Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Δημιουργία σχολικού δικτύου υπολογιστών μέσω πολιτικών του Ενεργού Καταλόγου της Microsoft**
Ονοματεπώνυμο Φοιτητή	**Βασιλική Παππά**
Πατρώνυμο	**Σπυρίδων**
Αριθμός Μητρώου	**ΜΠΠΛ/08062**
Επιβλέποντες	**Χρήστος Δουληγέρης, Καθηγητής** **Δρ. Σαράντης Μητρόπουλος**

Ημερομηνία Παράδοσης Ιανουάριος 2012

Τριμελής Εξεταστική Επιτροπή

Δουληγέρης Χρήστος Καθηγητής	Βέργαδος Δημήτριος Λέκτορας	Κοτζανικολάου Παναγιώτης Λέκτορας

Ευχαριστήριο

Με την ολοκλήρωση της πτυχιακής μου εργασίας θα ήθελα να ευχαριστήσω για την αμέριστη συμπαράστασή τους:

- τον καθηγητή Δουληγέρη Χρήστο, για την εμπιστοσύνη που μου έδειξε με την ανάθεση της εργασίας.
- τον διδάκτορα Σαράντη Μητρόπουλο για την καθοδήγηση και την εννοιολογική προσέγγιση του θέματος. Κυρίως όμως για την επίβλεψη και την υποστήριξη που μου παρείχε. Ακόμα και σε στιγμές αδυναμίας με υποστήριξε και με παρότρυνε να συνεχίσω.
- Το σχολείο στο οποίο εργάζομαι, που μου παρείχε όλο τον εξοπλοσμό για την πραγματοποίηση των εργαστηριακών μετρήσεων.
- Τέλος ένα μεγάλο ευχαριστώ στον σύζυγό μου Ηλία, στην αδερφή μου Εύα, στη φίλη μου Ελευθερία, για την υποστήριξη που μου παρείχαν και ένα μεγάλο συγνώμη στο μόλις ενός έτους παιδί μου για τις ώρες που δεν έπαιξα μαζί του.

Περίληψη

Αυτή η εργασία αναλύει βήμα βήμα την δημιουργία ενός σχολικού δικτύου με βασικό εργαλείο υλοποίησης τις πολιτικές ομάδων του Ενεργού Καταλόγου της Microsoft. Αρχικά γίνεται αναφορά στα λειτουργικά συστήματα Windows και Unix.

Αναλύονται έννοιες όπως δάσος, τομέας, τοποθεσίες, σχήμα οι ποίες σε συνδυασμό με τις οργανωτικές μονάδες, ομάδες, λογαριασμούς χρηστών και υπολογιστών δημιουργούν ένα δίκτυο υπολογιστών.

Συλλέγονται πληροφορίες και αναλύονται έτσι ώστε να έχουμε τη μέγιστη απόδοση του δικτύου. Σχεδιάζονται οι οργανωτικές μονάδες και οι ομάδες χρηστών και υπολογιστών. Ορίζουμε πολιτικές λειτουργίας ανά ομάδα.

Βασιζόμενοι στη θεωρία δημιουργούμε ένα δίκτυο 30 υπολογιστών με στόχο την εφαρμογή της θεωρίας και την εξαγωγή συμπερασμάτων. Είναι ο Ενεργός Κατάλογος αυτό υπόσχεται η Microsoft;

Abstract

This paper (document) analyzes step by step how to create a school system with the implementing tool the group policy of Active Directory. Initially, reference is made to the Windows and Unix operating systems.

Concepts such as forest, domain, sites and schema are analyzed. It also analyzes and plans organizational units, groups, user accounts and computers.

Information is collected and analyzed in order to have maximum network performance. Organizational units, user groups and computers are being planned and we define operational policies for each group.

Based in theory, we create a network of 30 computers to implement the theory and conclusions as well. Is Active Directory that promises Microsoft?

Περιεχόμενα

Δημιουργία Σχολικού Δικτύου Υπολογιστών. 8

Εισαγωγή 8

ΚΕΦΑΛΑΙΟ 1 – Λειτουργικά συστήματα διακομιστών 8

1.1 Γενικά 8

1.2 Λίγα λόγια για το Unix 9

1.3 Λίγα λόγια για τα Windows 10

1.4 Windows ή UNIX ? 11

ΚΕΦΑΛΑΙΟ 2 - Λίγα λόγια για τον Ενεργό Κατάλογο 12

2.1 Ενεργός Κατάλογος (Active Directory) 12

2.2 Τομέας (Domain) 13

2.3 Δάση τομέων και δέντρα τομέων 13

2.4 Οργανωτικές Μονάδες 14

2.5 Τοποθεσίες 15

2.6 Σχήμα 15

2.7 Πολιτική Ομάδων 15

2.8 Βασικές εργασίες διαχείρισης Active Directory 18

2.9 Λογαριασμοί υπολογιστών 19

2.10 Λογαριασμοί Χρηστών 23

2.11 Λογαριασμοί Ομάδων 28

2.12 Περιβάλλοντα ονομασίας, Διαχωρισμός, Αναπαραγωγή (Naming Contexts, Partitioning, Replication) 34

2.13 Εμπιστοσύνη με τον Kerberos 35

2.14 Αντιπροσωπεία της Αρχής (Delegation of Authority) 35

2.15 Active Directory και Windows 2008 Server 36

ΚΕΦΑΛΑΙΟ 3 –Ανάλυση αναγκών & Συλλογή Πληροφοριών 37

3.1 Φάση Ανάλυσης Αναγκών 37

3.2 Συλλογή στοιχείων 38

ΚΕΦΑΛΑΙΟ 4- Σχεδίαση υλικού 44

4.1 Φάση Σχεδίασης Υλικού 44

4.2 Λειτουργία Primary και Backup Domain Controller 47

4.3 Λειτουργία διακομιστή εφαρμογών 48
4.4 Διακομιστής Exchange 49
4.5 Διακομιστής Δεδομένων 50
4.6 ISA Server 50
4.7 Φάση Σχεδίασης Υλικού Δικτύου 50
ΚΕΦΑΛΑΙΟ 5 –Σχεδιασμός Δικτύου *53*
5.1 Σχεδιασμός Οργανωτικών Μονάδων, ομάδων, χρηστών και υπολογιστών 53
5.2 Σχεδιασμός πολιτικών ομάδων 55
ΚΕΦΑΛΑΙΟ 6 -Υλοποίηση Δικτύου *58*
6.1 Εγκατάσταση ελεγκτή τομέα 58
6.2 Unattended Installation of Active Directory Domain Services 70
ΚΕΦΑΛΑΙΟ 7- Ρόλοι διακομιστή *72*
7.1 Διακομιστής DHCP 72
7.2 Διακομιστής Εκτυπώσεων (Print Server) 74
7.3 Διακομιστής αρχείων (File Server) 75
ΚΕΦΑΛΑΙΟ 8 - Πολιτικές υπολογιστών *77*
8.1 Μετονομασία και αλλαγή κωδικού τοπικού διαχειριστή 77
8.2 Οθόνη Σύνδεσης (Log on screen) 78
8.3 Εγκατάσταση εκτυπωτών 78
ΚΕΦΑΛΑΙΟ 9 -Πολιτικές χρηστών *79*
9.1 Κωδικοί Πρόσβασης 79
9.2 Πολιτικές CTRL+ALT+DEL 81
9.3 Πολιτικές επιφάνειας εργασίας 81
9.4 Αντιστοίχιση δίσκων (MAP DRIVES) 83
9.5 Πολιτικές φακέλου ανακατεύθυνσης και προφίλ περιαγωγής. (Folder redirection and roaming profile) 85
9.6 Regional Settings 89
9.7 Απενεργοποίηση συσκευών usb, cd-rom, fdd. 89
9.8 Ώρες σύνδεσης (Log on hours) 90
9.9 Λήξη λογαριασμού χρήστη 91

9.10 Περιορισμός πρόσβασης σε υπολογιστές 92
9.11 Ρυθμίσεις Internet Explorer 92
9.12 Απενεργοποίηση δεξί κλικ 94
9.13 Δυνατότητες εγκατάστασης απεγκατάστασης λογισμικών 94
9.14 Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου. 95
9.15 Δεν λειτουργεί η γραμμή εντολών. 95
ΚΕΦΑΛΑΙΟ 10 - Συμπεράσματα μέσω εργαστηριακών μετρήσεων *96*
10.1 Ενεργός Κατάλογος και χρόνος 96
10.2 Ενεργός Κατάλογος και κόστος 104
10.3 Ενεργός Κατάλογος και Υπηρεσίες ασφάλειας 105
10.4 Ενεργός Κατάλογος και Σενάρια 105
10.5 Συμπεράσματα εργαστηριακών μετρήσεων 106
ΚΕΦΑΛΑΙΟ 11 - Το μέλλον *107*
ΚΕΦΑΛΑΙΟ 12- Συμπεράσματα *107*
ΠΑΡΑΡΤΗΜΑ *109*
ΒΙΒΛΙΟΓΡΑΦΙΑ *118*

Δημιουργία Σχολικού Δικτύου Υπολογιστών.

Εισαγωγή

Σε αυτή την εργασία θα ασχοληθούμε με το σχεδιασμό ενός σχολικού δικτύου υπολογιστών με την βοήθεια του Ενεργού Καταλόγου της Microsoft και τις Πολιτικές ομάδων. Ο Ενεργός Κατάλογος είναι ένα ενδιάμεσο λογισμικό που ενσωματώνεται στα Windows Server 2000, Windows Server 2003 και Windows Server 2008. Βοηθάει στην εύκολη και γρήγορη διαχείριση ενός δικτύου υπολογιστών. Αρχικά θα αναλύσουμε τον Ενεργό Κατάλογο και στη συνέχεια θα ξεκινήσουμε να στήνουμε βήμα βήμα το δίκτυό μας.

Για την δημιουργία ενός δικτύου χρειάζεται πρώτα από όλα ένας καλός σχεδιασμός ο οποίος περιλαμβάνει τρεις φάσεις:

- Φάση Ανάλυσης, στην οποία συλλέγονται πληροφορίες από έναν οργανισμό για το πληροφοριακό του σύστημα. Στη συνέχεια αυτές αξιολογούνται με στόχο την δημιουργία ενός αναβαθμισμένου ή νέου πληροφοριακού συστήματος. Η συλλογή πληροφοριών γίνεται τόσο με την βοήθεια της διοίκησης του εκάστοτε οργανισμού όσο και με τη βοήθεια των απλών χρηστών. (Ν.Άλωνιστιώτη,Β.Γαζής , Παν. Πειραιά)
- Φάση Σχεδίασης, στην οποία σχεδιάζεται το σύστημα, με κάθε λεπτομέρεια, σε κάθε του επίπεδο και με όλες τις παραμέτρους του. Σε αυτό το κεφάλαιο θα ασχοληθούμε με το σχεδιασμό του δικτύου σε επίπεδο χρηστών. Θα καταγράψουμε τις ανάγκες των χρηστών δηλαδή το τι εφαρμογές θέλουν να χρησιμοποιούν. Οι ανάγκες των χρηστών καθορίζονται από τις εργασίες τις οποίες κάνουν. Έτσι ένας καθηγητής θα πρέπει να έχει οπωσδήποτε ένα πρόγραμμα επεξεργασίας κειμένου ενώ ένας λογιστής αντίστοιχα ένα λογιστικό πρόγραμμα. Στην περίπτωση του διαδικτύου θα πρέπει να δοθούν αντίστοιχα δικαιώματα.
- Φάση Υλοποίησης, στην οποία οι τεχνικοί αναλαμβάνουν να υλοποιήσουν την δημιουργία του δικτύου. Το δίκτυο θα δημιουργηθεί σε περιβάλλον Windows 2008 server με Ενεργό Κατάλογο (Active Directory). Θα γίνει μια μικρή αναφορά στην τοπολογία του δικτύου. Επίσης θα αναφέρουμε τον τρόπο με τον οποίο θα σχεδιαστούν οι διακομιστές σε επίπεδο υλικού με στόχο την μεγαλύτερη ασφάλεια (σχεδιασμός raid). Τέλος θα γίνει μια εκτενείς αναφορά στον Ενεργό κατάλογο με εικόνες και αναλύσεις λειτουργιών του. Σε αυτό το σημείο να αναφέρουμε ότι το λειτουργικό σύστημα των χρηστών θα είναι Windows 7.

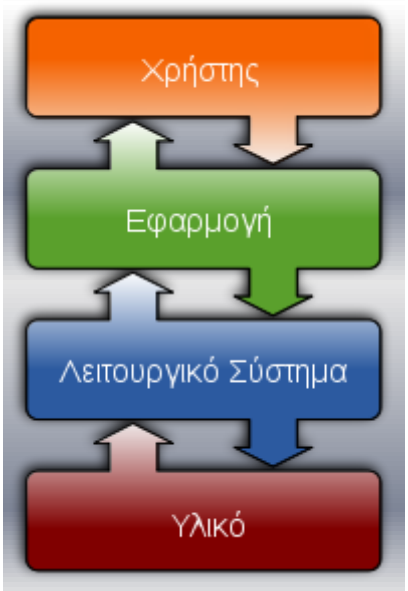
ΚΕΦΑΛΑΙΟ 1 – Λειτουργικά συστήματα διακομιστών

1.1 Γενικά

Το λειτουργικό σύστημα είναι ο τρόπος με τον οποίο ένας χρήστης επικοινωνεί με τον υπολογιστή. Είναι μία ενδιάμεση γλώσσα επικοινωνίας μιας και ο χρήστης δεν γνωρίζει γλώσσα μηχανής. Αποτελείται από ένα σύνολο προγραμμάτων γραμμένων σε γλώσσα μηχανής (ή ακόμα και C).

Το λειτουργικό σύστημα έχει ως στόχο την σωστή διαχείριση των πόρων του υλικού του υπολογιστή βάση των εντολών που δέχεται από τους χρήστες. Ουσιαστικά δίνει ένα εύχρηστο περιβάλλον (γραφικό ή με εντολές) στον χρήστη και στη συνέχεια μεταγλωττίζει τις εντολές προς εκτέλεση, σε γλώσσα μηχανής. Είναι υπεύθυνο για τη σωστή λειτουργία ενός υπολογιστή. Για παράδειγμα εξασφαλίζει την πρόσβαση σε έναν εκτυπωτή από μία εφαρμογή κάθε φορά.

Τα λειτουργικά συστήματα μπορούν να ομαδοποιηθούν ανάλογα με τη λειτουργικότητά τους σε: υπερυπολογιστές (supercomputing), φάρμες, κεντρικούς υπολογιστές (mainframes), διακομιστές (servers), σταθμούς εργασίας (workstations), επιτραπέζιους Η/Υ (desktops), φορητές συσκευές (tablet), συστήματα πραγματικού χρόνου (real time systems), ή ενσωματωμένα συστήματα (embedded systems). (http://el.wikipedia.org/wiki)



Εικόνα 1.1: Λειτουργικό ένα ενδιάμεσο στάδιο (http://el.wikipedia.org/wiki)

Ένα λειτουργικό σύστημα για διακομιστές έχει διαφορετικό ρόλο από ένα λειτουργικό σύστημα για έναν απλό υπολογιστή. Η βασικές διαφορές έγκειται στο ότι ο διακομιστής καλείται να διεκπεραιώσει αιτήσεις από άλλους υπολογιστές. Αιτήσεις όπως η σύνδεση σε ένα δίκτυο ή στο διαδίκτυο, πρόσβαση σε αρχεία και εκτυπωτές. Ουσιαστικά ένα λειτουργικό σύστημα διακομιστή είναι πολλαπλών καθηκόντων (multicasting).

Σήμερα έτσι όπως έχει διαμορφωθεί ο χώρος της πληροφορικής, υπάρχουν δύο βασικά λειτουργικά συστήματα, το Unix (με όλες τις διαφορετικές εκδόσεις) και τα Windows.

1.2 Λίγα λόγια για το Unix

Η ιστορία του UNIX ξεκίνησε τη δεκαετία του 1960 και μέχρι το 1978 εξελίχθηκε σε εφτά εκδόσεις. Το 1960 μια ομάδα από την General Electric σε συνεργασία με την MIT και BELL, εργαζόταν για να δημιουργήσει μία πλατφόρμα η οποία να εξυπηρετεί ταυτόχρονα πολλούς χρήστες και πολλές διεργασίες. Το UNIX είναι το αποτέλεσμα αυτής της έρευνας. Εξαρχής λοιπόν το UNIX σχεδιάστηκε και αναπτύχθηκε με σκοπό να εξυπηρετεί ένα δίκτυο υπολογιστών και όχι ένα απλό υπολογιστή. Η έβδομη έκδοση, η οποία κυκλοφόρησε το 1978, πυροδότησε μια διάσπαση στην ανάπτυξη του UNIX σε δύο κύριους κλάδους: SysV (σύστημα 5) και BSD (Berkeley Software Distribution). Η BSD προήλθε από το Πανεπιστήμιο της Καλιφόρνιας στο Berkeley. Η SysV αναπτύχθηκε από την AT&T και άλλες εταιρίες. Το Linux είναι ένα ελεύθερο, ανοιχτού κώδικα λειτουργικό σύστημα βασισμένο στο UNIX για προσωπικούς υπολογιστές που αρχικά αναπτύχθηκε το 1991. (http://el.wikipedia.org/wiki/Unix)

Το UNIX είναι ένα ανοικτού κώδικα multi-user και multi-casting λειτουργικό σύστημα. Πολλοί χρήστες τρέχουν πολλές διεργασίες ταυτόχρονα. Είναι σχεδιασμένο να είναι ανεξάρτητο από το υλικό του υπολογιστή. Είναι ένα περιβάλλον ανάπτυξης λογισμικού. Η φιλοσοφία του είναι να φτιάχνει ένα πρόγραμμα για να εξυπηρετεί καλά ένα σκοπό. Το UNIX αποτελείται από τα παρακάτω στοιχεία:

- Πυρήνας (kernel)
  - Ο πυρήνας του UNIX ο οποίος φορτώνεται στην εκκίνηση.
  - Διαχειρίζεται το σύνολο των πόρων του συστήματος, την παρουσίασή του σε κάθε χρήστη ως ένα συνεκτικό σύστημα. Παρέχει υπηρεσίες σε εφαρμογές των χρηστών, όπως η διαχείριση της συσκευής, τον προγραμματισμό διαδικασιών κ.λπ.
  - Παραδείγματα λειτουργιών που εκτελούνται από τον πυρήνα είναι τα εξής:
    - Διαχείριση μνήμης και κοινή χρήση αυτής σε κάθε διεργασία.
    - Προγραμματισμός της λειτουργίας της κεντρικής μονάδας επεξεργασίας έτσι ώστε η κάθε εργασία να εκτελείται στο πιο σύντομο χρόνο.

- Πραγματοποιεί την μεταφορά δεδομένων
- Μεταγλωττίζει και τρέχει εντολές από το κέλυφος
- Επιβάλει δικαιώματα πρόσβασης σε αρχεία.

○ Περιλαμβάνει μεγάλο αριθμό οδηγών συσκευών όπως κάρτες γραφικών και κάρτες ήχων.

• Κέλυφος (Shell) και Γραφικό Περιβάλλον (GUI)

○ Κάθε φορά που συνδεόμαστε σε ένα σύστημα Unix μπαίνουμε σε ένα πρόγραμμα κελύφους. Το κέλυφος είναι ο κέρσορας που αναβοσβήνει στην οθόνη και μας παροτρύνει να δώσουμε τις αντίστοιχες εντολές για να κάνουμε τις εργασίες μας.

○ Στη συνέχεια οι εντολές μεταγλωττίζονται σε γλώσσα μηχανής. Εκτελούνται και επιστρέφουν στην οθόνη το αποτέλεσμα σε γλώσσα φιλική προς τον χρήστη.

○ Κάθε κέλυφος μπορεί να εκτελεί διαφορετικές διεργασίες.

○ Κάθε χρήστης έχει τη δυνατότητα να χρησιμοποιεί διαφορετικά κελύφη.

○ Κάθε κέλυφος περιλαμβάνει την δική του γλώσσα προγραμματισμού. Τα αρχεία εντολών καλούνται "shell scripts" και χρησιμοποιούνται για να ολοκληρώσουν μια σειρά από διεργασίες.

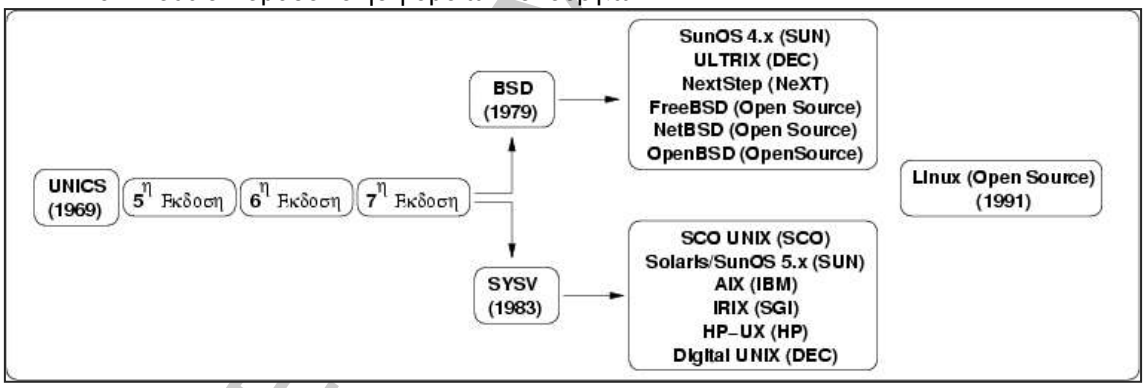
○ Αν θέλουμε μια σύγκριση με τα Windows το κέλυφος είναι το αντίστοιχο γραφικό περιβάλλον (Graphical User Interface) το οποίο υποστηρίζεται πλέον και από πολλές εκδόσεις Unix.

• Βοηθητικά (Utilities)

○ Το UNIX έχει αρκετά βοηθητικά προγράμματα γνωστά και ως εντολές (commands) καθώς και λειτουργίες όπως:

- Διόρθωση (editing)
- Συντήρηση αρχείων (file maintenance)
- Εκτυπώσεις (printing)
- Διαλογή (sorting)
- Υποστήριξη προγραμματισμού (programming support)
- online info

○ Modular: ομαδοποίηση όμοιων λειτουργιών



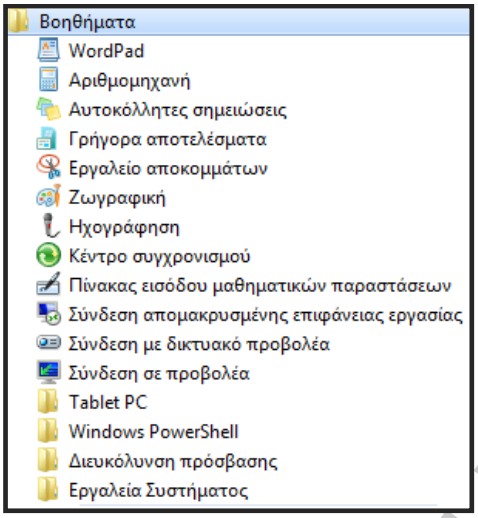
Εικόνα 1.2: Η ιστορία του Unix (http://ph150.edu.physics.uoc.gr/view.php?s=3&b=1&p=1)

1.3 Λίγα λόγια για τα Windows

Η ιστορία των Windows ξεκινάει το 1983 όπου η Microsoft έρχεται να αντικαταστήσει το λειτουργικό MS-DOS. Με τα Windows έχουμε τη εισαγωγή της λειτουργίας του ποντικιού και των παραθύρων. Ενός γραφικού περιβάλλοντος πολύ εύχρηστο και ευπαρουσίαστο σε σχέση με τον προκάτοχό του. Οι εκδόσεις των Windows εξελίσσονται πολύ γρήγορα από τα Windows 1.0 το 1985 μέχρι τα Windows 95 το 1995. Μέχρι το 1994 η Microsoft δεν είχε δημιουργήσει ένα λειτουργικό σύστημα που να μπορεί να υποστηρίζει multi-casting εφαρμογές και πολλαπλούς χρήστες. Το 1994 βγαίνουν στην αγορά τα Windows NT τα οποία κυκλοφορούν σε διάφορες εκδόσεις μέχρι το 2000. Το 2000 η Microsoft συστήνει τα Windows 2000 και τον Ενεργό Κατάλογο (Active Directory). Στη συνέχεια έχουμε τα Windows 2003 και σήμερα τα Windows server 2008. Κοινό χαρακτηριστικό των τριών τελευταίων εκδόσεων είναι ο Ενεργός Κατάλογος

για το οποίο θα μιλήσουμε αναλυτικά στο επόμενο κεφάλαιο. Τα στοιχεία που απαρτίζουν τα Windows είναι:

- Πυρήνας (kernel). Η βασική του δουλειά είναι να συνδέει τον χρήστη μέσω της διεπαφής του χρήστη (User Interface) με το υλικό του υπολογιστή (Hardware). Ο πυρήνας θα αναλάβει να τρέξει όλες τις απαραίτητες ρουτίνες για την ολοκλήρωση των αιτημάτων ενός χρήστη ή μιας εφαρμογής.
- Σύστημα διεπαφής χρήστη (Graphical User Interface). Αν και υποστηρίζουν και εντολές σε γραμμή εντολών (command line) τα windows υποστηρίζουν ένα πολύ εύχρηστο και φιλικό γραφικό περιβάλλον. Οι χρήστες δεν χρειάζεται πλέον να απομνημονεύουν εντολές.
- Βοηθητικά Προγράμματα (Utilities). Η Microsoft έχει ενσωματώσει αρκετά βοηθητικά προγράμματα στο λειτουργικό της και τα έχει ομαδοποίησει ανάλογα με την λειτουργία τους. Προγράμματα όπως η απλή αριθμομηχανή, απομακρυσμένη διαχείριση ή ακόμα και προγράμματα ελέγχου καλής λειτουργίας του συστήματος. (http://windows.microsoft.com/el-GR/windows/history)



Εικόνα 1.3: Βοηθητικά Προγράμματα

1.4 Windows ή UNIX ?

Υπάρχουν και στα δύο λειτουργικά συστήματα πλεονεκτήματα και μειονεκτήματα. Ας δούμε τα πιο βασικά από αυτά.

Κόστος Αγοράς: Το UNIX και οι διάφορες παραλλαγές-εκδόσεις είναι ένα λειτουργικό με ανοικτό κώδικα. Άρα δεν υπάρχει κόστος αγοράς για τους χρήστες. Ακόμα και κάποιες εκδόσεις του LINUX οι οποίες θα πρέπει να αγοραστούν οι τιμές τους είναι πολύ χαμηλές. Αντίθετα τα Windows είναι ένα λειτουργικό κλειστού κώδικα. Η αγορά του δε, είναι πολύ ακριβή. Ενδεικτικά μόνο να αναφέρουμε ότι η άδεια χρήσης των Windows server 2008 R2 με πέντε άδειες μόνο στοιχίζει περίπου 1000 δολάρια.

Εύχρηστο: Αν και υπάρχουν αρκετές εκδόσεις Linux κυρίως, οι οποίες υποστηρίζουν γραφικό περιβάλλον διεπαφής με τους χρήστες τα windows εξακολουθούν να είναι πιο εύχρηστα και πιο φιλικά. Άλλωστε αν και έχουν βγει αρκετές εκδόσεις των Windows το περιβάλλον δεν παρουσιάζει μεγάλες διαφορές.

Αξιοπιστία: Αν και οι τελευταίες εκδόσεις των Windows έχουν βελτιωθεί σημαντικά δεν μπορούν να φτάσουν σε αξιοπιστία το UNIX.

Λογισμικά: Λόγω του μεγάλου αριθμού χρηστών των Windows, υπάρχει πολύ μεγαλύτερη ποικιλία από διαθέσιμα προγράμματα λογισμικού, υπηρεσιών και παιχνιδιών.

Κόστος λογισμικών: Πολλά από τα προγράμματα, παιχνίδια και υπηρεσίες του UNIX είναι ανοικτού κώδικα και διατίθενται δωρεάν. Ακόμα και πολύπλοκα προγράμματα όπως το Open Office. Από την άλλη πλευρά, τα Windows αν και έχουν ενσωματωμένα πολλά προγράμματα υπάρχουν πολλά περισσότερα που θα πρέπει να αγοραστούν. Για παράδειγμα

το Microsoft Office (αντίστοιχο του Open Office) κοστίζει σαν αγορά από 100 έως 200 δολάρια για μία μόνο άδεια χρήσης.

Υλικό: Αν και οι κατασκευάστριες εταιρείες υλικού έχουν αρχίσει να συνεργάζονται και με το UNIX η αγορά των Windows είναι πολύ μεγαλύτερη οπότε η Microsoft υπερτερεί. Πιο εύκολα βρίσκεις οδηγούς για ένα υλικό για Windows από ότι για UNIX.

Ασφάλεια: Παρόλο που έχουν γίνει πολλές βελτιώσεις τα Windows εξακολουθούν να είναι πιο ευάλωτα σε ιούς και επιθέσεις από ότι το UNIX.

Ανοιχτός Κώδικας: Το UNIX είναι λειτουργικό ανοιχτού κώδικα και υπάρχουν λογισμικά που συνεργάζονται τα οποία επίσης είναι ανοιχτού κώδικα. Αυτό δίνει την δυνατότητα στους χρήστες να παραμετροποιήσουν το δικό τους περιβάλλον. Αντίθετα τα Windows είναι κλειστού κώδικα καθώς και η πλειοψηφία των λογισμικών που συνεργάζονται με αυτά.

Υποστήριξη: Αν και μπορεί να είναι πιο δύσκολο να βρεθούν χρήστες εξοικειωμένοι με όλες τις εκδόσεις του UNIX, υπάρχουν τεράστιες ποσότητες των διαθέσιμων βοηθημάτων τόσο στο διαδίκτυο όσο και σε βιβλιογραφία. Η Microsoft έχει τη δική της ομάδα υποστήριξης αλλά παρέχει και πολλά βοηθήματα στο διαδίκτυο.

(http://www.computerhope.com/issues/ch000575.htm)

Τα Windows διαδόθηκαν πολύ γρήγορα στην αγορά κυρίως λόγω του παραθυρικού τους περιβάλλον και παρόλο που δεν παρέχουν την ασφάλεια και την αξιοπιστία του UNIX έχουν κερδίσει την αγορά εργασίας. Θα πρέπει όμως να τονίσουμε ότι μεγάλοι οργανισμοί με πολύπλοκα συστήματα και mainframes παραμένουν σταθερά πιστοί στο UNIX.

Στη συνέχεια θα μιλήσουμε για τον Ενεργό Κατάλογο. Ένα λειτουργικό ενσωματωμένο στα Windows Server και θα υλοποιήσουμε ένα δίκτυο με τη βοήθεια αυτού.

ΚΕΦΑΛΑΙΟ 2 - Λίγα λόγια για τον Ενεργό Κατάλογο

2.1 Ενεργός Κατάλογος (Active Directory)

Ο όρος Κατάλογος (Directory) στην τεχνολογία των υπολογιστών έχει προέλθει από τον τηλεφωνικό κατάλογο. Σε αυτό βλέπουμε άσπρες και κίτρινες σελίδες. Το κοινό χαρακτηριστικό τους είναι η δυνατότητα αναζήτησης πληροφοριών. (Dias, 2002)

Τα Directories (κατάλογοι), όπως το Lightweight Directory Access Protocol (LDAP) και το Active Directory (AD) (Ενεργός Κατάλογος) είναι τύποι βάσεων δεδομένων . Ένας χρήστης μπορεί να βρει πληροφορίες στο δίκτυο χωρίς να χρειάζεται να γνωρίζει τη δομή του δικτύου. Παραδείγματος χάριν, ο χρήστης μπορεί να ψάξει στον Ενεργό Κατάλογο για διαμοιραζόμενα αρχεία χωρίς να χρειάζεται να ξέρει τα ονόματα των υπολογιστών που τα διαμοιράζει.

Η βασική υπηρεσία του LDAP είναι η αναζήτηση (searching) και είναι το πρότυπο πάνω στο οποίο έχει βασιστεί ο Ενεργός Κατάλογος. Είναι χτισμένο πάνω στο λειτουργικό σύστημα των Windows Server (2000, 2003, 2008) και με τη βοήθεια του γίνεται η επικύρωση των χρηστών και ο έλεγχος πρόσβασης. Οι διαχειριστές δικτύου είναι αυτοί που επωφελούνται άμεσα λόγω του ότι όλα πια είναι συγκεντρωμένα σε μια βάση η οποία διαχειρίζεται εύκολα.

Ο Ενεργός Κατάλογος αποθηκεύει όλες τις πληροφορίες περιοχών - τομέων με ένα κοινό και εξερευνήσιμο σχήμα. Όλοι οι λογαριασμοί χρηστών, οι λογαριασμοί υπολογιστών, οι ομάδες, οι κατάλογοι ελέγχου πρόσβασης (Access Control Lists), τα προσδιοριστικά ασφάλειας, οι πολιτικές αντικειμένων ομάδας (GPOs), ο διαμοιρασμός, οι εκτυπωτές, οι ιδιότητες για τους ανθρώπους και οι θέσεις τους, είναι αποθηκευμένα στην βάση του Ενεργού Καταλόγου. Επιπλέον, η Microsoft παρέχει μια κοινή κονσόλα διαχείρισης (Microsoft Management Console) για ευκολότερη διαχείριση.

Ο Ενεργός Κατάλογος είναι βασισμένος σε διάφορα πρότυπα, όπως το LDAP και X.500 (το σχήμα είναι βασισμένο σε X.500). Χρησιμοποιεί το σύστημα ονομάτων τομέων (Domain Name System - DNS). Οι τομείς DNS οργανώνονται σε μια ιεραρχική δομή και η ιεραρχία τους ορίζεται σε μια βάση τόσο ευρεία όσο και το ίδιο το διαδίκτυο. Μέσω του DNS μια ιεραρχία τομέα Ενεργού Καταλόγου μπορεί να οριστεί σε όλο το εύρος του διαδικτύου ή να είναι ξεχωριστή και ιδιωτική.

2.2 Τομέας (Domain)

Ένας τομέας Ενεργού Καταλόγου δεν είναι παρά μια ομάδα υπολογιστών οι οποίοι χρησιμοποιούν από κοινού μία βάση δεδομένων καταλόγου. Τα ονόματα των τομέων πρέπει να είναι μοναδικά. Υπάρχει πάντα ο γονικός τομέας (συνήθως ο πρώτος που δημιουργήθηκε) και οι υποτομείς ή θυγατρικοί τομείς. Η σχέση μεταξύ τους ακολουθεί μια ιεραρχική δομή από τον γονικό τομέα προς τον θυγατρικό.

Τα αντικείμενα που αποθηκεύονται στον τομέα είναι αυτά για τα οποία ενδιαφέρεται ένας χρήστης όπως εκτυπωτές, έγγραφα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, βάσεις δεδομένων, χρήστες, και άλλοι πόροι. Όλα τα αντικείμενα δικτύων υπάρχουν μέσα σε ένα τομέα και κάθε τομέας αποθηκεύει τις πληροφορίες μόνο για τα αντικείμενα που περιέχει. Ο Ενεργός Κατάλογος συνεργάζεται με ένα ή πολλούς τομείς. Η ομαδοποίηση (Group) των αντικειμένων σε έναν ή περισσότερους τομείς επιτρέπει μια οργανωμένη απεικόνιση και διαχείριση του δικτύου.

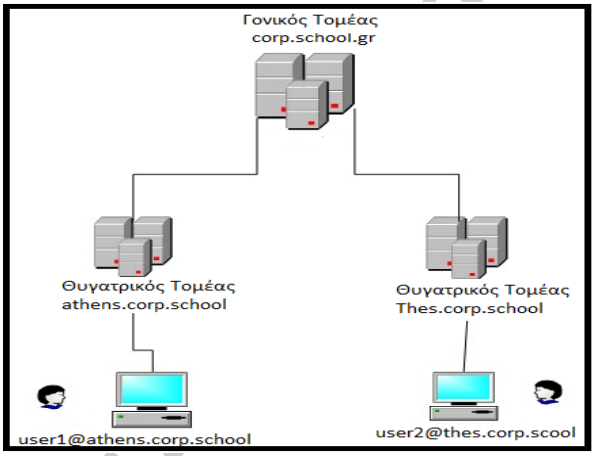
Ο τομέας έχει τα εξής χαρακτηριστικά:

- Όλα τα αντικείμενα δικτύων υπάρχουν μέσα σε ένα τομέα και κάθε τομέας αποθηκεύει τις πληροφορίες μόνο για τα αντικείμενα που περιέχει.
- Ένας τομέας είναι ένα όριο ασφάλειας. Η Access Control List (ACL) ελέγχει την πρόσβαση στα αντικείμενα του τομέα. Όλες οι πολιτικές ασφάλειας και χαρακτηριστικά όπως δικαιώματα διαχείρισης ανήκουν μόνο σε αυτόν.
- Ο διαχειριστής του τομέα έχει τα απόλυτα δικαιώματα να θέσει πολιτικές μόνο μέσα σε εκείνο το τομέα.

Ένας τομέας είναι ένα διαχειριστικό όριο, ένα όριο ασφάλειας, και αντιπροσωπεύει ένα όνομα (name space) που αντιστοιχεί σε ένα τομέα DNS.

Οι περισσότεροι μεγάλοι οργανισμοί ακολουθούν μια λογική δομή του οργανισμού που σχετίζεται με τις ευθύνες του κάθε τμήματος ή την ροή της εργασίας. Οι έννοια των τομέων είναι ιδανική για τον λογικό σχεδιασμό. Οι τομείς των Windows είναι οργανωμένοι με μια ιεραρχική δομή.

Θα πρέπει εδώ να τονίσουμε ότι στην ιεραρχική δομή των τομέων, τα δικαιώματα χρηστών και η πολιτική των ομάδων κληρονομούνται σε όλη την ιεραρχία των οργανωτικών μονάδων. Στην παρακάτω εικόνα βλέπουμε την ιεραρχική δομή που ακολουθούν οι τομείς. (γονικός τομέας και θυγατρικός).

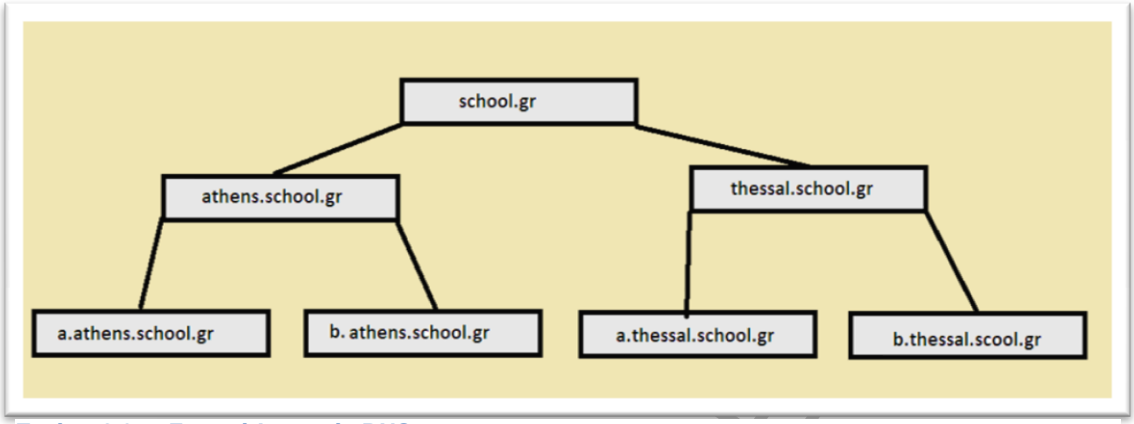


Εικόνα 2.2: Γονικός Τομέας 1

2.3 Δάση τομέων και δέντρα τομέων

Κάθε τομέας Ενεργού Καταλόγου έχει ένα όνομα τομέα DNS. Όταν υπάρχουν ένας οι περισσότεροι τομείς που χρησιμοποιούν από κοινού τα δεδομένα καταλόγου, αναφέρονται ως δάσος (forest). Τα ονόματα των τομέων αυτού του δάσους μπορεί να είναι ασυνεχή ή συνεχή στην ιεραρχία απόδοσης ονομάτων DNS.

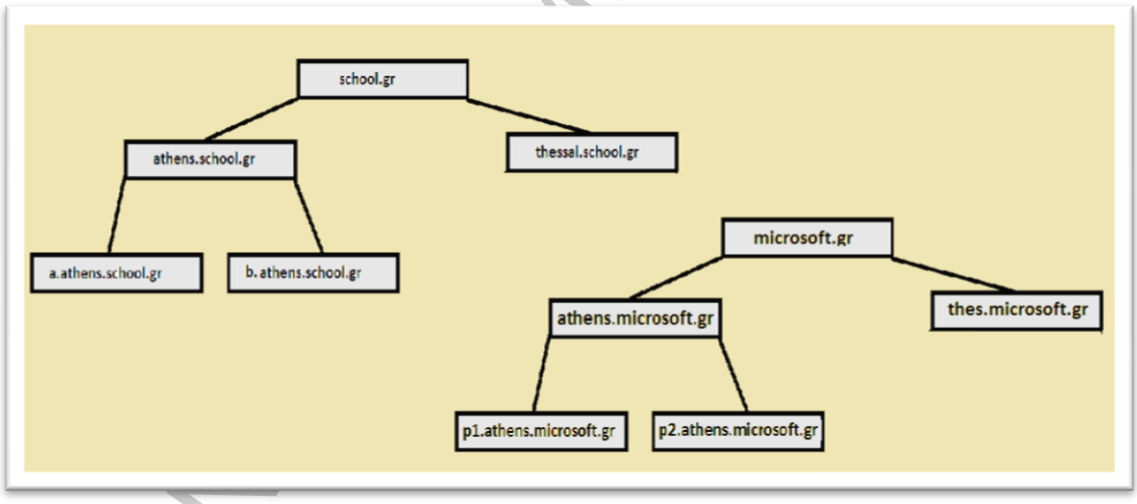
Όταν οι τομείς έχουν συνεχή δομή απόδοσης ονομάτων, τότε θεωρούνται ότι ανήκουν στο ίδιο δέντρο (domain tree). Όπως φαίνεται και από την εικόνα 2.3.1 ο βασικός τομέας (root) school.gr έχει δύο θυγατρικούς (athens.school.gr και thessal.school.gr). Με τη σειρά τους αυτοί έχουν υποτομείς. Όλοι οι τομείς αποτελούν τμήμα του ίδιου δέντρου επειδή έχουν τον ίδιο βασικό τομέα.



Εικόνα 2.3.1: Συνεχή Ιεραρχία DNS

Αν οι τομείς ενός δάσους έχουν ασυνεχή ονόματα DNS, σχηματίζουν ξεχωριστά δέντρα τομέων μέσα στο δάσος. Όπως φαίνεται και από την εικόνα 2.3.2 ένα δάσος τομέων μπορεί να έχει πολλά δέντρα τομέων.

