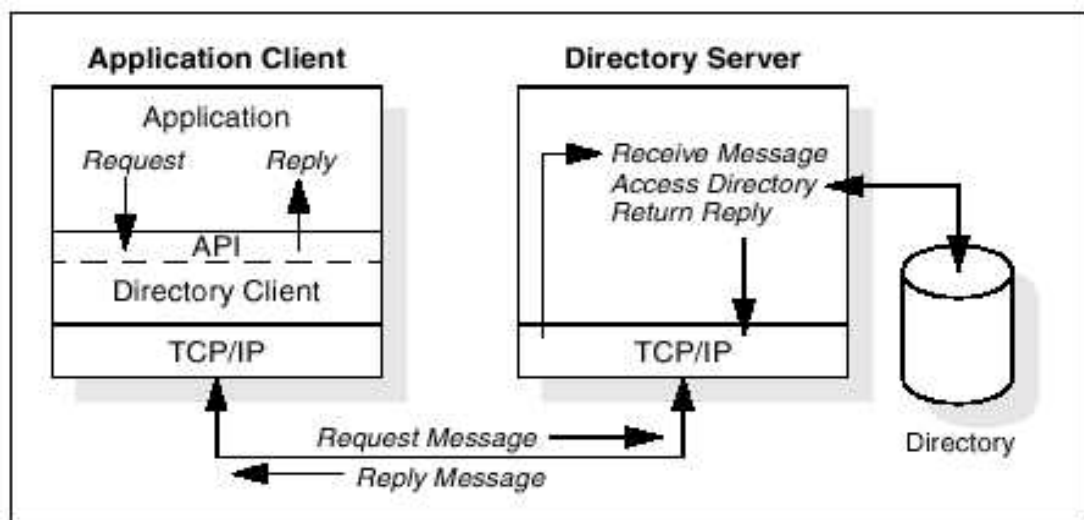
Ένα άλλο χαρακτηριστικό των directories είναι το γεγονός ότι δεν μπορούν να υποστηρίξουν transactions, δηλαδή λειτουργίες οι οποίες πρέπει είτε να ολοκληρωθούν οπωσδήποτε ή, αν αυτό δεν είναι δυνατόν, να μην ξεκινήσουν καθόλου. Παράδειγμα τέτοιας λειτουργίας αποτελεί η μεταβίβαση κεφαλαίου μεταξύ τραπεζικών λογαριασμών η οποία δεν επιτρέπεται να διακοπεί πριν την ολοκλήρωσή της και φυσικά υποστηρίζεται από ένα κλασσικό σύστημα διαχείρισης βάσεων δεδομένων.

Οι directories είναι συνήθως περιορισμένοι ως προς τους τύπους των δεδομένων που επιτρέπεται να αποθηκεύσουν. Έτσι, ένας directory εξειδικευμένος για την αποθήκευση στοιχείων των πελατών μιας επιχείρησης μπορεί να είναι περιορισμένος ώστε να αποθηκεύει μόνο στοιχεία όπως το όνομα του κάθε πελάτη, η διεύθυνσή του και ο τηλεφωνικός του αριθμός.

Τέλος, μία πολύ σημαντική διαφορά ανάμεσα στους directories και στις βάσεις δεδομένων αφορά τον τρόπο προσπέλασής τους. Οι περισσότερες βάσεις δεδομένων υποστηρίζουν μία πολύ ισχυρή μέθοδο προσπέλασης μέσω της γλώσσας SQL (Structured Query Language). Η SQL επιτρέπει πολύπλοκες λειτουργίες ερώτησης και ανανέωσης της βάσης. Από την άλλη μεριά οι directories χρησιμοποιούν ένα συγκεκριμένο πρωτόκολλο ελέγχου πρόσβασης (access protocol) όπως το X.500 και το LDAP.

1.5 Directory Clients & Servers (Πελάτες και Εξυπηρετητές)

Οι directories προσπελούνται συνήθως χρησιμοποιώντας το μοντέλο client-server. Μία εφαρμογή που θέλει να διαβάσει ή να γράψει πληροφορίες στον directory καλεί μία συνάρτηση (function) η οποία προκαλεί την αποστολή ενός μηνύματος σε μία άλλη διαδικασία. Η διαδικασία αυτή προσπελάει την πληροφορία στον directory και τα αποτελέσματα της ανάγνωσης ή της εγγραφής επιστρέφονται στην αρχική εφαρμογή όπως φαίνεται στην εικόνα 1.4.



Εικόνα 1.4: Αλληλεπίδραση μεταξύ client και server

Η εφαρμογή που ζητά την προσπέλαση του directory ονομάζεται directory client ενώ η διαδικασία που διεκπεραιώνει αυτή την απαίτηση ονομάζεται directory server. Γενικά οι servers παρέχουν συγκεκριμένες υπηρεσίες στους clients. Πολλές φορές ένας server είναι δυνατόν να μετατραπεί σε client έτσι ώστε να συγκεντρώσει τις απαραίτητες πληροφορίες για τη διεκπεραίωση μιας αίτησης.

2. X.500

Το X.500 αποτελεί μία σειρά προτύπων τα οποία αναπτύχθηκαν από την ISO/ITU-T και καθορίζουν τον τρόπο με τον οποίο οι πληροφορίες αποθηκεύονται και προσπελάζονται σε μία directory service. Η σειρά αυτή των προτύπων δημοσιεύθηκε για πρώτη φορά το 1988 αλλά ανανεώθηκε το 1993 και το 1997. Σήμερα, οι περισσότεροι X.500 directory servers ακολουθούν το πρότυπο του 1993 έχοντας υιοθετήσει και αρκετά χαρακτηριστικά του προτύπου του 1997 [17]. Τα πρότυπα αυτά δεν καθορίζουν τις εσωτερικές λειτουργίες ενός X.500 server. Αντίθετα, επικεντρώνονται στη δομή της πληροφοριών που αποθηκεύονται σε έναν X.500 server αλλά και στον τρόπο επικοινωνίας του με τους clients που απαιτούν πρόσβαση στις συγκεκριμένες πληροφορίες.

Μία καθολική directory service είναι συχνά σχεδιασμένη έτσι ώστε ο directory και η διαχείρισή του να βρίσκονται κατανεμημένοι σε μεγάλο αριθμό από ξεχωριστούς directory servers. Το X.500 επιτρέπει σε ένα χρήστη να απευθύνει ερωτήσεις σε οποιονδήποτε από τους directory servers, να λαμβάνει μία ενιαία όψη της καθολικής directory service και να διατυπώνει απαιτήσεις για πρόσβαση σε συγκεκριμένες πληροφορίες οι οποίες μπορούν να βρίσκονται σε οποιονδήποτε server ο οποίος αποτελεί μέρος του καθολικού directory.

2.1 Συστατικά μιας X.500 Directory Service

Το X.500, για να μπορεί να παρέχει μία καθολική directory service, καθορίζει ένα πολύπλοκο και 'βαρύ' σύνολο προτύπων. Τα πρότυπα αυτά απαιτούν από μία directory service να υποστηρίζει τα παρακάτω χαρακτηριστικά [5]:

- ο Ιεραρχική ονοματολογία η οποία καθορίζει τον τρόπο με τον οποίο οργανώνονται οι πληροφορίες αλλά και τον τρόπο με τον οποίο μπορεί να γίνει η αναφορά σ' αυτές.

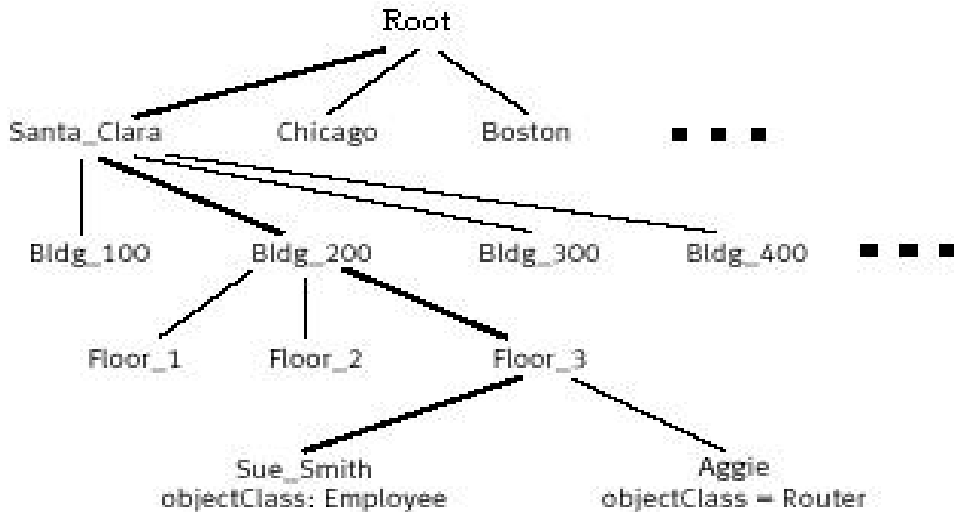
- ο Το πληροφοριακό μοντέλο (information model) που περιγράφει τη μορφή και τη δομή (schema) των πληροφοριών που αποθηκεύονται στον directory. Η έννοια του schema είναι ανάλογη με την περίπτωση ενός έντυπου στο οποίο πρέπει να σημειωθούν συγκεκριμένες πληροφορίες σε συγκεκριμένες θέσεις. Οποιοσδήποτε μπορεί να κατανοήσει τη δομή που απαιτείται να έχουν οι πληροφορίες, μπορεί και να συμπληρώσει το έντυπο.
- ο Το λειτουργικό μοντέλο (functional model) που καθορίζει το πρωτόκολλο πρόσβασης (directory access protocol) καθώς και τις λειτουργίες που μπορούν να επιτελεστούν επί των αποθηκευμένων πληροφοριών (read, write, search, authenticate).
- ο Το μοντέλο πιστοποίησης της ταυτότητας (authentication model) που προστατεύει τις αποθηκευμένες πληροφορίες από μη εξουσιοδοτημένη πρόσβαση.
- ο Το μοντέλο κατανεμημένης λειτουργίας (distributed operation model) που περιγράφει τον τρόπο με τον οποίο τα δεδομένα κατανέμονται στους διάφορους servers και τις λειτουργίες που πρέπει να εκτελούνται για το συγχρονισμό του καθολικού directory.

2.2 Η δενδρική δομή του X.500

Οι καταχωρήσεις σε έναν directory διευθετούνται με βάση μία ιεραρχική, δενδροειδή δομή η οποία αντανακλά πολιτικά όρια, γεωγραφικά όρια ή όρια ανάμεσα στα τμήματα μιας επιχείρησης. Η δομή αυτή ονομάζεται πληροφοριακό δένδρο (Directory Information Tree - DIT). Μεταξύ ενός συνόλου ονομάτων και των χαρακτηριστικών που περιγράφουν τις οντότητες οι οποίες έχουν τα συγκεκριμένα ονόματα υπάρχει μία καλά καθορισμένη σχέση, όπως φαίνεται και στην εικόνα 2.1, η διατήρηση της οποίας αποτελεί ευθύνη του directory.