Η πρόσβαση σε δομές τομέων γίνεται με το εργαλείο Active Directory Domain and Trust. Ουσιαστικά δηλώνουμε σχέσεις εμπιστοσύνης μεταξύ των τομέων με αποτέλεσμα να μπορούμε να έχουμε πρόσβαση σε αυτούς.



Εικόνα 2.3.2: Ασυνεχή Ιεραρχία DNS

2.4 Οργανωτικές Μονάδες

Η οργανωτική μονάδα (Organization Unit) είναι μια κρίσιμη λειτουργία που επηρεάζει την ασφάλεια, την πολιτική, την αποδοτικότητα, και το κόστος της διαχείρισης. Είναι υποομάδες τομέων οι οποίες συχνά αντικατοπτρίζουν τη λειτουργική ή επιχειρηματική δομή.

Τα αντικείμενα που τοποθετούνται σε μια οργανωτική μονάδα μπορούν να προέρχονται μόνο από τον γονικό τομέα. Μπορούμε να δημιουργήσουμε μια ιεραρχική δομή από οργανωτικές μονάδες όπου τα δικαιώματα των χρηστών και η πολιτικές των ομάδων κληρονομούνται.

Ένα από τα κύρια οφέλη των οργανωτικών μονάδων είναι η δυνατότητά τους να ολοκληρώσουν τις λειτουργίες του τομέα με στόχο την μείωση των τομέων. Οι οργανωτικές μονάδες χρησιμοποιούνται συνήθως για να συμπεριλάβουν τους λογαριασμούς χρηστών, ομάδων, και υπολογιστών. Ισχυρές διαμορφώσεις μπορούν να ληφθούν όταν συνδυάζονται με τις πολιτικές ασφαλείας των ομάδων.

Ένα άλλο όφελος των οργανωτικών μονάδων είναι η έννοια της μεταβίβασης της αρχής. Οι διαχειριστές των τομέων μπορούν να ορίσουν δικαιώματα διαχείρισης μέσω αυτών. Η τμηματοποίηση των εξουσιοδοτημένων δικαιωμάτων είναι αρκετά χρήσιμη. Για παράδειγμα μπορεί να υποβοηθήσει μια διαχειριστική ομάδα μοιράζοντας απλές και μεμονωμένες εργασίες όπως αλλαγή κωδικού πρόσβασης σε συγκεκριμένο προσωπικό.

2.5 Τοποθεσίες

Τοποθεσία (site) είναι μια ομάδα υπολογιστών σε ένα ή περισσότερα υποδίκτυα IP. Είναι η φυσική δομή ενός δικτύου η οποία είναι και ανεξάρτητη από τη λογική δομή των τομέων. Μπορούμε να έχουμε πολλές τοποθεσίες σε ένα τομέα ή μία τοποθεσία που θα εξυπηρετεί πολλούς τομείς.

2.6 Σχήμα

Το σχήμα υπαγορεύει τους ορισμούς για τον Ενεργό Κατάλογο. Εάν ένα αντικείμενο ή μια ιδιότητα δεν είναι στο σχήμα, εκείνο το αντικείμενο/χαρακτηριστικά δεν θα αποθηκευτούν στον Ενεργό Κατάλογο.

Ο κατάλογος περιέχει τις πληροφορίες υπό μορφή αντικειμένων και χαρακτηριστικών αντικειμένου. Στην πραγματικότητα είναι ένας τύπος βάσης. Τα δεδομένα που είναι λίγο πολύ στατικά και αναζητούνται συχνά μπορούν να αποθηκευτούν στο κατάλογο. Τα δεδομένα που αλλάζουν συχνά δεν είναι καλό να αποθηκευτούν στο κατάλογο. Παραδείγματος χάριν, οι ιδιότητες χρηστών όπως ο τηλεφωνικός αριθμός, ο ταχυδρομικός κώδικας, είναι αριθμοί – δεδομένα που δεν αλλάζουν συχνά (στατικά) και διαχειρίζονται εύκολα. Τα αρχεία καταγραφής συστήματος (systems log) και τα αρχεία συστήματος (file systems) είναι αρχεία που αλλάζουν συνεχώς (δυναμικά) γι αυτό και δεν αποθηκεύονται στο κατάλογο. Ο manager schema, καθορίζει ποια χαρακτηριστικά δημοσιεύονται στο σφαιρικό κατάλογο (Global Catalog).

2.7 Πολιτική Ομάδων

Οι πολιτικές ομάδων απλοποιούν την διαχείριση ενός δικτύου. Δημιουργώντας ομάδες με κοινά προνόμια ή μη και κοινό τρόπο πρόσβασης μειώνουμε τον χρόνο διαχείρισης. Οι βασικές εργασίες που μπορούμε να κάνουμε με τις πολιτικές των ομάδων είναι:

- Έλεγχος πρόσβασης σε συστατικά στοιχεία των Windows, σε πόρους του συστήματος, σε πόρους του δικτύου, σε βοηθητικά προγράμματα του πίνακα ελέγχου, στην επιφάνεια εργασίας και στο μενού εκκίνησης.
- Δημιουργία καταλόγων κεντρικής διαχείρισης για ειδικούς φακέλους όπως τον φάκελο Τα έγγραφά μου.
- Δημιουργία σεναρίων χρηστών ή και υπολογιστών που θα εκτελούνται σε συγκεκριμένες χρονικές στιγμές.
- Διευθέτηση πολιτικών για κλείδωμα λογαριασμών και κωδικούς πρόσβασης, λειτουργίες ελέγχου, ανάθεση δικαιωμάτων χρηστών και λειτουργίες ασφάλειας.

Η Microsoft είχε θέσει από το 1996 τους στόχους ZAW (Zero Administration for Windows), στόχοι μη επιτεύξιμοι για τότε. (http://searchwinit.techtarget.com/definition/Zero-Administration). Ο συνδυασμός των πολιτικών ομάδων με νέες τεχνολογίες έχουν πλησιάσει κατά πολύ αυτόν τον στόχο.

Θα πρέπει να τονίσουμε ότι παρόλο που τα οφέλη των πολιτικών ομάδων είναι μεγάλα θα πρέπει να αφιερωθεί αρκετός χρόνος για τον σχεδιασμό τους. Υπάρχουν πάνω από 700 διαφορετικές διαμορφώσεις.

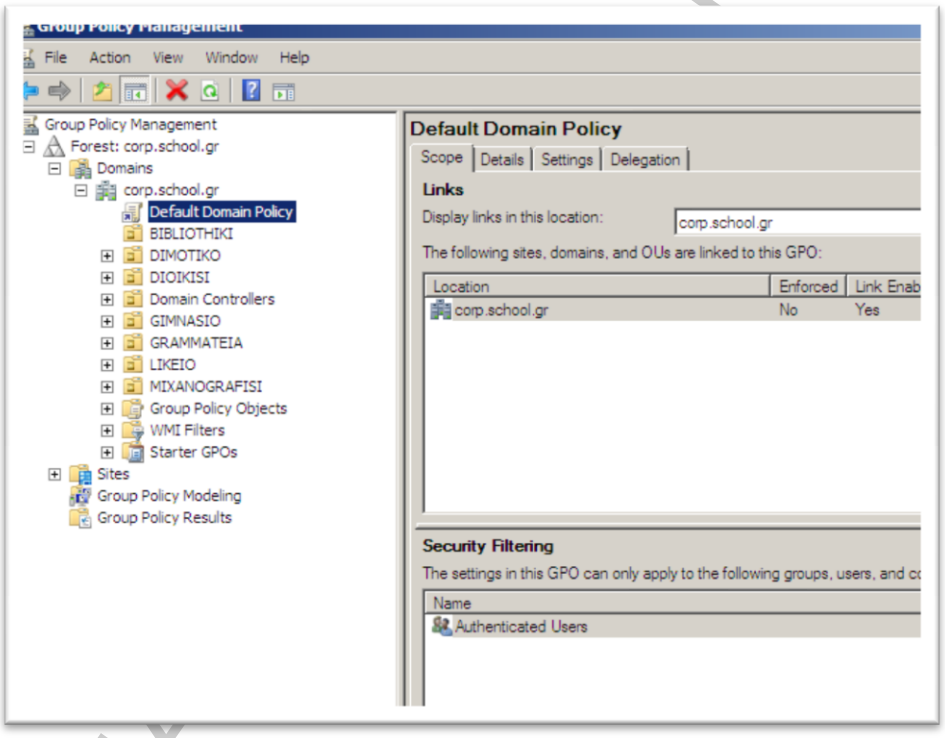
Επειδή ισχύει η αρχή της κληρονομικότητας καθώς και σχέσεις γονικές –θυγατρικές θα πρέπει να προσέχουμε τη σειρά εφαρμογής των πολιτικών η οποία έχει ως εξής:

1. Τοπικές πολιτικές ομάδων
2. Πολιτικές ομάδων τοποθεσιών
3. Πολιτικές ομάδων τομέων
4. Πολιτικές ομάδων οργανωτικών μονάδων
5. Πολιτικές ομάδων θυγατρικών οργανωτικών μονάδων

Η Microsoft μας παρέχει τα εξής διαχειριστικά εργαλεία των ομάδων:

- Group Policy Object Editor
- Group Policy Management Editor
- Group Policy Starter GPO Editor
- Local Group Policy Object Editor

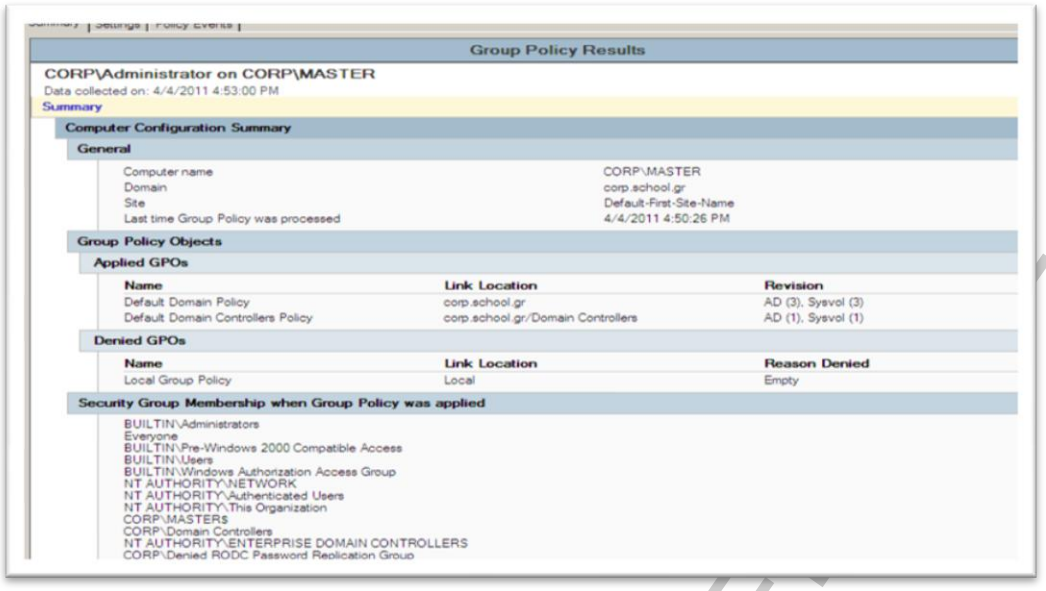
Και τα τέσσερα εργαλεία είναι παρόμοια. Η διαφορά τους έγκειται στο πεδίο εφαρμογής των πολιτικών. Αν θα ισχύουν στις ομάδες τοπικά ενός υπολογιστή ή στις ομάδες ενός τομέα. Στη συγκεκριμένη εργασία θα ασχοληθούμε με τις πολιτικές ομάδων σε ένα τομέα. Για να δούμε τις πολιτικές και να τις διαχειριστούμε επιλέγουμε Group Policy Management στο Administrative Tools (Εργαλεία διαχειριστή). Στην εικόνα 2.7.1 βλέπουμε την κονσόλα διαχείρισης πολιτικών ομάδων. Παρατηρούμε το δάσος, τους τομείς που βρίσκονται μέσα στο δάσος, και τις τοποθεσίες. Και στις τρεις περιπτώσεις μπορούμε να προσθέσουμε ή να αφαιρέσουμε δάση, τομείς και τοποθεσίες. Θα παρατηρήσουμε επίσης δύο ακόμα δοχεία (container), το Group Policy Modeling και το Group Policy Results. (Willam R. Stanek)



Εικόνα 2.7.1: Κονσόλα GPM

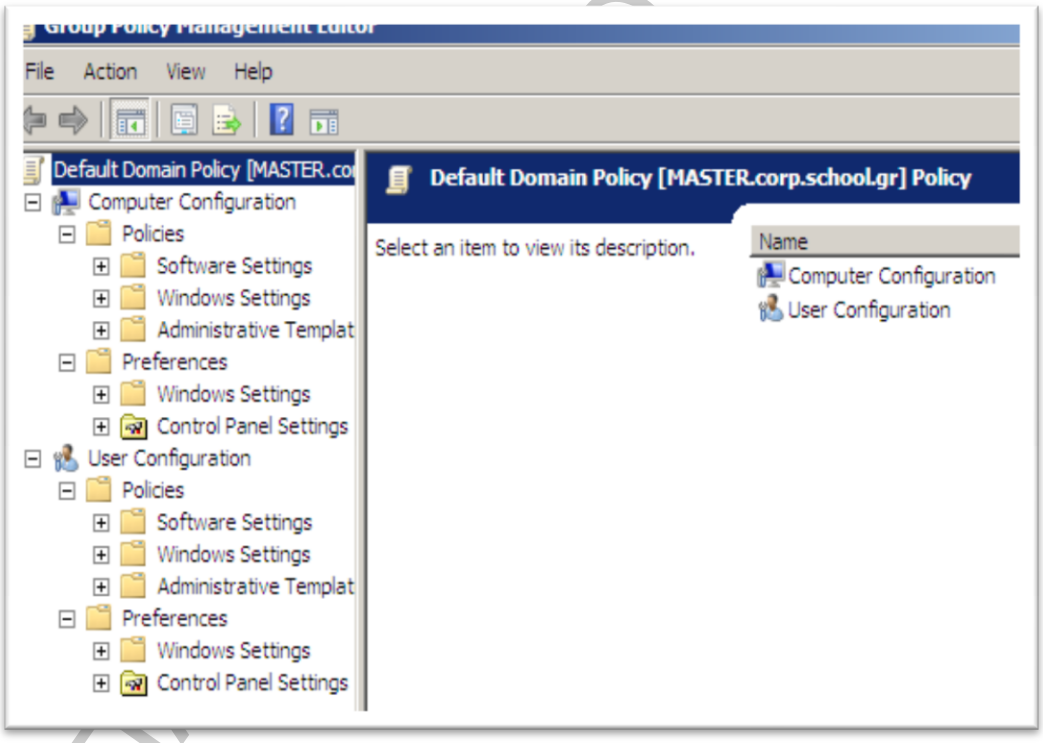
Το Group policy Modeling (Μοντελοποίηση πολιτικών ομάδων) μας δίνει τη δυνατότητα μέσω ενός βοηθού (wizard) να σχεδιάσουμε και να προσομοιώσουμε ρυθμίσεις για δοκιμαστικούς σκοπούς.

Το Group Policy Results (Αποτέλεσμα πολιτικών ομάδων) μας δίνει την δυνατότητα να δούμε πολιτικές και αποτελέσματα μέσω ενός wizard. Στην εικόνα 2.7.2 βλέπουμε τον τρόπο που εμφανίζονται τα αποτελέσματα.



Εικόνα 2.7.2: Group Policy Results

Ας δούμε όμως τον τρόπο με τον οποίο μπορούμε να επεξεργαστούμε τις πολιτικές μιας ομάδας. Κάνοντας δεξί κλικ στο Default Domain Policy επιλέγουμε Edit (Επεξεργασία). Ανοίγει το παράθυρο του διορθωτή πολιτικών όπως φαίνεται και στην εικόνα 2.7.3.



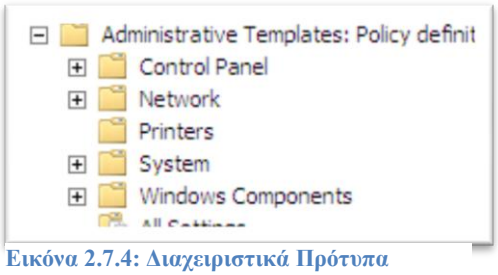
Εικόνα 2.7.3: Διορθωτής Πολιτικών

Ο GPO Editor (διορθωτής πολιτικών) χωρίζει τις πολιτικές σε πολιτικές υπολογιστών (computer configuration) και πολιτικές χρηστών (user configuration). Οι πολιτικές που εφαρμόζονται σε επίπεδο υπολογιστή είναι ανεξάρτητες από τον χρήστη που συνδέεται μέσω αυτού στο δίκτυο και αντίστοιχα οι πολιτικές που εφαρμόζονται σε χρήστες είναι ανεξάρτητες των υπολογιστών. Στον διορθωτή πολιτικών υπάρχει ένα προεπιλεγμένο σύνολο διαχειριστικών προτύπων ενώ έχουμε και την δυνατότητα να προσθέσουμε ή να αφαιρέσουμε.

Για κάθε ομάδα (υπολογιστών ή χρηστών) μπορούμε να επέμβουμε στις πολιτικές και στις Προτιμήσεις (Preferences).

Στην ομάδα πολιτικές έχουμε τις εξής δυνατότητες:

- Στις ρυθμίσεις λογισμικού (Software Settings) εγκαθίστανται ρυθμίσεις που καθορίζουν τον τρόπο εγκατάστασης λογισμικών. Ένα από το βασικά πλεονεκτήματα σε αυτή την ομάδα πολιτικών είναι ότι μπορούμε αυτόματα να εγκαταστήσουμε μια εφαρμογή – λογισμικό σε πολλούς υπολογιστές ταυτόχρονα χωρίς να χρειάζεται να γυρνάμε από υπολογιστή σε υπολογιστή.
- Στις ρυθμίσεις των Windows (Windows settings) καθορίζουμε πολιτικές για ανακατεύθυνση φακέλων, σενάρια (scripts), και ρυθμίσεις ασφαλείας.
- Στα διαχειριστικά πρότυπα (administrative templates: Policy definitions (ADMX files) retrieved from the local machine) υπάρχουν ρυθμίσεις που αφορούν εργασίες που γίνονται στον πίνακα ελέγχου, στο δίκτυο, στους εκτυπωτές, στο σύστημα και στα στοιχεία των Windows.



Εικόνα 2.7.4: Διαχειριστικά Πρότυπα

Στην ομάδα Προτιμήσεις (preferences) έχουμε τις εξής δυνατότητες:

- Ρυθμίσεις των Windows (Windows settings). Σε αυτό το σημείο υπάρχουν επιλογές για το περιβάλλον των windows, για τα αρχεία, τους φακέλους, το αρχείο ini, τη registry, το μοίρασμα πόρων και τις συντομεύσεις.
- Ρυθμίσεις στον πίνακα ελέγχου (Control panel settings). Εδώ μπορούμε να ρυθμίσουμε τις πηγές δεδομένων, τις συσκευές, τις ιδιότητες των φακέλων, τις τοπικές ομάδες και χρήστες, τις ιδιότητες του δικτύου, επιλογές ενέργειας, εκτυπωτές, προγραμματισμένες εργασίες και τέλος τις υπηρεσίες που τρέχουν ή όχι.

Όλες οι παραπάνω ρυθμίσεις – επιλογές των πολιτικών ομάδων ισχύουν και για τη διαμόρφωση χρήστη (user configuration) και για τη διαμόρφωση υπολογιστή (computer configuration). Θα πρέπει όμως να δούμε και κάποιες επιπλέον ρυθμίσεις που γίνονται μόνο στη διαμόρφωση χρήστη. Αυτές είναι η δυνατότητα υπηρεσιών απομακρυσμένης εγκατάστασης, ο φάκελος ανακατεύθυνσης (folder redirection), η επιφάνεια εργασίας των χρηστών, οι φάκελοι που διαμοιράζονται στο δίκτυο, το μενού εκκίνησης, η γραμμή εργασιών, η συντήρηση του internet explorer και οι αντιστοιχίσεις δίσκων (drive maps).

Όπως έχουμε αναφέρει ήδη οι υπάρχουσες πολιτικές ομάδων είναι πάνω από 700 και είναι δύσκολο να αναλυθούν στη συγκεκριμένη εργασία. Θα αναφερθούμε όμως αναλυτικότατα στις πολιτικές που θα χρησιμοποιήσουμε για τη δημιουργία των δικών μας ομάδων στο δίκτυό μας. Θα πρέπει δε να τονίσουμε ότι εκτός από τις έτοιμες πολιτικές που μας παρέχει η Microsoft μπορούμε να δημιουργήσουμε και εμείς με την βοήθεια των σεναρίων (scripts).

2.8 Βασικές εργασίες διαχείρισης Active Directory

Υπάρχουν πολλές ομάδες εργαλείων για τη διαχείριση των υπηρεσιών του Active Directory και ανάμεσά τους εργαλεία διαχείρισης με διασύνδεση γραφικών, εργαλεία της γραμμής εντολών (command prompt), και οργανωτικών μονάδων.

Τα εργαλεία που μας παρέχει η Microsoft μπορούν να προστεθούν ή να αφαιρεθούν από την κονσόλα διαχείρισης (MMC) ή να πάμε κατευθείαν στο μενού Administrative Tools (Εργαλεία Διαχείρισης). Τα βασικά εργαλεία είναι τα παρακάτω:

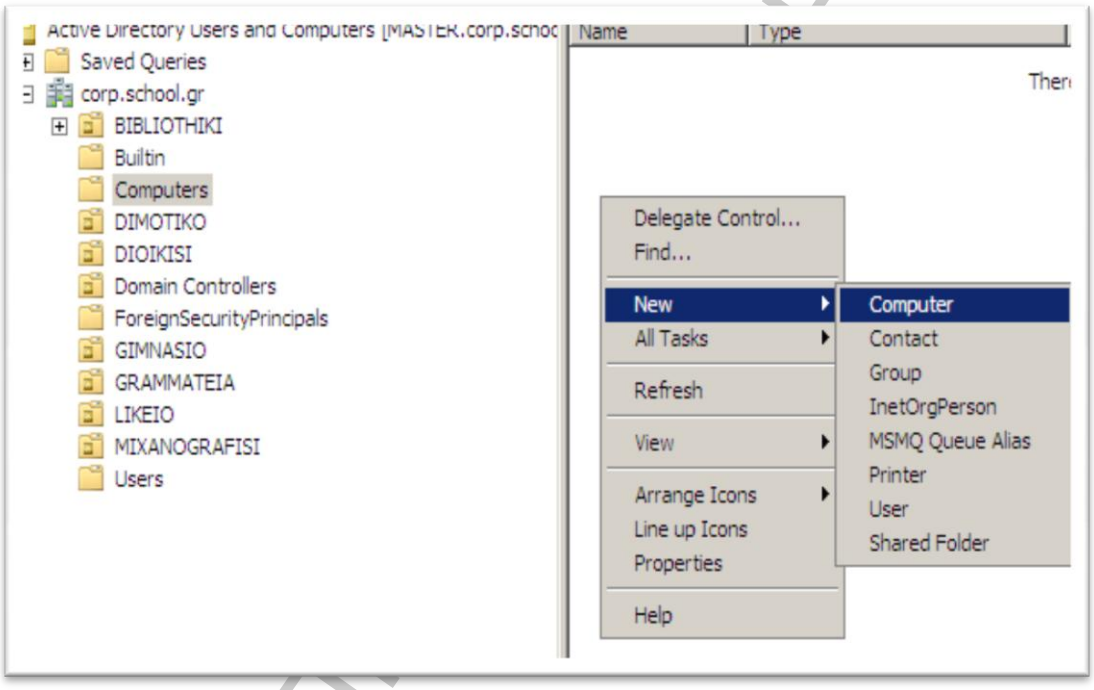
- Active Directory Users and Computers: Διαχείριση χρηστών, υπολογιστών και οργανωτικών μονάδων
- Active Directory Domains and Trusts: Διαχείριση των Τομέων σε σχέση με τα δέντρα και τα δάση.
- Active Directory Sites and Services: Διαχείριση τοποθεσιών και υποδικτύων.
- Group Policy Management Console: Διαχείριση του τρόπου χρήσης των πολιτικών ομάδων.

2.9 Λογαριασμοί υπολογιστών

Κάθε υπολογιστής ο οποίος έχει εγκατεστημένο ένα λειτουργικό σύστημα έχει στον τομέα ένα μοναδικό λογαριασμό υπολογιστή. Για να είναι σε θέση να κάνει χρήση των πόρων του τομέα θα πρέπει να γίνεται επικύρωση και έλεγχος από τον τομέα (authenticating and auditing). Μπορούμε να προσθέσουμε να αφαιρέσουμε, να απενεργοποιήσουμε και να κάνουμε επαναφορά (reset) σε ένα λογαριασμό υπολογιστή. Στα Windows 2008 υπάρχει το χαρακτηριστικό lastLogonTimestamp το οποίο μας δείχνει την τελευταία φορά που ένας υπολογιστής συνδέεται (logon) στον τομέα. Το DNS όνομα ενός πελάτη είναι το όνομα υπολογιστή (computer name).

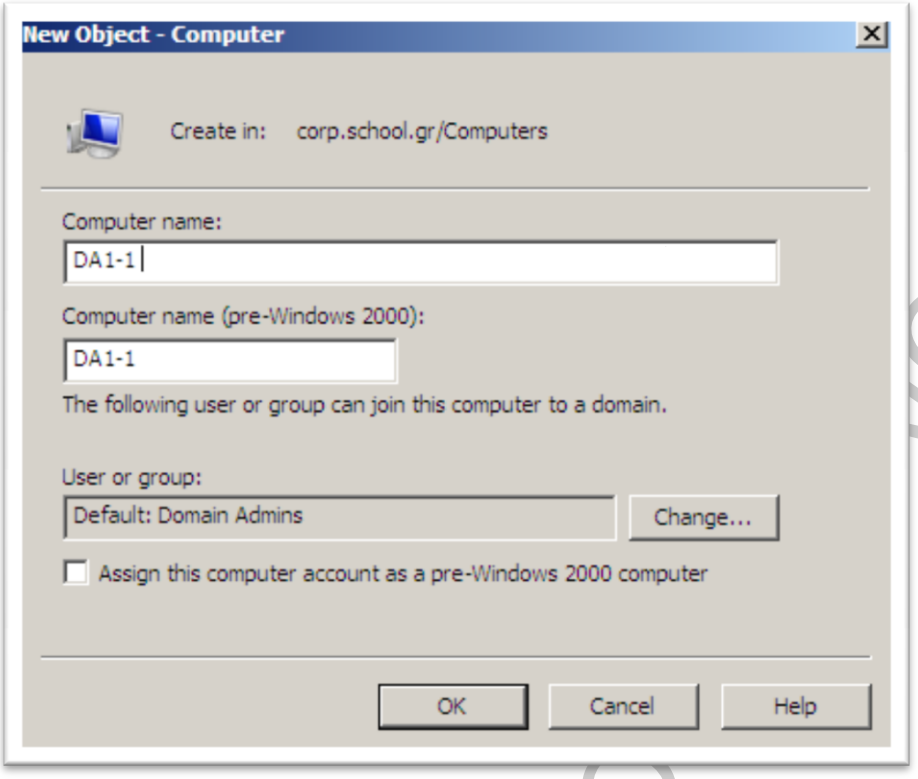
Για την δημιουργία ενός νέου λογαριασμού υπολογιστή θα πρέπει κάποιος να ανήκει στις ομάδες των Account Operators, Domain Admins ή Enterpise Admins.

Για να δημιουργήσουμε ένα καινούργιο λογαριασμό υπολογιστή μπορούμε να χρησιμοποιήσουμε το παραθυρικό περιβάλλον των windows ή χρησιμοποιώντας την γραμμή εντολών. Στην εικόνα 2.9.1 βλέπουμε το παραθυρικό περιβάλλον στο οποίο πηγαίνουμε επιλέγοντας Start\Administrative Tools\ActiveDirectory Users and Computers.



Εικόνα 2.9.1: Δημιουργία Υπολογιστή

Επιλέγοντας New\Computer ανοίγει ένα δεύτερο παράθυρο το οποίο μας ζητάει να γράψουμε το όνομα του υπολογιστή. Το όνομα θα πρέπει να είναι μοναδικό στον τομέα. Στη συνέχεια δηλώνουμε την ομάδα στην οποία θα ανήκει ο υπολογιστής.

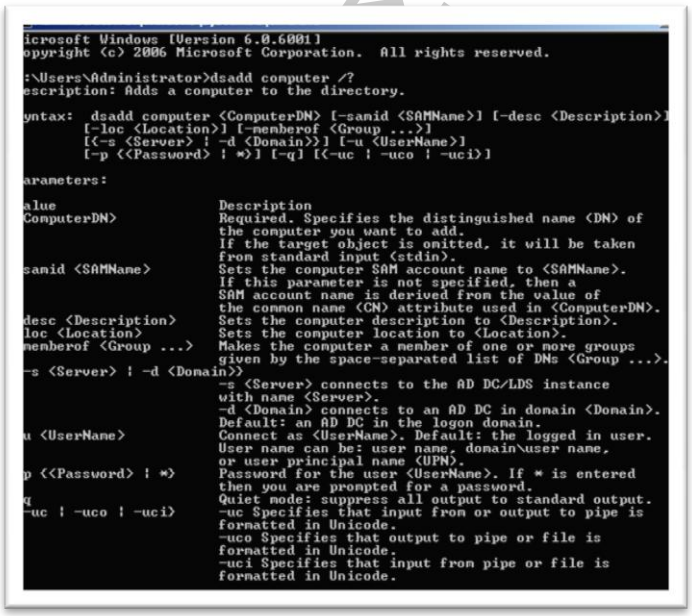


Εικόνα 2.9.2: Όνομα Υπολογιστή

Για να δημιουργήσουμε ένα λογαριασμό υπολογιστή σε γραμμή εντολών κάνουμε κλικ στο μενού start πληκτρολογούμε cmd και πατάμε enter. Πληκτρολογούμε την παρακάτω εντολή και πατάμε enter:

- dsadd computer <ComputerDN> όπου ComputerDN πληκτρολογούμε το όνομα του υπολογιστή

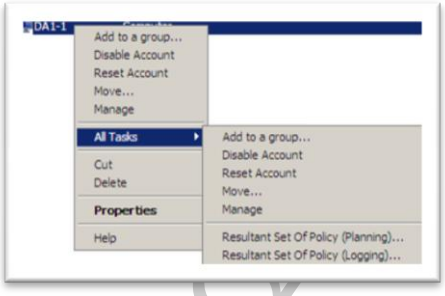
Θα πρέπει εδώ να προσθέσουμε ότι τα Windows 2008 έχουν και την λειτουργία help ? σε γραμμή εντολών όπως μπορούμε να δούμε και στην εικόνα 2.9.3, η οποία μας βοηθάει ανά πάσα στιγμή να βρούμε οδηγίες χρήσης και σύνταξης μίας εντολής.



Εικόνα 2.9.3: Γραμμές εντολών

Γενικά όλες οι εργασίες που μπορούμε να κάνουμε με την βοήθεια του γραφικού περιβάλλοντος γίνονται και με την χρήση της γραμμής εντολών.

Κάθε λογαριασμός ενός υπολογιστή που ανήκει σε ένα τομέα έχει κάποιες ιδιότητες. Οι βασικές του λειτουργίες είναι :



Εικόνα 2.9.4: Ιδιότητες Υπολογιστή

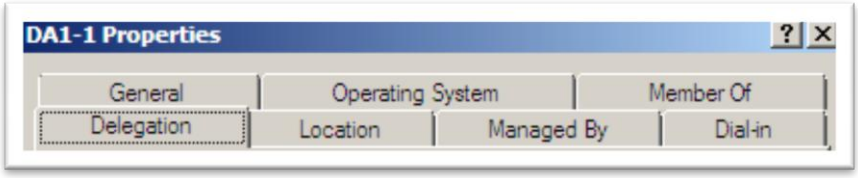
- Να τον προσθέσουμε σε μία ομάδα. Η αντίστοιχη εντολή σε γραμμή εντολών είναι:
  dsmod group <GroupDN> -addmbr <ComputerDN>
- Να τον απενεργοποιήσουμε. Η αντίστοιχη εντολή σε γραμμή εντολών είναι:
  dsmod computer <ComputerDN> -disabled {yes|no}
- Να κάνουμε επαναφορά (reset). Η αντίστοιχη εντολή σε γραμμή εντολών είναι:
  dsmod computer <ComputerDN> -reset
- Να το μετακινήσουμε.
- Να αναλάβουμε την απομακρυσμένη διαχείρισή του.
- Αποκοπή.
- Διαγραφή.
- Να δούμε και να επέμβουμε στις ιδιότητές του
- Προκύπτον σύνολο πολιτικής (προγραμματισμός)
- Προκύπτον σύνολο πολιτικής (logging)

Η περιγραφή των παραμέτρων καταγράφεται στον πίνακα 2.9.1.

Παράμετροι	**Περιγραφή**
<GroupDN>	Καθορίζει το αποκλειστικό όνομα του αντικειμένου της ομάδας στην οποία θέλουμε να προσθέσουμε το αντικείμενο υπολογιστή.
-addmbr	Θέτει την τιμή <ComputerDN> .
<ComputerDN>	Καθορίζει το αποκλειστικό όνομα του υπολογιστή που θα προστεθεί στην ομάδα. Το αποκλειστικό όνομα καθορίζει τη θέση του καταλόγου.
<ComputerDN>	Καθορίζει το αποκλειστικό όνομα του λογαριασμού υπολογιστή τον οποίο θέλουμε να απενεργοποιήσουμε ή να ενεργοποιήσουμε
-disabled	Θέτει ενεργοποίηση ή απενεργοποίηση συγκεκριμένων λογαριασμών υπολογιστών
{yes|no}	Καθορίζει το πότε ένας λογαριασμός είναι ενεργοποιημένος για να συνδεθεί
<ComputerDN>	Καθορίζει το αποκλειστικό όνομα ενός ή περισσοτέρων αντικειμένων υπολογιστή που θέλουμε να επαναφέρουμε.
-reset	Επαναφέρει το καθορισμένο αντικείμενο υπολογιστή.
<ComputerDN>	Καθορίζει το αποκλειστικό όνομα του υπολογιστή που θέλουμε να διαγράψουμε. Το αποκλειστικό όνομα καθορίζει τη θέση του καταλόγου.

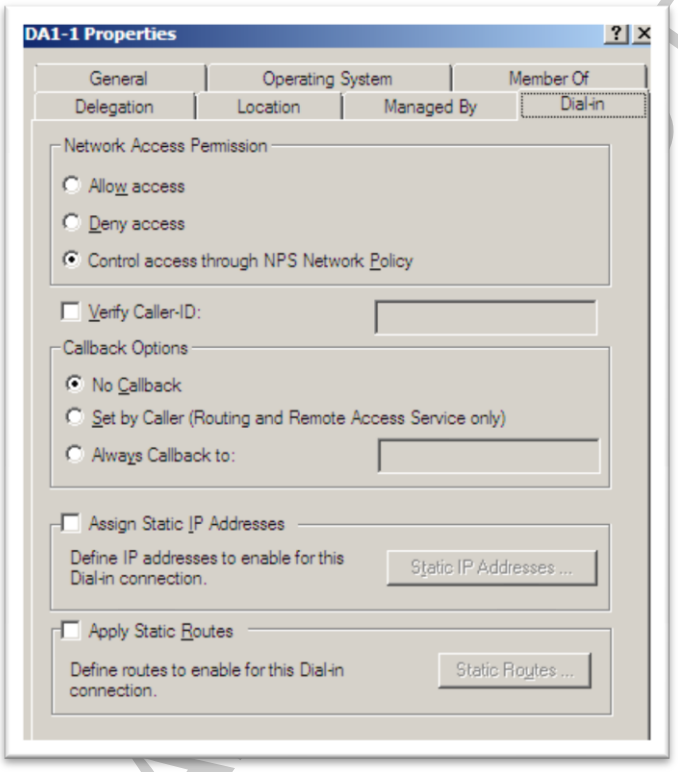
Πίνακας 2.9.1 : Παράμετροι Ομάδας

Ο κάθε υπολογιστής έχει και μια σειρά από ιδιότητες όπως βλέπουμε και στην εικόνα 2.9.5.



Εικόνα2.9.5: Ιδιότητες Υπολογιστή

- Στην καρτέλα General έχουμε μια γενική περιγραφή του υπολογιστή, το όνομά του, το DNS όνομα, τον τύπο του DC, το site στο οποίο ανήκει.
- Στην Καρτέλα Operating System αναφέρει το λειτουργικό σύστημα που είναι εγκατεστημένο, η έκδοσή του και το service pack του.
- Στην καρτέλα Member Of μας δείχνει σε ποιον τομέα ανήκει ο υπολογιστής και μας δίνεται η δυνατότητα να τον προσθέσουμε ή να τον αφαιρέσουμε από κάποιον τομέα.
- Στην καρτέλα Dial-in υπάρχουν επιλογές για επικοινωνία με τον υπολογιστή με τηλεφωνική γραμμή ή IP διεύθυνση.
- Στην καρτέλα Managed by έχουμε την δυνατότητα να ορίσουμε το ποιος θα διαχειρίζεται τον υπολογιστή και τα στοιχεία του. (Όνομα, διεύθυνση…).
- Στην καρτέλα Location βλέπουμε την τοποθεσία του υπολογιστή.
- Στην καρτέλα Delegation μπορούμε να ορίσουμε ή όχι τον συγκεκριμένο υπολογιστή για το αν θα αντιπροσωπεύει κάποιο άλλο αντικείμενο και σε τι επίπεδο εμπιστοσύνης.



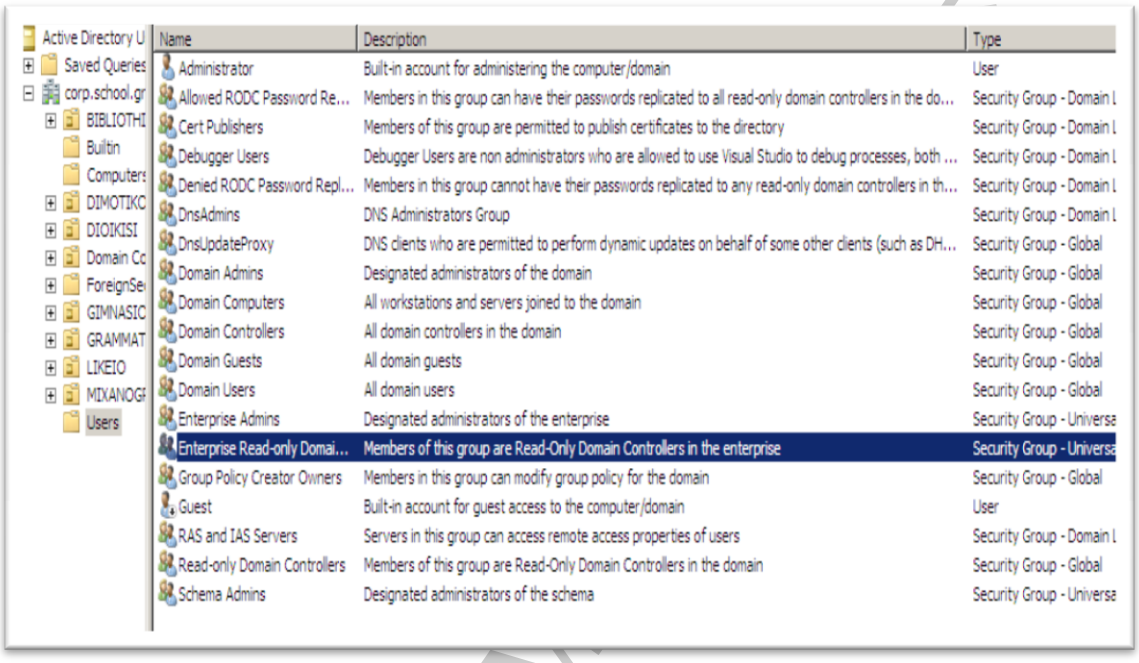
Εικόνα 2.9.6: Dial in (τρόπος σύνδεσης) Υπολογιστή

Όλες οι παραπάνω πληροφορίες και ιδιότητες ενός υπολογιστή βοηθούν στην καλύτερη γνώση και στην καλύτερη διαχείριση ενός δικτύου, δεν είναι όμως προαπαιτούμενες. Η βασική ρύθμιση είναι να δώσουμε ένα μοναδικό όνομα στον υπολογιστή.

Για να δηλώσουμε έναν νέο λογαριασμό υπολογιστή σε ένα τομέα μπορούμε επίσης απλά να συνδεθούμε (join) στον τομέα από τον συγκεκριμένο υπολογιστή και το όνομα του θα μπει αυτόματα στον τομέα. Το μόνο που θα πρέπει να γίνει στη συνέχεια είναι να το τοποθετήσουμε στην ομάδα που ανήκει. (Help Microsoft Windows Server 2008).

2.10 Λογαριασμοί Χρηστών

Οι λογαριασμοί χρηστών στον Ενεργό Κατάλογο αντιπροσωπεύουν φυσικές οντότητες όπως οι άνθρωποι. Μπορούμε να έχουμε λογαριασμούς που είναι αφιερωμένοι σε συγκεκριμένη λειτουργία. Κατά την αρχική εγκατάσταση η Microsoft έχει δημιουργήσει ομάδες λογαριασμών οι οποίες διευκολύνουν τη διαχείριση προσδίδοντας στους χρήστες που ανήκουν σε αυτές συγκεκριμένα δικαιώματα. Στην εικόνα 2.10.1 βλέπουμε τους ενσωματωμένους (build in) λογαριασμούς.



Εικόνα 2.10.1: Build in users

Θα παρατηρήσουμε τέσσερις διαφορετικούς τύπους από χρήστες - ομάδες. Ο administrator (διαχειριστής) και ο guest (καλεσμένος) είναι απλοί χρήστες. Υπάρχουν άλλες τρεις ομάδες:

- Security Group –Domain Local
- Security Group – Global
- Security Group – Universal.

Ο χρήστης administrator είναι ο πρώτος που δημιουργείται κατά την εγκατάσταση ενός τομέα και έχει πλήρη δικαιώματα μέσα σε αυτόν. Γι αυτό το λόγω θα πρέπει να έχει και ένα πολύ ισχυρό κωδικό. Επειδή είναι γνωστός ο εν λόγω λογαριασμός προτείνεται να τον μετονομάσουμε ή να τον απενεργοποιήσουμε. Θα πρέπει όμως να τονίσουμε ότι αν τον απενεργοποιήσουμε εξακολουθεί να λειτουργεί σε ασφαλή λειτουργία.

Ο χρήστης guest είναι εξαρχής απενεργοποιημένος. Είναι ένας απλός χρήστης του τομέα χωρίς πολλά δικαιώματα αλλά μπορεί ο διαχειριστής να του προσθέσει ή να αφαιρέσει δικαιώματα. Δημιουργήθηκε αρχικά για να εξυπηρετεί χρήστες που δεν ανήκουν σε έναν οργανισμό αλλά έχουν επισκεφτεί τον οργανισμό για κάποια παρουσίαση για παράδειγμα και θέλουν να έχουν προσωρινά μια απλή πρόσβαση στο διαδίκτυο. Η Microsoft προτείνει να μείνει απενεργοποιημένος και αν χρειαστεί τον ενεργοποιούμε προσωρινά.

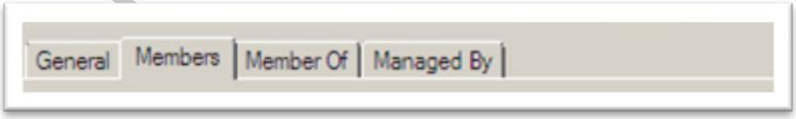
Στη συνέχεια η Microsoft έχει δημιουργήσει ομάδες ασφαλείας, τοπικές, σφαιρικές και καθολικές (security groups, local, global και universal). Έχει μοιράσει της βασικές λειτουργίες ενός δικτύου και σε κάθε ομάδα έχει δώσει συγκεκριμένα δικαιώματα και συγκεκριμένους χρήστες. Βέβαια όλα αυτά μπορούν να προσαρμοστούν στις ανάγκες του κάθε δικτύου. Για παράδειγμα τα μέλη της ομάδας Group Policy Creator Owners το μόνο που μπορούν να κάνουν είναι να αλλάζουν και να δημιουργούν πολιτικές ομάδων.

Στον παρακάτω πίνακα περιγράφουμε την λειτουργία των ενσωματωμένων χρηστών και ομάδων.

ΕΝΣΩΜΑΤΩΜΕΝΟΙ ΧΡΗΣΤΕΣ	ΡΟΛΟΙ
Administrator	Ενσωματωμένος λογαριασμός ο οποίος διαχειρίζεται τον τομέα.
Allowed RODC Password Replication Group	Τα μέλη αυτής της ομάδας μπορούν να έχουν κωδικούς πρόσβασης σε όλους τους ελεγκτές τομείς που είναι μόνο για ανάγνωση (read-only domain controllers)
Cert Publishers	Τα μέλη της ομάδας αυτής επιτρέπεται να δημοσιεύουν τα πιστοποιητικά στον κατάλογο
Debugger Users	Οι Debugger είναι χρήστες με μόνο δικαίωμα την χρήση του Visual Studio για τον εντοπισμό σφαλμάτων, τόσο τοπικά όσο και απομακρυσμένα. Μόνο έμπιστοι χρήστες θα πρέπει να προστεθούν σε αυτήν την ομάδα.
Denied RODC Password Replication Group	Τα μέλη αυτής της ομάδας δεν έχουν κωδικούς που να αναπαράγονται σε οποιοδήποτε ελεγκτή τομέα μόνο για ανάγνωση.
DnsAdmins	DNS ομάδα διαχειριστών
DnsUpdateProxy	DNS πελάτες (client) που τους επιτρέπεται να ασκούν δυναμικές ενημερώσεις για λογαριασμό ορισμένων άλλων πελατών (όπως οι διακομιστές DHCP).
Domain Admins	Διαχειριστές του Τομέα
Domain Computers	Όλους τους σταθμούς εργασίας και εξυπηρετητές που συνδέονται με τον Τομέα
Domain Controllers	Όλοι οι Ελεγκτές Τομέα στον Τομέα
Domain Guests	Όλοι οι επισκέπτες στον Τομέα
Domain Users	Όλοι οι χρήστες στον Τομέα
Enterprise Admins	Κεντρικοί διαχειριστές
Enterprise Read-only Domain Controllers	Τα μέλη αυτής της ομάδας είναι οι Read-Only Domain Controllers στον οργανισμό -επιχείρηση
Group Policy Creator Owners	Τα μέλη αυτής της ομάδας μπορούν να τροποποιήσουν τις πολιτικές ομάδων (GPO) στον Τομέα
guest	Ενσωματωμένος λογαριασμός για τους επισκέπτες για να έχουν πρόσβαση στον Τομέα
RAS and IAS Servers	Οι εξυπηρετητές αυτής της ομάδας υποστηρίζουν τις απομακρυσμένες προσβάσεις
Read-only Domain Controllers	Τα μέλη της ομάδας αυτής είναι Ελεγκτές Τομέα μόνο για ανάγνωση
Schema Admins	Διαχειριστές του Σχήματος

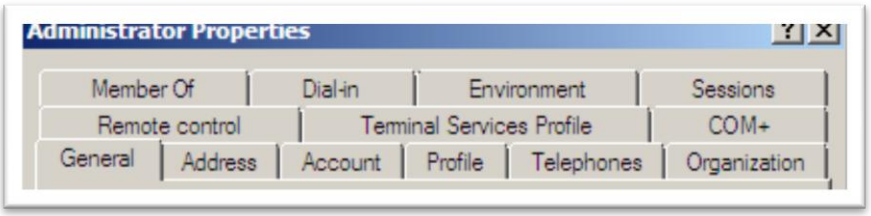
Ας δούμε όμως τις ιδιότητες των ενσωματωμένων ομάδων.

- Η καρτέλα General έχει μια γενική περιγραφή, το email, το scope και το group.
- Η καρτέλα Members δηλώνει τα μέλη της ομάδας.
- Η καρτέλα Member Of δηλώνει σε ποια ομάδα ανήκει.
- Η καρτέλα Managed By δηλώνει τα στοιχεία αυτού που διαχειρίζεται τον συγκεκριμένο λογαριασμό.



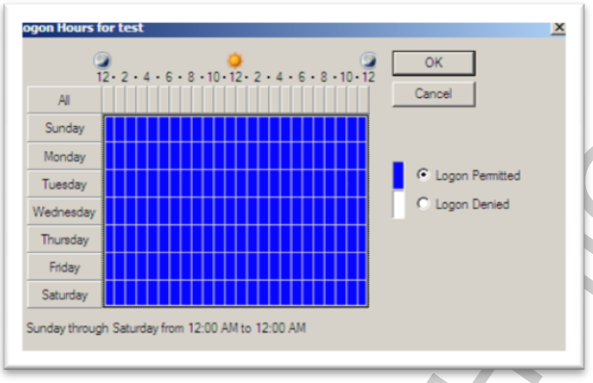
Εικόνα 2.10.2: Ιδιότητες Ομάδων

Οι χρήστες έχουν περισσότερες ιδιότητες από μία ομάδα χρηστών όπως βλέπουμε και στην εικόνα 2.10.3.



Εικόνα 2.10.3:Ιδιότητες Χρηστών

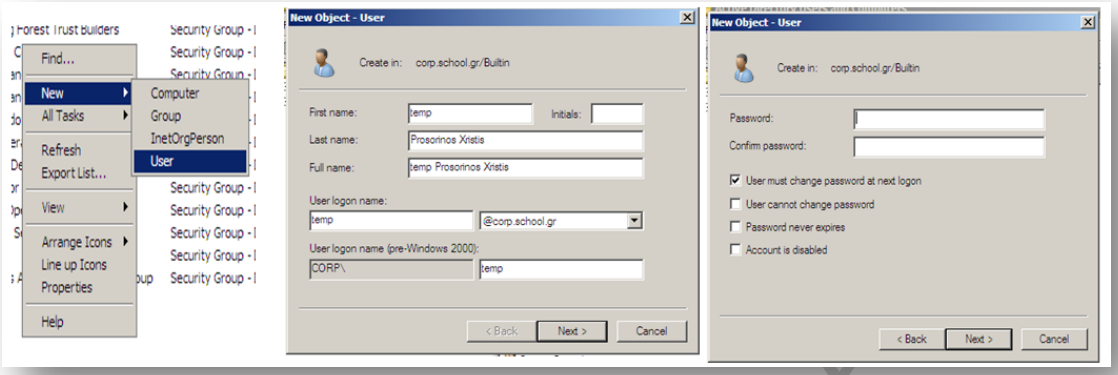
- Η καρτέλα Address δηλώνει αναλυτικά την διεύθυνση του χρήστη.
- Η καρτέλα Account μας δείχνει αρχικά το όνομα σύνδεσης του χρήστη. Υπάρχουν επιλογές όπως οι ώρες που θα έχει πρόσβαση ο χρήστης στο δίκτυο ή σε ποιους υπολογιστές θα έχει πρόσβαση. Μπορούμε να κλειδώσουμε έναν λογαριασμό, να του ορίσουμε ημερομηνία λήξης και να καθορίσουμε τον τρόπο που θα χειρίζεται τον κωδικό πρόσβασης του. Στον χρήστη administrator δεν έχουμε επιλογή των ωρών σύνδεσης γιατί ο administrator είναι ο διαχειριστής του δικτύου και θα πρέπει να έχει πάντα πρόσβαση σε αυτό.



Εικόνα 2.10.4: Ώρες Σύνδεσης Χρήστη

- Η καρτέλα Profile ορίζει το που βρίσκεται το προφίλ του χρήστη, ποια σενάρια (scripts) τρέχουν κατά την σύνδεση και που βρίσκεται ο προσωπικός του φάκελος.
- Στην καρτέλα Telephones καταγράφονται όλα τα τηλέφωνά του καθώς και η IP διεύθυνση.
- Στην καρτέλα Organization καταγράφονται τα στοιχεία του οργανισμού που δουλεύει ο χρήστης, το τμήμα και η θέση του.
- Στην καρτέλα COM+ δηλώνουμε το partition που αποθηκεύεται στον Ενεργό Κατάλογο.
- Στην καρτέλα Terminal Services Profile δηλώνουμε αν ο χρήστης έχει δικαίωμα να επικοινωνεί μέσω terminal (απομακρυσμένα).
- Στην καρτέλα Remote control δηλώνουμε το αν μπορούμε να ελέγχουμε απομακρυσμένα τον χρήστη και με ποιο τρόπο.
- Στην καρτέλα Environment έχουμε την επιλογή να ορίσουμε πια προγράμματα να τρέχουν κατά την εκκίνηση.
- Στην καρτέλα session δηλώνουμε το πότε ο χρήστης θα συνδέεται και για πόσο μέσω terminal services.

Για την δημιουργία ενός νέου χρήστη κάνουμε δεξί κλίκ στους χρήστες στο Active Directory και επιλέγουμε New\User, βάζουμε τα στοιχεία του και τον κωδικό του.



Εικόνα 2.10.5: Δημιουργία Νέου Χρήστη

Δικαίωμα δημιουργίας νέου χρήστη καθώς και οποιαδήποτε αλλαγή έχουν μόνο όσοι ανήκουν στις ομάδες Account Operators, Domain Admins και Enterprise Admins, ή θα πρέπει να έχουν οριστεί αντίστοιχα δικαιώματα σε κάποιον άλλον χρήστη. Σε περίπτωση που έχουμε διαγράψει κάποιον χρήστη και θέλουμε να δημιουργήσουμε καινούργιο με το ίδιο όνομα μπορούμε αλλά αυτό δεν σημαίνει ότι μεταφέρονται και οι ιδιότητες του αντικειμένου εξαιτίας του security identifier (SID). Η προεπιλεγμένη δημιουργία ενός display name (περιγραφή ονόματος) βασίζεται στη διαμόρφωση FirstNameLastName.

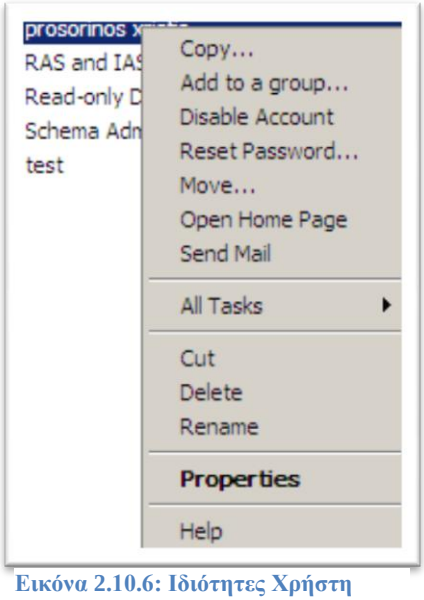
Για την δημιουργία ενός χρήστη με τη βοήθεια της γραμμής εντολών χρησιμοποιούμε την παρακάτω μέθοδο:

Σε γραμμή εντολών πληκτρολογούμε

dsadd user <UserDN> [-samid<SAMName>] -pwd {<Password>|}*

Ας δούμε όμως τι επιλογές έχουμε μετά την δημιουργία ενός χρήστη:

- Αντιγραφή ενός χρήστη. Κατά την αντιγραφή ενός χρήστη τα βασικά στοιχεία που αντιγράφονται είναι οι logon ώρες, οι περιορισμοί του χρήστη, το πότε λήγει ο λογαριασμός του. Μπορούμε να προσαρμόσουμε το πια στοιχεία θα αντιγραφούν αλλά θα πρέπει να είμαστε προσεκτικοί έτσι ώστε να μη υπάρξουν διπλοεγγραφές. Μπορούμε να επιλέξουμε ποιες ιδιότητες θα αντιγράψουμε από τον ένα χρήστη στον άλλο.
- Να προσθέσουμε έναν χρήστη σε μια ομάδα χρηστών. Με αυτό τον τρόπο ο χρήστης αποκτά τις ίδιες ιδιότητες -δικαιώματα με την ομάδα που τον έχουμε προσθέσει.
- Απενεργοποίηση ενός χρήστη. Συχνά χρειάζεται να κάνουμε κάποιες δοκιμές ή να δώσουμε προσωρινά δικαιώματα σε κάποιους χρήστες. Αντί να επεμβαίνουμε κάθε φορά σε κάποιους χρήστες προσθέτοντας ή αφαιρώντας δικαιώματα μπορούμε να δημιουργήσουμε έναν χρήστη που θα του ορίσουμε τα δικαιώματα που θέλουμε. Στη συνέχεια το ενεργοποιούμε ή τον απενεργοποιούμε ανάλογα με την χρήση του.



Εικόνα 2.10.6: Ιδιότητες Χρήστη

- Επαναφορά (reset). Χρειάζεται στη περίπτωση που κάποιος χρήστης ξεχάσει τον κωδικό του.

- Μετακίνηση σε άλλο φάκελο – ομάδα. Κατά την μετακίνηση ενός λογαριασμού χρήστη ο χρήστης κληρονομεί τα δικαιώματα της ομάδας στην οποία πηγαίνει. Για την μετακίνηση χρηστών μεταξύ τομέων δεν χρησιμοποιούμε το Active Directory Users and Computers αλλά το εργαλείο Active Directory Migration Tool (ADMT).
- Αποκοπή χρήστη.
- Διαγραφή Χρήστη. Κατά την διαγραφή ενός χρήστη διαγράφονται και όλες οι ιδιότητες του. Αν ξαναδημιουργήσουμε τον ίδιο χρήστη σαν όνομα, για τα Windows είναι διαφορετικός χρήστης (unique SID) και θα πρέπει να του ορίσουμε ξανά τις ιδιότητές του.
- Μετονομασία Χρήστη. Αλλάζει το όνομα ενός λογαριασμού χρήστη.

(Help Microsoft Windows Server 2008)

Παράμετροι	Περιγραφή
<UserDN>	Καθορίζει το αποκλειστικό όνομα του χρήστη αντικειμένου που θα προστεθεί
-samid	Τοποθέτηση τιμής <SAMName>
<SAMName>	Καθορίζει το Security Accounts Manager (SAM), όνομα με το μοναδικό όνομα λογαριασμού SAM για αυτό το χρήστη (για παράδειγμα, Linda). Εάν το όνομα SAM δεν έχει οριστεί, dsadd προσπαθεί να δημιουργήσει το όνομα του λογαριασμού SAM χρησιμοποιώντας μέχρι και τους πρώτους 20 χαρακτήρες από το κοινό όνομα (CN) των UserDN.
-pwd	Τοποθέτηση τιμής <Password>
<Password>	Καθορίζει τον κωδικό πρόσβασης που θα χρησιμοποιηθεί για το λογαριασμό χρήστη. Εάν αυτή η παράμετρος έχει οριστεί σε *, θα σας ζητηθεί κωδικός πρόσβασης χρήστη
<UserDN>	Καθορίζει το αποκλειστικό όνομα του αντικειμένου χρήστη που θα προστεθεί
-disabled	Θέτει την τιμή UF_ACCTDISABLED στο userAccountControl.
{yes|no}	Καθορίζει αν ο λογαριασμός χρήστη έχει απενεργοποιηθεί. Για σύνδεση (yes) ή όχι (no).
<UserDN>	Καθορίζει το αποκλειστικό όνομα του χρήστη για τον οποίο ο κωδικός πρόσβασης θα μηδενιστεί.
-pwd	Τοποθετεί το <NewPassword>.
<NewPassword>	Καθορίζει τον κωδικό πρόσβασης που θα αντικαταστήσει τον τρέχοντα κωδικό πρόσβασης χρήστη.
-mustchpwd	Τοποθετεί το pwdExpired flag.
{yes|no}	Καθορίζει την τιμή του pwdExpired flag.
<UserDN>	Καθορίζει το αποκλειστικό όνομα του αντικειμένου χρήστη που θα προστεθεί.
-newparent	Τοποθετεί το <ParentDN> value.
<ParentDN>	Καθορίζει τη νέα θέση στην οποία θέλουμε να μετακινήσουμε το αντικείμενο χρήστη. Η νέα θέση έχει καθοριστεί ως το αποκλειστικό όνομα του νέου κόμβου γονέα.
<ObjectDN>	Καθορίζει το αποκλειστικό όνομα του αντικειμένου χρήστη, που πρέπει να διαγραφεί

Πίνακας 2.10: Παράμετροι γραμμών εντολών

2.11 Λογαριασμοί Ομάδων

Μια ομάδα είναι μια συλλογή από λογαριασμούς χρηστών και υπολογιστών, επαφές, ή και άλλες ομάδες που μπορούν να διαχειρίζονται ως ενιαία μονάδα. Οι χρήστες και οι υπολογιστές που ανήκουν σε μια συγκεκριμένη ομάδα αναφέρεται ως μέλη της ομάδας. Οι ομάδες στον Ενεργό Κατάλογο είναι αντικείμενα καταλόγου ενός τομέα και μιας οργανωτικής μονάδας. Ο Ενεργός Κατάλογος προσφέρει μια σειρά από ενσωματωμένες ομάδες κατά την εγκατάσταση. Παρέχει επίσης μια επιλογή για να δημιουργήσουμε ομάδες. Στον πίνακα 2.11.1 βλέπουμε τις ενσωματωμένες ομάδες του Ενεργού καταλόγου.

Ομάδες	Ρόλοι
Account Operators	Τα μέλη της μπορούν να διαχειρίζονται τους χρήστες του τομέα και την ομάδα λογαριασμών.
Administrators	Οι διαχειριστές έχουν πλήρη και απεριόριστη πρόσβαση στον υπολογιστή του τομέα και στον ελεγκτή τομέα
Backup Operators	Οι Backup Operators μπορούν να παρακάμψουν τους περιορισμούς ασφαλείας με αποκλειστικό σκοπό τη δημιουργία αντιγράφων ασφαλείας ή την επαναφορά αρχείων
Certificate Service DCOM Access	Τα μέλη αυτής της ομάδας έχουν τη δυνατότητα να συνδεθούν με Αρχές Πιστοποίησης στα enterprise files
Cryptographic Operators	Μέλη που επιτρέπεται να εκτελούν κρυπτογραφικές λειτουργίες.
Distributed COM Users	Μέλη που έχουν τη δυνατότητα να ξεκινήσουν, ενεργοποιήσουν και χρησιμοποιήσουν τα Distributed COM, αντικείμενα σε αυτό το μηχάνημα.
Event Log Readers	Τα μέλη αυτής της ομάδας μπορούν να διαβάσουν αρχεία καταγραφής συμβάντων από το τοπικό μηχάνημα
Guests	Οι επισκέπτες έχουν την ίδια πρόσβαση με τα μέλη της ομάδας Users από προεπιλογή, εκτός από το λογαριασμό guest ο οποίος έχει περιορισμούς
IIS_IUSRS	Ενσωματωμένη ομάδα που χρησιμοποιείται από το Internet Information Services.
Incoming Forest Trust Builders	Τα μέλη αυτής της ομάδας μπορούν να δημιουργήσουν εισερχόμενες σχέσεις εμπιστοσύνης σε ένα δάσος
Network Configuration Operators	Τα μέλη σε αυτή την ομάδα μπορούν να έχουν ορισμένα διοικητικά προνόμια για να διαχειρίζονται την διαμόρφωση των χαρακτηριστικών γνωρισμάτων δικτύωσης
Performance Log Users	Τα μέλη αυτής της ομάδας μπορούν να προγραμματίσουν την καταγραφή των μετρητών επιδόσεων
Performance Monitor Users	Τα μέλη αυτής της ομάδας μπορούν να έχουν πρόσβαση στα δεδομένα του μετρητή επιδόσεων τοπικά και απομακρυσμένα
Pre-Windows 2000 Compatible Access	Μια ομάδα που έχει συμβατότητα με παλιότερους χρήστες
Print Operators	Τα μέλη που μπορούν να διαχειριστούν τους εκτυπωτές του τομέα
Remote Desktop Users	Στα μέλη αυτής της ομάδας παρέχεται το δικαίωμα σύνδεσης απομακρυσμένα.
Replicator	Υποστηρίζει αναπαραγωγή αρχείων (file replication) σε έναν τομέα
Server Operators	Τα μέλη αυτής της ομάδας μπορούν να διαχειρίζονται τους διακομιστές του τομέα
Terminal Server License Servers	Τα μέλη αυτής της ομάδας μπορούν να ενημερώσουν τους λογαριασμούς χρηστών στην υπηρεσία καταλόγου με πληροφορίες σχετικά με την έκδοση άδειας, για τους σκοπούς της

	παρακολούθησης και αναφοράς του TS Per user CAL χρήση.
Users	Οι χρήστες δεν έχουν το δικαίωμα να κάνουν τυχαία ή σκόπιμη αλλαγή στο σύστημα αλλά μπορούν να τρέξουν τις περισσότερες εφαρμογές
Windows Authorization Access Group	Τα μέλη αυτής της ομάδας έχουν πρόσβαση στο χαρακτηριστικό computed tokenGroupsGlobalAndUniversal του αντικειμένου χρήστη

Πίνακας 2.11.1: Ενσωματωμένες Ομάδες AD

Χρησιμοποιούμε ομάδες για τους παρακάτω λόγους:

- Απλοποίηση της διαχείρισης με την ανάθεση δικαιωμάτων σε έναν κοινόχρηστο πόρο σε μια ομάδα, και όχι σε μεμονωμένους χρήστες. Η εκχώρηση δικαιωμάτων σε μια ομάδα αποδίδει τα ίδια δικαιώματα πρόσβασης στους πόρους του δικτύου σε όλα τα μέλη της.
- Θέτοντας πολιτική σε μια ομάδα αυτόματα όλοι οι χρήστες της ομάδας έχουν συγκεκριμένα δικαιώματα. Αρκεί λοιπόν να προσθέσουμε σε αυτή την ομάδα χρήστες.
- Δημιουργία λίστας διανομής ηλεκτρονικού ταχυδρομείου.

Οι ομάδες χαρακτηρίζονται από το πεδίο εφαρμογής τους (scope) και τον τύπο (type).Το πεδίο εφαρμογής προσδιορίζει την εμβέλεια – ορατότητα της ομάδας. Προσδιορίζει επίσης και τον τομέα από τον οποίο μπορούμε να προσθέσουμε μέλη καθώς και τα κατοχυρωμένα δικαιώματα αυτών.

Ο τύπος της ομάδας καθορίζει τον τρόπο χρήσης μιας ομάδας. Στον Ενεργό Κατάλογο υπάρχουν δύο τύπο ομάδων. Ομάδες διανομής και ομάδες ασφαλείας (distribution groups and security groups). Οι ομάδες διανομής μπορούν να δημιουργήσουν λίστα διανομής ηλεκτρονικού ταχυδρομείου. Οι ομάδες ασφαλείας διαμοιράζουν δικαιώματα πρόσβασης στους πόρους του δικτύου. Πιο συγκεκριμένα οι ομάδες ασφαλείας δίνουν δικαιώματα πρόσβασης των χρηστών σε ομάδες και δικαιώματα πρόσβασης στους μοιραζόμενους πόρους του δικτύου (user rights and permissions).

Υπάρχουν ομάδες τις οποίες δεν μπορούμε να τροποποιήσουμε ή να δούμε τα μέλη της. Οι ομάδες αυτές αναφέρονται ως ιδιαίτερη ταυτότητα (special identities). Αποτελούνται δε από διαφορετικούς χρήστες σε διαφορετικές χρονικές στιγμές, ανάλογα με τις περιστάσεις.

- Η ομάδα Everyone είναι μια ειδική ταυτότητα που εκπροσωπεί όλους τους σημερινούς χρήστες του δικτύου, συμπεριλαμβανομένων των επισκεπτών και των χρηστών από άλλους τομείς.
- Η ομάδα Anonymous Logon εκπροσωπεί τους χρήστες και τις υπηρεσίες που έχουν πρόσβαση σε έναν υπολογιστή και τους πόρους του χωρίς να χρειάζεται ένα λογαριασμό χρήστη στον τομέα.
- Η ομάδα Network αντιπροσωπεύει τους χρήστες που έχουν πρόσβαση αυτήν την περίοδο σε έναν δεδομένο πόρο πέρα από το δίκτυο. Όταν ένας χρήστης έχει πρόσβαση σε έναν δεδομένο πόρο πέρα από το δίκτυο, ο χρήστης προστίθεται αυτόματα στην ομάδα Network.
- Η ομάδα Interactive αντιπροσωπεύει όλους τους χρήστες που συνδέονται αυτήν την περίοδο σε έναν ιδιαίτερο υπολογιστή και οι οποίοι έχουν πρόσβαση σε έναν δεδομένο πόρο αυτού. Όταν ένας χρήστης έχει πρόσβαση σε έναν δεδομένο πόρο σε έναν υπολογιστή, ο χρήστης προστίθεται αυτόματα στην ομάδα Interactive.
- Οι ενσωματωμένες ομάδες, όπως η ομάδα Domain Admins, είναι ομάδες ασφαλείας που δημιουργούνται αυτόματα όταν δημιουργείται ένας τομέας Ενεργού Καταλόγου.

Πολλές ενσωματωμένες ομάδες αναθέτουν αυτόματα μια σειρά δικαιωμάτων στους χρήστες που ανήκουν σε αυτήν για την πραγματοποίηση συγκεκριμένων εργασιών μέσα στον τομέα. Κατά την προσθήκη ενός χρήστη σε μια ομάδα, ο χρήστης αποκτά όλα τα δικαιώματα και τις άδειες που έχει η ομάδα.

Οι ενσωματωμένες ομάδες βρίσκονται στο δοχείο Built in (ενσωματωμένο) και το δοχείο χρήστες. Οι ενσωματωμένες ομάδες μέσα στο δοχείο Built in έχουν πεδίο εφαρμογής το πεδίο της ομάδας built in local. Το πεδίο εφαρμογής της ομάδας τους και το είδος δεν μπορεί να αλλάξει. Το δοχείο Χρήστες περιέχει ομάδες που ορίζονται με σφαιρική εμβέλεια (global scope)

και τις ομάδες που ορίζονται μέσα στον τομέα με τοπικής εμβέλεια (local scope). Η μετακίνησή τους επιτρέπεται σε άλλες ομάδες ή οργανωτικές μονάδες(OUs) μόνο μέσα στον ίδιο τομέα.

Οι ομάδες χαρακτηρίζονται από ένα πεδίο που προσδιορίζει την εμβέλειά τους (που είναι ορατοί και πόσο μπορούν να επηρεάσουν ένα δίκτυο). Υπάρχουν τρία πεδία ομάδας: τοπικά, σφαιρικά, και καθολικά.

Τοπικές ομάδες τομέα: Τα μέλη του τομέα των τοπικών ομάδων μπορούν να περιλαμβάνουν άλλες ομάδες και λογαριασμούς από Windows Server 2003, Windows 2000, Windows NT και Windows Server 2008. Τα δικαιώματα των μελών της συγκεκριμένης ομάδας έχουν ισχύ μόνο μέσα στον τομέα που ανήκουν. Οι τοπικές ομάδες βοηθάνε στη διαχείριση ενός μεμονωμένου τομέα, και μπορούν να περιέχουν:

- Ομάδες με σφαιρική (global) εμβέλεια
- Ομάδες με παγκόσμια εμβέλεια
- Λογαριασμούς χρηστών- υπολογιστών
- Άλλες ομάδες με τον τομέα τοπικής εμβέλειας
- Ένα μείγμα από διάφορες ομάδες

Σφαιρικές ομάδες τομέα: Τα μέλη της σφαιρικής ομάδας (global groups) μπορούν να ανήκουν και σε άλλες ομάδες ή λογαριασμούς μόνο από τον τομέα στον οποίο ανήκουν. Στα μέλη αυτών των ομάδων μπορούν να εκχωρηθούν δικαιώματα σε κάθε τομέα του δάσους.

Η χρήση των σφαιρικών ομάδων διευκολύνει την διαχείριση αντικειμένων καταλόγου που απαιτούν καθημερινή συντήρηση όπως οι λογαριασμοί χρηστών και υπολογιστών. Επειδή οι ομάδες με σφαιρική εμβέλεια δεν αναπαράγονται (replicated) έξω από το δικό τους τομέα, μπορούμε να κάνουμε αλλαγές σε μια ομάδα χωρίς να δημιουργούμε επιπλέον κίνηση στον καθολικό κατάλογο.

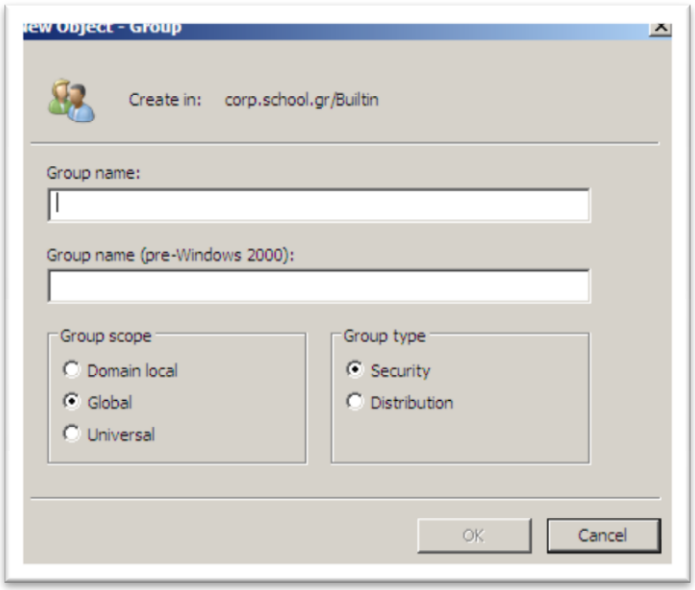
Καθολικές ομάδες τομέα: Τα μέλη της γενικής ομάδας μπορούν να ανήκουν και σε άλλες ομάδες οποιουδήποτε τομέα μέσα σε ένα δάσος και να έχουν δικαιώματα σε οποιοδήποτε τομέα του δάσους.

Η χρήση των ομάδων σφαιρικής εφαρμογής έχουν ορατότητα σε όλους τους τομείς ενός δάσους. Θα πρέπει λοιπόν αρχικά να προσθέσουμε τους λογαριασμούς σε σφαιρικές ομάδες και στη συνέχεια τις σφαιρικές ομάδες στις καθολικές. Με αυτόν τον τρόπο οποιαδήποτε αλλαγή γίνει σε σφαιρική ομάδα δεν επηρεάζει την καθολική.

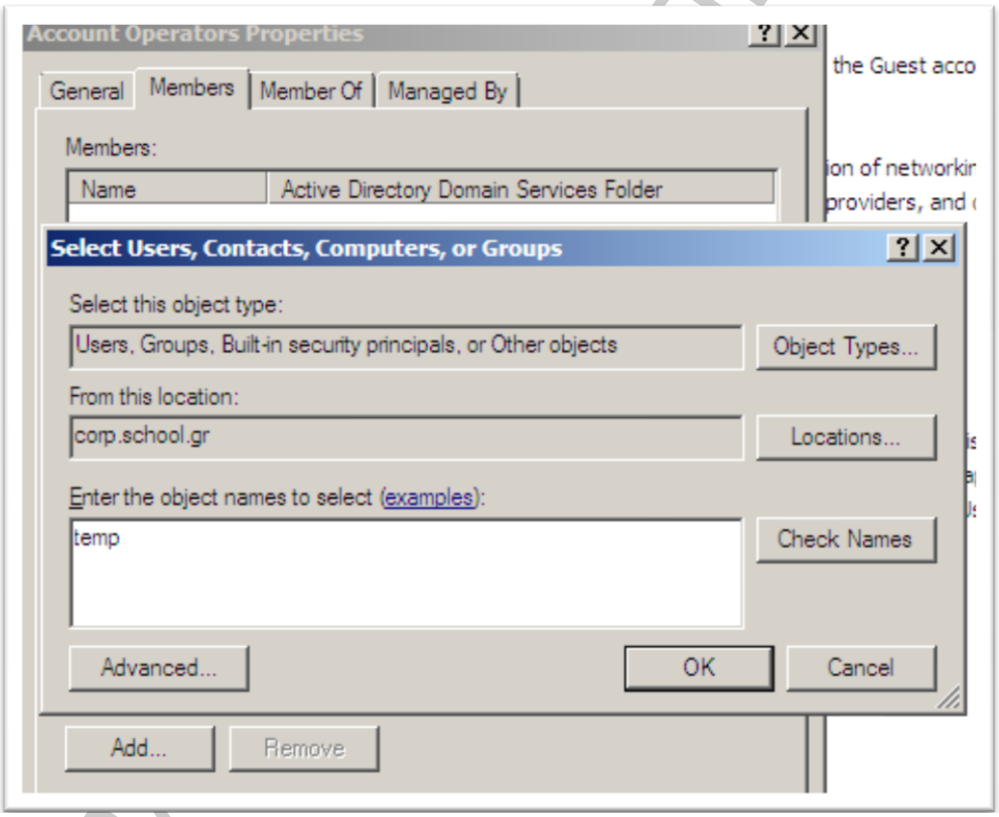
Η οποιαδήποτε αλλαγή της ομάδας επηρεάζει όλο το δίκτυο γι αυτό το λόγο δεν θα πρέπει να γίνεται συχνά.

Γενικά θα πρέπει να προσέχουμε με την χρήση των ομάδων. Θα πρέπει να προσέχουμε την αρχή της κληρονομικότητας, το φαινόμενο φώλιασμα (nest), και να δηλώνουμε πάντα τη σωστή πρωταρχική ομάδα σε έναν χρήστη.

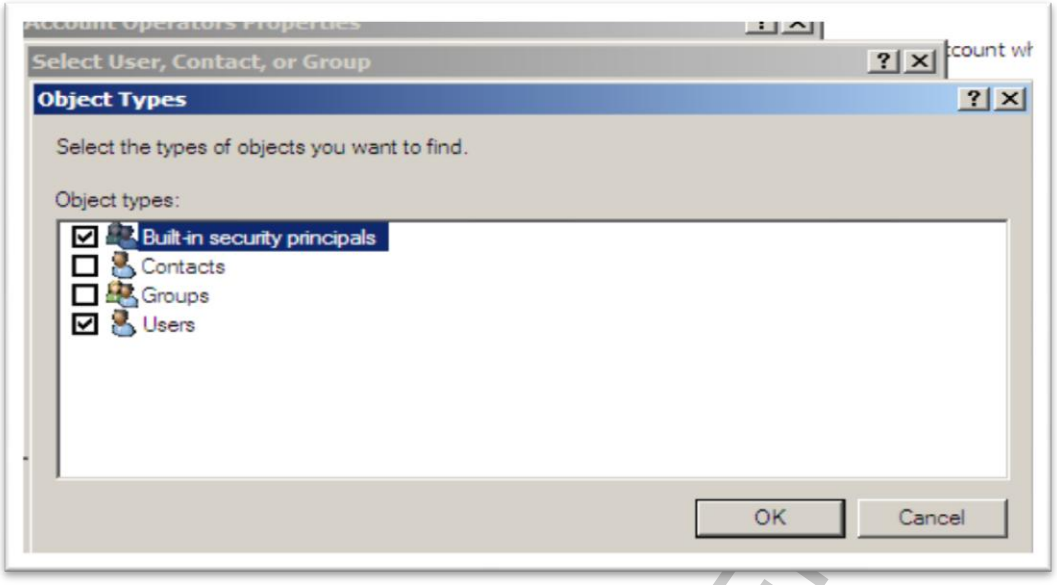
Για την δημιουργία μιας νέας ομάδας θα πρέπει να είμαστε μέλη των ομάδων Account Operators, Domains Admins, Enterprise Admins, ή κάποιας ομάδας που την έχουμε ορίσει ισοδύναμη με τις παραπάνω. Στην εικόνα 2.11.1 βλέπουμε πως δημιουργούμε μια ομάδα με το παραθυρικό περιβάλλον. Δηλώνουμε το όνομα της ομάδας, την εμβέλειά της και τον τύπο της. Στην εικόνα 2.11.2 βλέπουμε πως προσθέτουμε μέλη σε μια ομάδα. Στην εικόνα 2.11.3 βλέπουμε πως μπορούμε να μετατρέψουμε τον τύπο μιας ομάδας. Τέλος στην εικόνα 2.11.4 βλέπουμε πως μπορούμε να αλλάξουμε το πεδίο (εμβέλεια) μιας ομάδας.



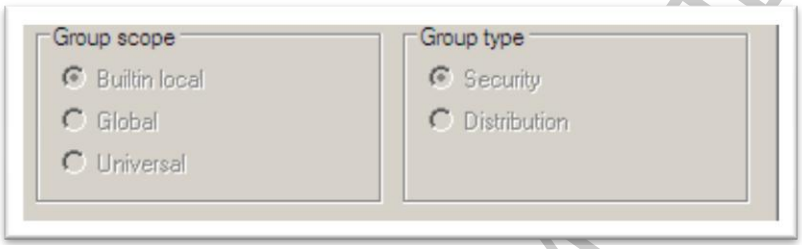
Εικόνα 2.11.1: Δημιουργία Ομάδας



Εικόνα 2.11.2: Προσθήκη μελών σε ομάδα



Εικόνα 2.11.3: Μετατροπή τύπου ομάδας



Εικόνα 2.11.4: Πεδίο ομάδας

Οι παραπάνω διαδικασίες γίνονται και σε γραμμή εντολών. Η εντολή *dsadd group <GroupDN> -samid<SAMName> -secgrp {yes|no} -scope {l|g|u}* δημιουργεί μια ομάδα. Για να προσθέσουμε μέλη σε μια ομάδα πληκτρολογούμε *dsmod group <GroupDN> -addmbr <MemberDN>* ενώ για να μετατρέψουμε ένα τύπο ομάδας πληκτρολογούμε *dsmod group <GroupDN> -secgrp {yes|no}.* Για να αλλάξουμε το πεδίο μιας ομάδας πληκτρολογούμε *dsmod group <GroupDN> -scope {L|G|U}* και για να τη διαγράψουμε *dsrm <GroupDN>.* Προσοχή όταν διαγράφουμε αντικείμενα στον ενεργό κατάλογο γιατί η διαγραφή τους είναι μόνιμη. Τέλος αν θέλουμε να κάνουμε εύρεση μίας ομάδας πληκτρολογούμε *dsget user <UserDN> -memberof.*

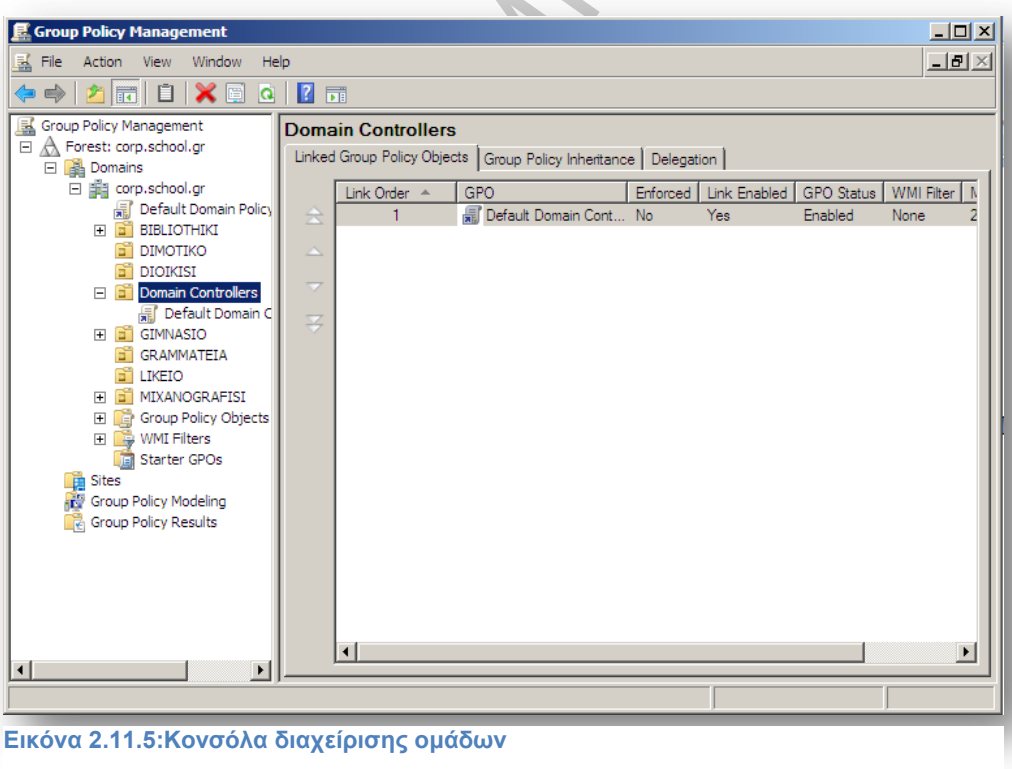
Στον πίνακα 2.11.1 βλέπουμε τις παραμέτρους κάθε εντολής.

Παράμετροι	**Περιγραφή**
<GroupDN>	Καθορίζει το αποκλειστικό όνομα του αντικειμένου της ομάδας που θα προστεθεί.
-samid	Τοποθετεί την τιμή <SAMName>.
<SAMName>	Καθορίζει το Security Accounts Manager (SAM) όνομα σαν μοναδικό (για παράδειγμα Operators).
-secgrp	Ορίζει την τιμή για τον τύπο της ομάδας.
{yes|no}	Καθορίζει αν η ομάδα που θέλουμε να προσθέσουμε είναι μια ομάδα ασφαλείας (yes) ή μια ομάδα διανομής (no).
-scope	Ορίζει την τιμή για το πεδίο εφαρμογής της ομάδας.
{l|g|u}	Καθορίζει αν το πεδίο εφαρμογής της ομάδας που θέλουμε να προσθέσουμε είναι τομέας local (l), global (g), είτε universal (u)

-addmbr	Θέτει την τιμή <MemberDN>.
<MemberDN>	Καθορίζει το αποκλειστικό όνομα του αντικειμένου που θέλουμε να προσθέσουμε στην ομάδα.
-secgrp	Ορίζει την τιμή του τύπου της ομάδας.
{yes|no}	Καθορίζει το αν ο τύπος της ομάδας είναι για την ομάδα ασφαλείας (yes) ή ομάδας διανομής (no).
{L|G|U}	Ορίζει ότι το πεδίο εφαρμογής της ομάδας έχει οριστεί σε local (L), global (G) ή universal (U). Αν το λειτουργικό επίπεδο του τομέα είναι σε μεικτό Windows δεν υποστηρίζεται. Επίσης, δεν είναι δυνατόν να μετατραπεί ένα τομέας local group σε global group ή το αντίστροφο.
-memberof	Καθορίζει την συμμετοχή στην ομάδα.
<UserDN>	Καθορίζει το αποκλειστικό όνομα του αντικειμένου χρήστη για τον οποίο θέλουμε να εμφανίσετε η συμμετοχή στην ομάδα.