Κάθε οντότητα του DIT έχει μοναδικό όνομα το οποίο ονομάζεται Distinguished Name (DN). Το DN μιας συγκεκριμένης οντότητας καθορίζεται από τη σχετική θέση της οντότητας αυτής στο DIT. Για παράδειγμα, το DN της Sue Smith θα είναι

‘Santa_Clara; Bldg_200; Floor_3; Sue_Smith’. Η λειτουργία των DNS είναι παρόμοια με τη λειτουργία των URLs, τα οποία παρέχουν πρόσβαση σε μοναδικές σελίδες του World Wide Web. Με παρόμοιο τρόπο τα DNS παρέχουν πρόσβαση σε μοναδικές οντότητες του directory.



Εικόνα 2.1: X.500 Directory Information Tree.

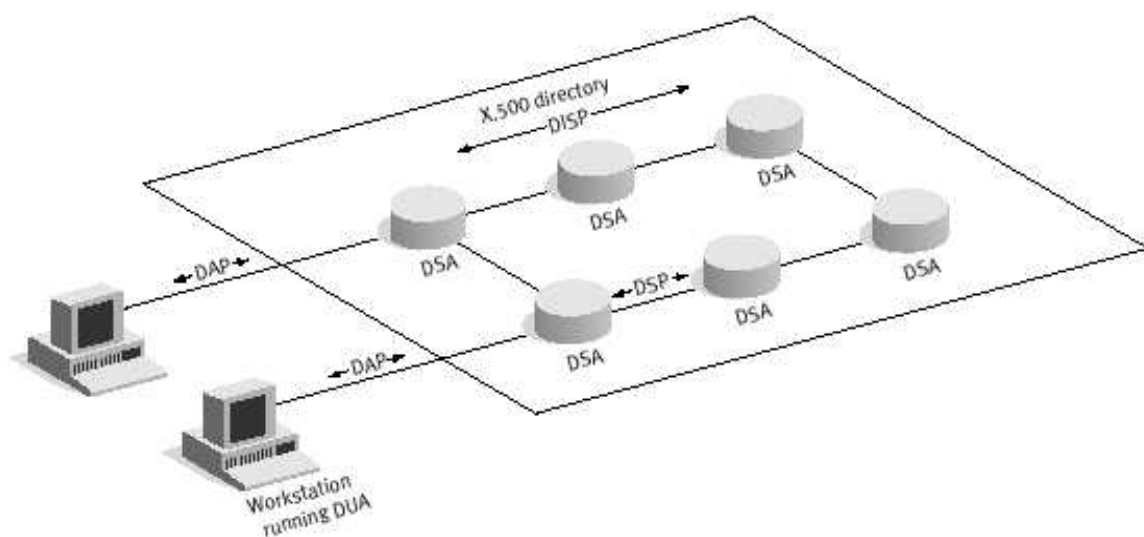
Κάθε οντότητα αντιπροσωπεύεται από μία συγκεκριμένη καταχώρηση στο DIT και περιλαμβάνει ένα σύνολο χαρακτηριστικών. Τα χαρακτηριστικά αυτά περιέχουν τις αποθηκευμένες πληροφορίες για κάθε οντότητα. Για παράδειγμα, τα χαρακτηριστικά που συνδέονται με την οντότητα ‘Sue_Smith’ είναι ο κωδικός αριθμός της, το τμήμα στο οποίο εργάζεται, το όνομα του προϊσταμένου της, ο αριθμός τηλεφώνου της, η ηλεκτρονική της διεύθυνση, η IP address του workstation της, το login name και το password της καθώς και τα δικαιώματα πρόσβασής της στο δίκτυο κ.τ.λ.

Εφόσον ο διαχειριστής του δικτύου πρέπει να διατηρεί πληροφορίες για διαφορετικούς τύπους οντοτήτων, το σύνολο των χαρακτηριστικών που αντιστοιχούν σε έναν εργαζόμενο είναι, σαφώς, διαφορετικό από το σύνολο των χαρακτηριστικών που αντιστοιχούν σε έναν printer, σε έναν router ή σε έναν file server. Επομένως, κάθε καταχώρηση στο DIT πρέπει να περιλαμβάνει ένα χαρακτηριστικό με το όνομα objectClass. Το χαρακτηριστικό αυτό καθορίζει τον τύπο της οντότητας (εργαζόμενος, switch, router κ.τ.λ) που αντιστοιχεί στη συγκεκριμένη καταχώρηση όπως, επίσης, και

ποια χαρακτηριστικά είναι απαραίτητο να έχουν κάποια τιμή και ποια όχι. Το σύνολο των χαρακτηριστικών που αποθηκεύονται για μία συγκεκριμένη οντότητα αποτελεί το schema της οντότητας αυτής.

2.3 Το λειτουργικό μοντέλο του X.500

Το DIT, που καθορίζει στην ουσία τη δομή ενός X.500 directory, αποτελεί ένα μόνο μέρος της καθολικής directory service. Το X.500 καθορίζει, επίσης, τους τύπους των πρακτόρων (agents) και τα πρωτόκολλα που εκτελούνται σε διάφορους servers και παρέχουν πρόσβαση στις αποθηκευμένες στον directory πληροφορίες. Η εικόνα 2.2 απεικονίζει το λειτουργικό μοντέλο ενός X.500 directory.



Εικόνα 2.2: Το λειτουργικό μοντέλο ενός X.500 Directory.

Ένας X.500 directory αποτελείται από ένα σύνολο πρακτόρων συστήματος directory (Directory System Agents – DSAs) οι οποίοι βρίσκονται κατανεμημένοι σε ολόκληρο το δίκτυο μιας επιχείρησης. Κάθε DSA διατηρεί ένα μόνο μέρος των πληροφοριών ολόκληρης της πληροφοριακής βάσης του directory (Directory Information Base – DIB) το οποίο ονομάζεται τεμάχιο (fragment). Ένας DSA μπορεί να απαντά σε ερωτήματα σχετικά με πληροφορίες που βρίσκονται στο δικό του fragment ή

να προωθεί τα ερωτήματα στους κατάλληλους DSAs που περιέχουν τις συγκεκριμένες πληροφορίες. Η λειτουργία αυτή είναι ο 'συνδεδετικός κρίκος' που συντηρεί την κατανεμημένη X.500 directory service.

Οι πράκτορες-χρήστες του directory (Directory User Agents – DUAs) είναι είτε αυτόνομα προγράμματα είτε διαδικασίες μέσα σε εφαρμογές οι οποίες παρέχουν τη διασύνδεση (interface) ανάμεσα στην επιφάνεια εργασίας (desktop) του χρήστη και σε έναν τοπικό DSA. Ένας DUA επικοινωνεί με έναν DSA μέσω του πρωτοκόλλου πρόσβασης στον directory (Directory Access Protocol – DAP). Ένα δεύτερο πρωτόκολλο, το πρωτόκολλο υπηρεσίας directory (Directory Service Protocol – DSP), μεταδίδει ένα ερώτημα μεταξύ των DSAs όταν αυτό δεν μπορεί να απαντηθεί από έναν τοπικό DSA. Τέλος, ένα τρίτο πρωτόκολλο, το πρωτόκολλο αντιγραφής πληροφορίας του directory (Directory Information Shadowing Protocol – DISP), επιτρέπει την αντιγραφή των πληροφοριών που διατηρούνται σε έναν DSA και σε άλλους DSAs. Το DISP είναι ένα πολύ ισχυρό εργαλείο, αφού επιτρέπει σε πολλαπλά αντίγραφα των πληροφοριών να ικανοποιούν τα ερωτήματα των χρηστών, κάτι που οδηγεί σε βελτίωση της απόδοσης του δικτύου και σε αύξηση της αντοχής του σε σφάλματα (fault tolerance).

Όταν ένα ερώτημα δεν μπορεί να απαντηθεί από έναν DSA, τότε θα πρέπει να διαδοθεί στους υπόλοιπους DSAs. Η διάδοση αυτή μπορεί να γίνει με τους εξής τρόπους [17]:

- ο **Chaining** (αλυσιδωτός): Αν ένας DSA δεν έχει τη ζητούμενη πληροφορία, το ερώτημα μεταδίδεται στον επόμενο. Αν η πληροφορία δεν υπάρχει ούτε σ' αυτόν, το ερώτημα μεταδίδεται στον επόμενο κ.ο.κ. Αν κανείς από τους DSAs δεν περιέχει τη ζητούμενη πληροφορία, τότε μπορεί να προκληθεί ένας ατέρμων βρόχος. Για την αποφυγή αυτού του φαινομένου, διατηρείται ένας κατάλογος με όλους τους DSAs που έχουν ερωτηθεί έτσι ώστε να αποφεύγεται η δεύτερη προσπέλαση του ίδιου DSA. Με την τεχνική αυτή δίνεται η εντύπωση στους DUAs ότι υπάρχει ένας μόνο DSA ο οποίος απαντά στα ερωτήματά τους και οι πιθανές απαντήσεις είναι δύο. Είτε επιστρέφεται η ζητούμενη πληροφορία, ή επιστρέφεται ένα μήνυμα λάθους που σημαίνει ότι η

ζητούμενη πληροφορία δεν βρίσκεται στον directory ή ότι προέκυψε κάποιο σφάλμα κατά την αναζήτησή της.

- ο **Referral** (αναφορικός): Αν η ζητούμενη πληροφορία δεν βρίσκεται σε έναν DSA, αυτός στέλνει ένα μήνυμα προς τον DUA παραπέμποντάς τον σε έναν άλλο DSA. Ο DUA πρέπει να έχει τη δυνατότητα αποκωδικοποίησης του μηνύματος ώστε να αποκαταστήσει μία σύνδεση με τον αναφερόμενο DSA. Η διαδικασία αυτή συνεχίζεται μέχρι τη λήψη της ζητούμενης πληροφορίας. Ο referral τρόπος διάδοσης του ερωτήματος απαιτεί μεγαλύτερη πολυπλοκότητα των DUAs, εφόσον θα πρέπει να είναι ικανοί να αποκωδικοποιούν τα μηνύματα που λαμβάνουν από τους DSAs και χρησιμοποιείται συνήθως σε περιπτώσεις όπου είναι απαραίτητο ένα υψηλό επίπεδο ασφάλειας. Η ασφάλεια παρέχεται με την απαίτηση κάθε DSA να λαμβανει πιστοποίηση ταυτότητας από τον DUA που τον προσπελαύνει.
- ο **Multicasting** (πολλαπλή εκπομπή): Όταν χρησιμοποιείται multicasting ο πρώτος DSA στέλνει το ερώτημα ταυτόχρονα σε πολλούς DSAs. Οι απαντήσεις από κάθε DSA συνδυάζονται και επιστρέφονται στον DUA ως μία απάντηση. Υπάρχουν δύο τρόποι πολλαπλής εκπομπής του ερωτήματος. Μπορεί να σταλεί σε πολλούς DSAs είτε σύγχρονα είτε σειριακά.

Όσον αφορά την ανάκτηση της πληροφορίας από έναν X.500 directory, αυτή μπορεί να γίνει με μία από τις παρακάτω λειτουργίες:

- ο **Read**: Εξάγει πληροφορίες για μία ρητά καθορισμένη οντότητα που βρίσκεται αποθηκευμένη στον directory.
- ο **Compare**: Συγκρίνει μία τιμή που παρέχει ο χρήστης με μία συγκεκριμένη τιμή στον directory.
- ο **List**: Παρέχει πληροφορίες για όλα τα 'παιδιά' μιας καταχώρησης στο DIT.
- ο **Search**: Παρέχει παρόμοια λειτουργικότητα με τη List αλλά για ένα συγκεκριμένο μέρος του DIT. Οι Boolean τελεστές AND, NOT και OR μπορούν να χρησιμοποιηθούν για το φιλτράρισμα των εξαγόμενων πληροφοριών.

2.4 Μειονεκτήματα του X.500

Παρά το στιβαρό και κατανοητό σύνολο χαρακτηριστικών του X.500, υπάρχουν πολλοί λόγοι για τους οποίους δεν έχει υλοποιηθεί μεγάλος αριθμός X.500 directories σε επιχειρησιακά δίκτυα:

- ο Το λογισμικό των X.500 servers είναι πολύπλοκο και παρουσιάζονται εξαιρετικές δυσκολίες στη συνεργασία του με τις σχετικά απλές directory services των επιχειρησιακών δικτύων.
- ο Υπάρχουν πολύ λίγα πακέτα λογισμικού για X.500 clients τα οποία είναι συνήθως πολύπλοκα και με μεγάλες απαιτήσεις σε υπολογιστική ισχύ, κάτι που καθιστά δύσκολη τη λειτουργία τους σε απλά PC.
- ο Το X.500 είναι στενά συνδεδεμένο με τα πρωτόκολλα του μοντάλου OSI και είναι πολύ δύσκολη η υλοποίησή του πάνω από TCP/IP.

Γενικά, καθώς το X.500 είναι ένα πρωτόκολλο του επιπέδου εφαρμογής (application level) του μοντέλου OSI για την επικοινωνία ενός DUA με έναν DSA μέσω του DAP χρησιμοποιείται η στοίβα πρωτοκόλλων του μοντέλου OSI. Το πρόβλημα είναι ότι η στοίβα των πρωτοκόλλων του μοντέλου OSI απαιτεί τεράστια ποσά μνήμης και μεγάλη υπολογιστική ισχύ. Για το λόγο αυτό η υλοποίηση X.500 directory services είναι προβληματική ακόμη και με τη βοήθεια των σημερινών πολύ ισχυρών υπολογιστικών συστημάτων.

3. LDAP (Lightweight Directory Access Protocol)

Το Lightweight Directory Access Protocol (LDAP) άρχισε να αναπτύσσεται στις αρχές της δεκαετίας του 90 στο Πανεπιστήμιο του Michigan ως μία ‘ελαφριά’ εναλλακτική λύση στο ‘βαρύ’ DAP του X.500. Το LDAP είναι σε σχέση με το X.500 ότι το IP σε σχέση με το OSI. Δίνει περισσότερη έμφαση στον ελαφρύ και λειτουργικό κώδικα παρά στα αυστηρά πρότυπα (standards), δεδομένης της άμεσης ανάγκης της αγοράς για directory services.

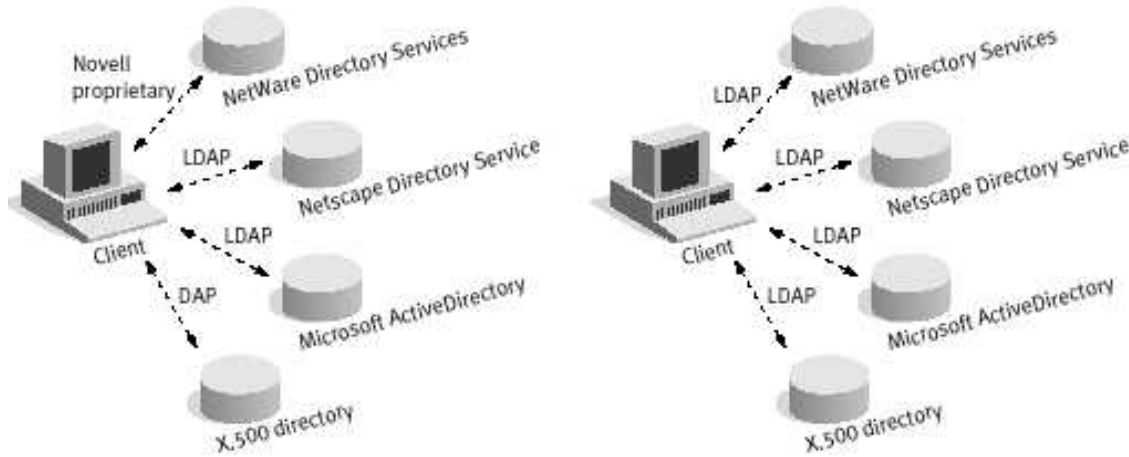
Το LDAP σχεδιάστηκε έτσι ώστε να παρέχει τις σημαντικότερες λειτουργίες του DAP, καθιστώντας, όμως, πιο εύκολη την υλοποίηση τους στην πλευρά των clients και ιδιαίτερα στην πλευρά των servers. Η εξέλιξη του LDAP έχει καταγραφεί σε ένα σύνολο Requests For Comments (RFCs) της Internet Engineering Task Force (IETF) [5]:

- ο RFC 1487 (Ιούλιος 1993): LDAPv1
- ο RFC 1777 (Μάρτιος 1995): LDAPv2
- ο RFC 2251 (Δεκέμβριος 1997): LDAPv3

Το LDAP αναπτύχθηκε απλά ως πρωτόκολλο πρόσβασης directory (directory access protocol) και όχι ως ολοκληρωμένο standard σαν το X.500. Το LDAP καθορίζει μόνο τον τρόπο με τον οποίο ένας client επικοινωνεί με έναν server για τη λήψη πληροφοριών. Δεν καθορίζει τη λειτουργία ολόκληρης της directory service.

Το σημαντικότερο πλεονέκτημα του LDAP είναι ότι παρέχει έναν τυποποιημένο μηχανισμό που επιτρέπει σε οποιονδήποτε client ή server και σε οποιαδήποτε εφαρμογή την πρόσβαση σε μία directory service που υποστηρίζει LDAP.

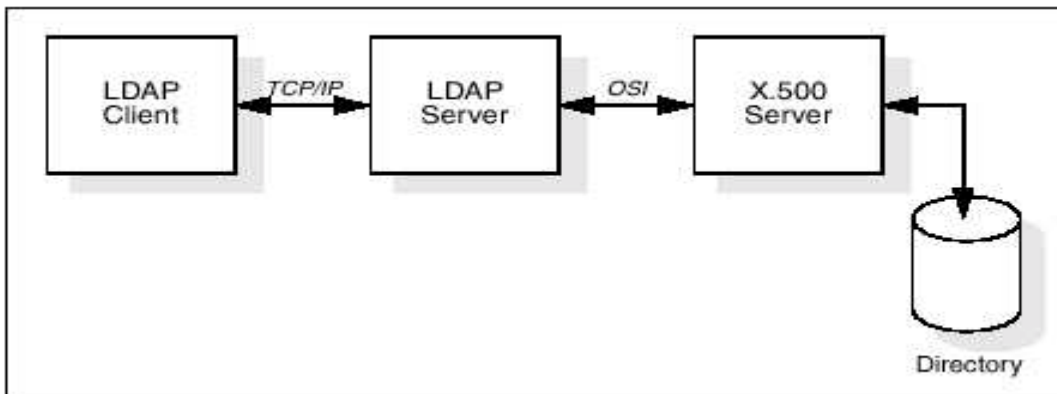
Στα αριστερά της εικόνας 3.1 ο client είναι υποχρεωμένος να εκτελεί πολλά πρωτόκολλα, ένα για κάθε directory service που θέλει να προσπελάσει. Στα δεξιά, ο client χρειάζεται μόνο να εκτελεί το LDAP ώστε να έχει πρόσβαση σε όλες τις directory services. Ο διαχειριστής του δικτύου εξακολουθεί να διαχειρίζεται πολλαπλές directory services αλλά καθένας από τους directories προσπελάζεται μέσω ενός κοινού πρωτοκόλλου πρόσβασης, του LDAP.



Εικόνα 3.1: Το LDAP παρέχει τυποποιημένη πρόσβαση σε κάθε directory.

3.1 Το LDAP ως ολοκληρωμένη Directory Service

Το LDAP καθορίζει ένα πρωτόκολλο επικοινωνίας, δηλαδή καθορίζει τη μορφή και τον τρόπο μεταφοράς των μηνυμάτων που χρησιμοποιούνται από έναν client για την προσπέλαση δεδομένων που βρίσκονται σε έναν X.500 directory. Αυτό σημαίνει ότι το LDAP δεν καθορίζει όλες τις πλευρές μιας directory service. Παρόλα αυτά υφίσταται ο όρος LDAP directory, η σημασία του οποίου θα πρέπει να διασαφηνιστεί.

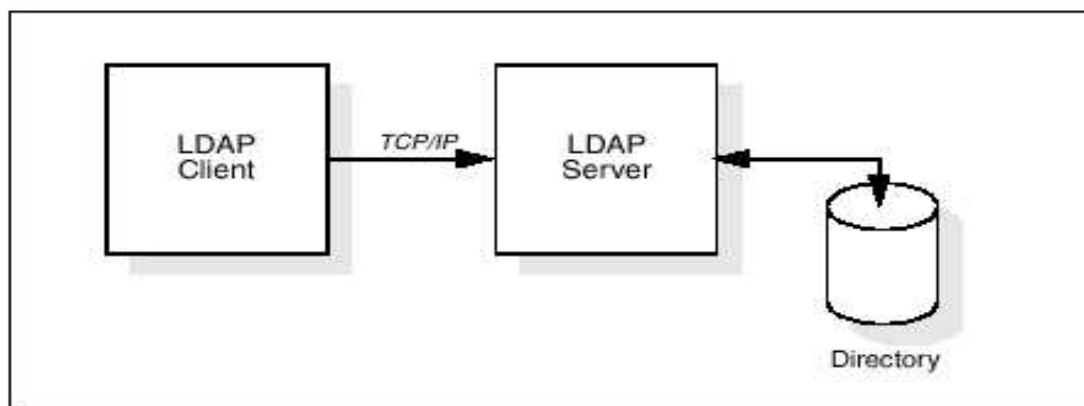


Εικόνα 3.2: Ο LDAP server δρα ως πύλη του X.500 server.