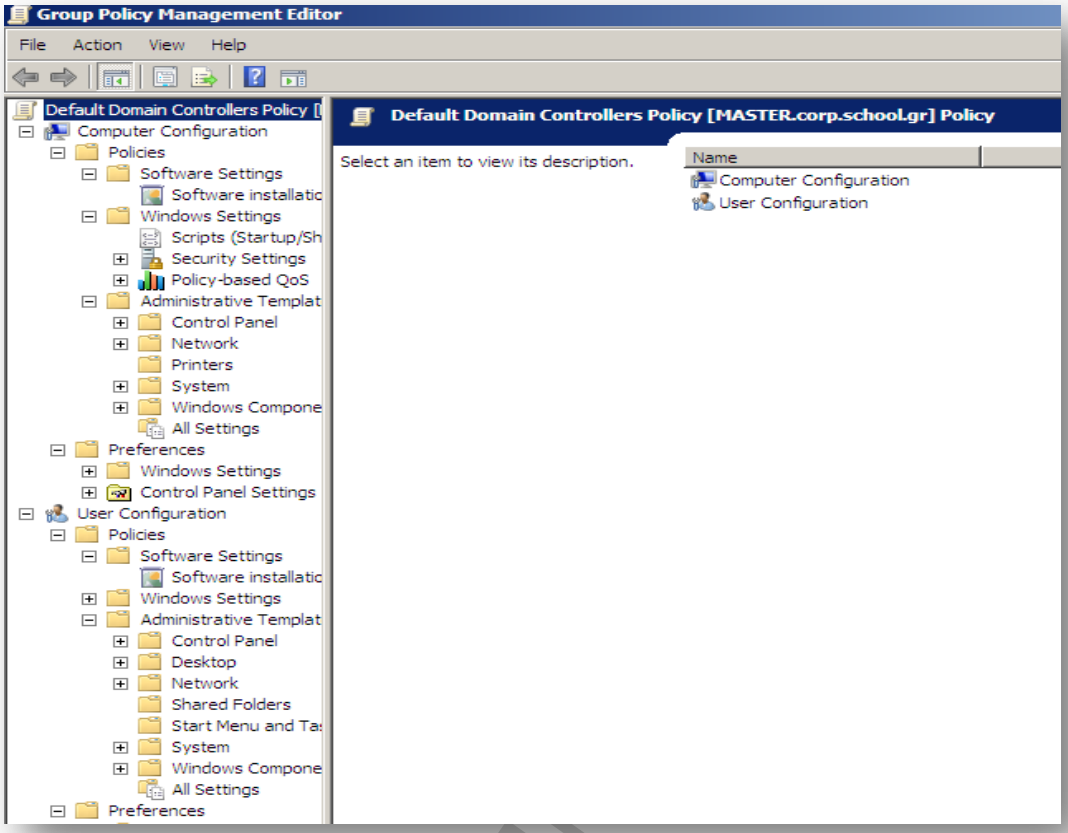
Πίνακας 2.11.1:Παράμετροι εντολών ομάδων

Τέλος το πιο σημαντικό ίσως κομμάτι του Ενεργού Καταλόγου είναι η ανάθεση δικαιωμάτων σε μια ομάδα. Θα πρέπει αρχικά να έχει εγκατασταθεί το Group Policy Management (GPO). Για να δούμε την κονσόλα θα πρέπει να πληκτρολογήσουμε στο Start, Run την εντολή gpmc.msc ή να πάμε στο Administrative tools. Το παράθυρο που ανοίγει είναι η κονσόλα του GPO. Κάνουμε δεξί κλίκ στο Default Domain Controllers Policy και επιλέγουμε edit (επεξεργασία). Θα παρατηρήσουμε ότι εμφανίζονται όλες οι οργανωτικές μονάδα (OUs) στις οποίες στη συνέχεια θα εφαρμόσουμε πολιτικές είτε για όλη την οργανωτική μονάδα είτε για ομάδες που ανήκουν σε αυτές.



Εικόνα 2.11.5:Κονσόλα διαχείρισης ομάδων

Για να δημιουργήσουμε πολιτικές αρκεί να κάνουμε δεξί κλικ στην επιλογή Domain Controllers και να επιλέξουμε New. Ανοίγει ο διορθωτής πολιτικών.



Εικόνα 2.11.5: Διορθωτής Πολιτικών

Σε αυτό το σημείο μπορούμε να ορίσουμε πολιτικές για τους υπολογιστές και για τους χρήστες. Πολιτικές σε επίπεδο λογισμικού, σε επίπεδο λειτουργικού, σε διαχειριστικό επίπεδο και στις προτιμήσεις των windows.

Για τις πολιτικές των ομάδων θα μιλήσουμε αναλυτικότερα στο κεφάλαιο που θα οργανώνουμε πλέον το δίκτυο μας. Πολιτικές όπως το ποιος θα έχει πρόσβαση σε ποιους πόρους του δικτύου. Ποιος θα μπορεί να εκτυπώνει, ποιος θα μπορεί να διαχειρίζεται την βάση δεδομένων της βιβλιοθήκης και ποιος θα μπορεί να δει απλά (read only) τα δεδομένα, τι θα βλέπει ο κάθε χρήστης στην οθόνη του και ότι χρειάζεται το ένα δίκτυο για να είναι ασφαλές και γρήγορο. (Help Microsoft Windows Server 2008)

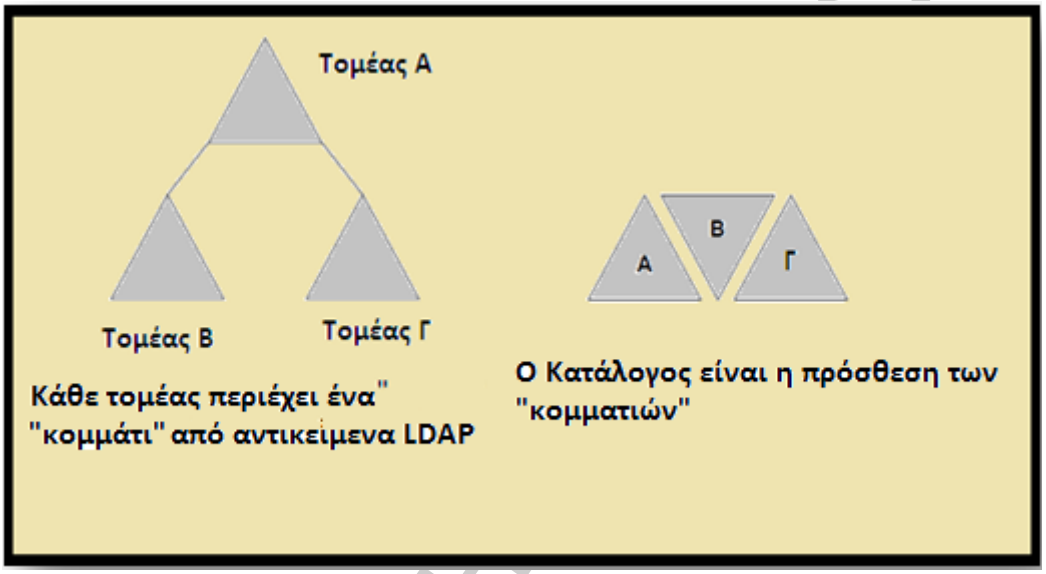
2.12 Περιβάλλοντα ονομασίας, Διαχωρισμός, Αναπαραγωγή (Naming Contexts, Partitioning, Replication)

Ο Ενεργός Κατάλογος περιέχει όλες τις πληροφορίες δικτύων για ένα δάσος. Κάθε τομέας έχει ξεχωριστή περιοχή (partition) του καταλόγου και έχει και άλλη ονομασία (naming contexts). Αυτή η περιοχή (partitioning) εξασφαλίζει ένα δομημένο κατάλογο. Αν και ένας τομέας περιέχει πολλά αντικείμενα, η προσθήκη του σε ένα δάσος έχει ελάχιστη επίδραση στους άλλους τομείς που ανήκουν στο ίδιο δάσος.

Ο Ενεργός Κατάλογος χωρίζεται σε τρεις ονομασίες πλαισίων: Domain Naming Context, Configuration Naming Context, and Schema Naming Context. Ένας τομέας έχει τη δική του περιβάλλοντα ονομασία (naming context). Το πεδίο αυτού εντοπίζεται σε όλα τα μέλη του τομέα. Ας δούμε τα άλλα δυο:

1. Η περιβάλλον ονομασία σχήματος (Schema Naming Context), που περιέχει τους ορισμούς των δεδομένων των αντικειμένων, είναι ένα χωριστό όνομα πλαισίου και αναπαράγεται σε κάθε ελεγκτή τομέα στο δάσος.
2. Η διαμόρφωση περιβάλλοντος ονομασίας (Configuration Naming Context) είναι επίσης ένα χωριστό όνομα πλαισίου και αναπαράγεται σε κάθε ελεγκτή τομέα στο δάσος. Η διαμόρφωση έχει δομικές πληροφορίες, όπως η θέση των τομέων η θέση των ελεγκτών τομέων, των υποδικτύων, των σφαιρικών κεντρικών υπολογιστών καταλόγων, και ενός πλήρους καταλόγου όλων των τομέων στο δάσος. Η διαμόρφωση έχει επίσης τις πληροφορίες για κάθε τομέα που δεν είναι στο δάσος αλλά έχει μια σχέση εμπιστοσύνης με οποιαδήποτε τομέα του δάσους.

Κάθε όνομα πλαισίου πρέπει να είναι ορατό μέσα στο πεδίο του. Έτσι το Domain Naming Context είναι ορατό σε όλους τους ελεγκτές τομείς σε έναν τομέα ενώ το Schema και το Configuration Context είναι ορατά σε κάθε ελεγκτή τομέα μέσα στο δάσος. (Dias, 2002)



Εικόνα 2.12:Naming Contexts, Partitioning, *and Replication*

2.13 Εμπιστοσύνη με τον Kerberos

Η εμπιστοσύνη (trust) επιτρέπει τη δυνατότητα της επικύρωσης των αρχών ασφαλείας από τομέα σε τομέα. Χρησιμοποιώντας τον Κέρβερο και τον Ενεργό Κατάλογο ισχύει η αρχή της μεταβατικότητας και η αμφίδρομη επικοινωνία μεταξύ των τομέων.

Αν ο τομέας Α έχει σχέση εμπιστοσύνης με τον τομέας Β και

Αν ο Τομέας Β έχει σχέση εμπιστοσύνης με τον τομέας Γ

Τότε ο τομέας Α έχει σχέση εμπιστοσύνης και με τον τομέας Γ.

Οι σχέσεις εμπιστοσύνης απλοποιούν τη διαχείριση και διευκολύνουν τη διανομή των πληροφοριών μέσα σε ένα δάσος. (Dias, 2002)

2.14 Αντιπροσωπεία της Αρχής (Delegation of Authority)

Το Delegation of Authority του Ενεργού Καταλόγου μείωσε τον απαιτούμενο αριθμό των τομέων. Είναι δυνατή πλέον η μεταβίβαση διαχείρισης δικαιωμάτων στις Οργανωτικές Μονάδες (OU). Πολλαπλοί τομείς μπορούν να αντικατασταθούν από ένα χρησιμοποιώντας όμως πολλές οργανωτικές μονάδες. (Dias, 2002)

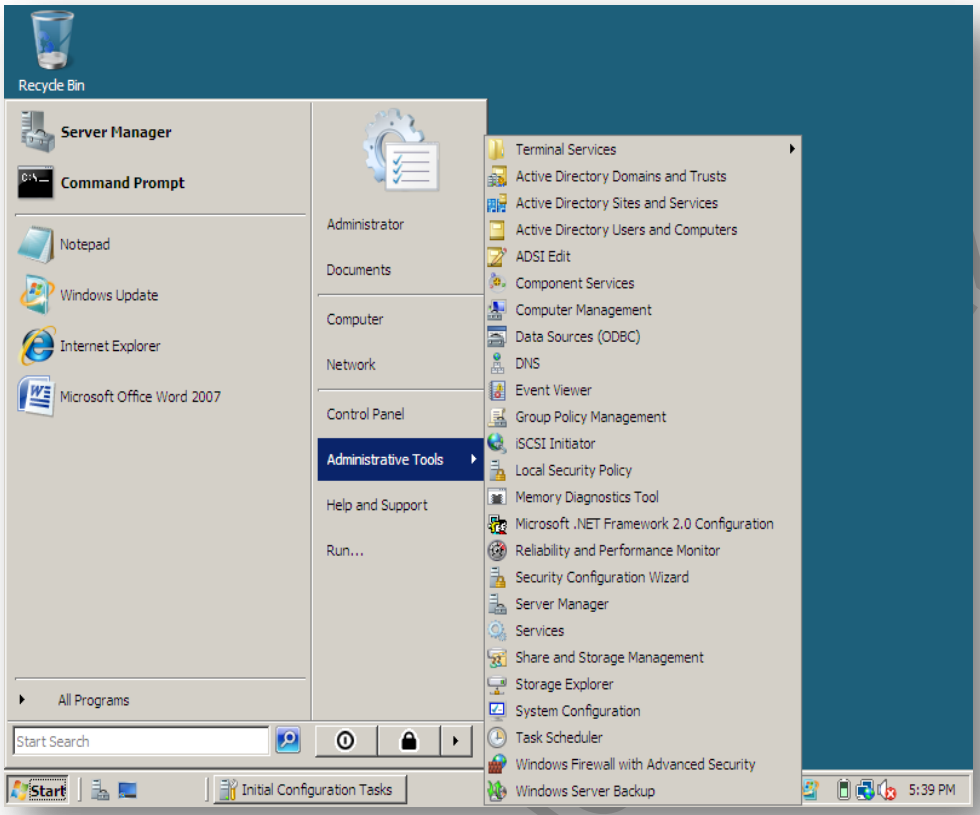
Ο διαχειριστής του τομέα μπορεί να δώσει δικαιώματα πλήρη ελέγχου σε ομάδες ασφαλείας (security group) των οργανωτικών μονάδων. Γενικότερα μπορούν όχι μόνο να δοθούν δικαιώματα και σε άλλους χρήστες αλλά μπορούν να δοθούν συγκεκριμένα δικαιώματα. Για παράδειγμα κάποιος να μπορεί να κάνει μόνο reset password (επαναφορά κωδικού).

2.15 Active Directory και Windows 2008 Server

Στα Windows Server 2008, η Microsoft τροποποίησε την υπηρεσία του Ενεργού Καταλόγου. Επαναπροσδιόρισε τη λειτουργικότητα των καταλόγων και δημιούργησε μια σειρά από υπηρεσίες (services) όπως:

- Active Directory Certificate Services (AD CS): Παρέχουν λειτουργίες απαραίτητες για την έκδοση και ανάκληση ψηφιακών πιστοποιητικών σε χρήστες, υπολογιστές και διακομιστές.
- Active Directory Domain Services (AD DS): Παρέχουν τις βασικές υπηρεσίες καταλόγου που απαιτούνται για τον ορισμό ενός τομέα, καθώς και την αποθήκη δεδομένων όπου αποθηκεύονται πληροφορίες για αντικείμενα του δικτύου οι οποίες είναι διαθέσιμες στους χρήστες.
- Active Directory Federation Services (AD FS): Αποτελούν συμπλήρωμα των λειτουργιών διαχείρισης της πρόσβασης και της πιστοποίησης ταυτότητας των υπηρεσιών AD DS, επεκτείνοντάς τις στον Παγκόσμιο Ιστό (World Wide Web)
- Active Directory Lightweight Directory Services (AD LDS): Παρέχουν μια αποθήκη δεδομένων για εφαρμογές που χρησιμοποιούν υπηρεσίες καταλόγου και οι οποίες δεν χρειάζονται τις υπηρεσίες AD DS ούτε είναι απαραίτητο να διατίθενται σε ελεγκτές τομέων.
- Active Directory Rights Management Services (AD RMS): Προσφέρουν ένα επίπεδο προστασίας στις πληροφορίες μιας επιχείρησης, το οποίο μπορεί να εκτείνεται πέρα από την ίδια την επιχείρηση προκειμένου να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, ιστοσελίδες του ενδοδικτύου και άλλα. (http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx).

  Στην Εικόνα 2:15 βλέπουμε τα διαχειριστικά εργαλεία.



Εικόνα 2.15: Administrative Tools

ΚΕΦΑΛΑΙΟ 3 –Ανάλυση αναγκών & Συλλογή Πληροφοριών

3.1 Φάση Ανάλυσης Αναγκών

Για την δημιουργία ενός δικτύου είναι απαραίτητη η καταγραφή – ανάλυση αναγκών του. Ο κάθε οργανισμός έχει διαφορετικές ανάγκες από ένα πληροφοριακό σύστημα. Η ανάλυση μας βοηθάει στα εξής:

- Να διαλέξουμε σωστά τις τεχνολογίες και τις υπηρεσίες που θα χρησιμοποιήσουμε.
- Να σχεδιάσουμε ένα δίκτυο το οποίο να είναι προσαρμοσμένο στις ανάγκες των χρηστών και του οργανισμού.
- Να καταλάβουμε καλύτερα ποια θα είναι η μελλοντική συμπεριφορά του δικτύου που σχεδιάζουμε.

Σε αυτή τη φάση θα πρέπει να γίνει κατανοητό το τι επιθυμεί ο πελάτης. Αναλαμβάνοντας το σχεδιασμό ενός καινούργιου δικτύου ή τη βελτίωση ενός υπάρχοντος, υπάρχει ανάγκη στενής συνεργασίας με τον πελάτη για τον καθορισμό των τεχνικών και επιχειρησιακών στόχων του δικτύου. Ένα από τα βασικά ερωτήματα του σχεδιασμού είναι η σχέση απόδοσης δικτύου – κόστος δικτύου. Στη συνέχεια και με την βοήθεια των χρηστών, του διαχειριστή δικτύου και της διοίκησης καθορίζονται οι ανάγκες (Εφαρμογές που θα πρέπει να λειτουργούν). Οι χρήστες σε ένα οργανισμό ποικίλουν τόσο σε σχέση με τις γνώσεις ως προς του ηλεκτρονικούς υπολογιστές όσο και ως προς τις εφαρμογές που λειτουργούν.

Καταγράφουμε τους ρόλους του δικτύου. Έτσι για μια εμπορική επιχείρηση μιλάμε για παραγωγή προϊόντων ή υπηρεσιών ενώ για ένα σχολικό δίκτυο μιλάμε κυρίως για εκπαιδευτικούς σκοπούς. Με την καταγραφή εντοπίζουμε τα κρίσιμα δεδομένα για τον οργανισμό καθώς και τις κρίσιμες λειτουργίες του.

Πρέπει λοιπόν να απαντηθούν οι παρακάτω ερωτήσεις:

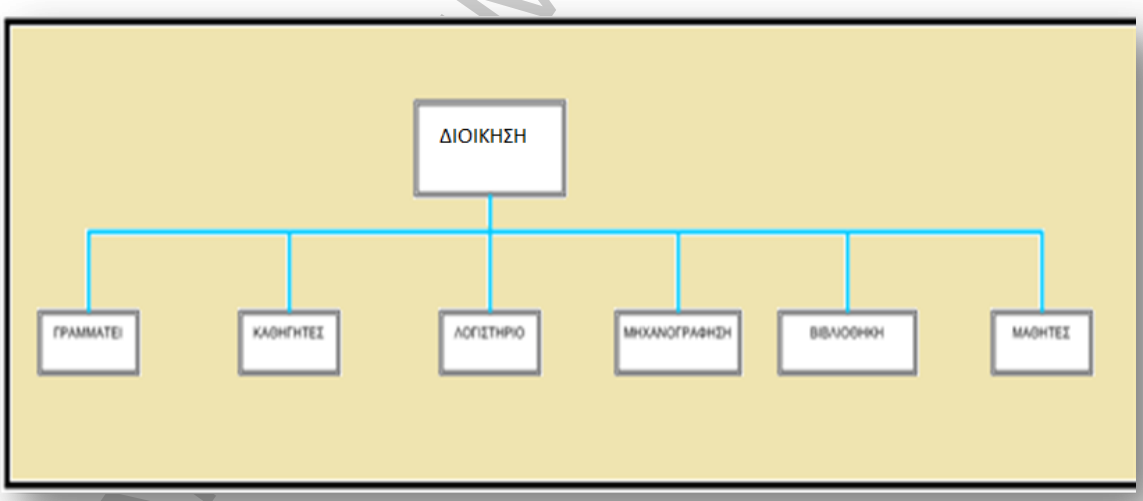
- Ποιες λειτουργίες της επιχείρησης βασίζονται στο δίκτυο; Ποια η φύση των εργασιών και κατά πόσο η επιχείρηση εξαρτάται από το δίκτυο;
- Ποιες οι επιχειρησιακές επιπτώσεις σε περίπτωση διακοπής λειτουργίας του δικτύου; Ποιο το κόστος του οργανισμού ανά ώρα σε περίπτωση διακοπής λειτουργίας του δικτύου;
- Ποια είναι τα δεδομένα των οποίων η απώλεια (καταστροφή ή κλοπή) μπορεί να προκαλέσει μεγάλες απώλειες εσόδων για την επιχείρηση;
- Χρησιμοποιούν οι πελάτες το δίκτυο και αν ναι ποιες οι ανάγκες τους; Οι ανάγκες των πελατών αναλύονται βάσει των κριτηρίων ποιότητας (ταχύτητα, καθυστέρηση, διαθεσιμότητα, αξιοπιστία, χωρητικότητα) καθώς και των κριτηρίων κόστους και ασφάλειας.
- Ποιες είναι οι εργασίες ανά χρήστη στο δίκτυο;

Για να απαντηθούν όλες αυτές οι ερωτήσεις ερχόμαστε σε επαφή με τη διοίκηση, τον διαχειριστή του δικτύου αλλά και χρήστες οι οποίοι απασχολούνται σε σημαντικές θέσεις.

3.2 Συλλογή στοιχείων

Αρχικά σε ένα δίκτυο γίνεται σαφής προσδιορισμός των τμημάτων που το απαρτίζουν. Σε ένα σχολικό δίκτυο υπάρχουν τα εξής τμήματα:

- Εργαστήρια
- Τάξεις
- Διοίκηση
- Οικονομικό τμήμα
- Γραφεία καθηγητών
- Βιβλιοθήκη
- Γραμματεία
- Τμήμα μηχανογράφησης



Εικόνα 3.2.1: Οργανόγραμμα σχολείου

Ερχόμαστε αρχικά σε επαφή με τον διαχειριστή του συστήματος ο οποίος μας καθορίζει την σημασία του δικτύου. Τα τμήματα Τάξεις, Εργαστήρια, Γραφείο καθηγητών, Βιβλιοθήκη, Διοίκηση, είναι σημαντικό να λειτουργούν καθημερινά τις διδακτικές ώρες χωρίς διακοπές και καθυστερήσεις για να μη χάνονται διδακτικές ώρες. Το Οικονομικό τμήμα, το τμήμα μηχανογράφησης και η Γραμματεία είναι τα πιο σημαντικά τμήματα των οποίων η λειτουργία δεν πρέπει να διακοπεί. Το οικονομικό τμήμα εξαρτάται άμεσα από το δίκτυο μιας και θα πρέπει να έχει πάντα πρόσβαση και στο διαδίκτυο (για επικοινωνία με ΙΚΑ…) αλλά και στη λογιστική βάση δεδομένων. Η γραμματεία θα πρέπει να έχει πάντα πρόσβαση στην βάση δεδομένων των

μαθητών. Το τμήμα μηχανογράφησης θα πρέπει να ελέγχει πάντα τη σωστή λειτουργία του συστήματος.

Σε περίπτωση διακοπής λειτουργίας δεν υπάρχουν οικονομικές συνέπειες για ένα σχολικό δίκτυο. Το κόστος μετριέται σε χαμένες διδακτικές ώρες ή διακοπή λειτουργίας του ταμείου. Η διακοπή λειτουργίας για μία μέρα είναι ανεκτή από όλα τα τμήματα. Μετά αρχίζουν οι δυσλειτουργίες. Άρα όσο αφορά τα βασικά στοιχεία ενός δικτύου (διακομιστές) θα πρέπει τόσο σε επίπεδο υλικού όσο και σε επίπεδο λογισμικού να μπορούν να ανακάμψουν από ένα πρόβλημα το πολύ μέσα σε μία μέρα. Όσο αφορά τα τερματικά καλό θα είναι να υπάρχουν δυο με τρεις υπολογιστές έτοιμοι προς χρήση (spare) σε περίπτωση που κάποιος χαλάσει.

Σε περίπτωση απώλειας δεδομένων αυτά που έχουν οικονομικές επιπτώσεις στο σχολείο είναι τα δεδομένα του Οικονομικού τμήματος, καθώς και τα δεδομένα του τμήματος μηχανογράφησης.

Πελάτες δεν χρησιμοποιούν το σχολικό δίκτυο.

Οι εργασίες ανά χρήστη στο δίκτυο ποικίλουν από το τμήμα στο οποίο ανήκει. Οι εργασίες των χρηστών καθορίζουν το κόστος του τερματικού σε επίπεδο υλικού αλλά και σε επίπεδο αδειών χρήσης λογισμικού. Ας ομαδοποιήσουμε όμως τους χρήστες βάση των αναγκών τους.

- Μαθητές. Βασική και ελεγχόμενη πρόσβαση στο διαδίκτυο και τοπικά στον υπολογιστή τους. Χρήση κειμενογράφου και προγραμμάτων πληροφορικής που διδάσκονται. Εκτύπωση εργασιών. Πρόσβαση μόνο για ανάγνωση στη βάση δεδομένων της βιβλιοθήκης. Οι δυνατότητες σε επίπεδο υλικού του υπολογιστή πρέπει να είναι κανονικές.
- Διοίκηση. Πλήρης πρόσβαση στο διαδίκτυο. Χρήση κειμενογράφου, εκτυπωτή, σαρωτή χρήση ηλεκτρονικού ταχυδρομείου. Τα δεδομένα είναι σημαντικά γι αυτό και η φύλαξή τους πρέπει να γίνεται στον διακομιστή. Πρόσβαση μόνο για ανάγνωση στη βάση δεδομένων της βιβλιοθήκης. Οι δυνατότητες σε επίπεδο υλικού του υπολογιστή πρέπει να είναι προχωρημένες.
- Λογιστές. Ελεγχόμενη πρόσβαση στο διαδίκτυο. Πλήρη πρόσβαση στη οικονομική βάση δεδομένων. Χρήση κειμενογράφου, εκτυπωτή και σαρωτή. χρήση ηλεκτρονικού ταχυδρομείου. Τα δεδομένα είναι σημαντικά γι αυτό και η φύλαξή τους πρέπει να γίνεται στον διακομιστή. Πρόσβαση μόνο για ανάγνωση στη βάση δεδομένων της βιβλιοθήκης. Οι δυνατότητες σε επίπεδο υλικού του υπολογιστή πρέπει να είναι προχωρημένες.
- Καθηγητές. Πλήρη πρόσβαση στο διαδίκτυο, χρήση κειμενογράφου, εκτυπωτή, σαρωτή. Χρήση ηλεκτρονικού ταχυδρομείου. Αποθήκευση των δεδομένων στον διακομιστή. Ο λογαριασμός τους να έχει μεταφερσιμότητα (roaming). Οι δυνατότητες σε επίπεδο υλικού του υπολογιστή πρέπει να είναι κανονικές.
- Γραμματεία. Πλήρη πρόσβαση στο διαδίκτυο, χρήση κειμενογράφου, εκτυπωτή, σαρωτή. Χρήση ηλεκτρονικού ταχυδρομείου. Αποθήκευση των δεδομένων στον διακομιστή. Οι δυνατότητες σε επίπεδο υλικού του υπολογιστή πρέπει να είναι προχωρημένες.
- Διαχειριστές δικτύου. Πλήρη πρόσβαση στο δίκτυο και στο διαδίκτυο. Χρήση προγραμμάτων παρακολούθησης δικτύου χρήση κειμενογράφου σαρωτή, εκτυπωτή. Αποθήκευση δεδομένων στον διακομιστή. Οι δυνατότητες σε επίπεδο υλικού του υπολογιστή πρέπει να είναι προχωρημένες.

Στη συνέχεια και μετά από συζητήσεις τόσο με τους χρήστες αλλά κυρίως με τον διαχειριστή του δικτύου συμπληρώνουμε τους παρακάτω πίνακες οι οποίοι προσδιορίζουν ανά τμήμα τις ανάγκες σε υλικό (υπολογιστές – εκτυπωτές …) αλλά και τις ανάγκες σε λογισμικό. Κάνουμε τη παραδοχή σε αυτό το σημείο ότι θα χρησιμοποιήσουμε windows 7 στους υπολογιστές ενώ ο διακομιστής θα έχει windows 2008 server edition και σε όλα τα τμήματα υπάρχει από ένας δικτυακός εκτυπωτής.

ΕΡΓΑΣΤΗΡΙΑ	
ΥΛΙΚΟ Η/Υ	Pentium 4 80 GB HDD 2 GB μνήμη
ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Ναι

ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Όχι
ΕΦΑΡΜΟΓΕΣ	• Συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • WorldLingo • Internet Explorer • NetControl2
ΠΡΟΣΒΑΣΕΙΣ	• Τα έγγραφά μου • Internet (περιορισμένη)

Πίνακας 3.2.1: Απαιτήσεις εργαστηρίων

ΤΑΞΕΙΣ	
ΥΛΙΚΟ Η/Υ	Pentium 4 80 GB HDD 2 GB μνήμη
ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Όχι
ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Ναι
ΕΦΑΡΜΟΓΕΣ	• Πρόγραμμα συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • WorldLingo • Πρόγραμμα διαδραστικού • Internet Explorer • NetControl2
ΠΡΟΣΒΑΣΕΙΣ	• Τα έγγραφά μου • Internet (περιορισμένη)

Πίνακας 3.2.2: Απαιτήσεις Τάξεων

ΔΙΟΙΚΗΣΗ	
ΥΛΙΚΟ Η/Υ	Pentium 4 80 GB HDD 2 GB μνήμη

ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Ναι
ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Όχι
ΕΦΑΡΜΟΓΕΣ	• Πρόγραμμα συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • Sql • ERP • Internet Explorer • Ηλεκτρονικό ταχυδρομείο • Πρόγραμμα αντιγραφής CD-DVD
ΠΡΟΣΒΑΣΕΙΣ	• Τα έγγραφά μου • Οικονομική βάση δεδομένων • Internet

Πίνακας 3.2.3: Απαιτήσεις διοίκησης

ΟΙΚΟΝΟΜΙΚΟ ΤΜΗΜΑ	
ΥΛΙΚΟ Η/Υ	Pentium 4 80 GB HDD 2 GB μνήμη
ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Ναι
ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Όχι
ΕΦΑΡΜΟΓΕΣ	• Πρόγραμμα συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • Sql • ERP • Internet Explorer • Ηλεκτρονικό ταχυδρομείο • Πρόγραμμα αντιγραφής CD-DVD
ΠΡΟΣΒΑΣΕΙΣ	• Τα έγγραφά μου • Οικονομική βάση δεδομένων • Internet

Πίνακας 3.2.4: Απαιτήσεις Οικονομικού Τμήματος

ΓΡΑΦΕΙΟ ΚΑΘΗΓΗΤΩΝ	
ΥΛΙΚΟ Η/Υ	Pentium 4 80 GB HDD 2 GB μνήμη
ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Ναι
ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Όχι
ΕΦΑΡΜΟΓΕΣ	• Πρόγραμμα συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • Internet Explorer • Ηλεκτρονικό ταχυδρομείο • Πρόγραμμα αντιγραφής CD-DVD
ΠΡΟΣΒΑΣΕΙΣ	• Τα έγγραφά μου • Internet

Πίνακας 3.2.5: Απαιτήσεις γραφείου καθηγητών

ΒΙΒΛΙΟΘΗΚΗ	
ΥΛΙΚΟ Η/Υ	Pentium 4 250 GB HDD 3 GB μνήμη
ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Ναι
ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Όχι
ΕΦΑΡΜΟΓΕΣ	• Πρόγραμμα συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • Internet Explorer • Ηλεκτρονικό ταχυδρομείο • Sql • Πρόγραμμα αντιγραφής CD-DVD
ΠΡΟΣΒΑΣΕΙΣ	• Τα έγγραφά μου • Internet • Βάση δεδομένων βιβλιοθήκης

Πίνακας 3.2.6: Απαιτήσεις βιβλιοθήκης

ΓΡΑΜΜΑΤΕΙΑ	
ΥΛΙΚΟ Η/Υ	Pentium 4 80 GB HDD 2 GB μνήμη
ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Ναι
ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Όχι
ΕΦΑΡΜΟΓΕΣ	• Πρόγραμμα συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • Internet Explorer • Ηλεκτρονικό ταχυδρομείο • Πρόγραμμα αντιγραφής CD-DVD • Sql
ΠΡΟΣΒΑΣΕΙΣ	• Τα έγγραφά μου • Internet • Βάση δεδομένων μαθητών

Πίνακας 3.2.7: Απαιτήσεις γραμματείας

ΤΜΗΜΑ ΜΗΧΑΝΟΓΡΑΦΗΣΗΣ	
ΥΛΙΚΟ Η/Υ	Pentium 4 80 GB HDD 2 GB μνήμη
ΕΚΤΥΠΩΤΗΣ	Ναι
ΣΑΡΩΤΗΣ	Ναι
ΔΙΑΔΡΑΣΤΙΚΟΣ ΠΙΝΑΚΑΣ	Όχι
ΕΦΑΡΜΟΓΕΣ	• Πρόγραμμα συμπίεσης –αποσυμπίεσης • Adobe reader • Flash player • Java • Κειμενογράφος • Πρόγραμμα εκτυπωτή • Internet Explorer • Ηλεκτρονικό ταχυδρομείο • Πρόγραμμα αντιγραφής CD-DVD • Sql • ERP • Πρόγραμμα απομακρυσμένης πρόσβασης

	• Προγράμματα ελέγχου δικτύου - εξυπηρετητών
ΠΡΟΣΒΑΣΕΙΣ	Πλήρη πρόσβαση παντού

Πίνακας 3.2.8: Απαιτήσεις μηχανογράφησης

Στη συνέχεια γίνεται καταγραφή αναγκών του διακομιστή. Ο διαχειριστής του δικτύου μας ενημερώνει για τις ανάγκες τους δηλαδή την χωρητικότητα και την προσβασιμότητα σε επίπεδο υλικού.

- Τα δεδομένα των χρηστών τα οποία και θα αποθηκεύονται στον διακομιστή είναι της τάξεως των 500GB ενώ αν υπολογίσουμε και τα προφίλ (profile) τους η χωρητικότητα αυξάνεται σημαντικά.
- Θα πρέπει να υπάρχει κεντρική διαχείριση των ηλεκτρονικών ταχυδρομείων των χρηστών, του ERP και SQL και των προσβάσεων τόσο στο ενδοδίκτυο (intranet) όσο και στο διαδίκτυο (internet).
- Θα πρέπει να υπάρχει καθημερινό backup του διακομιστή και θα πρέπει να είναι πάντα σε λειτουργία (on line) άρα είναι απαραίτητη η χρήση ups.
- Για μεγαλύτερη ασφάλεια και κυρίως συνεχή λειτουργία θα πρέπει να υπάρχει δεύτερος διακομιστής σε κάποια άλλη τοποθεσία του σχολείου όπου τα δεδομένα θα αντιγράφονται (replication) μεταξύ τους.
- Θα πρέπει η λειτουργία των χρηστών να μη διακόπτεται ακόμα και αν για κάποιο λόγο το δίκτυο σταματήσει να λειτουργεί (off line αρχεία, εκτός από τους μαθητές).
- Θα πρέπει όλοι οι λογαριασμοί εκτός των μαθητών να έχουν προφίλ περιαγωγής.

Η καταγραφή των παραπάνω αναγκών καθορίζει την επόμενη φάση η οποία είναι η φάση σχεδιασμού. Στο επόμενο κεφάλαιο θα σχεδιάσουμε το δίκτυο με στόχο να είναι πάντα διαθέσιμο (on line) και να είναι εύκολα επεκτάσιμο όποτε και αν χρειαστεί.

ΚΕΦΑΛΑΙΟ 4- Σχεδίαση υλικού

4.1 Φάση Σχεδίασης Υλικού

Η φάση σχεδίασης ξεκινάει από τον διακομιστή. Σε συνάρτηση πάντα με τον όγκο των δεδομένων, τον τύπο, την επεκτασιμότητα καθώς και την δυνατότητα για συνεχή λειτουργία γίνεται ο εξής σχεδιασμός. Σε ένα σχολικό δίκτυο όπου οι ανάγκες σε χωρητικότητα είναι τεράστιες, οι προσβασιμότητες και οι λειτουργίες των χρηστών ποικίλουν θα ήταν σκόπιμο να χωριστούν οι διακομιστές (servers). Έτσι προτείνονται τα εξής:

- Πρωτεύον ελεγκτής τομέας (active directory – profiles)
- Δευτερεύον ελεγκτής τομέας (Backup)
- Διακομιστής εφαρμογών(ERP, SQL …)
- Διακομιστής Exchange (mail server)
- Διακομιστής δεδομένων (data)
- ISA
- Backup Network Storage
- UPS

Σε φυσικό επίπεδο λοιπόν προτείνονται 5 φυσικοί διακομιστές και ένα εξωτερικό δικτυακό storage. Ο πρωτεύον ελεγκτής τομέας θα έχει τον Ενεργό Κατάλογο, τα προφίλ των χρηστών και θα έχει και τον ρόλο DHCP server για να μοιράζει στο δίκτυο IP διευθύνσεις. Ο ρόλος του DHCP server είναι σημαντικός σε ένα δίκτυο με πολλούς υπολογιστές μιας και δεν χρειάζεται να τοποθετήσουμε σε κάθε υπολογιστή ξεχωριστά την IP διεύθυνσή του. Επίσης διευκολύνει και το έργο της συντήρησης μιας και δεν χρειάζεται να θυμόμαστε ή να καταγράφουμε ποιος υπολογιστής έχει πια IP διεύθυνση.

Ο δευτερεύον ελεγκτής τομέας είναι κλώνος του πρωτεύον. Λέγοντας backup δεν εννοούμε τον διακομιστή backup που είχαμε σε ένα δίκτυο με Windows NT. Με την εισαγωγή

του Ενεργού Καταλόγου όλοι οι τομείς σε ένα δίκτυο έχουν την ίδια σημασία απλά διαχωρίζουμε τις εργασίες τους. Ανά τακτά χρονικά διαστήματα λοιπόν, (μπορούμε και να καθορίσουμε τον χρόνο), ότι υπάρχει στον πρωτεύον ελεγκτή τομέα αντιγράφεται και στον δευτερεύον. Τον ονομάζουμε δευτερεύον υπό την έννοια ότι αν για κάποιο λόγο τερματίσει την λειτουργία του ο πρωτεύον αναλαμβάνει αυτόματα αυτός να εξυπηρετεί το δίκτυο και μάλιστα χωρίς να διακοπεί η λειτουργία.

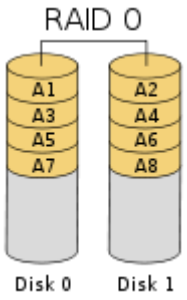
Ο Application Server ή διακομιστής εφαρμογών θα έχει όλες τις δικτυακές εφαρμογές. Ο mail server θα διαχειρίζεται το ηλεκτρονικό ταχυδρομείο των χρηστών. Τα δεδομένα των χρηστών θα φυλάγονται στον Data Server και τέλος ο ISA που θα είναι υπεύθυνος για τις προσβάσεις στο διαδίκτυο. Τέλος θα υπάρχει ένας δικτυακός χώρος αποθήκευσης (storage) σε ένα άλλο χώρο του σχολείου όπου καθημερινά θα γίνονται τα αντίγραφα ασφαλείας (backup). Αντίγραφα ασφαλείας θα γίνονται και σε κασέτες καθημερινά οι οποίες θα φυλάγονται σε θυρίδα.

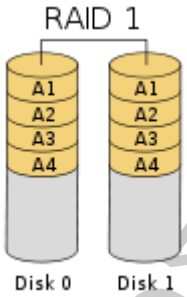
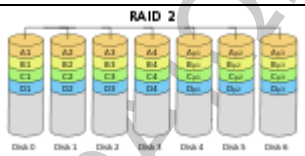
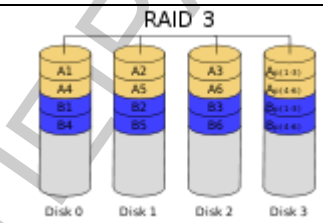
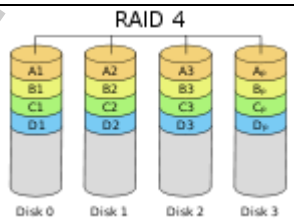
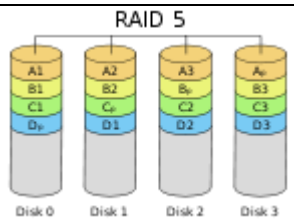
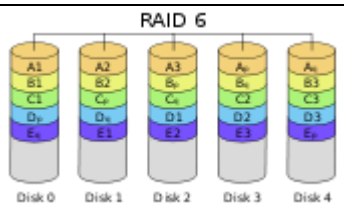
Η ασφάλεια λειτουργίας ενός δικτύου καθορίζεται σε δύο επίπεδα σε σχέση με το υλικό. Στο πρώτο επίπεδο θα πρέπει οι διακομιστές να λειτουργούν συνεχώς και σε δεύτερη φάση θα πρέπει να λειτουργούν ακόμα και σε φυσική καταστροφή του computer room.