Μία client εφαρμογή αρχικοποιεί ένα μήνυμα LDAP καλώντας ένα LDAP API (Application Programming Interface). Ωστόσο, ένας X.500 directory δεν καταλαβαίνει

τα μηνύματα LDAP. Στην πραγματικότητα ένας LDAP client και ένας X.500 server χρησιμοποιούν διαφορετικά πρωτόκολλα επικοινωνίας (TCP/IP και OSI αντιστοίχως). Έτσι, ο LDAP client επικοινωνεί με μία πύλη (gateway) η οποία προωθεί τα μηνύματα στον X.500 server, όπως φαίνεται και στην εικόνα 3.2. Αυτή η πύλη ονομάζεται LDAP server και εξυπηρετεί τις απαιτήσεις ενός LDAP client μετατρέπόμενος ο ίδιος σε client του X.500 server. Επομένως ο LDAP server πρέπει να χρησιμοποιεί τόσο το TCP/IP όσο και το OSI.

Με την αύξηση της χρήσης του LDAP και την αναγνώριση των ωφελειών του, οι επιχειρήσεις που δεν είχαν X.500 servers ή το κατάλληλο περιβάλλον για την υποστήριξή τους θέλησαν να αναπτύξουν directories προσπελάσιμους από LDAP clients. Η προφανής λύση ήταν η αποθήκευση των directories σε LDAP servers. Η προσέγγιση αυτή εξαλείφει την ανάγκη χρήσης της στοίβας πρωτοκόλλων του OSI. Βέβαια, ο LDAP server γίνεται πολύ περισσότερο πολύπλοκος καθώς πρέπει να αποθηκεύει τις καταχωρήσεις του directory. Ένας τέτοιος LDAP server ονομάζεται αυτόνομος (stand-alone) LDAP server γιατί δεν εξαρτάται πλέον από τον X.500 server. Εφόσον το LDAP δεν υποστηρίζει όλες τις λειτουργίες του X.500, ένας αυτόνομος LDAP server πρέπει να υποστηρίζει μόνο τις λειτουργίες που απαιτούνται από το LDAP



Εικόνα 3.3: Αυτόνομος LDAP server.

Από την οπτική γωνία του client, κάθε server που τρέχει το πρωτόκολλο LDAP είναι ένας LDAP directory server, είτε τρέχει στην πραγματικότητα το LDAP, είτε αποτελεί πύλη ενός X.500 server. Παρομοίως, κάθε directory προσπελάσιμος μέσω του LDAP ονομάζεται LDAP directory.

3.2 Αρχιτεκτονική του LDAP

Το LDAP έχει αναπτυχθεί ανεξάρτητα από το X.500 και υπάρχουν σήμερα πολλοί servers που βασίζονται αποκλειστικά στο LDAP και όχι στο X.500. Η επιτυχία του LDAP βασίζεται σε μεγάλο βαθμό στα παρακάτω χαρακτηριστικά που το καθιστούν εύκολο στην υλοποίηση, συγκρινόμενο με το X.500 και το DAP [6]:

- ο Το LDAP τρέχει πάνω από το TCP/IP και όχι από τη στοίβα πρωτοκόλλων του OSI. Το TCP/IP είναι λιγότερο απαιτητικό σε πόρους και πολύ περισσότερο ευρέως διαθέσιμο.
- ο Το λειτουργικό μοντέλο του LDAP είναι απλούστερο, καθώς παραλείπει σπάνια χρησιμοποιούμενα και εσωτερικά χαρακτηριστικά. Το γεγονός αυτό κάνει το LDAP ευκολότερο στην κατανόηση και στην υλοποίηση.
- ο Το LDAP χρησιμοποιεί σειρές χαρακτήρων (strings) για την αναπαράσταση των δεδομένων και όχι πολύπλοκα δομημένα συντακτικά.

Το LDAP καθορίζει το περιεχόμενο και τη μορφή των μηνυμάτων που ανταλλάσσονται ανάμεσα στον LDAP client και τον LDAP server. Τα μηνύματα αυτά προσδιορίζουν τις λειτουργίες που ο client ζητά από τον server και μεταφέρονται μέσω του πρωτοκόλλου TCP/IP.

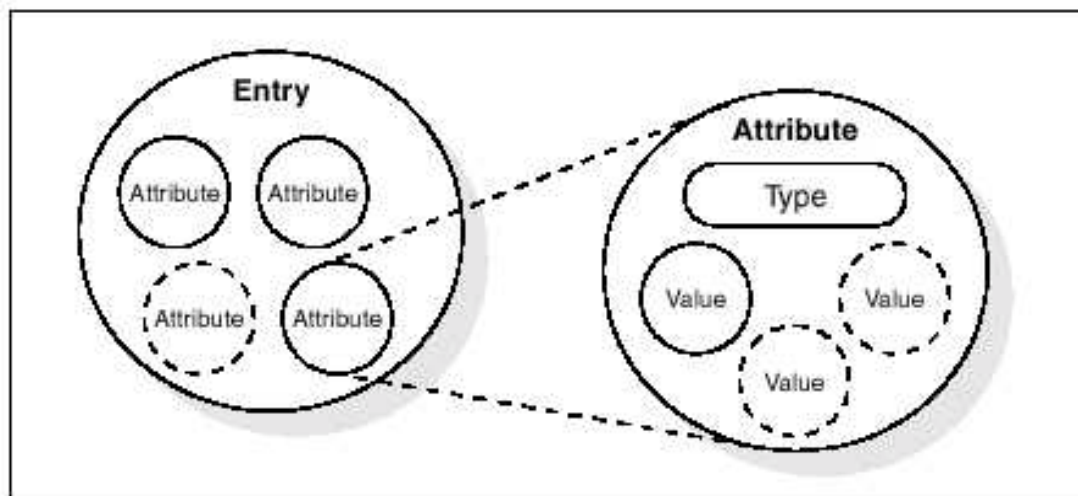
Ωστόσο, για το σχεδιαστή ενός LDAP directory, σημασία έχει όχι η μορφή των ανταλλασσόμενων μηνυμάτων αλλά το πώς είναι οργανωμένες οι πληροφορίες στον directory, ποιες είναι οι δυνατές λειτουργίες επί των πληροφοριών αυτών, πώς προστατεύονται κ.ο.κ. Το LDAP μπορεί να γίνει ευκολότερα κατανοητό με την εξέταση των μοντέλων στα οποία βασίζεται:

- ο **Information model (πληροφοριακό μοντέλο)**: Καθορίζει τη δομή των πληροφοριών που αποθηκεύονται σε έναν LDAP directory.
- ο **Naming model (μοντέλο ονοματολογίας)**: Περιγράφει τον τρόπο με τον οποίο οργανώνονται οι πληροφορίες στον directory.
- ο **Functional model (λειτουργικό μοντέλο)**: Προσδιορίζει τις λειτουργίες που μπορούν να επιτελεσθούν επί των αποθηκευμένων στον directory πληροφοριών.

- ο **Security model (μοντέλο ασφάλειας)**: Καθορίζει τον τρόπο προστασίας των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση.

3.2.1 Το πληροφοριακό μοντέλο

Η βασική μονάδα πληροφορίας που αποθηκεύεται στον directory ονομάζεται καταχώρηση (entry). Οι καταχωρήσεις αναπαριστούν αντικείμενα του πραγματικού κόσμου όπως ανθρώπους, οργανισμούς κ.τ.λ. Οι καταχωρήσεις αποτελούνται από ένα σύνολο χαρακτηριστικών (attributes) που περιέχουν πληροφορία σχετικά με το αντικείμενο. Κάθε χαρακτηριστικό έχει έναν τύπο (type), που καθορίζει τι τιμές μπορεί να πάρει, και μία ή περισσότερες τιμές. Η σχέση μεταξύ μίας καταχώρησης, των χαρακτηριστικών της και των τιμών τους φαίνεται στην εικόνα 3.4.



Εικόνα 3.4: Καταχωρήσεις, χαρακτηριστικά και τιμές.

Στον πίνακα 3.1 φαίνονται ορισμένα συνηθισμένα χαρακτηριστικά. Κάποια χαρακτηριστικά έχουν εναλλακτικά ονόματα τα οποία μπορούν να χρησιμοποιηθούν οπουδήποτε χρησιμοποιούνται και τα κανονικά ονόματα. Για παράδειγμα, το εναλλακτικό όνομα cn μπορεί να χρησιμοποιηθεί οπουδήποτε γίνεται αναφορά στο χαρακτηριστικό commonName.

Attribute, Alias	Syntax	Description	Example
commonName, cn	cis	Common name of an entry	John Smith
surname, sn	cis	Surname (last name) of a person	Smith
telephoneNumber	tel	Telephone number	512-838-6008
organizationalUnitName, ou	cis	Name of an organizational unit	itso
owner	dn	Distinguished name of the person that owns the entry	cn=John Smith, o=IBM, c=US
organization, o	cis	Name of an organization	IBM
jpegPhoto	bin	Photographic image in JPEG format	Photograph of John Smith

Πίνακας 3.1: Συνηθισμένα χαρακτηριστικά.

Τα schemas (σχήματα) καθορίζουν τον τύπο των αντικειμένων που μπορούν να αποθηκευτούν στον directory. Επίσης, καθορίζουν τα χαρακτηριστικά των αντικειμένων και αν αυτά είναι υποχρεωτικά ή προαιρετικά. Για παράδειγμα, στον καθορισμό του αντικειμένου ‘πρόσωπο’, το χαρακτηριστικό ‘επώνυμο’ είναι υποχρεωτικό ενώ το χαρακτηριστικό ‘περιγραφή’ είναι προαιρετικό. Ο έλεγχος του schema επιβεβαιώνει ότι όλα τα υποχρεωτικά χαρακτηριστικά ενός αντικειμένου αποθηκεύονται ενώ τα προαιρετικά μπορούν να συμπληρωθούν οποτεδήποτε. Ο πίνακας 3.2 απεικονίζει ένα μέρος ενός κοινού schema.

Object Class	Description	Required Attributes
InetOrgPerson	Defines entries for a person	commonName (cn) surname (sn) objectClass
organizationalUnit	Defines entries for organizational units	ou objectClass
organization	Defines entries for organizations	o objectClass

Πίνακας 3.2: Κλάσεις αντικειμένων και υποχρεωτικά χαρακτηριστικά.

Ορισμένα αντικείμενα παράγονται από άλλα αντικείμενα. Για παράδειγμα, αν έχει ήδη καθοριστεί μία κλάση αντικειμένων με όνομα 'person', τότε μία νέα κλάση με όνομα 'organizationalPerson' μπορεί να δημιουργηθεί, η οποία θα περιέχει τα ίδια χαρακτηριστικά με την 'person' και επιπλέον τα χαρακτηριστικά 'title' και 'officenumber'. Η κλάση 'person' ονομάζεται υπερκλάση ενώ η 'organizationalPerson' υποκλάση.

Τέλος, κάθε καταχώρηση έχει ένα ειδικό χαρακτηριστικό που ονομάζεται objectClass. Η τιμή του χαρακτηριστικού αυτού καθορίζει την κλάση αντικειμένων που αντιπροσωπεύει η καταχώρηση.