Θα χρησιμοποιηθεί το ίδιο υλικό σε κάθε διακομιστή εκτός από τον ISA Server στον οποίο δεν μας ενδιαφέρει να έχουμε μεγάλη χωρητικότητα σε δίσκους. Πως όμως διασφαλίζουμε την συνεχή λειτουργία αυτών;

Η τεχνολογία hot swap (εν θερμώ αντικατάσταση) μας δίνει την δυνατότητα αντικατάστασης ανταλλακτικού χωρίς να κλείσει κάποιος διακομιστής. Η τεχνολογία εν θερμώ αντικατάσταση καλύπτει τις μνήμες, τις κάρτες δικτύου, τους σκληρούς δίσκους, τα τροφοδοτικά, και τον ελεγκτή raid. Για τον παραπάνω λόγο έχουμε σε κάθε διακομιστή δύο τροφοδοτικά, δύο κάρτες δικτύου, δύο raid controller, δύο δίσκους, και διπλές μνήμες. Αξίζει σε αυτό το σημείο να πούμε δυο λόγια για την τεχνολογία RAID (Redundant Array of Independent Disks). Είναι μια τεχνολογία η οποία αυξάνει την πιθανότητα συνεχούς λειτουργίας των δίσκων. Ενώνει πολλούς φυσικούς δίσκους σε έναν λογικό δίσκο. Όταν κάποιος φυσικός δίσκος χαλάσει αναλαμβάνουν οι υπόλοιποι μέχρι να γίνει αντικατάσταση του ανταλλακτικού. Με την αντικατάσταση γίνεται rebuild του νέου ανταλλακτικού στην αρχική μορφή. Το σύστημα λειτουργεί κανονικά κατά την διάρκεια όλης αυτής της διαδικασίας. Το μόνο που πιθανά να παρατηρηθεί είναι μια μικρή καθυστέρηση στο δίκτυο.

Υπάρχουν 7 βασικά επίπεδα RAID. RAID 0, 1, 2, 3, 4, 5 και 6 όπως φαίνεται και στον πίνακα 4.1.

Επίπεδο	Περιγραφή	Ελάχιστοι δίσκοι	Εικόνα
RAID 0	Block level Striping (Αποκλεισμός σε επίπεδο διαγράμμισης)	2	

RAID 1	Καθρέπτης (Mirroring)	2	
RAID 2	Επίπεδο διαγράμμισης bit με ειδικό κώδικα Haming	3	
RAID 3	Επίπεδο διαγράμμισης Byte με αφιερωμένη ισοτιμία	3	
RAID 4	Επίπεδο διαγράμμισης αποκλεισμού με ειδική ισοτιμία	3	
RAID 5	Επίπεδο διαγράμμισης αποκλεισμού με ισοτιμία διανομής	3	
RAID 6	Επίπεδο διαγράμμισης αποκλεισμού με διπλή ισοτιμία διανομής	4	

Πίνακας 4.1: Επίπεδα RAID

Στον ISA server επιλέγουμε 3 δίσκους σε RAID 5.

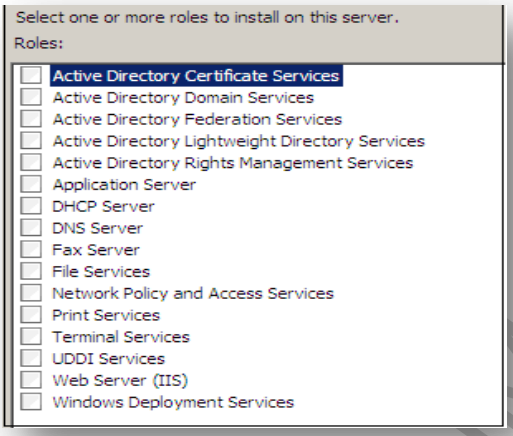
Στους υπόλοιπους διακομιστές λόγω της κρισιμότητας των δεδομένων και των μεγάλων χωρητικοτήτων επιλέγομε RAID 1. Στο RAID 1 υπάρχουν δύο φυσικοί δίσκοι από 1 Terabyte οι οποίοι ενώνονται σε έναν λογικό δίσκο. Ο κάθε δίσκος περιέχει ακριβώς τα ίδια αρχεία. Ο ένας είναι καθρέπτης του άλλου (mirror). Σε περίπτωση που χαλάσει ο ένας δίσκος εξακολουθεί να λειτουργεί ο διακομιστής με τον άλλον μέχρι να αντικατασταθεί το χαλασμένο ανταλλακτικό.

Οι κατασκευάστριες εταιρείες δίνουν σαν τεχνικό χαρακτηριστικό των διακομιστών τον χρόνο down time ο οποίος ορίζει τον χρόνο στον οποίο ο διακομιστής δεν θα λειτουργεί. Ο χρόνος αυτός ορίζεται με τη σημερινή τεχνολογία σε λιγότερο από μία ώρα τον χρόνο. (http://en.wikipedia.org/wiki/RAID)

4.2 Λειτουργία Primary και Backup Domain Controller

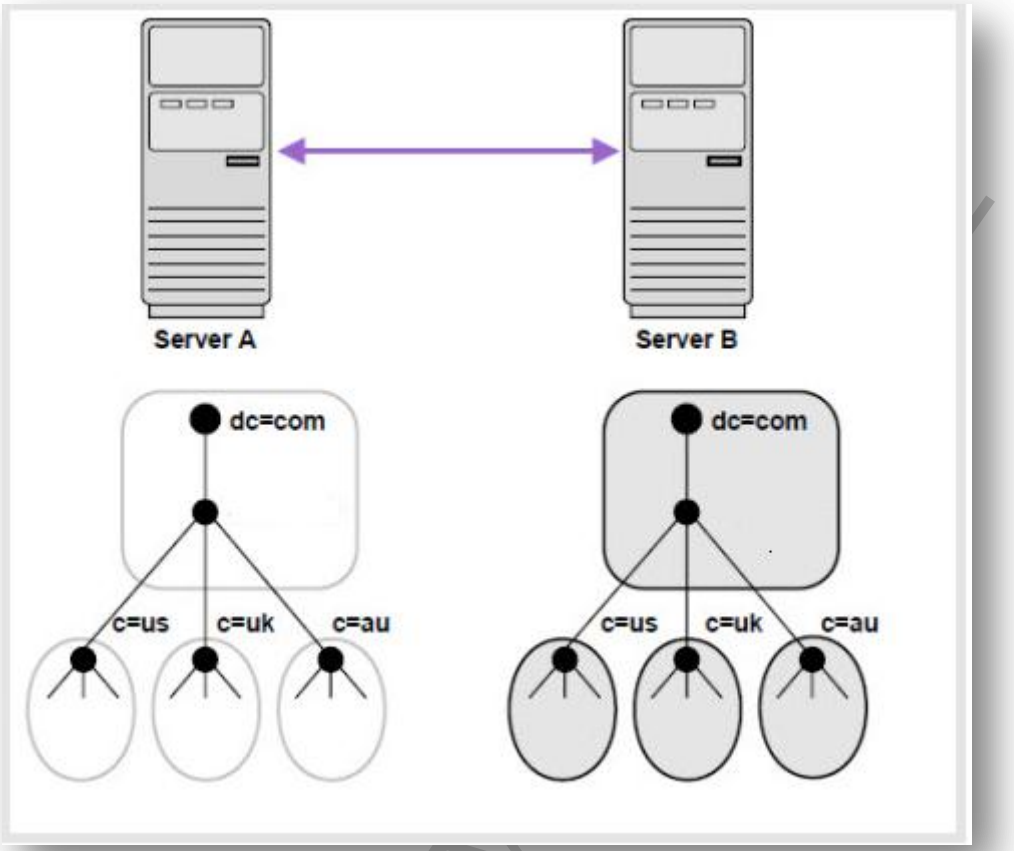
Ο πρωτεύον ελεγκτής τομέας έχει τον Ενεργό Κατάλογο και τα προφίλ των χρηστών. Ο δευτερεύον ελεγκτής τομέας είναι κλώνος του πρωτεύον. Ο ρόλος του δευτερεύον ελεγκτή τομέα είναι η διασφάλιση της συνεχής λειτουργίας του δικτύου σε περίπτωση που σταματήσει να λειτουργεί ο πρωτεύον. Σε ιδανικές συνθήκες προτείνεται να βρίσκεται σε διαφορετικό φυσικό χώρο διασφαλίζοντας την συνεχή λειτουργία του δικτύου ακόμα και σε φυσική καταστροφή του πρωτεύον. Ένα λειτουργικό σύστημα για διακομιστή καλείται να εκτελέσει πολλές λειτουργίες - ρόλους. Το λειτουργικό της Microsoft Windows 2008 Server έχει 16 διαφορετικούς ρόλους όπως φαίνεται και στην εικόνα 4.2.1. Ανάλογα με το τι λειτουργίες θα διαχειρίζεται ένας διακομιστής προσθέτουμε τους αντίστοιχους ρόλους. Θα πρέπει σε αυτό το σημείο να αναφέρουμε ότι κάθε διακομιστής σαν μηχανή μπορεί να διαχειριστεί όλους τους ρόλους ή για πολύ σημαντικούς ρόλους να έχουμε ξεχωριστές μηχανές – διακομιστές.

Σε ένα σχολικό δίκτυο στο οποίο η βάση δεδομένων του Ενεργού Καταλόγου είναι μεγάλη χρησιμοποιούμε ξεχωριστή μηχανή – διακομιστή. Έτσι PDC (Primary Domain Controller) έχει τον κατάλογο και τα προφίλ των χρηστών.



Εικόνα 4.2.1: Ρόλοι διακομιστή

Ο BDC (Backup Dpmain Controller) είναι ένας πανομοιότυπος διακομιστής με τον PDC (τόσο σε επίπεδο υλικού όσο και σε επίπεδο λογισμικού), ή αλλιώς κλώνος. Ο σκοπός του είναι να λειτουργήσει αυτόματα σε περίπτωση μη λειτουργίας του PDC. Χρησιμοποιείται η τεχνολογία File Replication Service (FRS) της Microsoft. Τα αρχεία από τον έναν διακομιστή αντιγράφονται στον άλλον. Γίνεται έλεγχος για τυχόν τροποποίηση αυτών βάση ημερομηνίας και ώρας ή για καινούργια και αντιγράφονται στον BDC. Στην εικόνα 4.2.2 βλέπουμε δύο διακομιστές όπου ένας είναι κλώνος του άλλου.

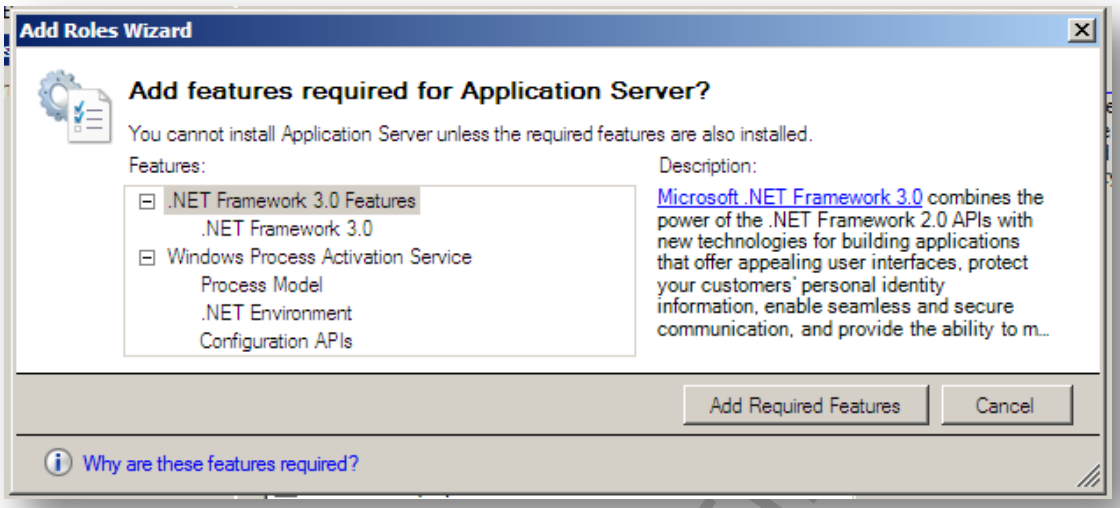


Εικόνα 4.2.2: Διακομιστές κλώνοι

4.3 Λειτουργία διακομιστή εφαρμογών

Ο διακομιστής εφαρμογών λόγω του μεγάλου όγκου δεδομένων χτίζεται σε ξεχωριστή μηχανή. Σε αυτόν γίνεται εγκατάσταση η βάση δεδομένων του λογιστηρίου, η βάση δεδομένων των μαθητών και η βάση δεδομένων της βιβλιοθήκης.

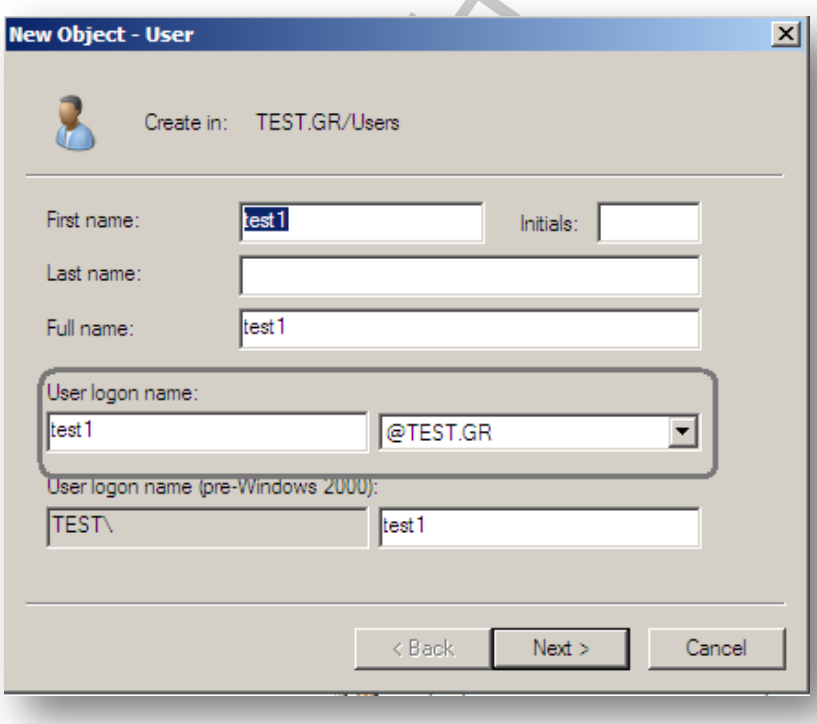
Για την λειτουργία του διακομιστή εφαρμογών θα πρέπει να εγκατασταθούν το .Net framework 3.0 και το Windows Process Activation Service όπως φαίνεται και στην εικόνα 4.3.



Εικόνα 4.3: Προσθήκη ρόλων

4.4 Διακομιστής Exchange

Ο Exchange server είναι ο διακομιστής που διαχειρίζεται το ηλεκτρονικό ταχυδρομείο όλων των μελών του σχολείου. Ο όγκος δεδομένων και εδώ είναι μεγάλος γι αυτό το λόγο χρησιμοποιούμε ξεχωριστή μηχανή. Ο Exchange server είναι πρόγραμμα το οποίο εγκαθιστάτε στα windows 2008 server. Το θετικό είναι ότι σαν προϊόν της ίδιας εταιρείας συνεργάζεται με τον Ενεργό Κατάλογο. Χρησιμοποιεί τη βάση δεδομένων των χρηστών και δημιουργεί τα αντίστοιχα ηλεκτρονικά ταχυδρομείο όπως φαίνεται και από την εικόνα 4.4.



Εικόνα 4.4: Ενεργός κατάλογος και ηλεκτρονικό ταχυδρομείο

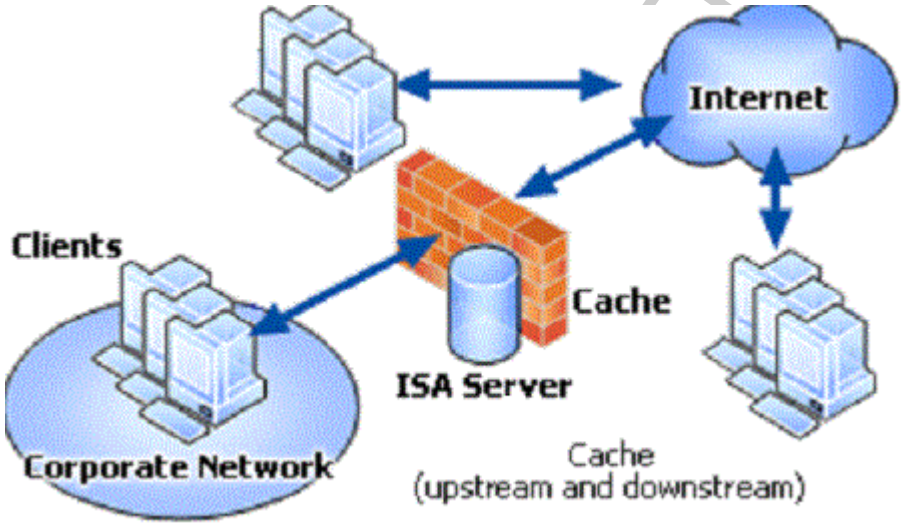
4.5 Διακομιστής Δεδομένων

Στον διακομιστή δεδομένων αποθηκεύονται τα δεδομένα των χρηστών (folder redirection). Σε αυτόν τον διακομιστή αυτό που μας ενδιαφέρει είναι η χωρητικότητα. Θα πρέπει να αποθηκεύονται όλα τα αρχεία των χρηστών γι αυτό και πρέπει να γίνει πολύ καλή μελέτη. Θα πρέπει να αποθηκεύονται όλα τα αρχεία με τις εξής επεκτάσεις: .doc, .xls, .ppt, και .pdf από όλα το προσωπικό (καθηγητές –γραμματείες –λογιστές). Μόνο οι γραμματείες μπορούν να αποθηκεύουν φωτογραφίες σε μορφή .jpeq. Οι μαθητές δεν αποθηκεύουν στον διακομιστή αλλά τοπικά στον υπολογιστή τους. Τα παραπάνω θα γίνουν με την βοήθεια των πολιτικών ομάδων που θα δούμε αναλυτικά παρακάτω.

Ανάλογα λοιπόν με τον όγκο των δεδομένων αντίστοιχες χωρητικότητες πρέπει να έχει και ο διακομιστής συν την μελλοντική αύξηση των δεδομένων.

4.6 ISA Server

Ο Microsoft ISA Server (Internet Security and Acceleration Server) παρέχει δύο βασικές υπηρεσίες. Ένα επιχειρησιακό τοίχο προστασίας (Enterprise firewall) και ένα διακομιστή μεσολάβησης (Proxy Server). Επίσης ο ISA είναι υπεύθυνος για τις αδειοδοτήσεις των απομακρυσμένων προσβάσεων. Στο δίκτυό μας μόνο ο διαχειριστής του δικτύου έχει απομακρυσμένη πρόσβαση. Στην εικόνα 4.6 βλέπουμε πως ο ISA μεσολαβεί για την ασφαλή πρόσβαση ενός ιδιωτικού δικτύου σε ένα δημόσιο.



Εικόνα 4.6: Λειτουργία ISA server

4.7 Φάση Σχεδίασης Υλικού Δικτύου

Οι υπολογιστές που θα χρησιμοποιηθούν στο δίκτυο επιλέγονται βάση των εργασιών των χρηστών. Το ιδανικό σενάριο είναι να έχουμε ίδιο υλικό σε όλους τους υπολογιστές του δικτύου. Αυτό διευκολύνει τη διαχείρισή και την συντήρησή τους. Οι υπολογιστές που απαρτίζουν ένα δίκτυο συνήθως δεν έχουν ομοιομορφία ούτε προς το υλικό ούτε προς το λογισμικό. Πιο συγκεκριμένα το λογισμικό είναι που διαμορφώνει τις υπολογιστικές δυνατότητες. Έτσι άλλη υπολογιστική δύναμη πρέπει να έχει ένας υπολογιστής που κάνει χρήση εφαρμογών γραφείου και άλλη υπολογιστική δύναμη ένας υπολογιστής που κάνει χρήση εφαρμογών εικόνων.

Σε ένα σχολικό δίκτυο υπάρχουν τμήματα όπως τα εργαστήρια τα οποία παρουσιάζουν ομοιομορφία ως προς το λογισμικό οπότε μπορούμε να τα ομαδοποιήσουμε και ως προς το υλικό. Ας δούμε λοιπόν για κάθε κατηγορία χρηστών ξεχωριστά.

- Μαθητές (Υπολογιστές εργαστηριών). Όχι ιδιαίτερα μεγάλες ανάγκες σε επεξεργαστική δύναμη. Υπάρχει ανάγκη όμως για μεγάλη χωρητικότητα σε δίσκους γιατί ο κάθε μαθητής

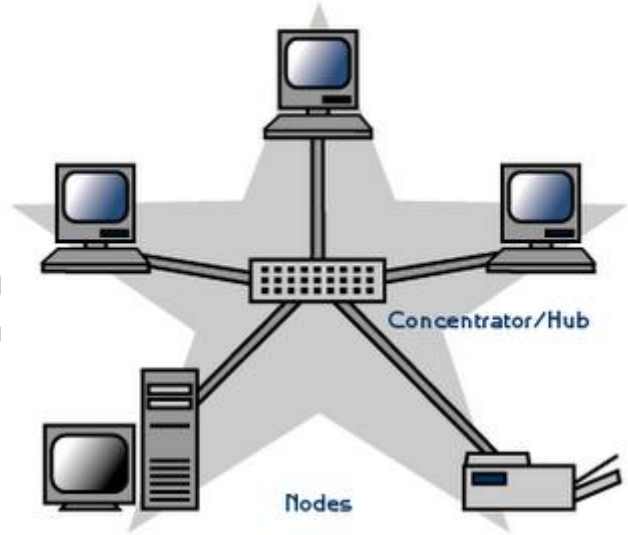
αποθηκεύει τοπικά και σε κάθε υπολογιστή κάθονται πολλοί μαθητές (όσοι και οι τάξεις του σχολείου)

- Καθηγητές (Υπολογιστές τάξεων και γραφείου καθηγητών). Οι υπολογιστές στις τάξεις και στο γραφείο των καθηγητών θα πρέπει να έχουν μεγάλη επεξεργαστική δύναμη και μνήμη γιατί θα πρέπει να έχουμε μεγάλη ταχύτητα. Η χωρητικότητα των δίσκων επίσης πρέπει να είναι μεγάλη γιατί τον ίδιο υπολογιστή χρησιμοποιούν πολλοί καθηγητές με προφίλ περιαγωγής (roaming profile) και δυνατότητα συγχρονισμού (synchronization). Δύο λειτουργίες που θα αναλύσουμε παρακάτω όταν θα φτιάχνουμε τις πολιτικές ομάδων.
- Η γραμματεία η οποία διαχειρίζεται κυρίως την βάση δεδομένων των μαθητών θα πρέπει έχει υψηλή επεξεργαστική δύναμη και μνήμη αλλά η χωρητικότητα του δίσκου δεν μας ενδιαφέρει να είναι μεγάλη γιατί αποθηκεύει στον File Server.
- Οι λογιστές θέλουν υπολογιστική δύναμη και μνήμη μιας και διαχειρίζονται την ERP βάση. Η χωρητικότητα του δίσκου δεν μας ενδιαφέρει να είναι μεγάλη γιατί αποθηκεύει στον File Server.
- Ο βιβλιοθηκάριος θέλει υπολογιστική δύναμη και μνήμη μιας και διαχειρίζονται την βάση δεδομένων. Η χωρητικότητα του δίσκου δεν μας ενδιαφέρει να είναι μεγάλη γιατί αποθηκεύει στον File Server
- Η διοίκηση θέλει ταχύτητα άρα επεξεργαστική δύναμη και μνήμη. Η χωρητικότητα του δίσκου δεν μας ενδιαφέρει να είναι μεγάλη γιατί αποθηκεύει στον File Server
- Η μηχανογράφηση θέλει ταχύτητα άρα επεξεργαστική δύναμη και μνήμη. Η χωρητικότητα του δίσκου δεν μας ενδιαφέρει γιατί αποθηκεύει στον File Server.

Αν και οι ανάγκες σε υλικό μπορεί να ποικίλουν οι κατασκευάστριες εταιρείες έχουν κατεβάσει αρκετά τις τιμές ώστε υπολογιστές με υψηλή επεξεργαστική δύναμη, μνήμη και μεγάλη χωρητικότητα να είναι σε πολύ καλές τιμές. Αν θέλουμε λοιπόν να έχουμε ομοιόμορφο περιβάλλον εργασίας, θα μπορούσαμε σε επίπεδο υλικού να έχουμε τους ίδιους υπολογιστές.

Για να υπάρχει καλύτερη διαχείριση του δικτύου σε κάθε εργαστήριο τοποθετείται και ένα hub το οποίο συνδέει τους υπολογιστές του εργαστηρίου με το υπόλοιπο δίκτυο . Για τις τάξεις τοποθετούμε σε κάθε όροφο και ένα hub. Και αντίστοιχα για τους γραμματεία – διοίκηση – λογιστήριο άλλο hub. Χρησιμοποιούμε τοπολογία αστέρα για την σύνδεση. Στην τοπολογία αστέρα έχουμε το μειονέκτημα ότι αν χαλάσει το hub έχει μείνει εκτός λειτουργίας ένα ολόκληρο τμήμα. Ταυτόχρονα όμως έχουμε απομονώσει το πρόβλημα άρα είναι και πιο εύκολη η επίλυση – αντικατάστασή του.

Σε κάθε τμήμα – εργαστήριο υπάρχει και ένα δικτυακό πολυμηχάνημα (εκτυπωτής – σαρωτής – fax) εκτός από τις τάξεις. Στον πρωτεύων ελεγκτή τομέα ενεργοποιούμε και την υπηρεσία Print Server για την οποία θα μιλήσουμε αναλυτικότερα παρακάτω καθώς θα προσθέσουμε τους εκτυπωτές στον Ενεργό Κατάλογο.



Εικόνα 4.7: Τοπολογία Αστέρα

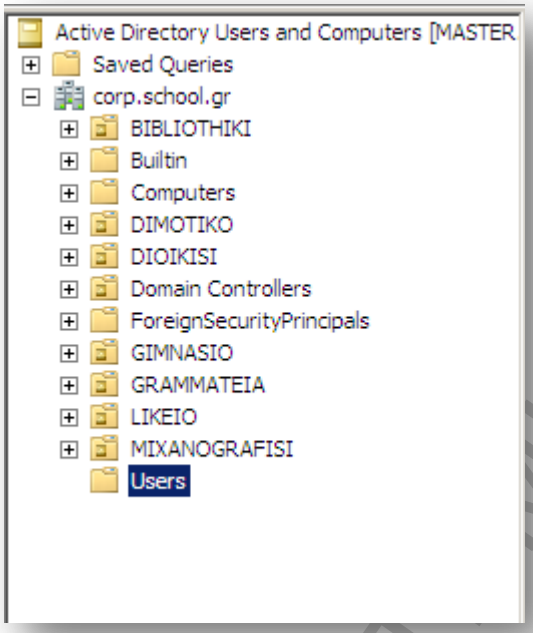
Για υψηλές ταχύτητες δικτύου χρησιμοποιούμε οπτική ίνα με αντίστοιχα 1000άρες κάρτες δικτύου στους υπολογιστές.

ΚΕΦΑΛΑΙΟ 5 –Σχεδιασμός Δικτύου

5.1 Σχεδιασμός Οργανωτικών Μονάδων, ομάδων, χρηστών και υπολογιστών

Οι οργανωτικές μονάδες συνήθως συσχετίζονται με την οργανωτική δομή ενός οργανισμού. Αν δούμε ένα οργανόγραμμα θα δούμε ότι δεν διαφέρει και πολύ από τον σχεδιασμό των οργανωτικών μονάδων. Αυτό γίνεται γιατί συνήθως τα μέλη ενός τμήματος διαχειρίζονται και έχουν πρόσβαση στα ίδια λογισμικά και στους ίδιους διαμοιραζόμενους πόρους.

Έτσι και στην εργασία μας θα δημιουργήσουμε οργανωτικές μονάδες αντίστοιχες με τα τμήματα του σχολείου όπως βλέπουμε και στην παρακάτω εικόνα.



Εικόνα 5.1.1: Οργανωτικές μονάδες

Κάθε οργανωτική μονάδα χωρίζεται σε υποομάδες και μέσα σε αυτές υπάρχουν οι λογαριασμοί χρηστών. Έτσι λοιπόν δημιουργήσαμε την παρακάτω δομή

Οργανωτικές Μονάδες
DIMOTIKO
GIMNASIO
LIKEIO
BIBLIOTHIKI
DIOIKISI
GRAMMATEIA
MIXANOGRAFISI
LOGISTIRIO
KATHIGITES

Σε κάθε οργανωτική μονάδα υπάρχουν ομάδες χρηστών ανάλογα με το τμήμα.

- Στην οργανωτική ομάδα DIMOTIKO ανήκουν οι ομάδες D-A, D-B, D-C, D-D, D-E, D-ST. Έξι ομάδες για τις έξι τάξεις του δημοτικού.
- Στην οργανωτική μονάδα GIMNASIO υπάρχουν οι ομάδες G-A, G-B, G-C.
- Στην οργανωτική μονάδα LIKEIO υπάρχουν οι ομάδες L-A, L-B, L-C.
- Στην οργανωτική μονάδα BIBLIOTHIKI υπάρχουν οι ομάδες XRISTES, B-MANAGE.
- Στην οργανωτική μονάδα DIOIKISI υπάρχει μία ομάδα D-MANAGE.
- Στην οργανωτική μονάδα GRAMMATEIA υπάρχει μία ομάδα GRAM.
- Στην οργανωτική μονάδα MIXANOGRAFISI υπάρχει μία ομάδα IT.
- Στην οργανωτική μονάδα LOGISTIRIO υπάρχουν δύο ομάδες TAMIAS, L-MANAGE.
- Στην οργανωτική μονάδα KATHIGITES υπάρχουν δύο ομάδες οι KATHIGITES και οι DASKALOI.

Θα παρατηρήσουμε ότι οι ονομασίες που δίνονται στις οργανωτικές μονάδες και στις ομάδες αντικατοπτρίζουν την πραγματική δομή του οργανισμού. Με αυτόν τον τρόπο πέρα του ότι έχουμε ένα δομημένο Κατάλογο διευκολύνεται πάρα πολύ η διαχείρισή του.

Στην εικόνα 5.1.2 θα παρατηρήσουμε ότι όλες οι ομάδες ανήκουν στον τοπικό τομέα σε ασφαλή ομάδα (Security Group - Domain Local). Μόνο η ομάδα IT ανήκει στον σφαιρικό κατάλογο, και αυτό έγινε προληπτικά γιατί το δίκτυό μας αποτελείται από ένα δάσος και ένα τομέα αλλά μελλοντικά μπορεί να δημιουργηθεί και άλλος τομέας.

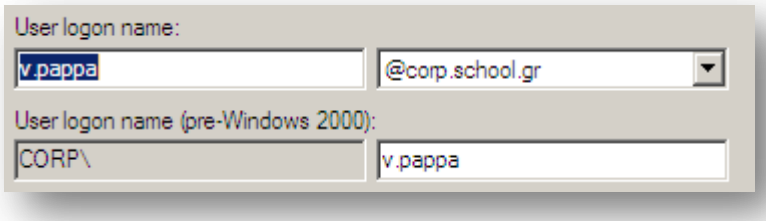
XRISTES	Security Group - Domain Local
B-MANAGE	Security Group - Domain Local
D-A	Security Group - Domain Local
D-B	Security Group - Domain Local
D-C	Security Group - Domain Local
D-D	Security Group - Domain Local
D-E	Security Group - Domain Local
D-ST	Security Group - Domain Local
G-A	Security Group - Domain Local
G-B	Security Group - Domain Local
G-C	Security Group - Domain Local
L-A	Security Group - Domain Local
L-B	Security Group - Domain Local
L-C	Security Group - Domain Local
D-MANAGE	Security Group - Domain Local
GRAM	Security Group - Domain Local
TAMIAS	Security Group - Domain Local
L-MANAGE	Security Group - Domain Local
IT	Security Group - Global

Εικόνα 5.1.2: Ομάδες Δικτύου

Δημιουργώντας τις οργανωτικές μονάδες και τις ομάδες παρατηρήσαμε τα εξής:

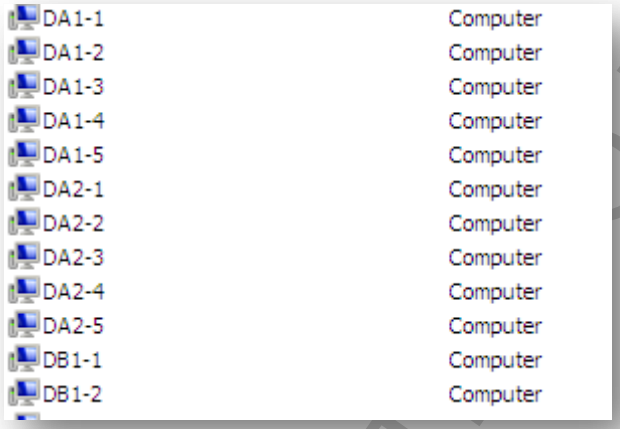
- Μία ομάδα μπορεί να έχει το ίδιο όνομα με μια οργανωτική μονάδα.
- Το όνομα μίας ομάδας πρέπει να είναι μοναδικό στον τομέα.
- Αν δηλώσουμε μια ομάδα εξαρχής σαν τοπική ομάδα η μόνη επιλογή που έχουμε στη συνέχεια είναι να γίνει καθολική. Το ίδιο συμβαίνει και με την σφαιρική ομάδα.

Στη συνέχεια με την ίδια λογική δημιουργούμε τους λογαριασμούς χρηστών. Ακολουθούμε πάντα την ίδια πολιτική. Χρησιμοποιούμε μικρούς λατινικούς χαρακτήρες. Το πρώτο γράμμα του ονόματός τους, το πρώτο γράμμα του ονόματος του πατέρα, τελεία και το επώνυμο ολόκληρο. Θα μπορούσαμε να βάζαμε και την τάξη αλλά μετά κάθε χρονιά θα έπρεπε να κάνουμε και μετονομασία των χρηστών. Ενώ τώρα το μόνο που χρειάζεται είναι μετακίνηση στην αντίστοιχη ομάδα.



Εικόνα 5.1.3: Δημιουργία χρήστη

Στη συνέχεια σχεδιάζουμε την ονομασία των λογαριασμών υπολογιστών. Και αυτή η ονομασία πρέπει να είναι μοναδική. Τα ονόματα υπολογιστών θα πρέπει να βοηθάνε τον διαχειριστή να καταλάβει που βρίσκεται χωροταξικά ο υπολογιστής και ποιοι χρήστες των χειρίζονται. Έτσι τα ονόματα υπολογιστών θα ξεκινάνε από D για το δημοτικό, C για το Γυμνάσιο και L για το Λύκειο, ενώ στη συνέχεια θα αναγράφεται το αντίστοιχο τμήμα και ο αριθμός υπολογιστή. Δηλαδή βάζοντας όνομα υπολογιστή DA1-1 εννοούμε τον υπολογιστή 1, του πρώτου τμήματος (1), της πρώτης τάξης (A), του δημοτικού (D). Αντίστοιχη θα είναι η κωδικοποίηση των υπόλοιπων τμημάτων όπως φαίνεται και στην εικόνα 5.1.4.



Εικόνα 5.1.4: Όνομα Υπολογιστών

5.2 Σχεδιασμός πολιτικών ομάδων

Ο σχεδιασμός των πολιτικών ομάδων είναι ένα μεγάλο κεφάλαιο της Microsoft. Στα Windows server 2008 υπάρχουν πάνω από 700 πολιτικές. Θα πρέπει να σχεδιάσουμε το δίκτυό μας σε σχέση με το τι θέλουμε να κάνει ο κάθε χρήστης ή υπολογιστής. Αντί λοιπόν να βάζουμε πολιτικές ανά αντικείμενο δημιουργούμε ομάδες με κοινά λειτουργικά χαρακτηριστικά και προσδίδουμε σε αυτές πολιτικές. Με την αρχή της κληρονομικότητας αυτές μεταφέρονται στα αντικείμενα.

Για τη δημιουργία του δικτύου μας έχουμε δημιουργήσει 19 ομάδες οι οποίες ανήκουν σε 8 οργανωτικές μονάδες. Εφόσον έχουμε ήδη δημιουργήσει τις ομάδες θα πρέπει να δούμε τους χρήστες μας ώστε να τους κατατάξουμε σε μια ομάδα.

Ομάδες D-A, D-B: Μαθητές Α και Β δημοτικού. Οι χρήστες είναι μαθητές πρώτης και δευτέρας δημοτικού. Είναι η πρώτη επαφή με υπολογιστή.

- Θα πρέπει να μάθουν το όνομα χρήστη τους, αλλά δεν έχουν κωδικό πρόσβασης.
- Ο λογαριασμός χρήστη θα απενεργοποιείται μετά από 10 χρόνια ενώ θα λειτουργεί καθημερινά 8 το πρωί με 4 το απόγευμα εκτός Σαββάτου και Κυριακής.

- Μετά την είσοδο στον υπολογιστή ο μαθητής θα πρέπει να βλέπει στην επιφάνεια εργασίας μόνο τα μαθήματα, που δίνονται σε ηλεκτρονική μορφή από το παιδαγωγικό ινστιτούτο, τη ζωγραφική των Windows.
- Θα εκτυπώνουν στον δικτυακό εκτυπωτή που βρίσκεται στην τάξη τους.
- Ο εκτυπωτής είναι ρυθμισμένος να τυπώνει αυτόματα σε απλό χαρτί και με χαμηλή ποιότητα (draft).
- Το δεξί κλικ δεν λειτουργεί.
- Δεν θα πρέπει να έχουν την επιλογή να κλειδώνουν έναν υπολογιστή (ctrl+alt+del).
- Δεν λειτουργούν επίσης το cd, το usb και το floppy.
- Τέλος αποθηκεύουν τοπικά τις εργασίες τους ή δικτυακά στο δίσκο αντιστοίχησης στον υπολογιστή μου.

Ομάδες D-C, D-D, D-E, D-ST: Μαθητές Γ, Δ, Ε, και ΣΤ δημοτικού. Οι χρήστες είναι μαθητές της τρίτης, τετάρτης, πέμπτης και έκτης δημοτικού.

- Στη πρώτη σύνδεση (logon) που θα κάνουν θα πρέπει να τους ζητάει αλλαγή κωδικού.
- Ο καινούργιος κωδικός που θα βάλουν θα πρέπει να αποτελείται από τρεις αριθμούς και τρία γράμματα και δεν θα λήγει.
- Ο λογαριασμός χρήστη θα λειτουργεί καθημερινά 8 το πρωί με 4 το απόγευμα εκτός Σαββάτου και Κυριακής.
- Στην επιφάνεια εργασίας θα υπάρχουν εικονίδια με τα μαθήματα που δίνονται σε ηλεκτρονική μορφή από το παιδαγωγικό ινστιτούτο, η ζωγραφική των Windows, Word, Excel, PowerPoint, Internet Explorer.
- Θα υπάρχει δυνατότητα εκτύπωσης στον δικτυακό εκτυπωτή της τάξης.
- Ο εκτυπωτής είναι ρυθμισμένος να τυπώνει αυτόματα σε απλό χαρτί και με χαμηλή ποιότητα (draft).
- Δεν θα πρέπει να έχουν την επιλογή να κλειδώνουν έναν υπολογιστή (ctrl+alt+del).
- Το δεξί κλικ δεν επιτρέπεται ενώ δεν λειτουργούν cd,και floppy.
- Στο usb έχουν δυνατότητα read, write μόνο για .doc, .xls,. ppt.
- Αποθηκεύουν τοπικά τις εργασίες τους ή στον δίσκο αντιστοίχησης στον υπολογιστή μου.

Ομάδες G-A, G-B, G-C: Μαθητές Α, Β, Γ γυμνασίου. Οι χρήστες είναι μαθητές Α, Β, και Γ γυμνασίου.

- Η επιφάνεια εργασίας είναι η κλασική επιφάνεια των Windows.
- Δεν μπορούν να κάνουν κατάργηση εγκατάστασης ή νέα εγκατάσταση.
- Δεν μπορούν επίσης να αλλάξουν τις ιδιότητες του δικτύου.
- Είναι εγκατεστημένα τα λογισμικά του γυμνασίου.
- Δεν λειτουργούν cd, floppy.
- Στο usb έχουν δυνατότητα read, write μόνο για .doc, .xls,. ppt
- Περιορισμένη πρόσβαση στο διαδίκτυο.
- Θα υπάρχει δυνατότητα εκτύπωσης στον δικτυακό εκτυπωτή της τάξης.
- Ο εκτυπωτής είναι ρυθμισμένος να τυπώνει αυτόματα σε απλό χαρτί και με χαμηλή ποιότητα (draft).
- Δεν θα πρέπει να έχουν την επιλογή να κλειδώνουν έναν υπολογιστή (ctrl+alt+del)
- Αποθηκεύουν τοπικά τις εργασίες τους ή στον δίσκο αντιστοίχησης.

Ομάδες L-A, L-B, L-C: Μαθητές Α,Β, Γ λυκείου. Οι χρήστες είναι μαθητές Α, Β και Γ λυκείου. Αρκετά έμπειροι χρήστες πλέον και όχι μόνο.

- Δεν έχουν πρόσβαση στο δεξί κλικ.
- Δεν μπορούν να κάνουν κατάργηση εγκατάστασης ή νέα εγκατάσταση.
- Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου.
- Δεν λειτουργεί η γραμμή εντολών.
- Ο λογαριασμός κλειδώνει στην τρίτη προσπάθεια λάθους κωδικού και ή ξεκλειδώνει μόνος την επόμενη μέρα ή ο καθηγητής μπορεί να τον ξεκλειδώσει.
- Θα υπάρχει δυνατότητα εκτύπωσης στον δικτυακό εκτυπωτή της τάξης.
- Ο εκτυπωτής είναι ρυθμισμένος να τυπώνει αυτόματα σε απλό χαρτί και με χαμηλή ποιότητα (draft).
- Δεν λειτουργούν cd, floppy.

- Στο usb έχουν δυνατότητα read, write μόνο για .doc, .xls,. ppt
- Δεν επιτρέπεται το κατέβασμα από internet video, τραγούδια.
- Δεν θα πρέπει να έχουν την επιλογή να κλειδώνουν έναν υπολογιστή (ctrl+alt+del)
- Αποθηκεύουν τοπικά τις εργασίες τους ή στον δίσκο αντιστοίχησης στον υπολογιστή μου.

Ομάδα KATHIGITES και DASKALOI. Οι χρήστες αυτής της ομάδας είναι οι καθηγητές και οι δάσκαλοι. Συνδέονται στο σχολικό δίκτυο σε πολλούς υπολογιστές.

- Δεν πρέπει να έχουν την επιλογή να κλειδώνουν έναν υπολογιστή (ctrl+alt+del). Αποθηκεύουν κεντρικά στον φάκελο ανακατεύθυνσης τα αρχεία τους ενώ το προφίλ τους είναι προφίλ περιαγωγής.
- Έχουν δυνατότητα να λειτουργούν και με αρχεία χωρίς σύνδεση (offline).
- Δεν έχουν πρόσβαση στο δεξί κλικ.
- Δεν μπορούν να κάνουν κατάργηση εγκατάστασης ή νέα εγκατάσταση. Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου.
- Δεν λειτουργεί η γραμμή εντολών.
- Ο λογαριασμός κλειδώνει στην τρίτη προσπάθεια λάθους κωδικού και ξεκλειδώνει από τον διαχειριστή.
- Έχουν τη δυνατότητα να ξεκλειδώσουν λογαριασμό μαθητή.
- Μπορούν να εκτυπώσουν σε πολλούς εκτυπωτές ενώ μπορούν να διαχειρίζονται την ουρά εκτύπωσης στον εκτυπωτή της τάξης που βρίσκονται.
- Έχουν φάκελο αντιστοίχησης στον υπολογιστή τους όπου μπορούν να μοιραστούν αρχεία με μαθητές ή συναδέλφους τους.

Ομάδα Grammateia. Οι χρήστες αυτής της ομάδας χειρίζονται εφαρμογές γραφείου, συνδέονται στο διαδίκτυο, χειρίζονται την βάση δεδομένων των μαθητών, έχουν ηλεκτρονικό ταχυδρομείο.

- Αποθηκεύουν κεντρικά στον φάκελο ανακατεύθυνσης τα αρχεία τους ενώ το προφίλ τους είναι προφίλ περιαγωγής.
- Έχουν δυνατότητα να λειτουργούν και με αρχεία χωρίς σύνδεση (offline).
- Δεν έχουν πρόσβαση στο δεξί κλικ.
- Δεν μπορούν να κάνουν κατάργηση εγκατάστασης ή νέα εγκατάσταση.
- Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου.
- Δεν λειτουργεί η γραμμή εντολών.
- Ο λογαριασμός κλειδώνει στην τρίτη προσπάθεια λάθους κωδικού και ξεκλειδώνει από τον διαχειριστή.
- Εκτυπώνουν σε πολλούς εκτυπωτές και έχουν δυνατότητα να επιλέξουν τις ιδιότητες του εκτυπωτή (ποιότητα εκτύπωσης..)
- Έχουν φάκελο αντιστοίχησης στον υπολογιστή τους όπου μπορούν να μοιραστούν αρχεία με συναδέλφους τους.

*Ομάδα Dioikisi.*Σε αυτή την ομάδα ανήκει το διοικητικό προσωπικό. Οι χρήστες της χειρίζονται εφαρμογές γραφείου, συνδέονται στο διαδίκτυο, χειρίζονται την βάση δεδομένων των μαθητών, την λογιστική βάση, την βάση της βιβλιοθήκης, έχουν ηλεκτρονικό ταχυδρομείο.

- Αποθηκεύουν κεντρικά στον φάκελο ανακατεύθυνσης τα αρχεία τους ενώ το προφίλ τους είναι προφίλ περιαγωγής.
- Έχουν δυνατότητα να λειτουργούν και με αρχεία χωρίς σύνδεση (offline).
- Δεν έχουν πρόσβαση στο δεξί κλικ.
- Δεν μπορούν να κάνουν κατάργηση εγκατάστασης ή νέα εγκατάσταση.
- Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου.
- Δεν λειτουργεί η γραμμή εντολών.
- Ο λογαριασμός κλειδώνει στην τρίτη προσπάθεια λάθους κωδικού και ξεκλειδώνει από τον διαχειριστή.
- Εκτυπώνουν σε πολλούς εκτυπωτές και έχουν δυνατότητα να επιλέξουν τις ιδιότητες του εκτυπωτή (ποιότητα εκτύπωσης).
- Έχουν φάκελο αντιστοίχησης στον υπολογιστή τους όπου μπορούν να μοιραστούν αρχεία με συναδέλφους τους.

Ομάδα Logistirio. Εδώ ανήκουν οι λογιστές και οι ταμίες. Οι χρήστες της χειρίζονται εφαρμογές γραφείου, συνδέονται στο διαδίκτυο, χειρίζονται την λογιστική βάση, έχουν ηλεκτρονικό ταχυδρομείο.

- Αποθηκεύουν κεντρικά στον φάκελο ανακατεύθυνσης τα αρχεία τους ενώ το προφίλ τους είναι προφίλ περιαγωγής.
- Έχουν δυνατότητα να λειτουργούν και με αρχεία χωρίς σύνδεση (offline).
- Δεν έχουν πρόσβαση στο δεξί κλικ.
- Δεν μπορούν να κάνουν κατάργηση εγκατάστασης ή νέα εγκατάσταση.
- Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου.
- Δεν λειτουργεί η γραμμή εντολών.
- Ο λογαριασμός κλειδώνει στην τρίτη προσπάθεια λάθους κωδικού και ξεκλειδώνει από τον διαχειριστή.
- Εκτυπώνουν σε πολλούς εκτυπωτές και έχουν δυνατότητα να επιλέξουν τις ιδιότητες του εκτυπωτή (ποιότητα εκτύπωσης..)
- Έχουν φάκελο αντιστοίχησης στον υπολογιστή τους όπου μπορούν να μοιραστούν αρχεία με συναδέλφους τους.

Ομάδα Biblio. Οι χρήστες σε αυτή την ομάδα χειρίζονται την βάση δεδομένων της βιβλιοθήκης, συνδέονται στο διαδίκτυο, έχουν ηλεκτρονικό ταχυδρομείο.

- Αποθηκεύουν κεντρικά στον φάκελο ανακατεύθυνσης τα αρχεία τους ενώ το προφίλ τους είναι προφίλ περιαγωγής.
- Έχουν δυνατότητα να λειτουργούν και με αρχεία χωρίς σύνδεση (offline).
- Δεν έχουν πρόσβαση στο δεξί κλικ.
- Δεν μπορούν να κάνουν κατάργηση εγκατάστασης ή νέα εγκατάσταση.
- Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου.
- Δεν λειτουργεί η γραμμή εντολών.
- Ο λογαριασμός κλειδώνει στην τρίτη προσπάθεια λάθους κωδικού και ξεκλειδώνει από τον διαχειριστή.
- Εκτυπώνουν στον εκτυπωτή της βιβλιοθήκης και έχουν δυνατότητα να επιλέξουν τις ιδιότητες του εκτυπωτή (ποιότητα εκτύπωσης..)
- Έχουν φάκελο αντιστοίχησης στον υπολογιστή τους όπου μπορούν να μοιραστούν αρχεία με συναδέλφους τους.

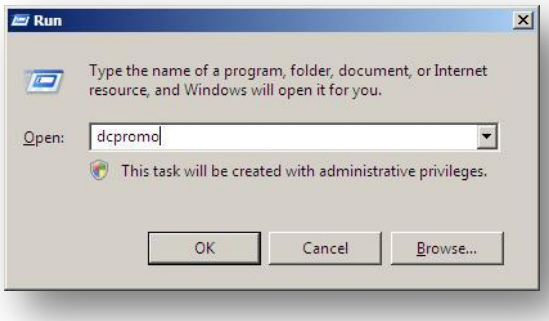
Ομάδα IT. Οι χρήστες αυτής της ομάδας είναι οι διαχειριστές όλου του δικτύου. Έχουν πλήρη πρόσβαση και δικαιώματα σε όλους τους πόρους του δικτύου.

ΚΕΦΑΛΑΙΟ 6 - *Υλοποίηση Δικτύου*

6.1 Εγκατάσταση ελεγκτή τομέα

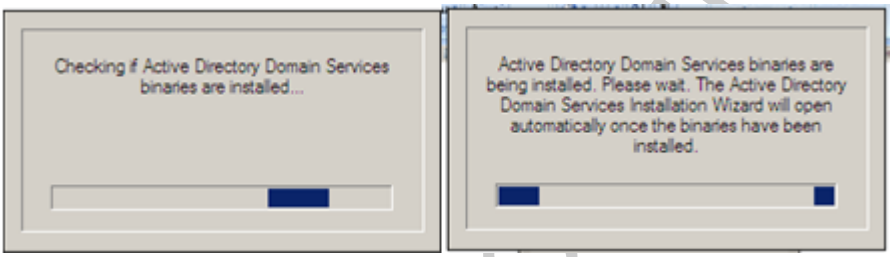
Σε αυτό το κεφάλαιο θα δούμε αναλυτικά πως δημιουργείται ένας ελεγκτής τομέας στα Windows 2008 Server και το χτίσιμο βήμα βήμα του Ενεργού Καταλόγου.

Η τυπική εγκατάσταση των Windows δεν δημιουργεί Ελεγκτή Τομέα. Για να αναβαθμίσουμε το λειτουργικό από το μενού Start πληκτρολογούμε την εντολή dcpromo (promote to domain controller) και πατάμε εκτέλεση.



Εικόνα 6.1.1: Εγκατάσταση Ελεγκτή Τομέα

Εκτελώντας την εντολή dcpromo ουσιαστικά δίνουμε την εντολή να ξεκινήσει ένα wizard (βοηθητικό πρόγραμμα) που μας βοηθάει να εγκαταστήσουμε τα Active Directory Domain Services.

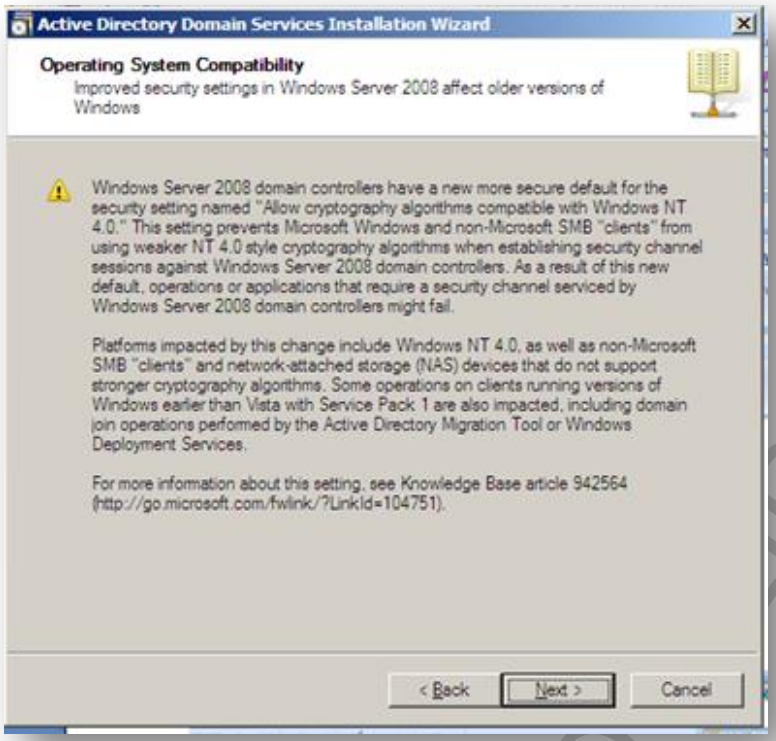


Εικόνα 6.1.2: Έλεγχος για το αν υπάρχει ήδη Ενεργός Κατάλογος

Αρχικά γίνεται ένας έλεγχος για το αν υπάρχει ήδη εγκατεστημένο Active Directory Domain Services. Αν δεν υπάρχει εγκατεστημένο τότε ξεκινάει ο wizard, ένα βοηθητικό πρόγραμμα που μας οδηγεί βήμα βήμα στην ολοκλήρωση της εγκατάστασης.

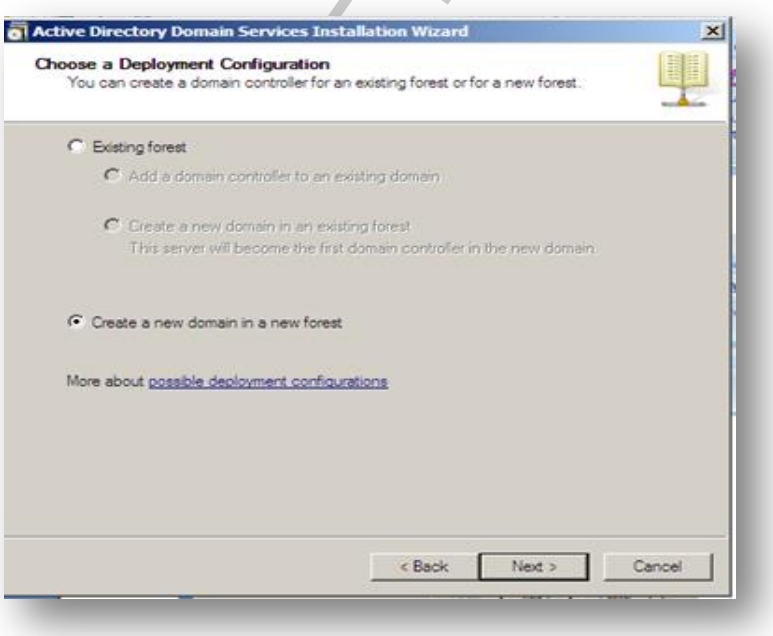
Εικόνα 6.1.3: Βοηθητικό πρόγραμμα AD

Εμφανίζεται ένα μήνυμα συμβατότητας το οποίο αναφέρει ότι το λειτουργικό Windows 2008 πιθανά να μην είναι απόλυτα συμβατό με παλιότερα λειτουργικά γιατί χρησιμοποιεί πιο εξελιγμένους αλγόριθμους κρυπτογράφησης.



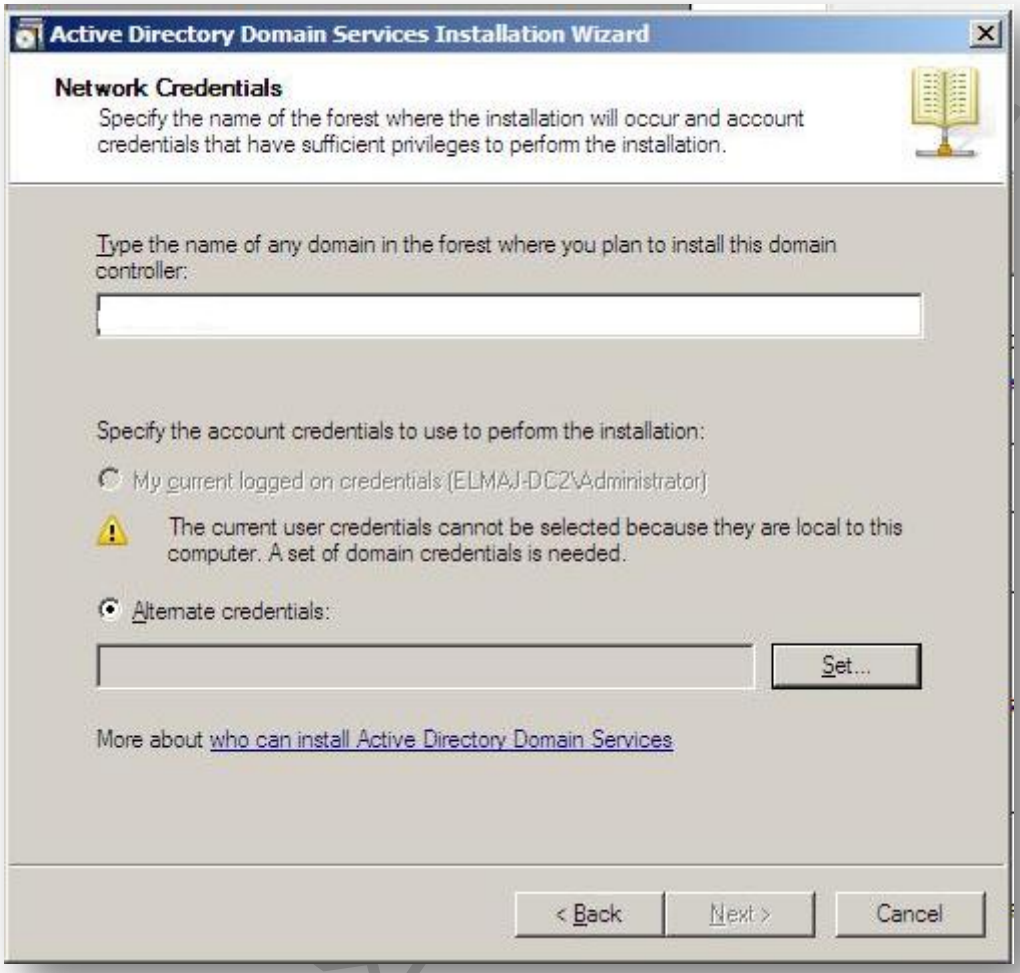
Εικόνα 6.1.4:Συμβατότητα λειτουργικού συστήματος

Ακολουθεί μήνυμα για το αν ο Domain Controller θα ανήκει σε κάποιο δάσος ή αν θα δημιουργηθεί νέο. Πριν επιλέξουμε θα πρέπει να γνωρίζουμε καλά τι θέλουμε να κάνουμε. Αν υπάρχει κάποιο δάσος στο οποίο θέλουμε να ανήκει ο ελεγκτής τομέας μας θα πρέπει να επιλέξουμε το Existing forest και στη συνέχεια αν θα δημιουργήσουμε καινούργιο τομέα ή θα γίνει μέλος σε ένα υπάρχον τομέα. Όπως ήδη έχουμε αναφέρει η έννοια του δάσους είναι η συνύπαρξη πολλών τομέων με σχέσεις εμπιστοσύνης μεταξύ τους.

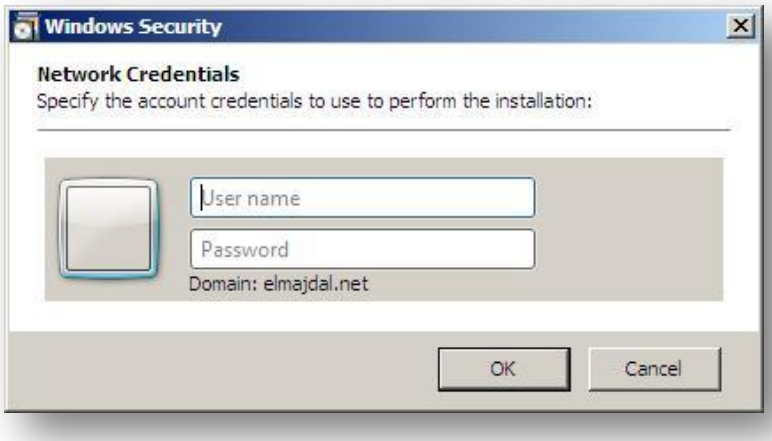


Εικόνα 6.1.5: Επιλογή διαμόρφωσης

Αν επιλέξουμε ο ελεγκτής τομέας να ανήκει σε ένα υπάρχον τομέα ενός δάσους θα πρέπει να γνωρίζουμε το όνομα αυτού και φυσικά τους κωδικούς του διαχειριστή για να μας επιτρέψει να γίνουμε μέλη αυτού. Ουσιαστικά και πλήρη δικαιώματα έχει το group των enterprise admins και το group των domain admins.

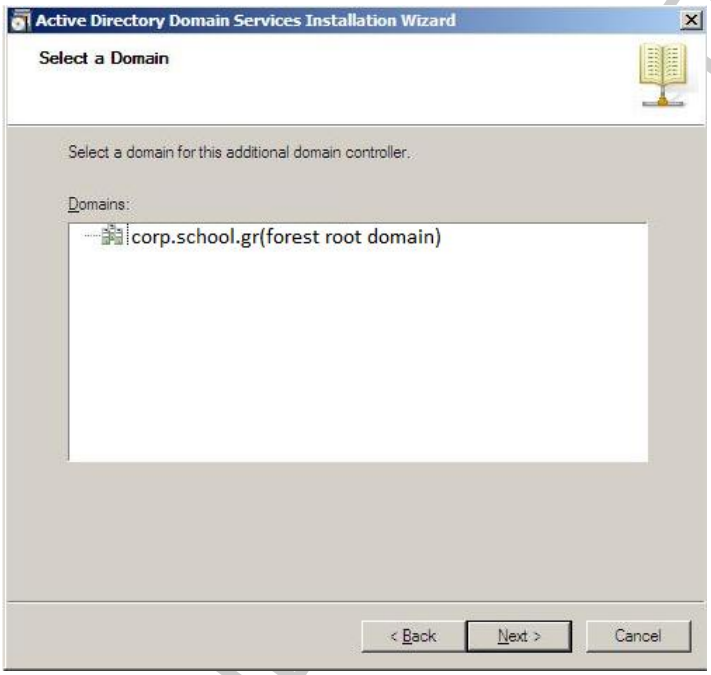


Εικόνα 6.1.6: Δικτυακές πιστοποίησης δάσους



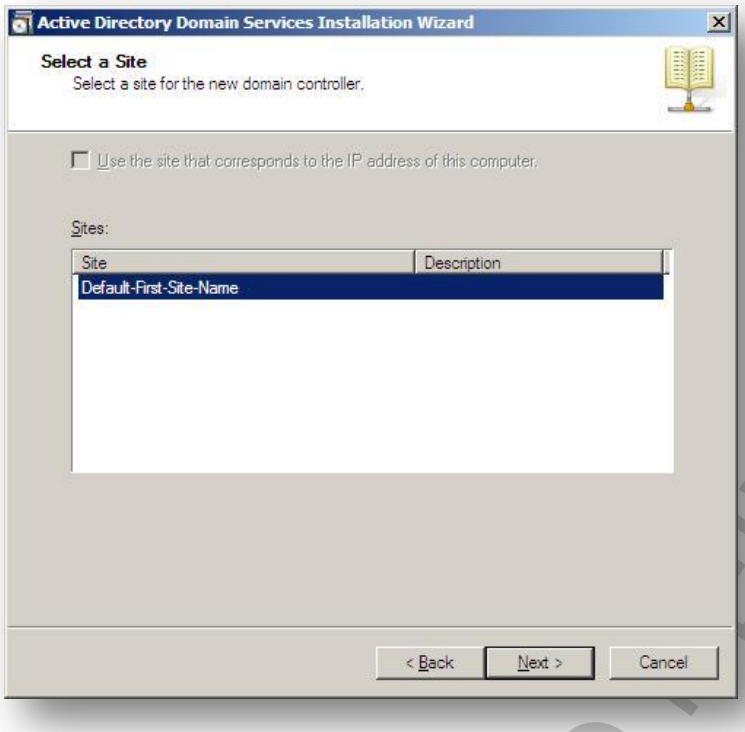
Εικόνα 6.1.7: Θα πρέπει να γνωρίζουμε τους κωδικούς του Enterpise Admin

Στη συνέχεια θα πρέπει να επιλέξουμε τον τομέα στον οποίο θα ανήκει. Στο παράδειγμα της εικόνας υπάρχει ένα τομέας οπότε επιλέγεται αυτόματα αυτός. Αν είχαμε πολλούς τομείς θα εμφανιζόταν εδώ και θα επιλέγαμε.



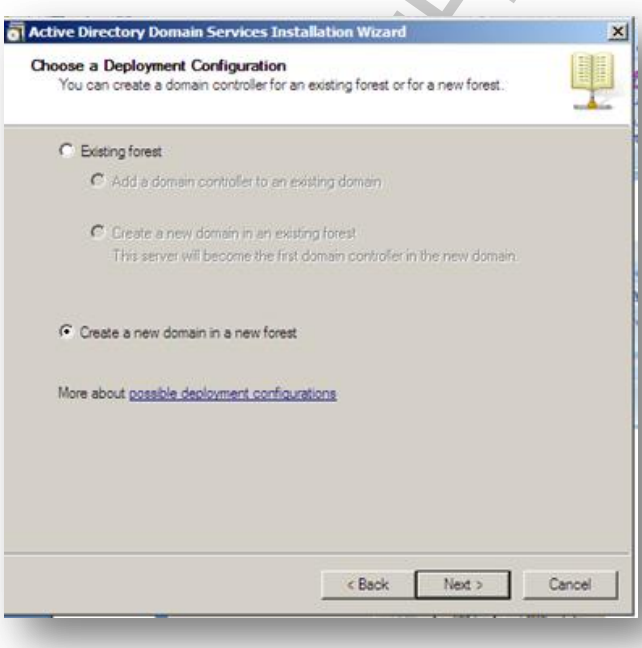
Εικόνα 6.1.8: Επιλογή Τομέα

Στο παράθυρο Select a Site είτε επιλέγουμε το Use the site that corresponds to the IP address of this computer, είτε επιλέγουμε ένα site από αυτά που θα εμφανιστούν. Αν υπάρχει ένας ελεγκτής τομέα και μία τοποθεσία θα είναι επιλεγμένα από μόνα τους.



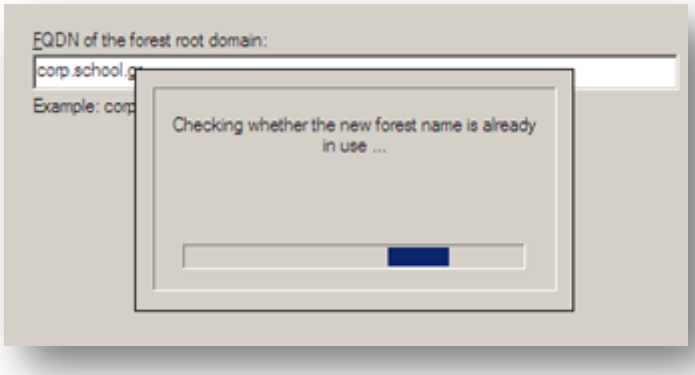
Εικόνα 6.1.9: Επιλογή Τοποθεσίας

Στην εργασία μας θα χτίσουμε ένα νέο τομέα σε ένα νέο δάσος. Στη συνέχεια σε αυτό το δάσος θα μπορούσαμε να προσθέσουμε και άλλους τομείς. Αφού μιλάμε για σχολικό δίκτυο θα μπορούσε να υπήρχε ένα δάσος του πανελλήνιου σχολικού δικτύου και κάθε σχολική μονάδα να ήταν ένας ξεχωριστός τομέας.



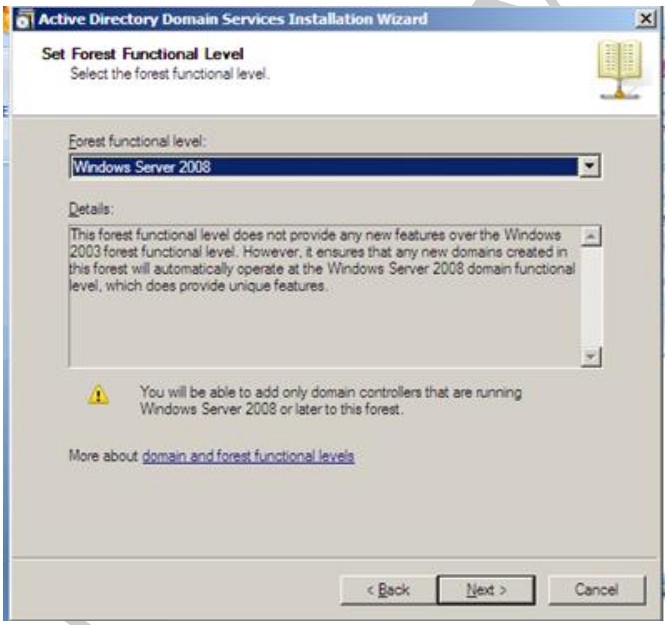
Εικόνα 6.1.10: Δημιουργία νέου τομέα σε νέο δάσος

Θα πρέπει να ονομάσουμε το δάσος και τον τομέα μας. Η ονομασία είναι corp.school.gr. Γίνεται έλεγχος στο διαδίκτυο για το αν υπάρχει ήδη η συγκεκριμένη ονομασία. Κάθε ονομασία θα πρέπει να είναι μοναδική.



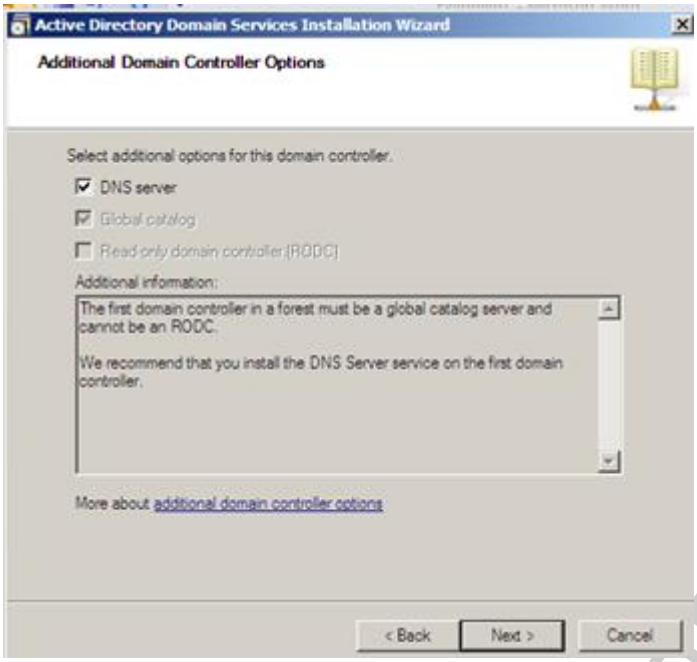
Εικόνα 6.1.10: Έλεγχος ονόματος

Η επόμενη επιλογή που εμφανίζεται κατά την εγκατάσταση είναι να επιλέξουμε το επίπεδο λειτουργικότητας του δάσους. Αν όλοι οι ελεγκτές τομείς σε ένα τομέα ή ένα δάσος έχουν Windows 2003 Server και το επίπεδο λειτουργικότητας είναι επίσης σε Windows 2003 τότε όλες οι δυνατότητες του αντίστοιχου λειτουργικού είναι διαθέσιμες. Οι επιπλέον λειτουργίες δεν θα υποστηρίζονται από τον ελεγκτή τομέα με παλιότερη έκδοση λειτουργικού.



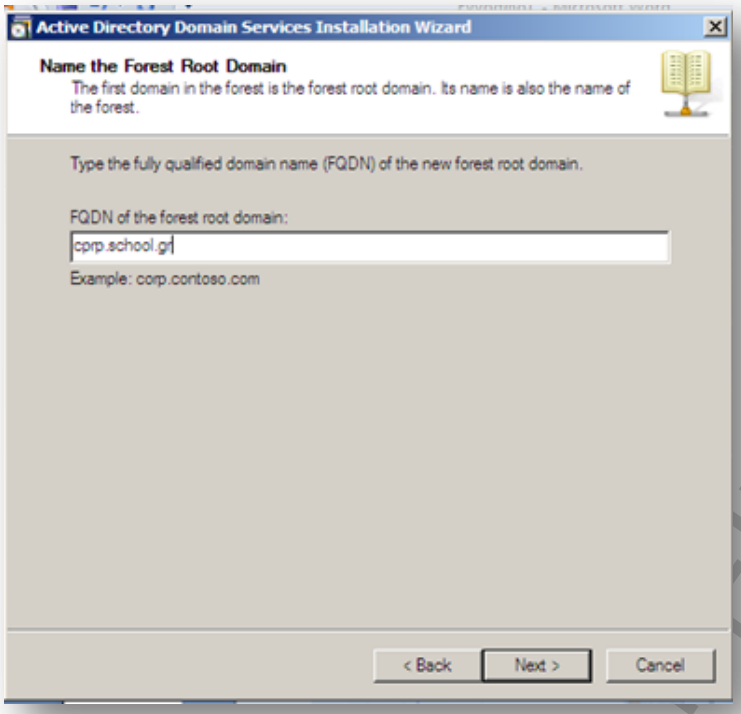
Εικόνα 6.1.11: Επίπεδο λειτουργικότητας

Επιπλέον επιλογές **(**Additional Domain Controller Options**).** Προτείνεται από την Microsoft ο πρώτος ελεγκτής τομέας να είναι και ο DNS server. Πρέπει να είναι στο global catalog server του δάσους και σε καμιά περίπτωση δεν πρέπει να είναι Read Only Domain Controller.(Ελεγκτής τομέας μόνο για ανάγνωση)



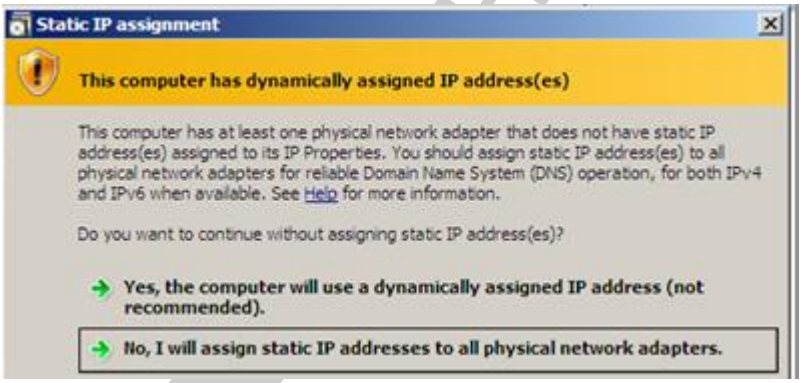
Εικόνα 6.1.12: Επιλογές ελεγκτή τομέα

Πληκτρολογούμε το όνομα του forest root domain. Το forest root domain είναι το όνομα του πρώτου τομέα σε ένα δάσος και το όνομα του δάσους. Τα αρχικά FQDN προέρχονται από τις λέξεις Full Qualified Domain Name. Το συγκεκριμένο όνομα θα πρέπει να είναι μοναδικό.



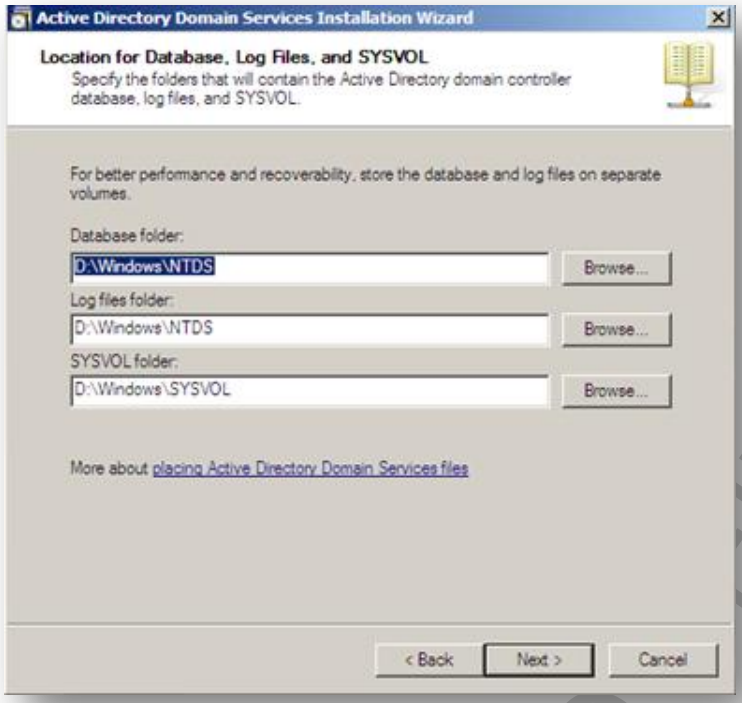
Εικόνα 6.1.13: Όνομα του forest root domain

Αν στον υπολογιστή –διακομιστή δεν έχουμε δώσει κάποια διεύθυνση IP θα εμφανιστεί μήνυμα που βλέπουμε στην εικόνα 6.1.14 το οποίο θα μας παροτρύνει να βάλουμε μια στατική IP διεύθυνση (static IP address). Στις ιδιότητες του δικτύου ορίζουμε την static IP.



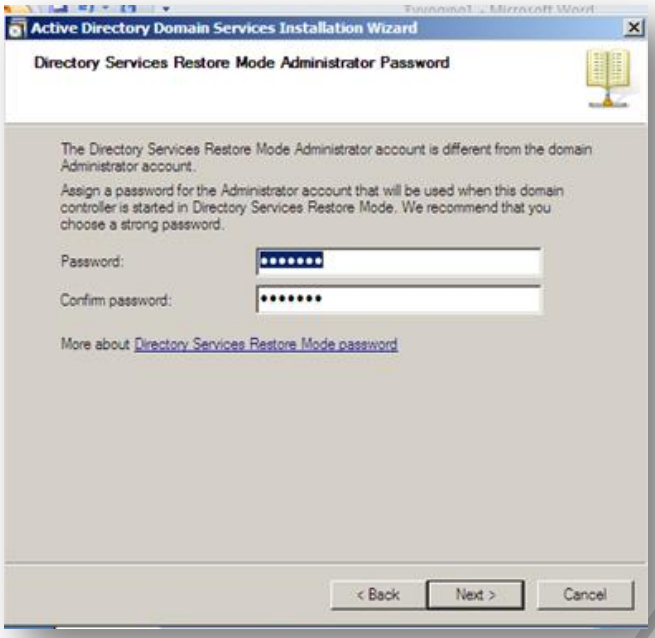
Εικόνα 6.1.14: Προειδοποιητικό μήνυμα για στατική IP διεύθυνση

Στη συνέχεια θα πρέπει να δηλωθεί η διαδρομή (path) στην οποία θα εγκατασταθούν η βάση δεδομένων του Ενεργού Καταλόγου, τα αρχεία καταγραφής (log files) και το SYSVOL. Η βάση δεδομένων αποθηκεύει πληροφορίες για τους χρήστες, τους υπολογιστές και τα άλλα αντικείμενα στο δίκτυο. Τα log files είναι αρχεία που καταγράφουν ενέργειες που γίνονται στον Ενεργό Κατάλογο όπως πληροφορίες αναβάθμισης ενός αντικειμένου. Το SYSVOL αποθηκεύει τις πολιτικές των ομάδων (group policy objects) και τα σενάρια (scripts). Η προεπιλεγμένη θέση αυτών είναι στο φάκελο των Windows. Υπάρχει βέβαια και η επιλογή αλλαγής θέσης εγκατάστασης (browse). Για μεγαλύτερη ασφάλεια (backup or recovery) η Microsoft προτείνει την εγκατάσταση των συγκεκριμένων αρχείων σε ξεχωριστά volume label.



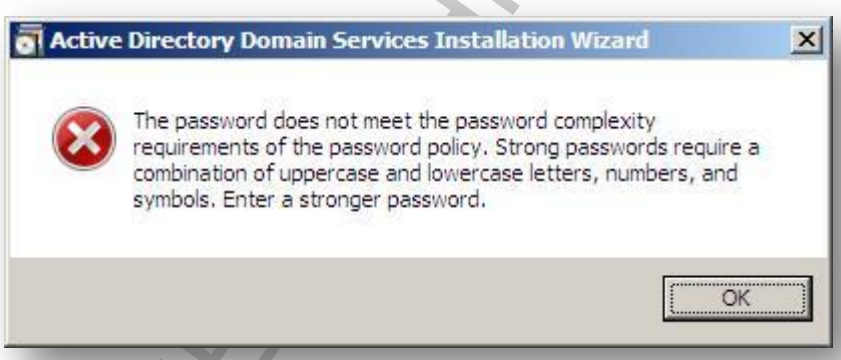
Εικόνα 6.1.15: Τοποθεσία βάσης δεδομένων Ενεργού καταλόγου

Στο παράθυρο Directory Services Restore Mode Administrator Password **(**DSRM**),** βάζουμε έναν κωδικό πρόσβασης και το επιβεβαιώνουμε (confirm). Αυτός ο κωδικός χρησιμοποιείται σε περίπτωση που το Active Directory Domain Services δεν «τρέχει» ο domain controller ξεκινάει σε λειτουργία Directory Services Restore Mode με στόχο να διορθώσει το πρόβλημα.



Εικόνα 6.1.16: Restore Mode

Ο κωδικός θα πρέπει να ταιριάζει με την προεπιλεγμένη πολιτική των κωδικών των Windows server 2008. Αν και θα αναφερθούμε παρακάτω με λεπτομέρειες για την συγκεκριμένη πολιτική να πούμε σε αυτό το σημείο ότι ο κωδικός πρέπει να είναι ένας συνδυασμός κεφαλαία και μικρά γράμματα, αριθμούς και σύμβολα. Σε αντίθετη περίπτωση θα δούμε μήνυμα της εικόνας 6.1.17.

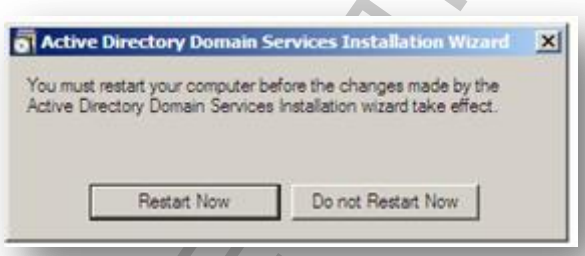


Εικόνα 6.1.17: Πολιτική κωδικού

Εμφανίζεται το παράθυρο που μας λέει περιληπτικά τις ρυθμίσεις που έχουμε επιλέξει. Μπορούμε να κάνουμε εξαγωγή σε αρχείο (export settings) τις ρυθμίσεις για να μπορέσουμε να τις χρησιμοποιήσουμε σαν backup.

Εικόνα 6.1.18: Όλες οι επιλογές πριν την εγκατάσταση

Στη συνέχεια ο Wizard ολοκληρώνει την εγκατάσταση και κάνουμε επανεκκίνηση τον διακομιστή μας. (Help Microsoft Windows Server 2008)



Εικόνα 6.1.19: Ολοκλήρωση εγκατάστασης και επανεκκίνηση

6.2 Unattended Installation of Active Directory Domain Services

Πριν ολοκληρωθεί η εγκατάσταση του Ενεργού Καταλόγου υπάρχει η επιλογή δημιουργίας ενός αρχείου το οποίο καταγράφει όλες τις ρυθμίσεις που έχουμε κάνει όταν αναβαθμίζουμε (promote) ένα υπολογιστή σε ελεγκτή τομέα. Αυτό το αρχείο μπορεί να χρησιμοποιηθεί για γρήγορη εγκατάσταση πολλών ελεγκτών τομέων κάνοντας απλά μία εισαγωγή (import) αυτού. Το συγκεκριμένο αρχείο είναι το answer file και είναι σε μορφή text και παρέχει αυτόματα όλες τις απαντήσεις για τον Ενεργό Κατάλογο. Η διαδικασία έχει ως εξής:

- Πληκτρολογούμε σε γραμμή εντολών:
  dcpromo /answer [: filename]

ή

dcpromo /unattend [: filename]

όπου filename το όνομα του answer file.Το αρχείο έχει τα παρακάτω στοιχεία

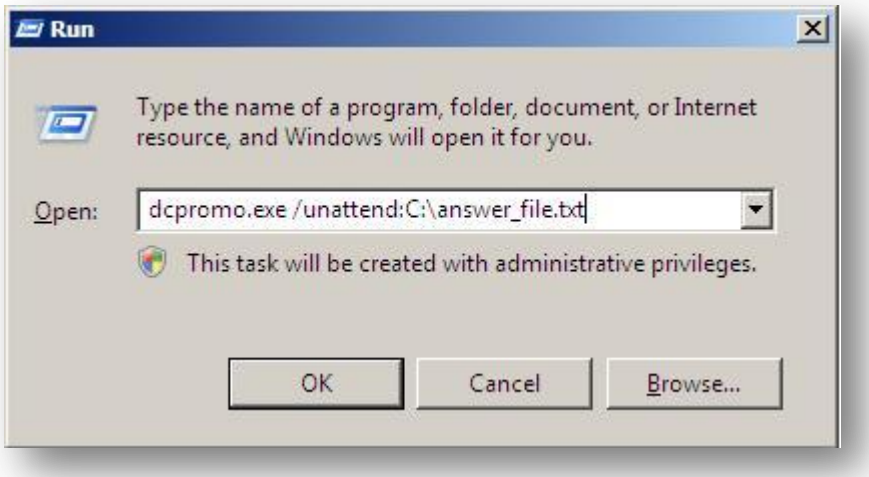
```
; DCPROMO unattended file
; Usage:
; dcpromo.exe /unattend:C:\answer_file.txt
; or dcpromo.exe /answer:\answer_file.txt
;
[DCInstall]
; New forest promotion
ReplicaOrNewDomain=Domain
NewDomain=Forest
NewDomainDNSName=school.gr
ForestLevel=3
DomainNetbiosName=SCHOOL
DomainLevel=3
InstallDNS=Yes
ConfirmGc=Yes
CreateDNSDelegation=No
DatabasePath="C:\Windows\NTDS"
LogPath="C:\Windows\NTDS"
SYSVOLPath="C:\Windows\SYSVOL"
; Set SafeModeAdminPassword to the correct value prior to using the unattend file
SafeModeAdminPassword=MyPassword23$
; Run-time flags (optional)
; RebootOnCompletion=Yes
```

Ας δούμε όμως τι σημαίνουν τα παραπάνω.