3.2.2 Το μοντέλο ονοματολογίας

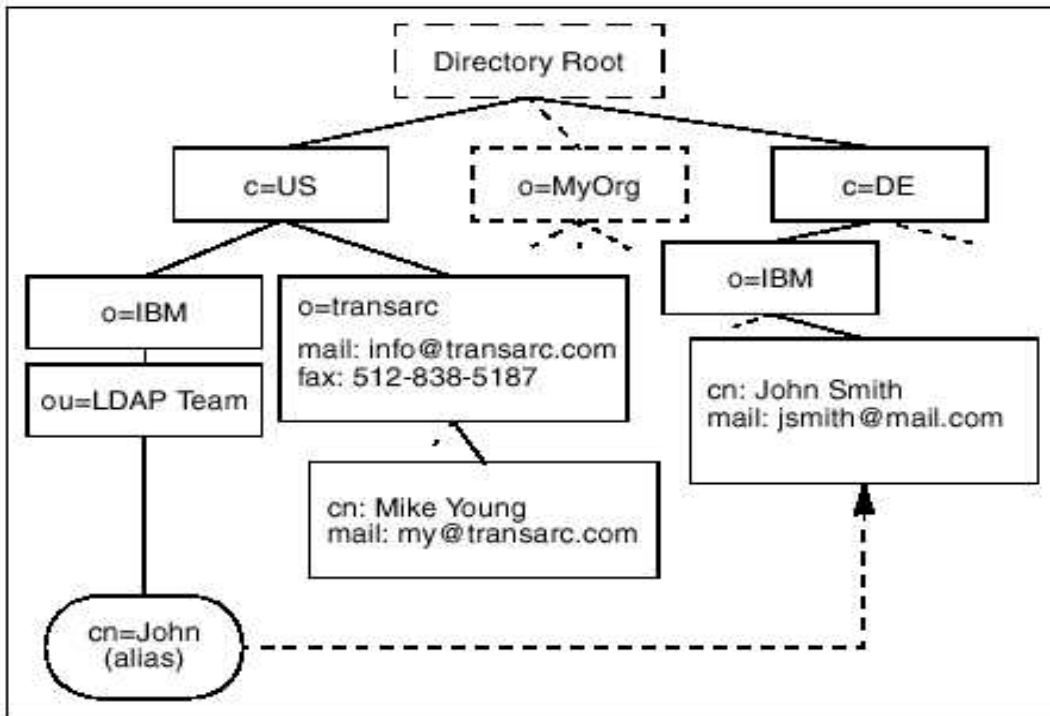
Το μοντέλο ονοματολογίας του LDAP καθορίζει τον τρόπο με τον οποίο οργανώνονται και προσδιορίζονται οι καταχωρήσεις. Η οργάνωσή τους γίνεται με βάση μία δενδροειδή δομή που, όπως και στο X.500, ονομάζεται Directory Information Tree (DIT). Οι καταχωρήσεις οργανώνονται μέσα στο DIT με βάση το αναγνωριστικό τους όνομα (Distinguished Name – DN). Το DN είναι ένα μοναδικό όνομα για κάθε οντότητα που την προσδιορίζει μονοσήμαντα και αποτελείται από μία σειρά σχετικών αναγνωριστικών ονομάτων (RDNs). Κάθε RDN σε ένα DN αντιστοιχεί σε ένα 'κλαδί' του DIT που οδηγεί από τη ρίζα στη συγκεκριμένη καταχώρηση.

Κάθε RDN εξάγεται από τα χαρακτηριστικά της συγκεκριμένης καταχώρησης. Στην απλούστερη περίπτωση, ένα RDN έχει τη μορφή <attribute name>=<value> και το DN αποτελείται από μία σειρά RDNs χωρισμένα με κόμμα.

Στην εικόνα 3.5 φαίνεται ένα παράδειγμα ενός DIT. Κάθε ορθογώνιο παριστάνει μία καταχώρηση. Η ρίζα του DIT δεν υφίσταται στην πραγματικότητα, ενώ τα χαρακτηριστικά καταγράφονται μέσα σε κάθε καταχώρηση.

Η οργάνωση των καταχωρήσεων του DIT περιορίζεται από τον τρόπο με τον οποίο έχουν καθοριστεί οι κλάσεις αντικειμένων που καταχωρούνται σ' αυτό. Είναι σύνηθες το φαινόμενο να ακολουθείται μία γεωγραφική ή οργανωσιακή διάταξη. Για παράδειγμα, οι καταχωρήσεις που αντιπροσωπεύουν χώρες βρίσκονται στην κορυφή

του DIT. Κάτω από τις χώρες μπορεί να βρίσκονται εθνικοί οργανισμοί, πολιτείες, περιφέρειες κ.τ.λ. Στο επόμενο επίπεδο, οι καταχωρήσεις μπορεί να αντιπροσωπεύουν επιπρόσθετες υποδιαιρέσεις των οργανισμών ή των περιφερειών. Τέλος, στο χαμηλότερο επίπεδο βρίσκονται οι καταχωρήσεις που αντιπροσωπεύουν οποιοδήποτε αντικείμενο όπως πρόσωπα, εκτυπωτές, servers κ.τ.λ. Το βάθος του DIT δεν είναι αυστηρά περιορισμένο και προσαρμόζεται στις ανάγκες της συγκεκριμένης εφαρμογής.



Εικόνα 3.5: Ένα Directory Information Tree (DIT).

Οι καταχωρήσεις ονομάζονται ανάλογα με τη θέση τους στο DIT. Η καταχώρηση στην κάτω δεξιά γωνία της εικόνας 3.5 έχει το DN 'cn=John Smith, o=IBM, c=DE'. Τα DNS διαβάζονται από τα φύλλα προς τη ρίζα, σε αντίθεση με τα ονόματα των αρχείων. Το DN μίας καταχώρησης καθορίζεται με την είσοδό της στο DIT.

3.2.3 Το λειτουργικό μοντέλο

Το LDAP προσδιορίζει τις λειτουργίες για την προσπέλαση και την τροποποίηση των καταχωρήσεων του DIT. Οι λειτουργίες αυτές μπορούν να διαιρεθούν στις παρακάτω κατηγορίες:

- ο **Ερώτηση (query)**: Περιλαμβάνει τις λειτουργίες αναζήτησης και σύγκρισης, που χρησιμοποιούνται για την εξαγωγή πληροφορίας από τον directory.
- ο **Ενημέρωση (update)**: Περιλαμβάνει τις λειτουργίες της πρόσθεσης, διαγραφής και τροποποίησης που χρησιμοποιούνται για την ενημέρωση των πληροφοριών που αποθηκεύονται στον directory.
- ο **Πιστοποίηση ταυτότητας (authentication)**: Περιλαμβάνει τις λειτουργίες σύνδεσης, αποσύνδεσης και εγκατάλειψης που χρησιμοποιούνται για τη σύνδεση σε έναν LDAP server και την απόδοση δικαιωμάτων πρόσβασης.

3.2.4 Το μοντέλο ασφάλειας

Το μοντέλο ασφάλειας του LDAP βασίζεται στις λειτουργίες σύνδεσης. Υπάρχουν πολλές λειτουργίες σύνδεσης και επομένως ο μηχανισμός ασφάλειας που υλοποιείται σε κάθε περίπτωση είναι διαφορετικός. Μία περίπτωση είναι, όταν ένας client ζητά πρόσβαση να παρέχει ένα DN που προσδιορίζει τον εαυτό του καθώς και ένα password καιμένου. Αν δεν έχουν οριστεί τα DN και password, εγκαθίσταται μία ανώνυμη σύνδεση. Η χρήση passwords καιμένου δεν ενδείκνυται όταν η υπηρεσία μεταφοράς των δεδομένων δεν μπορεί να εγγυηθεί την εμπιστευτικότητα και επομένως ένα τέτοιο password μπορεί να αποκαλυφθεί σε μη εξουσιοδοτημένα άτομα.

Στο LDAPv3 υπάρχει μία λειτουργία σύνδεσης που υποστηρίζει το μηχανισμό Simple Authentication and Security Layer (SASL). Ο μηχανισμός αυτός παρέχει ένα γενικό πλαίσιο στο οποίο είναι διαθέσιμες πολλές μέθοδοι πιστοποίησης της ταυτότητας του client στον server. Επιπλέον, μία επέκταση του LDAPv3 που αφορά την ασφάλεια είναι η επέκταση για Transport Layer Security (TLS), η οποία καθορίζει λειτουργίες που

χρησιμοποιούν την TLS ως μέσο για την απόκρυψη μίας συνόδου LDAP και την προστασία της από μη εξουσιοδοτημένη πρόσβαση.

Εφόσον, λοιπόν, γίνει η πιστοποίηση της ταυτότητας ενός client, οι πληροφορίες ελέγχου πρόσβασης καθορίζουν αν ο client έχει τα δικαιώματα προσπέλασης που θα του επιτρέψουν να εκτελέσει τη λειτουργία την οποία απαιτήσε.

3.3 Το LDAP ως μέρος της λύσης για καθολικές Directory Services

Το LDAP έχει γίνει εξαιρετικά δημοφιλές στην κοινότητα του Internet, καθώς ένας μεγάλος αριθμός κατασκευαστών δικτυακών προϊόντων έχει στηρίξει την ανάπτυξή του. Και αυτό γιατί το LDAP έχει πολλά πλεονεκτήματα που δεν μπορούν να αγνοηθούν [5]:

- ο Το LDAP καθορίζει ένα απλό πρότυπο το οποίο παρέχει ανοιχτή πρόσβαση σε directory services και συμβάλλει στην ενοποίηση ετερογενών directories.
- ο Ελαχιστοποιώντας την πολυπλοκότητα του λογισμικού των directory clients, το LDAP βοήθησε στη ραγδαία εξάπλωση των εφαρμογών οι οποίες χρησιμοποιούν τις directory services μέσω προσωπικών υπολογιστών και άλλων συστατικών των δικτύων.
- ο Με την υποστήριξη των αυτόνομων servers, το LDAP απλοποιεί και ενθαρρύνει την ανάπτυξη 'ελαφρών' directory services σε επιχειρησιακά δίκτυα.
- ο Πολλά Application Programming Interfaces (APIs) έχουν καθοριστεί για το LDAP, τα οποία διευκολύνουν τους διαχειριστές συστημάτων στο να παρέχουν πρόσβαση στον directory στις εφαρμογές τους.
- ο Η μελλοντική ανάπτυξη και εξέλιξη του LDAP θα παραμείνει υπό την εποπτεία της IETF.

Παρόλα τα πλεονεκτήματά του, το LDAP δεν είναι δυνατόν να λύσει όλα τα προβλήματα στο χώρο των directories, ενώ τα δίκτυα των επιχειρήσεων είναι δύσκολο να συγκλίνουν σε μία απλή directory service. Το LDAP, απλώς εξασφαλίζει ότι ένας συμβατός με το LDAP directory παρέχει ένα κοινό interface και συμφωνεί με το

μοντέλο ονοματολογίας του X.500. Το LDAP δεν καθορίζει το schema για την οργάνωση των δεδομένων που αποθηκεύονται στον directory. Ένα τέτοιο κοινό schema για την περιγραφή των δεδομένων είναι το κομμάτι που λείπει από το puzzle των directories.

4. Το πληροφοριακό μοντέλο των DEN

Το Μάιο του 1997 η Microsoft και η Cisco αποφάσισαν τη δημιουργία ενός de facto standard για την ολοκλήρωση των δικτύων και των directory services. Για το λόγο αυτό δημιουργήθηκε η Directory Enabled Networks (DEN) initiative (πρωτοβουλία). Το Σεπτέμβριο του 1997, στο συνέδριο των επαγγελματιών αναπτυκτών συστημάτων της Microsoft στο San Diego, οι δύο ιδρυτικές εταιρείες της DEN initiative ανακοίνωσαν τη στήριξη της πρωτοβουλίας αυτής από είκοσι εταιρείες κατασκευής δικτυακών προϊόντων. Ένας από τους πρωταρχικούς στόχους της DEN initiative ήταν η ανάπτυξη του πληροφοριακού μοντέλου (information model) των DEN το οποίο καθορίζει τη δομή των πληροφοριών (schema) και τον τρόπο αποθήκευσής τους στον directory.

Το Φεβρουάριο του 1998, με στόχο την επιβεβαίωση ότι το πληροφοριακό μοντέλο που θα αναπτυσσόταν θα γινόταν πρότυπο, η DEN initiative τέθηκε υπό την εποπτεία της Desktop Management Task Force (DMTF). Οι προηγούμενες επιτυχίες της DMTF στον τομέα της προτυποποίησης αποτέλεσαν εγγύηση για την επιτυχία των σκοπών της DEN initiative. Έτσι, το πληροφοριακό μοντέλο των DEN που δημιουργήθηκε αποτελείται από τρία μέρη [21]:

- ο Έξι βασικές ιεραρχίες κλάσεων που δημιουργούν το βασικό πλαίσιο για την αντιπροσώπευση των δικτυακών στοιχείων και υπηρεσιών. Οι κλάσεις αυτές είναι οι Network Device, Network Protocol, Network Media, Network Service, Profile και Policy. Να σημειωθεί ότι στις κλάσεις αυτές δεν συμπεριλαμβάνεται η κλάση Top από την οποία παράγονται όλες οι υπόλοιπες καθώς και άλλες σημαντικές κλάσεις όπως οι ManagedSystemElement, Application, Person, Location και LinkedContainer.
- ο Ένα εκτεταμένο schema βασισμένο στην κληρονομικότητα για τη μοντελοποίηση ιδιοτήτων και πληροφοριών που εξαρτώνται από συγκεκριμένες εφαρμογές.
- ο Απλούς μηχανισμούς για τη δημιουργία σχέσεων ανάμεσα στα αντικείμενα.

4.1 Κλάσεις των DEN

Το πληροφοριακό μοντέλο των DEN αποτελεί μία συσσώρευση των εννοιών του μοντέλου CIM (Common Information Model), το οποίο είναι ένα αντικειμενοστρεφές μοντέλο των πληροφοριών που απαιτούνται για τη διαχείριση διαφόρων όψεων πολύπλοκων υπολογιστικών συστημάτων και των εννοιών του X.500, καθώς και μία συλλογή από νέες έννοιες και ιδέες.

4.1.1 Επιρροές του X.500

Το X.500 παρέχει τις παρακάτω έννοιες στο πληροφοριακό μοντέλο των DEN:

- ο **Top**: Η κλάση αυτή αποτελεί τη ρίζα του DIT.
- ο **Person**: Αναφέρεται στις κλάσεις Person, OrganizationalPerson και Residential Person. Επιπρόσθετα, το X.500 ορίζει την κλάση StrongAuthenticationUser. Η κλάση αυτή χρησιμοποιείται από τα DEN για την καταγραφή του ιδιοκτήτη ή του διαχειριστή μιας συσκευής ή μιας υπηρεσίας.
- ο **Group**: Το X.500 ορίζει τις κλάσεις GroupOfNames και GroupOfUniqueNames. Τα DEN χρησιμοποιούν τις κλάσεις αυτές για την ομαδοποίηση χρηστών και συσκευών.
- ο **Organization**: Το X.500 ορίζει τρεις κλάσεις που αντιπροσωπεύουν επιχειρήσεις, τμήματα επιχειρήσεων και θέσεις στις επιχειρήσεις. Τα DEN επεκτείνουν αυτή την έννοια ώστε να περιλαμβάνει συσκευές και υπηρεσίες.
- ο **Application**: Το X.500 και το CIM ορίζουν την έννοια της εφαρμογής. Τα DEN προσθέτουν πληροφορία έτσι ώστε οι κλάσεις αυτές να μπορούν να σχετισθούν με δικτυακά στοιχεία και υπηρεσίες.
- ο **Alias, DSA**: Το X.500 ορίζει και άλλες σημαντικές έννοιες όπως οι Alias (ψευδώνυμο) και DSA (Directory System Agent), οι οποίες είναι σημαντικές για τη σωστή λειτουργία των directories.

4.1.2 Επιρροές του CIM

Το CIM παρέχει τις παρακάτω έννοιες στο πληροφοριακό μοντέλο των DEN:

- ο **Product, FRU**: Το CIM ορίζει μία συλλογή κλάσεων που αντιπροσωπεύουν προϊόντα και ανταλλακτικά προϊόντων. Τα DEN δεν χρησιμοποιούν τις κλάσεις αυτές.
- ο **ManagedSystemElement**: Το CIM ορίζει τις κλάσεις PhysicalElement και LogicalElement: Οι κλάσεις των DEN που αντιστοιχούν στη διαχείριση των φυσικών και λογικών όψεων παράγονται από αυτές τις κλάσεις.
- ο **Configuration**: Το CIM ορίζει τις κλάσεις Configuration και Setting. Τα DEN επεκτείνουν την έννοια αυτή ώστε να μοντελοποιήσουν την παραμετροποίηση δικτυακών στοιχείων και υπηρεσιών.
- ο **Service**: Το CIM ορίζει τις βασικές κλάσεις Service και ServiceAccessPoint οι οποίες είναι σημαντικές στον καθορισμό των δικτυακών υπηρεσιών. Τα DEN εκλεπτύνουν τον ορισμό των κλάσεων αυτών επικεντρώνοντας το ενδιαφέρον στον ορισμό, τη διαχείριση και την παροχή των δικτυακών υπηρεσιών.
- ο **Software**: Το CIM ορίζει τις κλάσεις SoftwareFeature και SoftwareElement. Τα DEN εκλεπτύνουν τις κλάσεις αυτές για να παραστήσουν τις συγκεκριμένες απαιτήσεις των δικτυακών στοιχείων και υπηρεσιών.
- ο **System**: Το CIM ορίζει μία ιεραρχία κλάσεων που προέρχονται από τη System. Τα DEN χρησιμοποιούν τις κλάσεις αυτές για να υλοποιήσουν την έννοια του λογικού δικτυακού στοιχείου.
- ο **Location**: Το CIM ορίζει την κλάση Location η οποία προσδιορίζει τη διεύθυνση ενός φυσικού στοιχείου. Τα DEN επεκτείνουν την κλάση αυτή ώστε να περιγράφει δικτυακά στοιχεία και υπηρεσίες.
- ο **Check and Action**: Το CIM ορίζει τις δύο υψηλού επιπέδου κλάσεις Check και Action. Η κλάση Check είναι μία συνθήκη η οποία αναμένεται να είναι αληθής και η Action μία λειτουργία που επιτρέπει την αλλαγή της κατάστασης του λογισμικού. Τα DEN επεκτείνουν αυτές τις κλάσεις για να ενσωματώσουν την παραμετροποίηση και την επανεκκίνηση δικτυακών συσκευών.
- ο **Application**. Ορίζεται από το CIM και το X.500.

4.1.3 Νέες έννοιες των DEN

Βελτιωμένες έννοιες και έννοιες που έχουν επεκταθεί:

- ο **NetworkService**: Ορίζεται ως η ρίζα των κλάσεων που αναφέρονται σε δικτυακές υπηρεσίες. Παράγεται από την κλάση Service του CIM.
- ο **NetworkProtocol**: Ορίζεται ως η ρίζα των κλάσεων που αναφέρονται στα πρωτόκολλα των δικτύων.
- ο **Enhancements to PhysicalPackage and Card**: Το X.500 ορίζει τη γενική έννοια της συσκευής. Τα DEN επεκτείνουν τις κλάσεις PhysicalPackage και Card για να συμπεριλάβουν τη λειτουργικότητα που απαιτείται από τις δικτυακές συσκευές.
- ο **NetworkElement**: Τα DEN επεκτείνουν τον ορισμό του CIM για τα λογικά στοιχεία ώστε να περιλάβουν τα δικτυακά στοιχεία.

Νέες έννοιες των DEN:

- ο **Policy**: Τα DEN παρέχουν έναν γενικό και έναν εξειδικευμένο – που αφορά τα δίκτυα – ορισμό της πολιτικής.
- ο **Profile**: Είναι ένα περίγραμμα των χαρακτηριστικών και των συμπεριφορών που περιγράφουν ένα αντικείμενο ή ένα σύνολο αντικειμένων.
- ο **NetworkMedia**: Είναι μία νέα κλάση που συνδέει τα μέσα μιας συγκεκριμένης διασύνδεσης (interface) με τις υπηρεσίες που εκτελούνται σ' αυτή.

5. Επιχειρησιακές αλλαγές

Είναι γεγονός ότι οι περισσότερες αλλαγές στην υποδομή και την τεχνολογία μιας επιχείρησης απαιτούν ουσιαστικές μεταβολές τόσο των επιχειρηματικών διαδικασιών, όσο και των συνηθειών που επικρατούν μέσα στην επιχείρηση. Αν οι απαιτούμενες μεταβολές δεν ληφθούν υπόψιν μέσα στο πλαίσιο της αλλαγής της τεχνολογικής υποδομής, η απόδοση της συγκεκριμένης επένδυσης είναι πολύ πιθανό να είναι κατά πολύ μικρότερη της αναμενόμενης.

Οι directory services είναι ιδιαίτερα ευπαθείς σε τέτοιες καταστάσεις καθώς αγγίζουν όλες τις εφαρμογές και τις διαδικασίες μιας επιχείρησης αλλά και πολλά δεδομένα τα οποία πρέπει να αποθηκευθούν στον directory κάτι που έχει ως αποτέλεσμα την αλλαγή της ιδιοκτησίας των δεδομένων αυτών.

Επομένως, τα βήματα που απαιτούνται για τη δημιουργία μιας directory service σε μία επιχείρηση πρέπει να γίνουν με μεγάλη προσοχή. Τα βήματα αυτά δίνονται στη συνέχεια σε σχέση με τον τομέα της επιχείρησης που επηρεάζει το καθένα [6]:

Επιχειρησιακές διαδικασίες

- ο Καθορισμός των χρηστών των δεδομένων του directory, των διασυνδέσεων μέσω των οποίων θα χρησιμοποιούνται τα δεδομένα (π.χ. browsers), των απαιτήσεων και των περιορισμών τους.
- ο Καθορισμός των εφαρμογών που θα χρησιμοποιούν τον directory και των απαιτήσεών τους.
- ο Καθορισμός της ιδιοκτησίας των δεδομένων.