- NewDomainDNSName=school.gr νέος τομέας
- ForestLevel=3. Το επίπεδο λειτουργίας του δάσους είναι για Windows 2008 server. Αν είχαμε Windows server 2003 αυτό θα είχε την τιμή 2 και για Windows 2000 θα είχε την τιμή 1.
- DomainNetbiosName=SCHOOL , Αυτό είναι το όνομα του NETBIOS.
- DomainLevel=3 Το επίπεδο λειτουργίας του τομέα είναι για Windows 2008 server. Αν είχαμε Windows server 2003 αυτό θα είχε την τιμή 2 και για Windows 2000 θα είχε την τιμή 1.
- InstallDNS=Yes Εγκατάσταση της υπηρεσίας DNS
- DatabasePath="D:\Windows\NTDS". Που αποθηκεύεται η βάση
  LogPath="D:\Windows\NTDS" Που αποθηκεύονται τα log files
  SYSVOLPath="D:\Windows\SYSVOL" Που αποθηκεύεται το SYSVOL
- SafeModeAdminPassword=MyPassword23$. Όπως ήδη έχουμε αναφέρει ο κωδικός είναι πολύπλοκος.

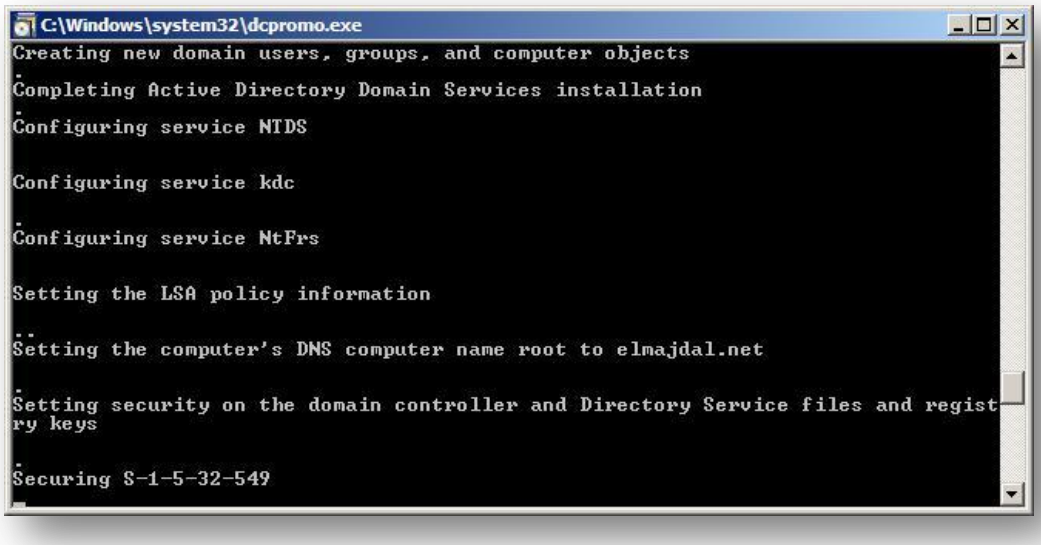
Έχοντας ολοκληρώσει τη παραμετροποίηση του αρχείου μπορούμε να φτιάξουμε πολλούς ελεγκτές τομείς τρέχοντας απλά την παρακάτω εντολή:

dcpromo.exe/unattend:C:\answer_file.txt



Εικόνα 6.2.1: Εκτέλεση Unattended εγκατάστασης

Ξεκινάει η διαδικασία χωρίς εμείς να επέμβουμε πουθενά.



Εικόνα 6.2.2: Διαδικασία unattended εγκατάστασης

Με την ολοκλήρωση ο διακομιστής κάνει μόνος του επανεκκίνηση (RebootOnCompletion=Yes). (Help Microsoft Windows Server 2008)

ΚΕΦΑΛΑΙΟ 7- Ρόλοι διακομιστή

7.1 Διακομιστής DHCP

Το πρωτόκολλο Dynamic Host Configuration Protocol (DHCP) είναι ένα πρωτόκολλο δικτύου το οποίο αναθέτει μέσω ενός διακομιστή αυτόματα και δυναμικά IP διευθύνσεις. Μοιράζει ένα πεδίο (scope) διευθύνσεων το οποίο το καθορίζουμε εμείς.

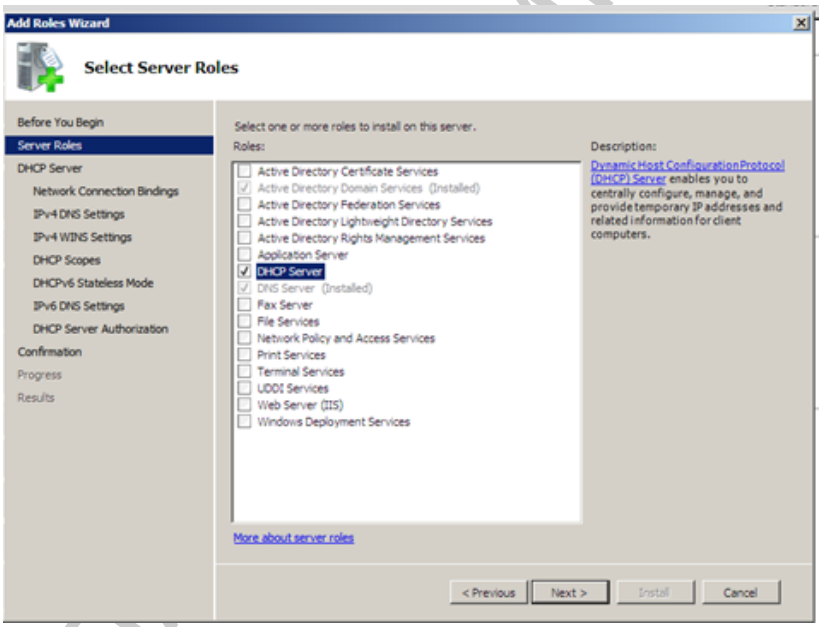
Πλεονεκτήματα του DHCP server:

- Για την υλοποίηση των DHCP υπηρεσιών δεν απαιτείται επιπλέον κόστος λόγω του ότι είναι ενσωματωμένη υπηρεσία των Windows
- Κεντρική, απλούστερη διαχείριση της διευθυνσιοδότησης IP.
- Κεντρική εγκατάσταση προεπιλεγμένης πύλης, μάσκας υποδικτύου και επίθεμα DNS.
- Επειδή το σύστημα εκχωρεί διευθύνσεις IP, αυτό οδηγεί σε λιγότερα λάθη.
- Αποτρέπεται ο διπλασιασμός(duplicate) IP διευθύνσεων.
- Η υπηρεσία DHCP μπορεί να εκχωρήσει διευθύνσεις IP για να φιλοξενεί host και multicast ομάδες.
- Η ενσωμάτωση του DHCP με το Dynamic DNS (DDNS) καθιστά πιο εύκολη τη διαχείριση των IP διευθύνσεων
- Εύκολη παρακολούθηση των διαθέσιμων IP διευθύνσεων και δυνατότητα ειδοποίησης όταν αυτές λιγοστεύουν.
- Η συνεργασία Ενεργού Καταλόγου με τον DHCP server οδηγεί σε μεγαλύτερη ασφάλεια.
- Η δυναμική διευθυνσιοδότηση του DHCP καθιστά πιο ομαλή την μετάβαση από μικρά σε μεγάλα δικτυακά περιβάλλοντα.

Μειονεκτήματα:

- Αν υπάρχει μόνο ένας DHCP server σε ένα δίκτυο και για κάποιο λόγο σταματήσει να λειτουργεί τότε όλο το δίκτυο δεν λειτουργεί.
- Αν ένα δίκτυο έχει πολλά τμήματα (segment) τότε θα πρέπει να εγκαταστήσουμε σε κάθε τμήμα ένα DHCP.
- Τυχόν λανθασμένες διαμορφώσεις μεταδίδονται στους DHCP πελάτες.
- Υπάρχουν κάποιες εφαρμογές οι οποίες δεν λειτουργούν καλά με DHCP server. (http://www.tech-faq.com/understanding-dhcp.html)

Η εγκατάσταση είναι απλή. Στο Server manager επιλέγουμε Add roles και επιλέγουμε DHCP server.



Εικόνα 7.1.1: Προσθήκη ρόλου διακομιστή DHCP

Ακολουθούμε τις οδηγίες του βοηθού εγκατάστασης (wizard) όπου δηλώνουμε τον τομέα στον οποίο ανήκει, τον διαχειριστή και τις IP.

Το πεδίο στο δίκτυό μας έχει ως εξής:

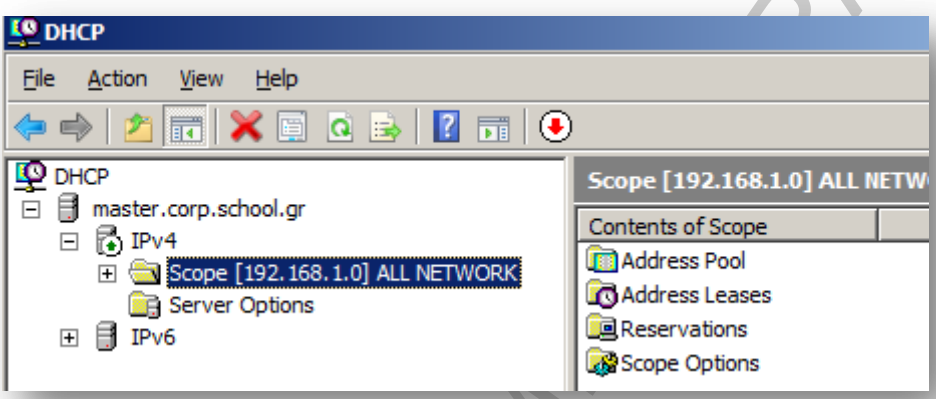
- Ελεγκτής τομέας: στατική IP 192.168.1.79 με μάσκα 255.255.255.0
- Πεδίο δικτύου : Ορίζουμε το πεδίο 192.168.1.1 έως 192.168.1.254
- Πεδίου εκτυπωτών: Οι εκτυπωτές είναι όλοι δικτυακοί με στατικές IP διευθύνσεις από τη 192.168.1.181 ως τη 192.168.1.201. (18 εκτυπωτές για κάθε τμήμα)

- Πεδίο λοιπόν δικτυακών εξοπλισμών : πιθανοί άλλοι ελεγκτές τομέα ή δρομολογητές οι οποίοι επίσης θα πρέπει να έχουν στατικές IP.

Η βασικές ιδιότητες ενός διακομιστή DHCP λοιπόν είναι το address pool όπου καθορίζουμε το εύρος των διαμοιραζόμενων IP. Όταν ένας υπολογιστής συνδέεται στο δίκτυο πέρα από την επικύρωση του χρήστη ζητάει και μια IP διεύθυνση την οποία θα του αποδώσει ο δοακομιστής DHCP. Η απόδοση IP γίνεται τυχαία (random) αρχικά. Στη συνέχεια δε ο κάθε υπολογιστής παίρνει την ίδια IP για 6 μέρες (προεπιλεγμένη τιμή των Windows η οποία μπορεί να αλλάξει).

Όπως βλέπουμε και στην εικόνα 7.1.2 οι βασικές ρυθμίσεις του DHCP server είναι:

- Scope : Πεδίο δικτύου
- Address Pool: Το σύνολο των IP διευθύνσεων που είναι έτοιμος ένας DHCP server να εκχωρήσει
- Address leases: Το σύνολο των μισθωμένων IP διευθύνσεων
- Reservations: IP διευθύνσεις που κρατούνται για συγκεκριμένο σκοπό πχ. για να εκχωρηθεί ως στατική σε κάποιο δρομολογητή.



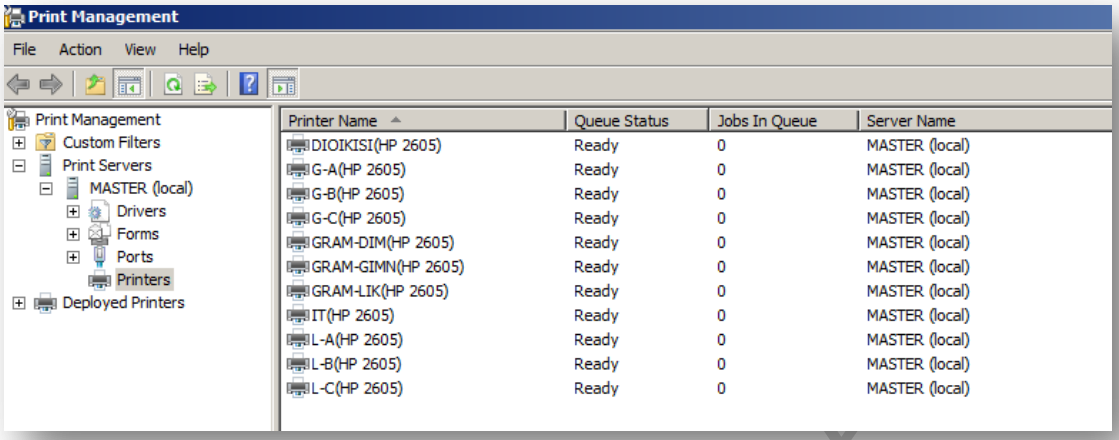
Εικόνα 7.1.2: Διακομιστής DHCP

7.2 Διακομιστής Εκτυπώσεων (Print Server)

Η ανάπτυξη ενός Print Server μπορεί να γίνει με τρεις τρόπους και να επιφέρει αντίστοιχα πολλά πλεονεκτήματα. Μπορούμε απλά να εγκαταστήσουμε εκτυπωτές μέσω πολιτικών ομάδων κάτι που δεν απαιτεί αλληλεπίδραση με τον εκτυπωτή. Μπορούμε να επιλέξουμε για κάθε εκτυπωτή που εγκαθίσταται σε ένα δίκτυο να εμφανίζεται στον κατάλογο και να επιλέγει ο χρήστης αν θα τον προσθέσει στην λίστα του. Τέλος μπορούμε να εγκαταστήσουμε τον Print Manager και στη κονσόλα του να προσθέσουμε όλους τους εκτυπωτές έτσι ώστε ή να τους αναθέσουμε μέσω πολιτικών στους χρήστες ή να τους εμφανίσουμε στον κατάλογο και να επιλέξουν οι χρήστες. Για την καλύτερη διαχείριση των εκτυπωτών και τον τρόπο με τον οποίο εκτυπώνουν, προσθέτουμε στον ελεγκτή τομέα μας τον ρόλο του διακομιστή εκτυπώσεων (Print Server). Τα βασικά πλεονεκτήματα είναι δύο:

- Εγκατάσταση όλων τον οδηγών εγκατάστασης των εκτυπωτών κεντρικά στον διακομιστή για να μη χάνουμε χρόνο σε αναζήτηση.
- Κεντρική και εύκολη διαχείριση εκτυπωτών και εκτυπώσεων.

Αρχικά προσθέτουμε τον ρόλο του διακομιστή εκτυπώσεων. Στη συνέχεια ανοίγουμε το Administrative Tools και επιλέγουμε Print Management για να ανοίξει η κονσόλα. Εδώ ξεκινάμε και κάνουμε εγκατάσταση τους εκτυπωτές και τους οδηγούς εγκατάστασης (εικ. 7.2.1). Θα παρατηρήσουμε ότι στους οδηγούς εγκατάστασης θα πρέπει να υπάρχει ένα αρχείο .inf που θα ενημερώνει για το μοντέλο του εκτυπωτή. Το πρόβλημα εδώ είναι ότι μερικές κατασκευάστριες εταιρείες έχουν δημιουργήσει αυτόματους οδηγούς εγκατάστασης (.exe αρχείο) το οποίο δεν συνεργάζεται με τον print Manager. (http://www.petri.co.il/windows-2008-print-server-management.htm).

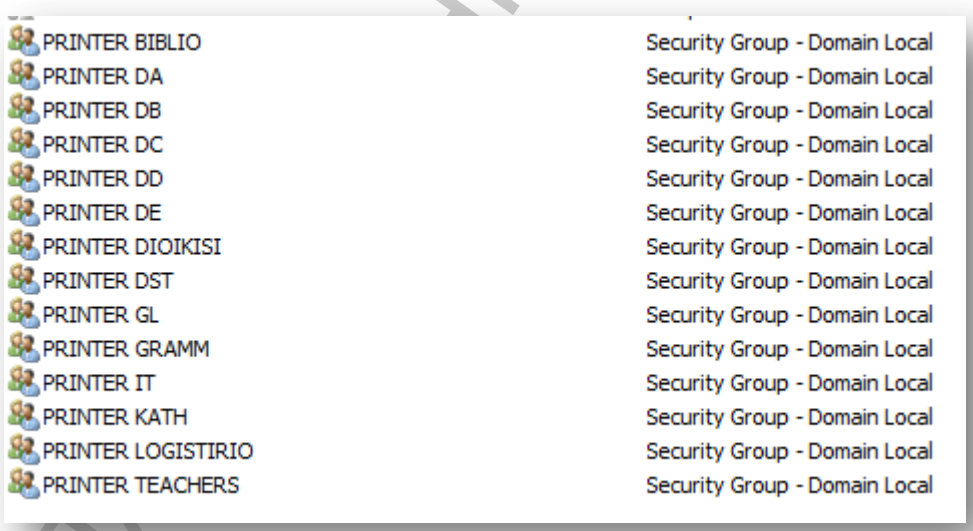


Εικόνα 7.2.1: Διαχειριστής εκτυπώσεων

Αφού ολοκληρώσουμε την εγκατάσταση όλων των δικτυακών εκτυπωτών στο print management ενεργοποιούμε την επιλογή list in directory για να έχουμε την δυνατότητα να τους αναζητούμε παντού στο δίκτυο.

Η λύση των πολιτικών ομάδων μας δίνει την δυνατότητα να αναθέσουμε κατευθείαν σε υπολογιστή ή χρήστη έναν εκτυπωτή. Αν η ανάθεση γίνει σε χρήστη (User Configuration\Preferences\ControlPanel\Printer) έχουμε και την επιλογή να θέσουμε προεπιλεγμένο εκτυπωτή. Αν η ανάθεση γίνει σε υπολογιστή δεν μπορούμε να επιλέξουμε τον προεπιλεγμένο εκτυπωτή.

Στη συνέχεια δημιουργούμε ομάδες υπολογιστών για κάθε τάξη –τμήμα (μέλη των ομάδων είναι οι υπολογιστές των αντίστοιχων τμημάτων) όπως φαίνεται και στην εικόνα 7.2.2 και αναθέτουμε σε κάθε υπολογιστή έναν και μόνο εκτυπωτή.



Εικόνα 7.2.2: Δημιουργία ομάδων εκτυπώσεων

7.3 Διακομιστής αρχείων (File Server)

Στα Windows Server 2008 περιλαμβάνεται η υπηρεσία αρχείων Distributed File System (DFS), η οποία παρέχει στους πελάτες καλύτερη και απλούστερη πρόσβαση σε δεδομένα και αρχεία. Το DFS Replication (DFS-R) αναπαράγει μερικές αλλαγές αρχείων για να κρατήσει πολλαπλά

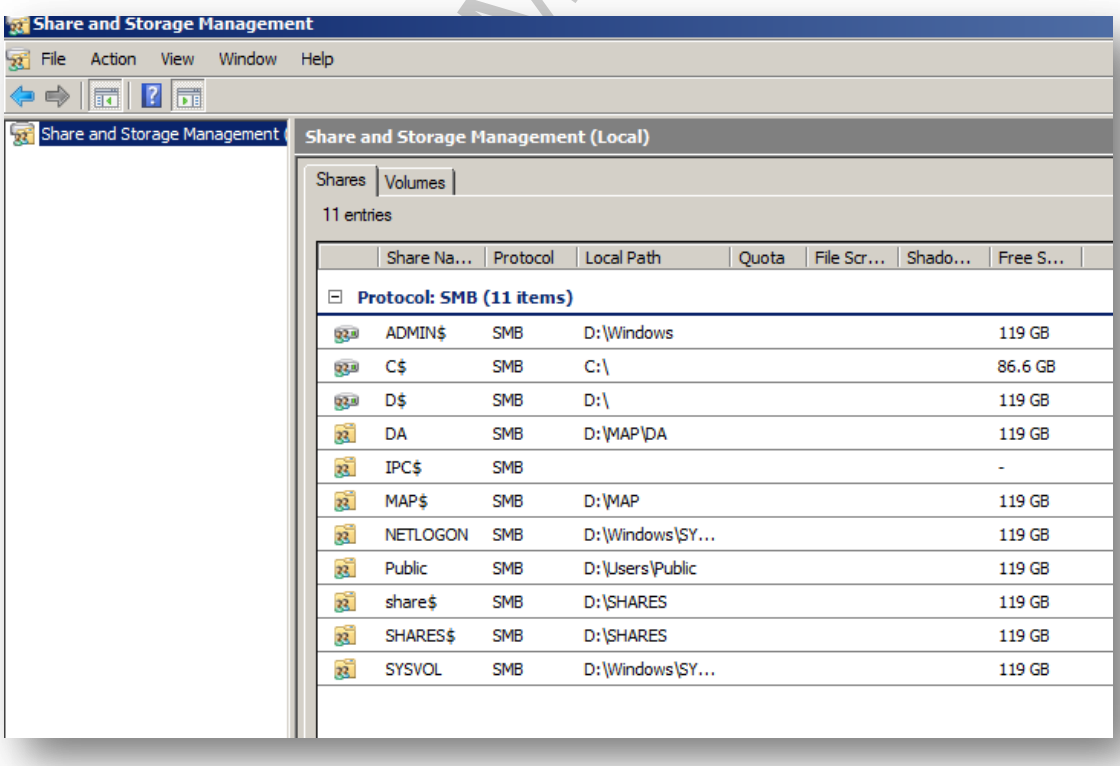
αντίγραφα αρχείων στο synchronization. Το DFS Namespaces (DFS-N) δημιουργεί κοινόχρηστα αρχεία επιτρέποντας στους χρήστες να έχουν πρόσβαση στα δεδομένα τους χωρίς να γνωρίζουν που βρίσκονται.

Τα βασικά πλεονεκτήματα του διακομιστή αρχείων είναι:

- Καλύτερη πρόσβαση σε δεδομένα
- Υποστήριξη φακέλων ανακατεύθυνσης
- Υποστήριξη cluster
- Φακέλους και αρχεία μόνο για ανάγνωση
- Κεντρική διαχείριση κοινόχρηστων φακέλων και αρχείων

Προσθέτουμε τον ρόλο του File server στον διακομιστή μας όπου στην συνέχεια αντιστοιχίζουμε δικαιώματα σε φακέλους και χρήστες. Ο file server είναι υπεύθυνος για την σωστή κοινή χρήση αρχείων. Στην εικόνα 7.3 βλέπουμε ότι μέσω του Share and Storage Management μπορούμε να επεξεργαστούμε όλους τους κοινόχρηστους φακέλους. Κάνοντας διπλό κλικ πάνω σε ένα αντικείμενο βλέπουμε τι ιδιότητες του έχουμε αναθέσει και μπορούμε να τις αλλάξουμε. Τοποθετώντας σε ένα κοινόχρηστο φάκελο την ονομασία του και στο τέλος το σύμβολο $ του δίνουμε την ιδιότητα κρυφού κοινόχρηστου φακέλου. Μπορούμε να επιλέξουμε σε κάθε φάκελο τους χρήστες που θα μπορούν να το βλέπουν αλλά και τι δικαιώματα έχουν σε αυτόν. Οι επιλογές που έχουμε σε κάθε κοινόχρηστο φάκελο είναι:

- Πλήρης Έλεγχος
- Τροποποίηση
- Ανάγνωση και εκτέλεση
- Λίστα περιεχομένων φακέλου
- Ανάγνωση
- Εγγραφή
- Ειδικά δικαιώματα
  (http://www.microsoft.com/windowsserver2008/en/us/file-print.aspx)
  (Help Microsoft Windows Server 2008)

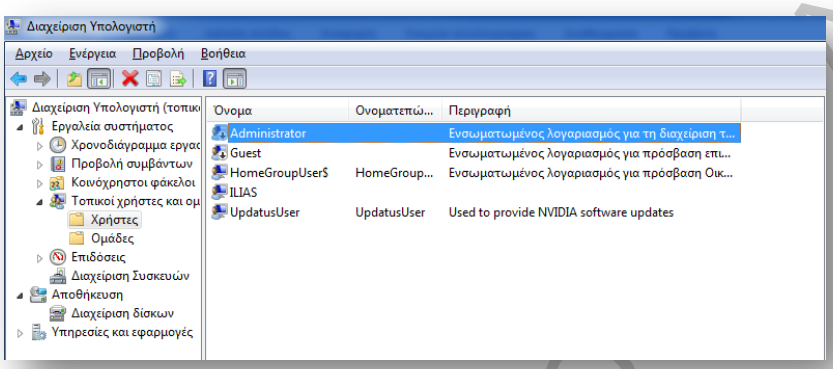


Εικόνα 7.3: Διαχείριση κοινόχρηστων φακέλων

ΚΕΦΑΛΑΙΟ 8 - Πολιτικές υπολογιστών

8.1 Μετονομασία και αλλαγή κωδικού τοπικού διαχειριστή

Την πρώτη φορά που κάνουμε εγκατάσταση ένα λειτουργικό σύστημα σε έναν υπολογιστή δημιουργούνται δύο χρήστες ο guest και ο administrator. Αυτοί οι δύο χρήστες είναι τοπικοί δηλαδή υπάρχουν μόνο στον συγκεκριμένο υπολογιστή. Για παράδειγμα ο υπολογιστής του σπιτιού μας που δεν ανήκει σε ένα τομέα έχει τους ενσωματωμένους χρήστες administrator και guest (συνήθως απενεργοποιημένους στα Windows 7) και μπορούμε να φτιάξουμε και εμείς χρήστες με τα αντίστοιχα δικαιώματα. Αυτοί οι χρήστες υπάρχουν και έχουν δικαιοδοσία μόνο στον συγκεκριμένο υπολογιστή. Είναι οι τοπικοί χρήστες (local users). Ο τοπικός διαχειριστής (administrator) έχει πλήρη δικαιώματα στον συγκεκριμένο υπολογιστή.

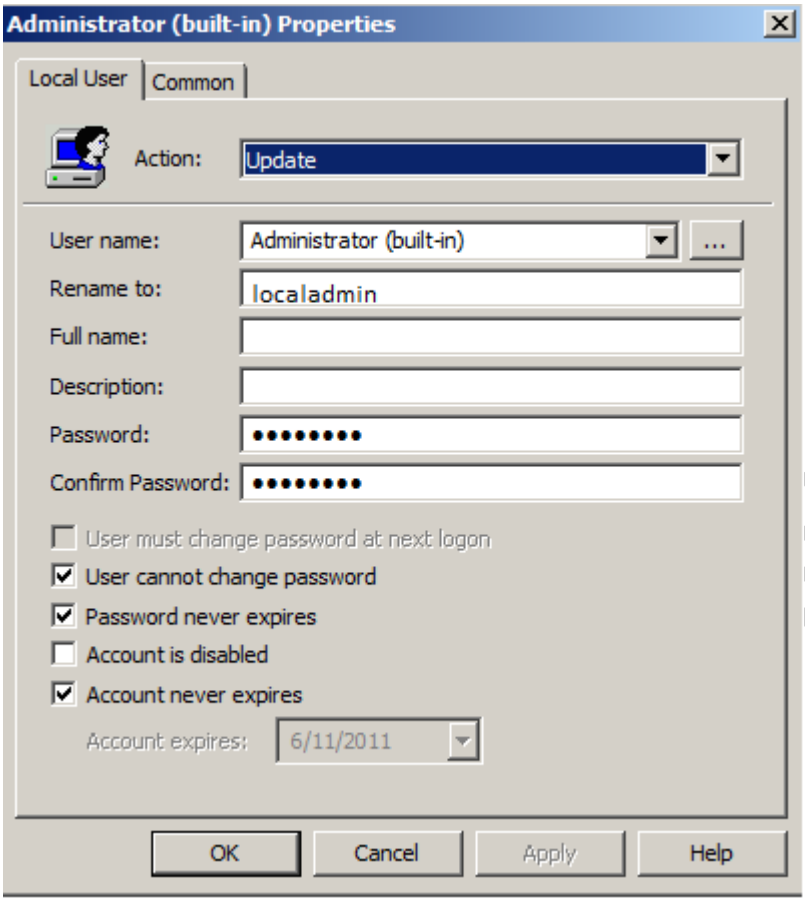


Εικόνα 8.1.1: Τοπικοί Χρήστες

Όταν ο ίδιος υπολογιστής γίνει μέλος σε ένα τομέα (join to domain) δημιουργείται και το προφίλ του χρήστη που ανήκει στον τομέα. Αυτός ο χρήστης είναι χρήστης τομέα (domain user) με δικαιώματα που του έχει αναθέσει ο διαχειριστής του τομέα.

Ο τοπικός διαχειριστής έχει πλήρη δικαιώματα στον τοπικό υπολογιστή. Αν κάποιος γνωρίζει τους κωδικούς μπορεί ακόμα και να βλάψει το μηχάνημα. Είναι επιτακτική ανάγκη λοιπόν να ελέγχουμε και τον κωδικό χρήσης του τοπικού διαχειριστή του κάθε μηχανήματος για την αποφυγή εσκεμμένων επιθέσεων στον τομέα μας.

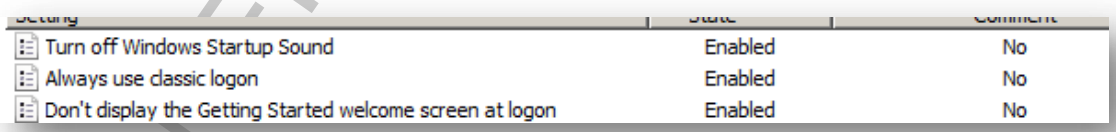
Δημιουργήσαμε λοιπόν μία οργανωτική μονάδα την οποία την ονομάσαμε SCHOOL COMPUTERS και μεταφέραμε εκεί όλους τους υπολογιστές. Στη συνέχεια δημιουργήσαμε μια πολιτική με την οποία όλοι οι υπολογιστές να έχουν σαν τοπικό διαχειριστή τον χρήστη localadmin και κωδικό local. Η πολιτική αυτή βρίσκεται στο Computer Configuration\Preferences\Control Panel\ Local Users and Computers.



Εικόνα 8.1.2: Αλλαγή τοπικού διαχειριστή

8.2 Οθόνη Σύνδεσης (Log on screen)

Κατά την σύνδεσή μας σε ένα υπολογιστή που ανήκει σε ένα τομέα βλέπουμε την οθόνη σύνδεσης που συνήθως εμφανίζει τα πλαίσια για να πληκτρολογήσουμε το όνομα χρήστη και τον κωδικό πρόσβασης. Μέσα από πολιτική θέτουμε όλους τους υπολογιστές να ανοίγουν στην κλασική οθόνη, να μην ακούγεται ο ήχος εκκίνησης των windows, και να μη εμφανίζεται η οθόνη Καλωσήρθατε. Αυτές οι επιλογές βρίσκονται στο Computer Configuration\AdministrativeTemplates\System\Logon.

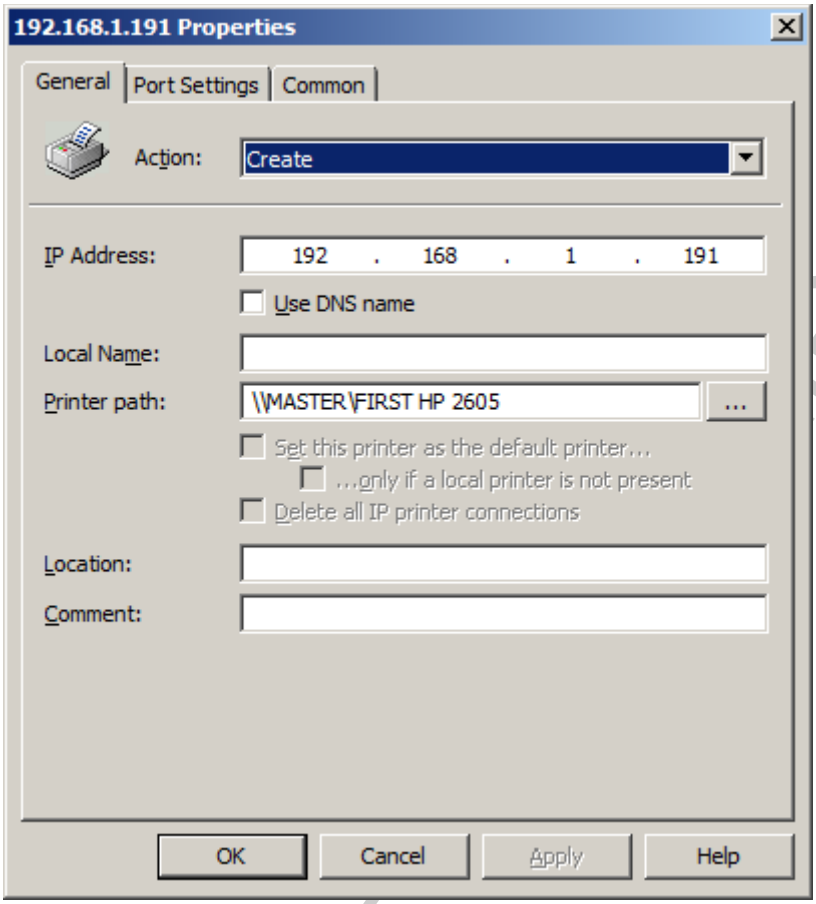


Εικόνα 8.2.1: Επιλογές οθόνης σύνδεσης

8.3 Εγκατάσταση εκτυπωτών

Ο εκτυπωτής που θα τυπώνει ο κάθε χρήστης θα πρέπει να είναι χωροταξικά ο πιο κοντινός του. Για παράδειγμα ένας καθηγητής ο οποίος διδάσκει σε πολλές αίθουσες θα πρέπει κάθε φορά να μπορεί να τυπώνει στον εκτυπωτή της εκάστοτε αίθουσας. Στα Windows 2008 έχουμε την δυνατότητα να εγκαταστήσουμε μέσω πολιτικών ομάδων στον χρήστη τον προεπιλεγμένο εκτυπωτή και όχι στον υπολογιστή. Έτσι δημιουργήσαμε για τους μαθητές κάθε τάξης μία ομάδα χρηστών και τους αναθέσαμε τον προεπιλεγμένο εκτυπωτή. Για τους καθηγητές δημιουργήσαμε

μία ομάδα έτσι ώστε να έχουν προεπιλεγμένο εκτυπωτή τον εκτυπωτή που βρίσκεται στο γραφείο τους και δικαίωμα επιλογής των άλλων. Στα υπόλοιπα τμήματα τυπώνει ο καθένας στο γραφείο. Όπως βλέπουμε στην εικόνα 7.2.1 με την βοήθεια του διαχειριστή εκτυπώσεων έχουμε προσθέσει όλους τους εκτυπωτές του δικτύου μαζί με τους οδηγούς τους. Στη συνέχεια (εικόνα 7.2.2) δημιουργήσαμε τις ομάδες προς εκτύπωση. Τέλος δημιουργούμε τις πολιτικές μέσα από το User Configuration\ Preferences\ControlPanel\Printer.



Εικόνα 8.3: Εγκατάσταση εκτυπωτή μέσω πολιτικών

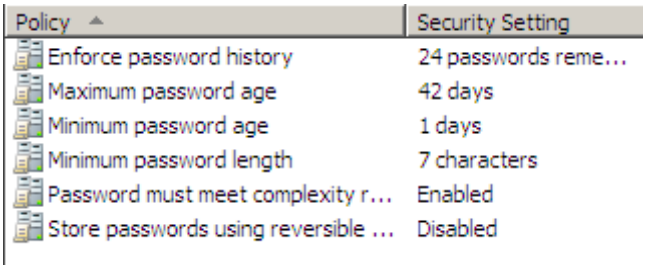
ΚΕΦΑΛΑΙΟ 9 -Πολιτικές χρηστών

9.1 Κωδικοί Πρόσβασης

Η πρώτη πολιτική που θα πρέπει να τεθεί είναι η πολιτική των κωδικών πρόσβασης και κλειδώματος λογαριασμού. Σε προηγούμενα λειτουργικά συστήματα της Microsoft η δυνατότητα δημιουργίας διαφορετικών κωδικών ανά ομάδα και το κλείδωμα των λογαριασμών χρηστών πραγματοποιούνταν με τη βοήθεια του Default Domain Policy. Για διαφορετικές πολιτικές έπρεπε να δημιουργηθούν φίλτρα ή πολλαπλοί τομείς. Στα Windows 2008 πολιτική fine- grained password policy απλοποίησε την όλη διαδικασία. Η πολιτική fine-grained password αποτελείται από τις εξής κλάσεις αντικείμενα:

- Password Settings Container. Αποθηκεύει το Password Settings objects (PSOs) του τομέα.
- Password Settings. Ρυθμίσεις κωδικών.

Η Microsoft έχει δημιουργήσει προεπιλεγμένες πολιτικές για τους κωδικούς ασφαλείας με στόχο την ασφάλεια του συστήματος.

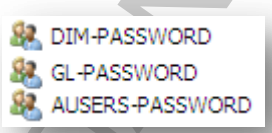


Εικόνα 9.1.1:Προεπιλεγμένες ρυθμίσεις κωδικών

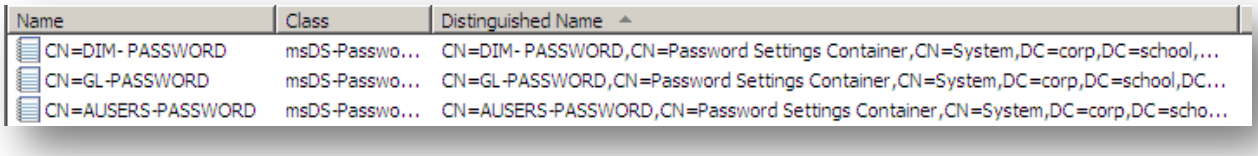
Όπως παρατηρούμε από την παραπάνω εικόνα έχουμε τις εξής επιλογές:

- Ιστορικό κωδικού (Enforced password history). Καθορίζουμε το πόσες φορές πρέπει να αλλαχτεί ένας κωδικός πριν ξαναχρησιμοποιηθεί. Η τιμή ορίζεται από 0 ως 24 κωδικούς.
- Μέγιστη ηλικία – διάρκεια κωδικού (Maximum password age). Καθορίζουμε τη μέγιστη ηλικία του κωδικού από 0 μέρες (δεν λήγει ποτέ) μέχρι 999 μέρες. Η προεπιλεγμένη τιμή είναι 42 μέρες.
- Ελάχιστη ηλικία – διάρκεια κωδικού (Minimum password age). Καθορίζουμε την μικρότερη σε μέρες λειτουργίας του κωδικού. Αυτή η τιμή πρέπει να είναι μεταξύ 0 και 998 μέρες. Θα πρέπει δε να είναι πάντοτε μικρότερη από την Μέγιστη ηλικία.
- Ελάχιστο μήκος κωδικού (Minimum length password). Καθορίζει τον αριθμό των αλφαριθμητικών χαρακτήρων που απαρτίζουν τους κωδικούς. Η τιμή του μπορεί να είναι από 0 ως 14 χαρακτήρες ενώ η προεπιλεγμένη τιμή του είναι 7.
- Πολυπλοκότητα κωδικών (Password must meet complexity requirements). Καθορίζει την πολυπλοκότητα ενός κωδικού. Αν είναι ενεργοποιημένη τότε ένας κωδικός θα πρέπει να περιέχει τους παρακάτω κανόνες:
    1. Να μην περιλαμβάνεται στον κωδικό το όνομα χρήστη ή δύο συνεχόμενα γράμματα του ονόματος.
    2. Να αποτελείται από τουλάχιστον έξι χαρακτήρες
    3. Να περιέχει χαρακτήρες από τις εξής κατηγορίες:
        i. Κεφαλαία αγγλικά (A ως Z)
        ii. Πεζά αγγλικά (a ως z)
        iii. Αριθμούς από το 0 ως το 9.
        iv. Μη αριθμητικούς χαρακτήρες όπως !, @, #, $, …
- Κρυπτογραφημένη αποθήκευση κωδικού (Store password using reversible encryption). Η συγκεκριμένη επιλογή κάνει αναστρέψιμη κρυπτογράφηση στους κωδικούς. Προτείνεται να είναι απενεργοποιημένη εκτός αν υπάρχουν χρήστες που μπαίνουν απομακρυσμένα μέσω διαδικτύου και επιβάλλεται υψηλή ασφάλεια.

Για το δίκτυό μας δημιουργήσαμε τρεις ομάδες χρηστών. Οι μαθητές δημοτικού οι οποίοι δεν έχουν κωδικό, οι μαθητές γυμνασίου – λυκείου που έχουν απλό κωδικό έξι χαρακτήρων και όλοι οι υπόλοιποι χρήστες οι οποίοι ακλουθούν την πολιτική της πολυπλοκότητας κωδικού με μόνη διαφορά ότι δεν λήγει ποτέ. Οι πολιτικές ανατέθηκαν στις ομάδες μέσω PSO. (Help Microsoft Windows Server 2008)



Εικόνα 9.1.2: Δημιουργία ομάδων κωδικών



Εικόνα 9.1.3: Δημιουργία PSO

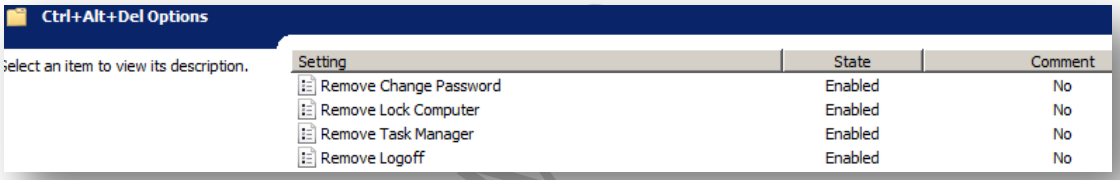
Στο παράρτημα Α μπορούμε να δούμε όλη την διαδικασία δημιουργίας κωδικών.