Υποδομή

- ο Προσδιορισμός της υπάρχουσας τεχνολογικής υποδομής.
- ο Προσδιορισμός του όγκου των δεδομένων και του αριθμού των προσπελάσεων στα συγκεκριμένα δεδομένα.

Δεδομένα

- ο Προσδιορισμός των χώρων αποθήκευσης και της μορφής των δεδομένων.
- ο Προσδιορισμός των διαχειριστών των δεδομένων και εξασφάλιση της συνεργασίας τους.
- ο Προσδιορισμός της χρήσης των δεδομένων και των μεθόδων πρόσβασης σ'αυτά.

Τεχνολογία

- ο Επιλογή συγκεκριμένης τεχνολογίας για την υλοποίηση του directory.
- ο Επιλογή συγκεκριμένης τεχνολογίας για τη δημιουργία meta-directory.

Σχεδιασμός του directory

- ο Καθορισμός των δεδομένων που θα αποθηκεύονται στον directory.
- ο Καθορισμός των χαρακτηριστικών που θα αποθηκεύονται για κάθε καταχώρηση.
- ο Σχεδιασμός του schema.
- ο Σχεδιασμός του directory information tree.

Ανθρωποι και διαδικασίες

- ο Καθορισμός και εκπαίδευση ομάδας τεχνικής υποστήριξης.
- ο Καθορισμός απαιτήσεων ασφάλειας.
- ο Δημιουργία διαδικασιών ανάπτυξης, παροχής συμβουλών και υποστήριξης.

Διαχείριση

- ο Δημιουργία ομάδας διαχείρισης.
- ο Δημιουργία πλάνου για την εκπαίδευση των χρηστών του directory.
- ο Επιλογή εργαλείων ανάπτυξης εφαρμογών.

6. Scalable Device Configuration Management & Policy Based Networking

Ανάμεσα στις υπηρεσίες που προσφέρει μία καθολική directory service, δύο από τις σημαντικότερες είναι η δυνατότητα αυτόματης παραμετροποίησης των συσκευών οι οποίες συνδέονται στο δίκτυο και η λειτουργία του δικτύου με βάση συγκεκριμένες πολιτικές. Για τις λειτουργίες αυτές, συνήθως χρησιμοποιούνται οι αγγλικοί όροι που αναφέρονται ως scalable device configuration management [5] και policy based networking [3].

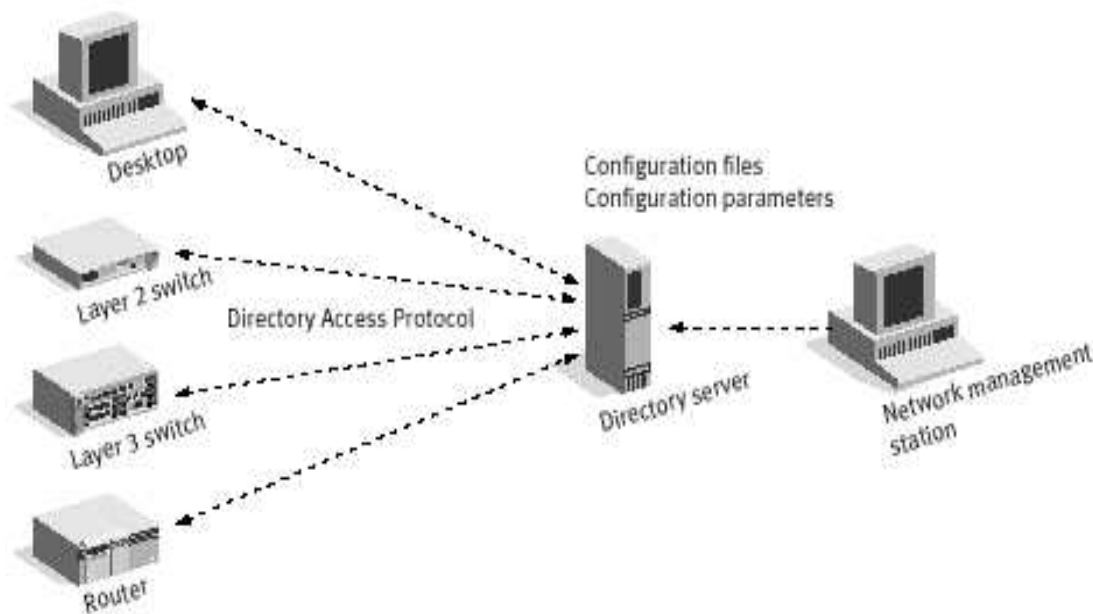
6.1 Scalable Device Configuration Management

Η υποστήριξη από τους directories της λειτουργίας της αυτόματης παραμετροποίησης των συσκευών που συνδέονται στο δίκτυο επιτρέπει στις συσκευές αυτές να λαμβάνουν τις παραμέτρους τους απευθείας από έναν directory server. Τα οφέλη μιας τέτοιας προσέγγισης είναι προφανή καθώς αυξάνεται το μέγεθος των δικτύων των επιχειρήσεων.

Αν ένα δίκτυο έχει ήδη δέκα παραμετροποιημένους routers, ο διαχειριστής του δικτύου δε χρειάζεται παραμετροποιήσει ξεχωριστά τον ενδέκατο. Αντίθετα, ο νέος router απλά εξετάζει τον directory, βρίσκει τις προοριζόμενες γι' αυτόν παραμέτρους και γίνεται αυτόματα μέρος του δικτύου.

Για την αυτόματη παραμετροποίηση των συσκευών απαιτείται από το διαχειριστή του δικτύου να έχει αποθηκεύσει τις παραμέτρους για κάθε κόμβο του δικτύου σε έναν κοινό directory όπως φαίνεται στην εικόνα 6.1. Έτσι, αντι να 'κατεβάζει' τις παραμέτρους μέσω TFTP ή να εγκαθιστά μία σύνδεση Telnet για κάθε συσκευή, ο διαχειριστής του δικτύου παραμετροποιεί κάθε κόμβο αποθηκεύοντας τις παραμέτρους

του (IP address, subnet mask, default gateway κ.τ.λ) στην καταχώρηση του directory που αντιστοιχεί στον συγκεκριμένο κόμβο.



Εικόνα 6.1: Αυτόματη παραμετροποίηση συσκευών.

Όταν μία νέα συσκευή συνδέεται στο δίκτυο, εγκαθιστά μία σύνδεση με τον directory server μέσω του directory access protocol και λαμβάνει τις απαραίτητες για τη λειτουργία του παραμέτρους. Με τον τρόπο αυτό οι directories παίζουν σημαντικό ρόλο στην απλοποίηση της διαχείρισης του δικτύου και στην επίτευξη του στόχου της plug n' play δικτύωσης.

6.2 Policy Based Networking

Η λειτουργία του δικτύου με βάση συγκεκριμένες πολιτικές (policy based networking) είναι πολύ πιο πολύπλοκη από την αυτόματη παραμετροποίηση των συσκευών. Μία πολιτική (policy) είναι ένας κανόνας που καθορίζει τον τρόπο με τον οποίο ένας κόμβος του δικτύου διαχειρίζεται τις απαιτήσεις για τη χρήση δικτυακών πόρων και αποθηκεύεται στον directory του δικτύου. Στην ουσία αποτελεί ένα μηχανισμό που επιτρέπει τη σωστή και αποδοτική χρήση των πόρων του δικτύου.

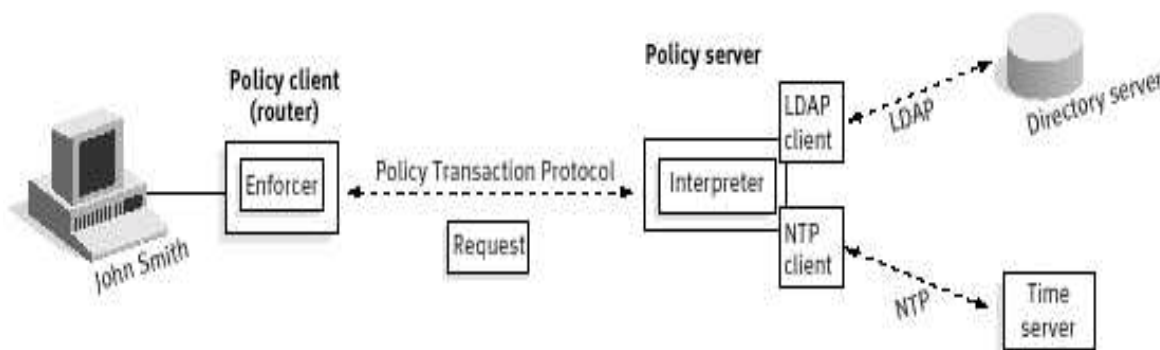
Τα policy based δίκτυα προσφέρουν πολύ μεγάλη ευελιξία και τη δυνατότητα παροχής υπηρεσιών διαφοροποιημένων ως προς το πρόσωπο στο οποίο παρέχονται. Στα policy based δίκτυα η έμφαση δίνεται σε κανόνες που αφορούν τους χρήστες και όχι στις παραμέτρους που αφορούν τις συσκευές.

Για παράδειγμα, ο διαχειριστής ενός δικτύου μπορεί να θέλει να περιορίσει τη δυνατότητα των χρηστών να έχουν πρόσβαση σε κάποια από τις βάσεις δεδομένων της επιχείρησης ανάλογα με την ώρα, την ημερομηνία και τη θέση του χρήστη στην επιχείρηση. Η λειτουργία αυτή απαιτεί την ύπαρξη ενός policy server ο οποίος συγκεντρώνει τις απαραίτητες πληροφορίες, παίρνει μία απόφαση και τη στέλνει στον κατάλληλο κόμβο του δικτύου μέσω ενός policy transaction protocol.

Σε γενικές γραμμές, τα στοιχεία που απαιτούνται για τη λήψη μιας policy based απόφασης είναι τα εξής:

- ο Information storage (αποθήκευση πληροφοριών).
- ο Policy requester (ο ζητών την policy based απόφαση).
- ο Policy interpreter (ο 'μεταφραστής' της πολιτικής).
- ο Policy enforcer (ο επιβάλλον την απόφαση).

Τα στοιχεία αυτά απεικονίζονται στην εικόνα 6.2.



Εικόνα 6.2: Βασικό μοντέλο για policy based δικτύωση.

Η αποθήκευση των πληροφοριών έχει να κάνει με το schema το οποίο καθορίζει τη δομή των πληροφοριών –πολιτικών στη συγκεκριμένη περίπτωση- που αποθηκεύονται στον directory.

Μία αίτηση για policy based απόφαση δημιουργείται όταν ο policy client ζητά πρόσβαση σε δικτυακούς πόρους. Για παράδειγμα, η έναρξη εκτέλεσης μιας εφαρμογής,

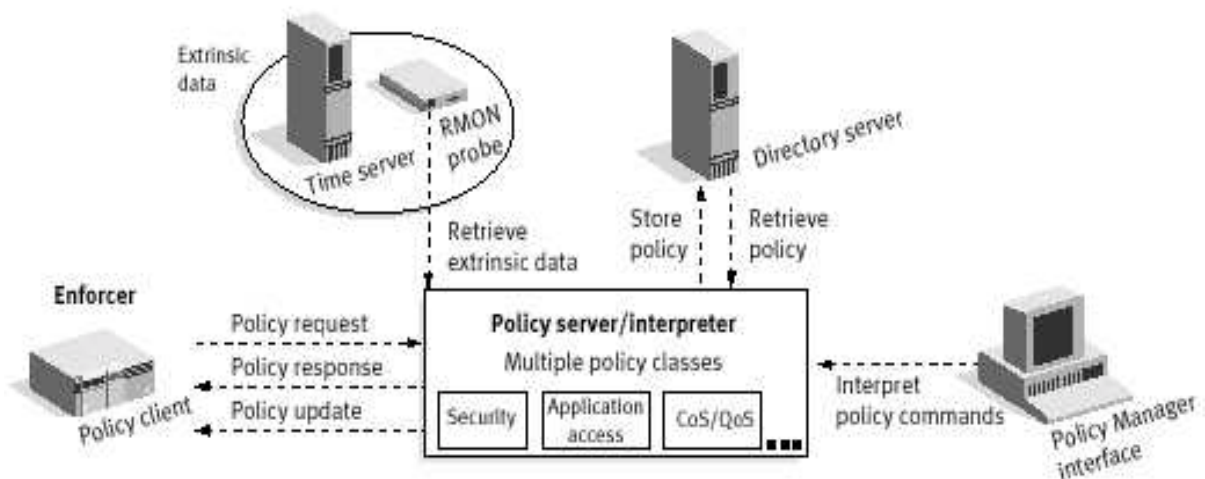
η κλήση ενός server απομακρυσμένης πρόσβασης ή η έναρξη ροής πληροφοριών μπορεί να δημιουργήσουν την αίτηση για μια policy based απόφαση.

Η μετάφραση μιας αίτησης για policy based απόφαση εκτελείται από μία δικτυακή συσκευή η οποία εκτιμά όλα τα στοιχεία της αίτησης σε συνδυασμό με τις συγκεκριμένες πολιτικές που σχετίζονται με τη συγκεκριμένη αίτηση. Σε πολλές περιπτώσεις, ο policy interpreter χρειάζεται να προσπελάσει μεγάλο αριθμό πηγών πληροφορίας πριν καταλήξει στην απόφαση.

Η επιβολή της απόφασης είναι η διαδικασία που εκτελείται από έναν κόμβο του δικτύου έτσι ώστε να επιβεβαιωθεί ότι εκτελέστηκε η ληφθείσα απόφαση. Η επιβολή εκτελείται από το συγκεκριμένο υλικό ή λογισμικό του policy client και μπορεί να είναι φιλτράρισμα πακέτων, απόδοση προτεραιοτήτων, απόδοση εύρους ζώνης κ.τ.λ.

Το σημαντικότερο, ίσως, ρόλο σε ένα policy based δίκτυο παίζει ο policy server ή policy interpreter. Ο policy server είναι κάτι πολύ περισσότερο από έναν απλό έξαγωγή δεδομένων, εφόσον αυτός λαμβάνει την policy based απόφαση. Οι σημαντικότερες λειτουργίες ενός policy server φαίνονται στην εικόνα 6.3 και είναι οι παρακάτω:

- ο Μετάφραση εντολών για λήψη policy based αποφάσεων.
- ο Αποθήκευση των αποφάσεων.
- ο Αποδοχή αιτημάτων για λήψη αποφάσεων.
- ο Ανάκτηση πολιτικών που βρίσκονται αποθηκευμένες σε directories.
- ο Ανάκτηση εξωτερικών δεδομένων
- ο Λήψη αποφάσεων.



Εικόνα 6.3: Λειτουργίες ενός policy server.

7. Προβλέψεις

Σύμφωνα με άρθρο του Salvatore Salamone στο τεύχος του Ιουνίου 2000 του περιοδικού Business Communications Review [29] οι προβλέψεις για το μέλλον των directory enabled networks δεν είναι πολύ αισιόδοξες. Συγκεκριμένα ο Salamone γράφει: « Ένα directory enabled network δεν πρέπει να στηθεί μία φορά και στη συνέχεια να ξεχαστεί. Αντιθέτως πρέπει συνεχώς να συγκεντρώνονται πληροφορίες σχετικές με την κατάσταση του δικτύου και με συγκεκριμένες εφαρμογές, οι οποίες στη συνέχεια μπορούν να χρησιμοποιηθούν για την αύξηση της απόδοσης του δικτύου. Ουσιαστικά, ένα directory enabled network χρησιμοποιεί τις πληροφορίες αυτές για να αυτοπροσαρμόζεται δυναμικά, έτσι ώστε να διατηρεί την ίδια υψηλή απόδοση κάτω από οποιεσδήποτε συνθήκες.

Τουλάχιστον αυτή ήταν η υπόσχεση. Στην πράξη, ωστόσο, τα directory enabled networks, δεν έχουν πλησιάσει αυτό το επίπεδο αυτοματοποίησης και δεν υπάρχει μία συγκεκριμένη προσέγγιση υλοποίησής τους. Επιπλέον, υπάρχει σύγχυση σχετικά με το τι είναι τα directory enabled networks, καθώς οι κατασκευάστριες εταιρείες χρησιμοποιούν όρους όπως directory enabled networking, policy based network και quality of service αναφερόμενες σε συστήματα διαχείρισης που επιτρέπουν την επίτευξη συγκεκριμένων επιπέδων αξιοπιστίας.»

Την απάντηση στην απαισιόδοξη αυτή πρόβλεψη δίνει στο τεύχος της 29/5/2000 του περιοδικού Network World [22] ο John McConell, πρόεδρος της McConell Associates λέγοντας: «Υπάρχει ακόμη μεγάλο ενδιαφέρον για τα directory enabled networks και την αξία που έχουν για τη διαχείριση και τον έλεγχο όλων των ειδών πληροφορίας.»

Ίσως η αλήθεια να βρίσκεται κάπου στη μέση. Παρόλα αυτά όμως, τα πλεονεκτήματα που προσφέρουν τα directory enabled networks μαζί με το γεγονός ότι στηρίζονται από εταιρείες-κολοσσούς στο χώρο τους δίνουν το δικαίωμα να πιστεύουμε ότι το μέλλον τους προβλέπεται, αν όχι λαμπρό, τουλάχιστον αισιόδοξο.

ΑΝΑΦΟΡΕΣ

WEB SITES

1. www.ee.umanitoba.ca/~blight/networks/DEN.html

Site με πολλά resources σχετικά με τα directory enabled networks.

2. www.tml.hut.fi/studies/Tik-110.300/1998/Essays/den.html

Άρθρο σχετικό με directory services, LDAP, X.500.

3. www.microsoft.com/windows2000/library/technologies/communications/denuse.asp

Περιγραφή της υλοποίησης των directory enabled networks με χρήση των windows2000.

4. www.cisco.com/warp/public/cc/techno/network/dirserv/den/prodlit

Άρθρα σχετικά με τη συνεργασία της Cisco με τη Microsoft για τη δημιουργία της DEN initiative.

5. www.3com.com/technology/tech_net/white_papers/500665.html

Περιγραφή της υλοποίησης των directory enabled networks και ειδικότερα του policy powered networking με προϊόντα της 3com.

6. www.cnilive.com/html/archives.html

Ερευνητικά άρθρα για πολλά θέματα και κυρίως για directory services.

7. www.murchiso.com/den

Site με πολλά resources της DEN initiative.

8. www.simc-inc.org/meetings98-99/Dec04-1998/Default.htm

Site σχετικό με τα συνέδρια της Securities Industry Middleware Council.

9. www.sunworld.com/swol-10-1996/swol-10-ldap.html

Άρθρα σχετικά με τη λειτουργία του X.500 και του LDAP

10. www.innosoft.com/directory-solutions/index.html

To site της innosoft international inc. σχετικό με enterprise directory solutions και high performance messaging

11. www.redbooks.ibm.com/abstracts/sg244986.html

Πλήρης περιγραφή της λειτουργίας του LDAP

12. www.fit.qut.edu.au/DataComms/itn540/gallery/a100/mitchell/den.htm

Διπλωματική εργασία σχετική με directory enabled networks και ευφυή δίκτυα

13. www.enterasys.com/products/whitepapers/den

Τεχνολογικός οδηγός σχετικός με directory enabled networking

14. developer.novell.com/nds

Περιγραφή του προϊόντος της Novell, NDS eDirectory

15. www.dmtf.org

Το επίσημο site της DMTF με πολλά τεχνικά θέματα σχετικά με directory enabled networks, Common Information Model κ.τ.λ.

16. www.ldapconnect.com/articles

Πολλά άρθρα σχετικά με το LDAP.

17. www.metadirectory.co.uk

Site με resources, τόσο για directory enabled networks, όσο και για LDAP και X.500

18. www.ietf.org

Το επίσημο site της IETF με πολλά internet drafts και Requests for Comments.

19. www.oblix.com/pointofentry/ldap/index.html

Το επίσημο site της oblix με άρθρα, βιβλία message boards και πολλά άλλα resources για το LDAP.

20. www.cis.ohio-state.edu/~jain/refs/den_refs.htm

Πάρα πολλά RFCs και Internet drafts που αναφέρονται σε directory enabled networks.

BIBΛΙΑ – ΠΕΡΙΟΔΙΚΑ

21. Directory Enabled Networking, John Strasser, Fred Baker, Macmillan
Technical Publishing

22. Network World, 29/5/2000, By Jim Duffy

What happened to DEN?

23. Computer World, 30/8/1999, By Michael Vizard, Stephanie Sanborn

Directory offerings aimed to ease administration

24. CRN, 2/3/1998, By Stuart Glascock

Directory-Enabled Networks Standard Is Near

25. Internet Week, 17/11/1997, By Amy Rogers

Directory Services Taken To Task – Vendors question ‘openness’ of the DEN spec

26. Network Computing, 4/9/2000, By Jonathan Feldman

Directory Services Sweeten DHCP

27. PC Magazine, 16/12/1997, By Tim Jones, Mark Wahl, Steve Kille

Network Winner: LDAP, Version 3.0

28. PC Week, 26/6/1998, By Claudia Graziano

LDAP 3.0 on the move

29. Business Communication Review, June 2000, By Salvatore Salamone

Directory-Enabled Networking – Can The Promise Be Fulfilled?

30. Network World, 14/8/2000, By Dave Kearns

Directories Remain A Great Mystery Of Life.