9.2 Πολιτικές CTRL+ALT+DEL

Όταν σε ένα υπολογιστή πατήσουμε CTRL+ALT+DEL εμφανίζονται οι παρακάτω επιλογές

- Κλείδωμα υπολογιστή
- Αποσύνδεση
- Αλλαγή κωδικού
- Έναρξη Διαχείρισης Εργασιών

Στους μαθητές δεν θα πρέπει να λειτουργεί ο συνδυασμός CTRL+ALT+DEL ενώ σε όλους τους άλλους χρήστες θα λειτουργεί. Προσθέτουμε μία πολιτική στις ομάδες των μαθητών όπου απενεργοποιούμε τις επιλογές του CTRL+ALT+DEL. Πηγαίνουμε λοιπόν στο User Configuration\Administrative Templates\System\CTRL+ALT+DEL.

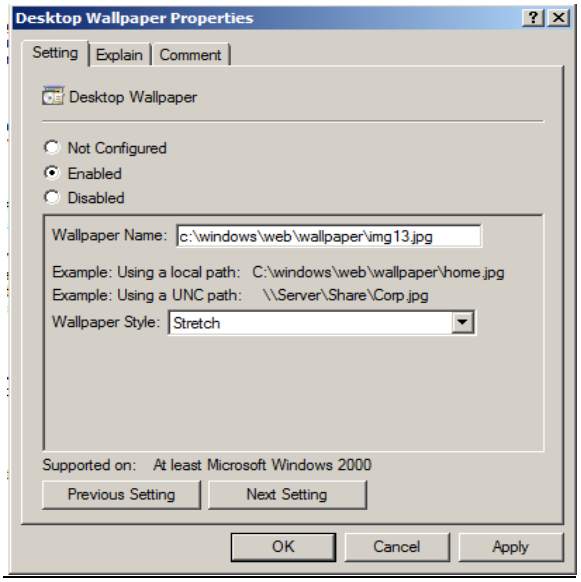


Εικόνα 9.2: Επιλογές CTRL+ALT+DEL

9.3 Πολιτικές επιφάνειας εργασίας

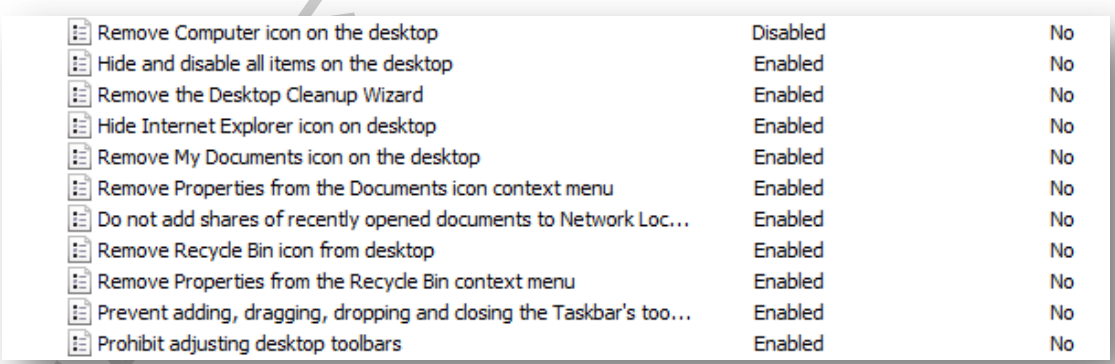
Στους μαθητές του δημοτικού θα βάλουμε συγκεκριμένες επιλογές. Θα παραμετροποιήσουμε την επιφάνεια εργασίας τους έτσι ώστε να μη γίνονται λάθη λόγω απειρίας. Στο User Configuration\Policies\Administrative Templates\Desktop\ Start menu and Taskbar έχουμε τις επιλογές που θέλουμε. Ας τα δούμε όμως μερικές από αυτές.

- Δήλωση συγκεκριμένης ταπετσαρίας σε όλους τους χρήστες του δημοτικού. Η εικόνα βρίσκεται τοπικά στην ίδια διαδρομή σε κάθε υπολογιστή.



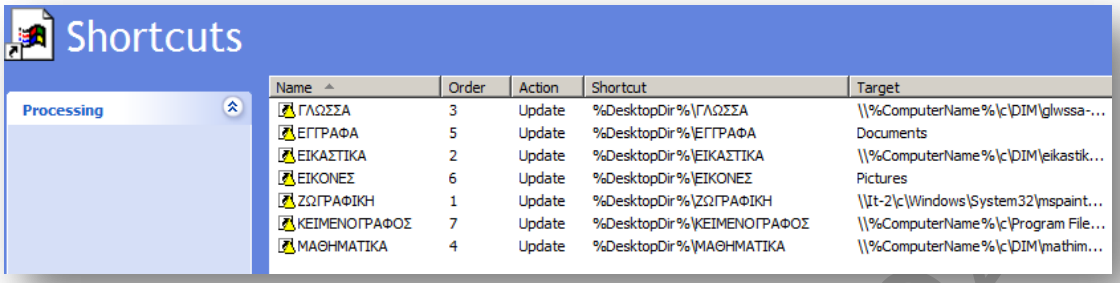
Εικόνα 9.3.1: Δημιουργία κοινής επιφάνειας εργασίας

- Απενεργοποιούμε την χρήση του δεξί κλικ του ποντικιού .
- Απόκρυψη όλων των εικονιδίων από την επιφάνεια εργασίας (τα έγγραφά μου, internet explorer…) εκτός από το Ο Υπολογιστής μου.
- Κλειδώνουμε το μενού εκκίνησης να εμφανίζει μόνο τον φάκελο τα έγγραφά μου και τις εικόνες μου.
- Κλειδώνουμε την task bar να έχει μόνο την ώρα και τη γλώσσα του πληκτρολογίου.
- Τέλος το μόνο που βλέπουν οι μαθητές του δημοτικού και μπορούν μα επεξεργαστούν είναι οι συντομεύσεις των παρακάτω εφαρμογών:
    - εφαρμογές των μαθημάτων τους από το παιδαγωγικό ινστιτούτο
    - την ζωγραφική των Windows
    - Τα έγγραφά μου
    - Τις εικόνες μου
    - Τον υπολογιστή μου από όπου βλέπουν τον δίσκο αντιστοίχησής τους.
    - Τον προεπιλεγμένο εκτυπωτή της τάξης τους.



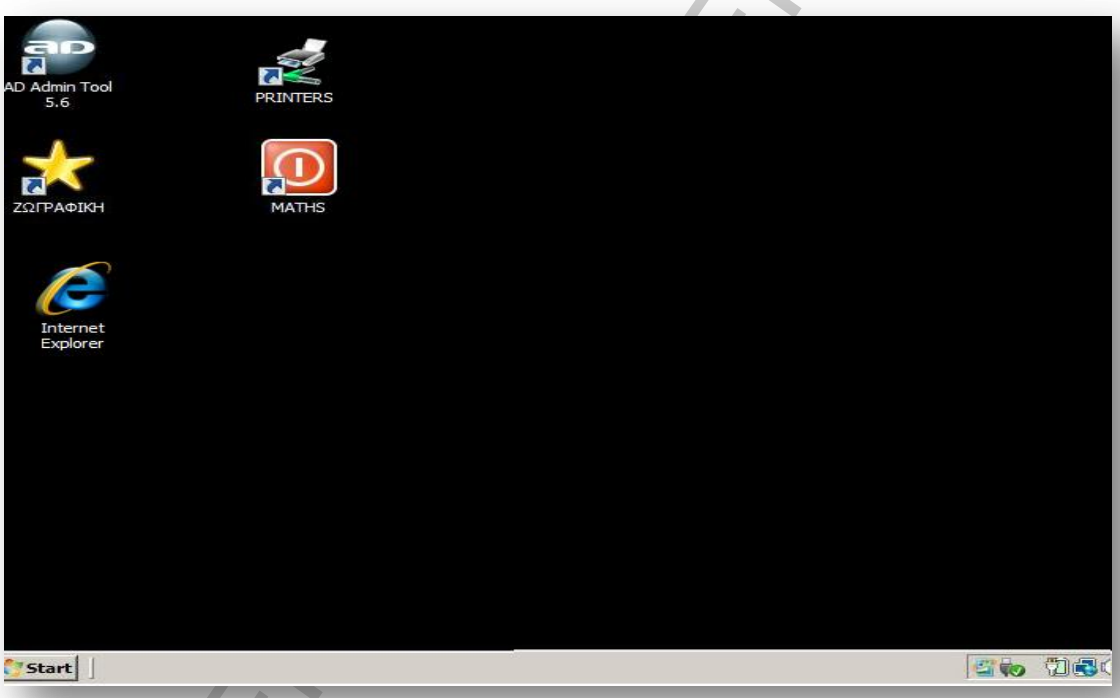
Εικόνα 9.3.2: Πολιτικές επιφάνειας εργασίας

Αφού ολοκληρώσουμε τις επιλογές μας στη συνέχεια τοποθετούμε τις συντομεύσεις των εφαρμογών που θα λειτουργούν. Στο User Configuration\Preferences\Windows Settings\Shortcuts τις συντομεύσεις των χρηστών στην επιφάνεια εργασίας.



Εικόνα 9.3.3: Δημιουργία συντομεύσεων στην επιφάνεια εργασίας

Όταν ανοίγει τον υπολογιστή του ένας μαθητής βλέπει την εικόνα 9.3.4 χωρίς να έχει άλλες επιλογές. Με παρόμοιο τρόπο παραμετροποιούμε την επιφάνεια εργασίας των υπόλοιπων χρηστών.



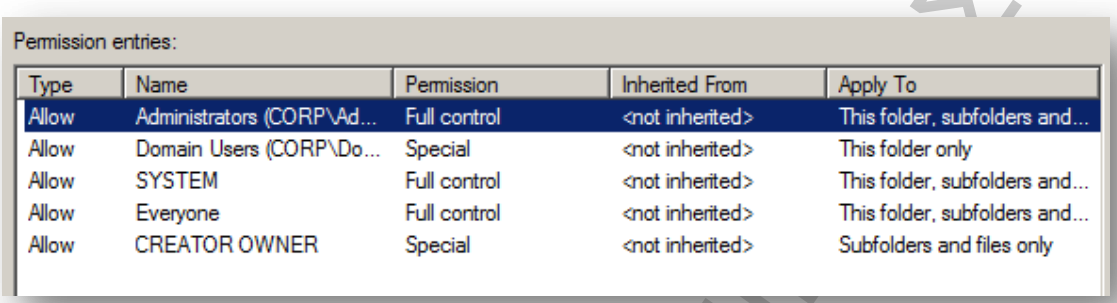
Εικόνα 9.3.4: Επιφάνεια εργασίας μαθητών

9.4 Αντιστοίχιση δίσκων (MAP DRIVES)

Δημιουργώντας δίσκους αντιστοίχισης ουσιαστικά δίνουμε ένα drive letter (c:, d:) σε ένα κοινόχρηστο φάκελο που βρίσκεται στο δίκτυο. Με τον τρόπο αυτό δημιουργούμε εύκολη πρόσβαση σε πόρους του δικτύου. Πριν την ύπαρξη των GPOs για να δημιουργήσουμε ένα δίσκο αντιστοίχησης έπρεπε να χρησιμοποιήσουμε την εντολή net use U: \\users\da. Τώρα πια δεν χρειάζεται να αποστηθίζουμε ή να ψάχνουμε τις εντολές και την σύνταξή τους.

Για την σωστή διαχείριση των φακέλων που διαμοιράζουμε στο δίκτυο θα πρέπει να οργανώσουμε πρώτα τα δικαιώματα σε κάθε φάκελο έτσι ώστε να υπάρχει πρόσβαση σε κάθε φάκελο μόνο από εξουσιοδοτημένους χρήστες αλλά και προς αποφυγή λάθους (σβήσιμο αρχείων). Θα πρέπει να ακολουθήσουμε τα παρακάτω βήματα:

- Δημιουργία πολιτικών για συγκεκριμένους χρήστες που θα βλέπουν τον δίσκο αντιστοίχησης. Θα πρέπει να δοθούν στον φάκελο NTFS δικαιώματα ως εξής:
  - Creator Owner: Full Control, Subfolders and Files Only
  - Administrator: None
  - Security group of users needing to put data on share: List Folder/Read Data, Create Folders/Append Data - This Folder Only
  - Everyone: No permissions
  - Local System: Full Control, This Folder, Subfolders and Files


Permission entries:

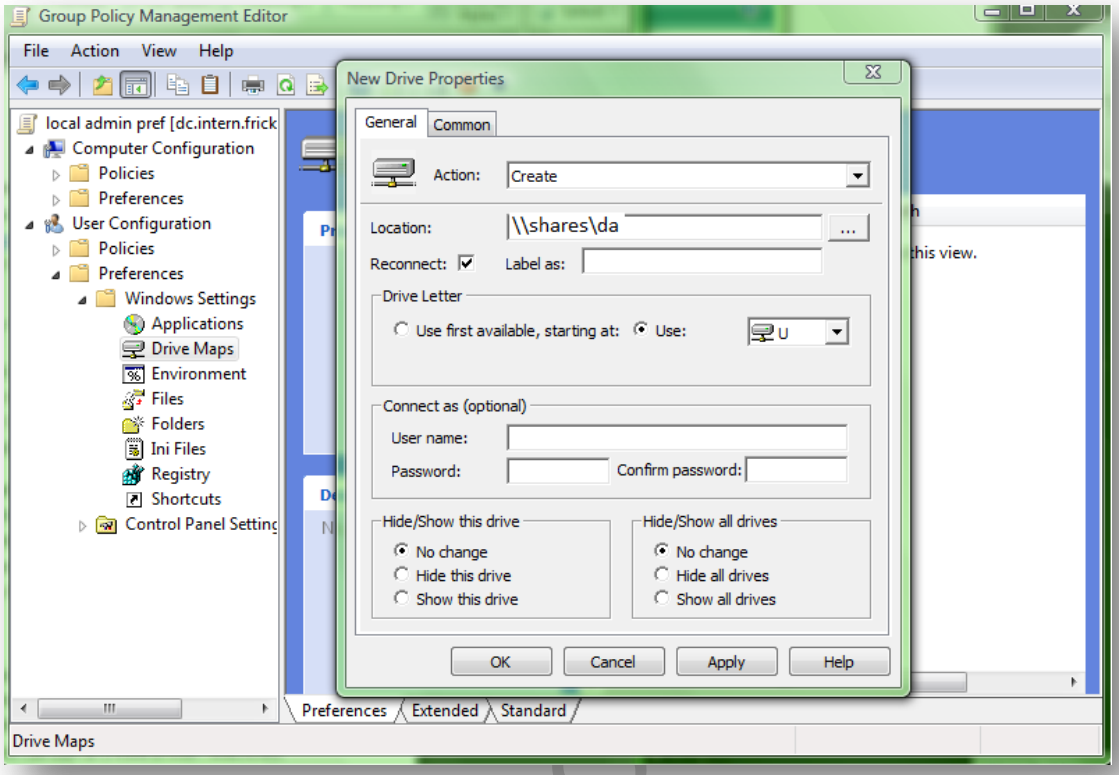
Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (CORP\Ad...	Full control	<not inherited>	This folder, subfolders and...
Allow	Domain Users (CORP\Do...	Special	<not inherited>	This folder only
Allow	SYSTEM	Full control	<not inherited>	This folder, subfolders and...
Allow	Everyone	Full control	<not inherited>	This folder, subfolders and...
Allow	CREATOR OWNER	Special	<not inherited>	Subfolders and files only

Εικόνα 9.4.1: Δημιουργία δικαιωμάτων φακέλων

- Αφού δημιουργήσουμε τον φάκελο που θα μοιράσουμε στο δίκτυο, τον ονομάζουμε map$. Με τον συμβολισμό $ δεν φαίνεται ο φάκελος στο My network places.

Στον τομέα μας λοιπόν για εύκολη και γρήγορη πρόσβαση σε κοινόχρηστους φακέλους δημιουργούμε μέσα στο φάκελο map υποφακέλους για κάθε τμήμα. Έτσι στον φάκελο DA έχουν πρόσβαση οι μαθητές του δημοτικού της πρώτης τάξης και ο δάσκαλός τους. Εκεί υπάρχει ένας υποφάκελος *Μόνο για ανάγνωση* όπου οι μαθητές μπορούν μόνο να αναγνώσουν ενώ ο δάσκαλος έχει πλήρη δικαιώματα, και ένας υποφάκελος *full* στον οποίο έχουν πλήρη πρόσβαση και οι μαθητές. Αντίστοιχα για κάθε τάξη και τμήμα δημιουργείτε και από ένας φάκελος.

Για την δημιουργία δίσκου αντιστοίχισης μέσω πολιτικών ομάδων τρέχουμε το gpmc.msc και στη συνέχεια ακολουθούμε την διαδρομή User Configuration\Preferences\ Windows Settings. Δεξί κλικ στο Drive Maps και τον δημιουργούμε. Μπορούμε να δημιουργήσουμε, να αντικαταστήσουμε, να αναβαθμίσουμε ή ακόμα και να διαγράψουμε ένα drive letter. Θα πρέπει δε να ορίσουμε την διαδρομή του φακέλου στο δίκτυο, το drive letter που του αναθέτουμε, το αν θα συνδέεται κάθε φορά που ο χρήστης συνδέεται στο δίκτυο και ίσως κάποια ετικέτα.



Εικόνα 9.4.2: Δημιουργία Map drive

9.5 Πολιτικές φακέλου ανακατεύθυνσης και προφίλ περιαγωγής. (Folder redirection and roaming profile)

Το προφίλ του κάθε χρήστη δημιουργείται τοπικά την πρώτη φορά που συνδέεται στον υπολογιστή. Περιλαμβάνει τις ρυθμίσεις και τα αρχεία του και βρίσκεται στον φάκελο users. Για να υπάρχει πρόσβαση σε αυτά από όλους τους υπολογιστές του δικτύου η Microsoft έχει προτείνει δύο τεχνολογίες των οποίων ο συνδυασμός επιφέρει τα μέγιστα αποτελέσματα χρήσης: τα προφίλ περιαγωγής (roaming profiles) και τον φάκελο ανακατεύθυνσης (folder redirection).

Ο φάκελος ανακατεύθυνσης επιτρέπει στους διαχειριστές να ανακατευθύνουν την πορεία ενός φακέλου σε μια νέα θέση, ενώ το προφίλ περιαγωγής μεταφέρει το φάκελο του προφίλ σε μια διαφορετική θέση. Η θέση μπορεί να είναι ένας φάκελος στον τοπικό υπολογιστή ή ένας κοινόχρηστος φάκελος στο δίκτυο. Οι χρήστες μπορούν να εργαστούν από οποιοδήποτε υπολογιστή στο δίκτυο χωρίς να χρειάζεται να μεταφέρουν αρχεία ή ρυθμίσεις.

Οι φάκελοι οι οποίοι μπορούν να ανακατευθυνθούν είναι:

- AppData/Roaming
- Contacts
- Desktop
- Documents
- Downloads
- Favorites
- Links
- Music
- Pictures
- Saved Games

- Searches
- Start Menu
- Videos

Θα πρέπει να γίνει με προσοχή η επιλογή φακέλων που θα οδηγηθούν στον φάκελο ανακατεύθυνσης και αυτό γιατί θα πρέπει να υπολογιστεί τόσο η χωρητικότητα των δεδομένων αλλά και η άσκοπη κυκλοφορία στο δίκτυο. Για παράδειγμα ο φάκελος Video θα πρέπει να βρίσκεται στον φάκελο ανακατεύθυνσης ή όχι. Φυσικά εξαρτάται από τις εργασίες των χρηστών αλλά σε αυτό το σημείο θα πρέπει να γνωρίζουμε ότι αν επιλέξουμε όλους τους φακέλους θα χρειαστούμε αντίστοιχα μεγάλο αποθηκευτικό χώρο.

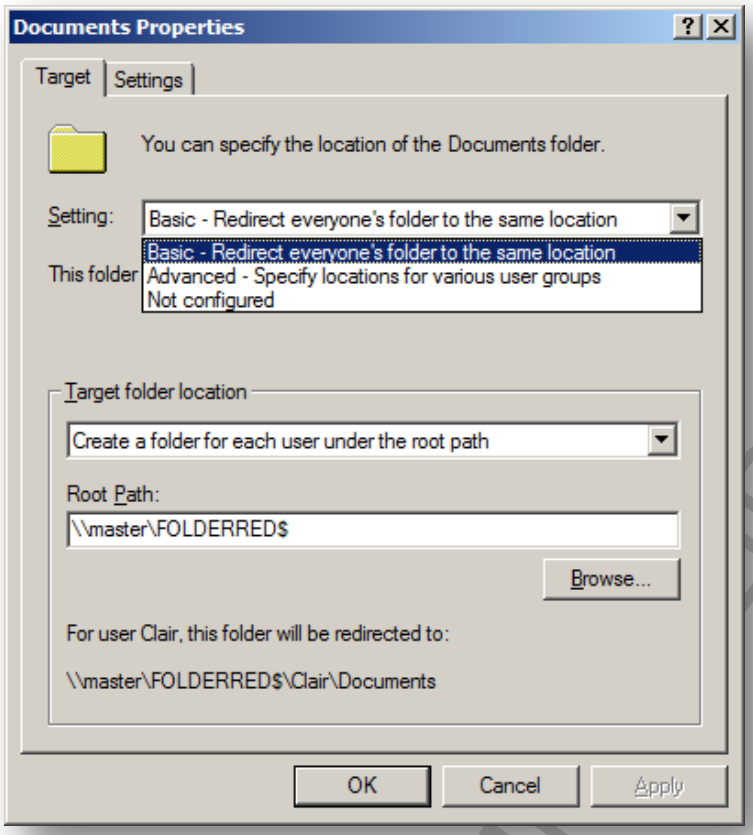
Τα πλεονεκτήματα του φακέλου ανακατεύθυνσης είναι τα εξής:

- Τα δεδομένα του χρήστη είναι διαθέσιμα σε όποιο υπολογιστή του δικτύου και αν βρίσκεται.
- Η τεχνολογία off line file (αρχεία χωρίς σύνδεση) δίνει τη δυνατότητα πρόσβασης στα δεδομένα ακόμα και αν το δίκτυο δεν λειτουργεί. Αυτό γίνεται γιατί κάθε φορά που ο χρήστης συνδέεται σε ένα τομέα από έναν υπολογιστή τότε αυτό κάνει συγχρονισμό τον αντίστοιχο φάκελο ανακατεύθυνσης. Ουσιαστικά δημιουργεί και τοπικά τον λογαριασμό του χρήστη και αντιγράφει εκεί ότι βρίσκεται στον φάκελο ανακατεύθυνσης. Αν το δίκτυο σταματήσει να λειτουργεί ο χρήστης εξακολουθεί να εργάζεται τοπικά και όταν επανέλθει το δίκτυο γίνεται συγχρονισμός δεδομένων.
- Ο συνδυασμός roaming profile (προφίλ περιαγωγής) και φακέλου ανακατεύθυνσης κάνει ταχύτερη την σύνδεση και την αποσύνδεση των χρηστών μιας και ο συγχρονισμός γίνεται στο παρασκήνιο και όχι κατά την σύνδεση ή την αποσύνδεση.
- Τα δεδομένα του χρήστη για ασφάλεια μπορούν να ανακατευθυνθούν σε άλλο τμήμα (partition) ή δίσκο από αυτό που βρίσκεται το λειτουργικό σύστημα.
- Ο φάκελος ανακατεύθυνσης και ο φάκελος των προφίλ είναι εύκολα διαχειρίσιμοι από τον διαχειριστή για να δημιουργεί αντίγραφα ασφαλείας αλλά και για να προσδιορίζει την ποσότητα σε χώρο αποθήκευσης ανά χρήστη.

Πριν προχωρήσουμε στη δημιουργία των πολιτικών θα πρέπει αρχικά να δημιουργήσουμε τους φακέλους τους οποίους θα τους κάνουμε κοινόχρηστους. Δημιουργούμε δύο διαφορετικούς φακέλους. Τον φάκελο FOLDERED$ ο οποίος Θα είναι ο φάκελος ανακατεύθυνσης των αρχείων και το φάκελο PROFILES$ όπου θα αποθηκεύονται τα προφίλ των χρηστών. Και στους δύο φακέλους θα πρέπει να δοθούν δικαιώματα πρόσβασης όπως βλέπουμε παρακάτω.

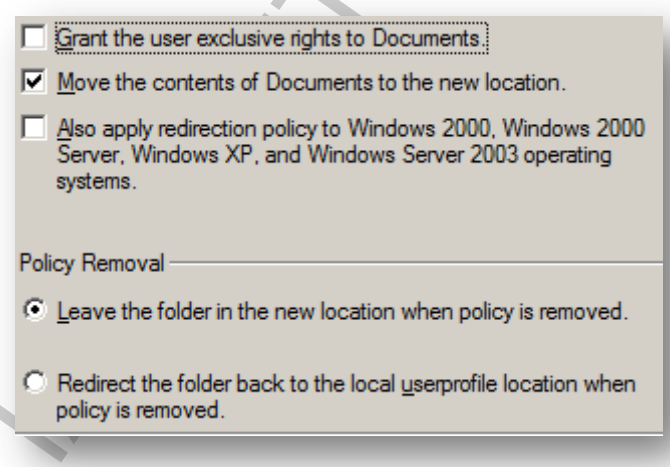
- NTFS δικαιώματα για το προφίλ περιαγωγής του γονικού φακέλου:
  - Creator Owner: Full Control, Subfolders and Files Only
  - Administrator: None
  - Security group of users needing to put data on share: List Folder/Read Data, Create Folders/Append Data - This Folder Only
  - Everyone: No permissions
  - Local System: Full Control, This Folder, Subfolders and Files
- Κοινόχρηστου επιπέδου δικαιώματα (SMB) για το προφίλ περιαγωγής
  - Security group of users needing to put data on share: List Folder/Read Data, Create Folders/Append Data – Full Control
  - Everyone: No permissions
- NTFS δικαιώματα για κάθε φάκελο που περιέχει το προφίλ περιαγωγής του κάθε χρήστη:
  - %Username%: Full Control, Owner of Folder
  - Local System: Full Control
  - Administrators: No Permissions
  - Everyone: No permissions

Για να δηλώσουμε μέσω πολιτικών ομάδων τον φάκελο ανακατεύθυνσης αφού τρέξουμε την εντολή gpmc.msc επιλέγουμε UserConfiguration\Policies\Windows Settings\Folder Redirection**.** Παρατηρούμε ότι η πολιτική για τον φάκελο ανακατεύθυνσης εφαρμόζεται μόνο στους χρήστες (user configuration) και φυσικά θα πρέπει με μεγάλη προσοχή να επιλέξουμε τους φακέλους. Όπως φαίνεται και από την εικόνα 9.5.1 θα πρέπει να επιλέξουμε τον τρόπο αποθήκευσης και να δηλώσουμε το που θα αποθηκεύονται. Εμείς λοιπόν έχουμε επιλέξει να γίνεται ανακατεύθυνση όλων των φακέλων στην ίδια διαδρομή δημιουργώντας όμως για κάθε χρήστη τον δικό του φάκελο.



Εικόνα 9.5.1: Δημιουργία φακέλου ανακατεύθυνσης

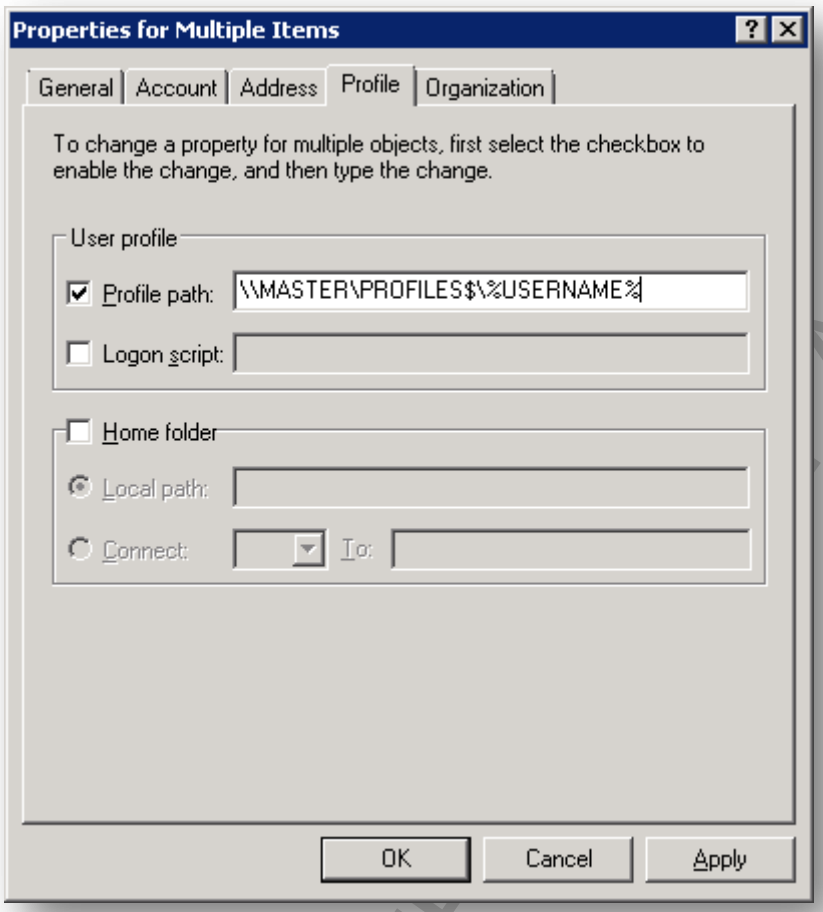
Στις ρυθμίσεις μπορούμε να επιλέξουμε να έχει δικαιώματα και ο διαχειριστής στους φακέλους, να συνεργάζεται και με παλιότερα λειτουργικά και τι θα γίνει αν αφαιρεθεί η πολιτική.



Εικόνα 9.5.2: Ρυθμίσεις φακέλου ανακατεύθυνσης

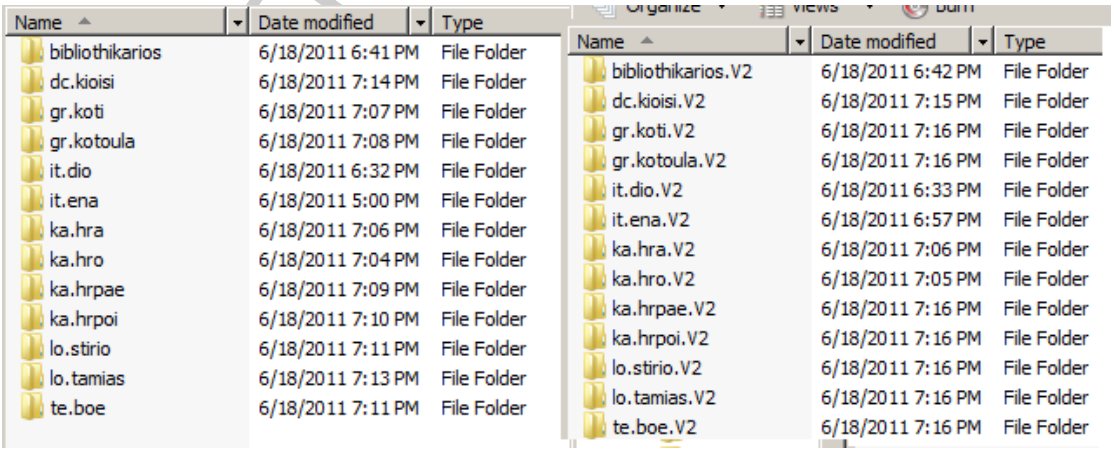
Για τις ανάγκες του δικτύου θα δώσουμε πολιτικές φακέλου ανακατεύθυνσης και προφίλ περιαγωγής σε όλους τους χρήστες εκτός από τους μαθητές. Για να ορίσουμε την διαδρομή του προφίλ περιαγωγής δεν χρειάζεται να πάμε σε κάθε χρήστη ξεχωριστά αρκεί να επιλέξουμε

τους χρήστες που θέλουμε και με δεξί κλικ ανοίγουν οι ιδιότητες πολλαπλών αντικειμένων (Properties for Multiple Items)



Εικόνα 9.5.3:Δημιουργία προφίλ περιαγωγής

Παρατηρούμε ότι στον φάκελο ανακατεύθυνσης δημιουργείται για κάθε χρήστη ένας φάκελος με το όνομά του και αντίστοιχα στον φάκελο με τα προφίλ ένας φάκελος με το όνομα του χρήστη και κατάληξη v2. (Help Microsoft Windows Server 2008)



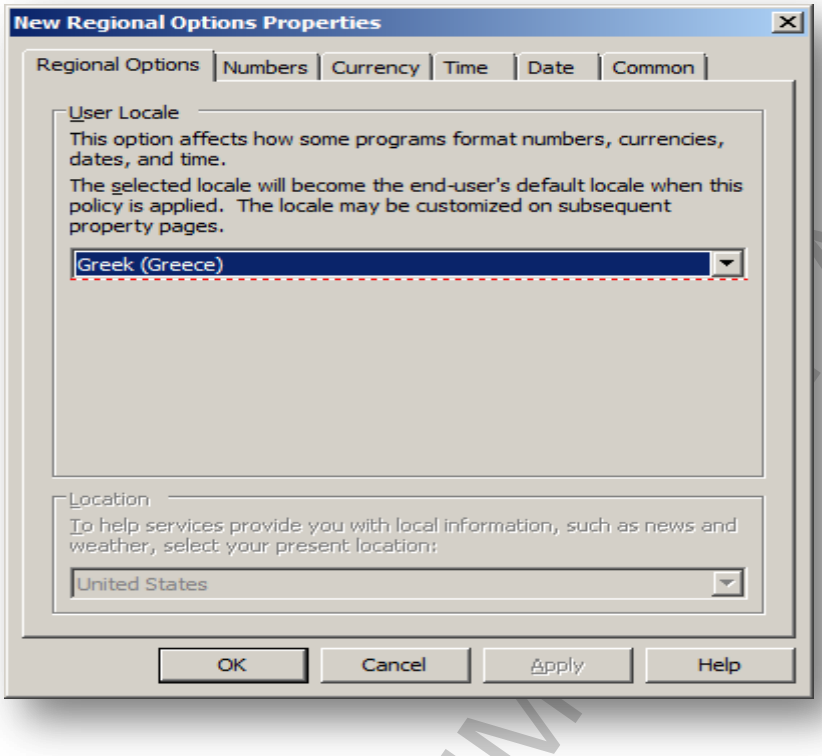
Name	Date modified	Type
bibliothikarios	6/18/2011 6:41 PM	File Folder
dc.kioisi	6/18/2011 7:14 PM	File Folder
gr.koti	6/18/2011 7:07 PM	File Folder
gr.kotoula	6/18/2011 7:08 PM	File Folder
it.dio	6/18/2011 6:32 PM	File Folder
it.ena	6/18/2011 5:00 PM	File Folder
ka.hra	6/18/2011 7:06 PM	File Folder
ka.hro	6/18/2011 7:04 PM	File Folder
ka.hrpae	6/18/2011 7:09 PM	File Folder
ka.hrpoi	6/18/2011 7:10 PM	File Folder
lo.stirio	6/18/2011 7:11 PM	File Folder
lo.tamias	6/18/2011 7:13 PM	File Folder
te.boe	6/18/2011 7:11 PM	File Folder

Name	Date modified	Type
bibliothikarios.V2	6/18/2011 6:42 PM	File Folder
dc.kioisi.V2	6/18/2011 7:15 PM	File Folder
gr.koti.V2	6/18/2011 7:16 PM	File Folder
gr.kotoula.V2	6/18/2011 7:16 PM	File Folder
it.dio.V2	6/18/2011 6:33 PM	File Folder
it.ena.V2	6/18/2011 6:57 PM	File Folder
ka.hra.V2	6/18/2011 7:06 PM	File Folder
ka.hro.V2	6/18/2011 7:05 PM	File Folder
ka.hrpae.V2	6/18/2011 7:16 PM	File Folder
ka.hrpoi.V2	6/18/2011 7:16 PM	File Folder
lo.stirio.V2	6/18/2011 7:16 PM	File Folder
lo.tamias.V2	6/18/2011 7:16 PM	File Folder
te.boe.V2	6/18/2011 7:16 PM	File Folder

Εικόνα 9.5.4: Folder redirection & profile folder

9.6 Regional Settings

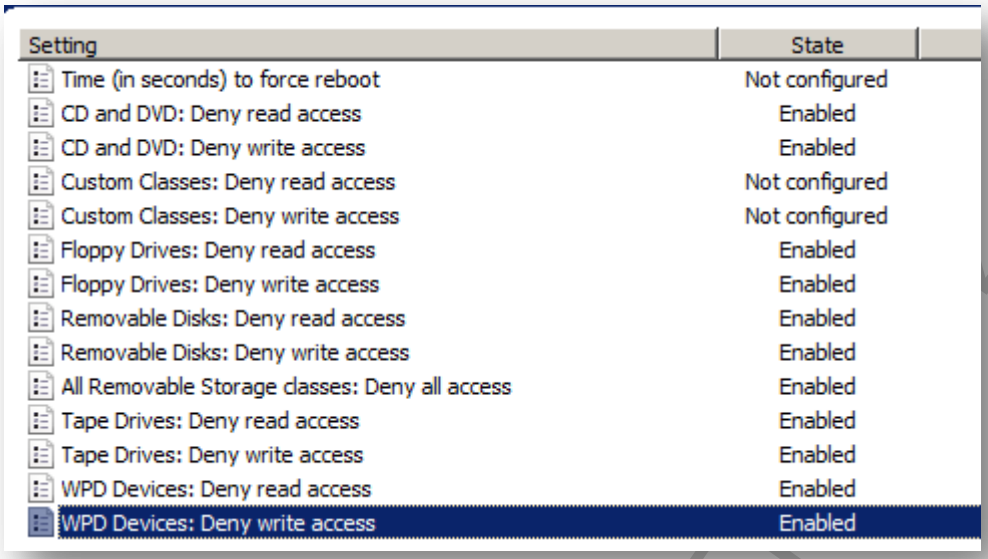
Ορίζουμε με πολιτική την γλώσσα λειτουργίας μαζί με τις ρυθμίσεις (νομισματικές, τρόπος εμφάνισης της ώρας, ημερομηνία…). Η συγκεκριμένη πολιτική μπαίνει μόνο σε χρήστες και όχι σε υπολογιστές.



Εικόνα 9.6: Τοπικές Ρυθμίσεις

9.7 Απενεργοποίηση συσκευών usb, cd-rom, fdd.

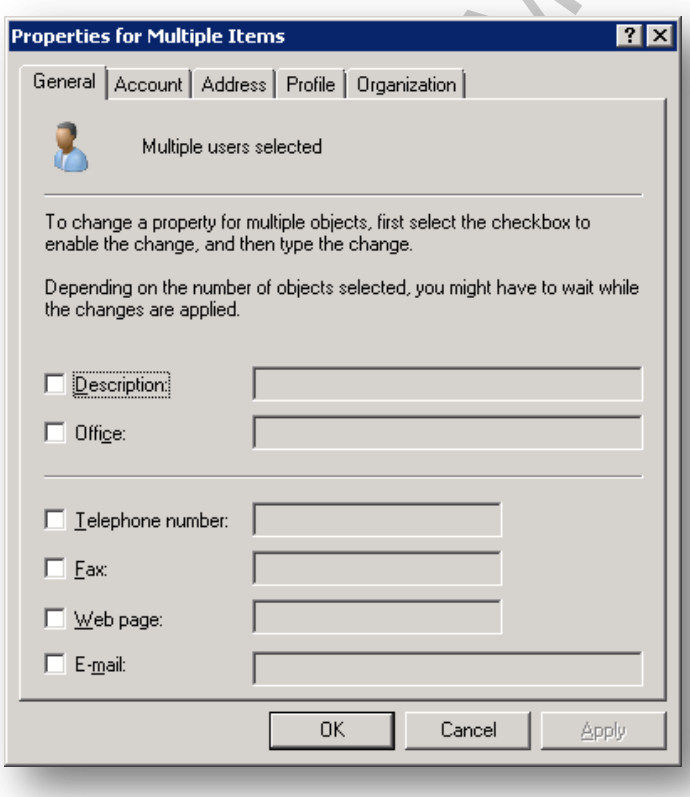
Οι συσκευές usb, cd-rom, fdd είναι συσκευές με τις οποίες μπορούμε εύκολα να αποθηκεύσουμε και να μεταφέρουμε αρχεία από υπολογιστή σε υπολογιστή. Για την προστασία των υπολογιστών απενεργοποιούμε τις λειτουργίες αυτών των συσκευών. Πηγαίνουμε λοιπόν στο User Configuration και επιλέγουμε συγκεκριμένες λειτουργίες. Για παράδειγμα για την ομάδα των μαθητών του δημοτικού επιλέγουμε All removable storage deny access.



Εικόνα 9.7: Ρυθμίσεις εξωτερικών μονάδων αποθήκευσης

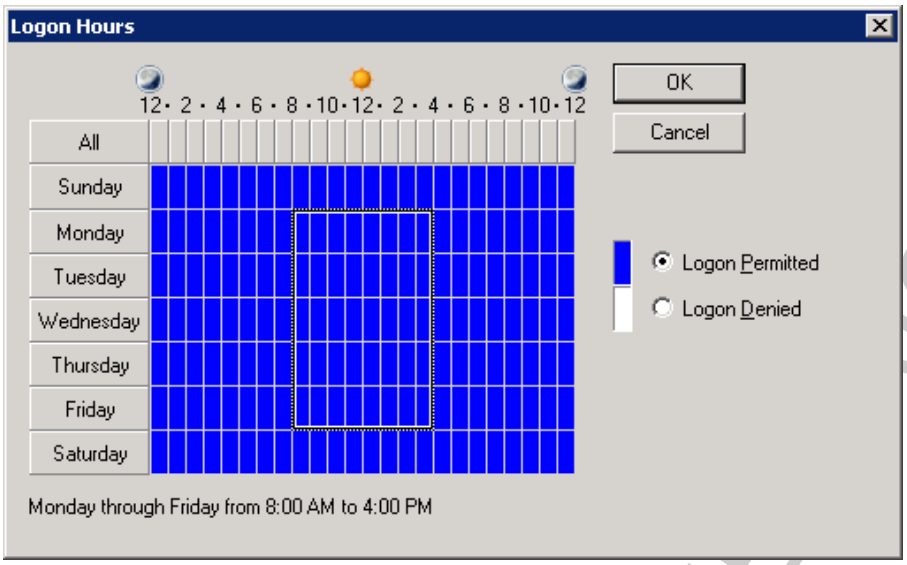
9.8 Ώρες σύνδεσης (Log on hours)

Για μεγαλύτερη ασφάλεια του δικτύου μπορούμε να ορίσουμε τις ώρες τις οποίες μπορεί να συνδέεται ένας χρήστης. Αν θέλουμε να αλλάξουμε την πολιτική σε πολλούς χρήστες ταυτόχρονα, τους επιλέγουμε και με δεξί κλικ πάμε στις ιδιότητες πολλαπλών αντικειμένων.



Εικόνα 9.8.1: Ώρες λειτουργίας χρηστών

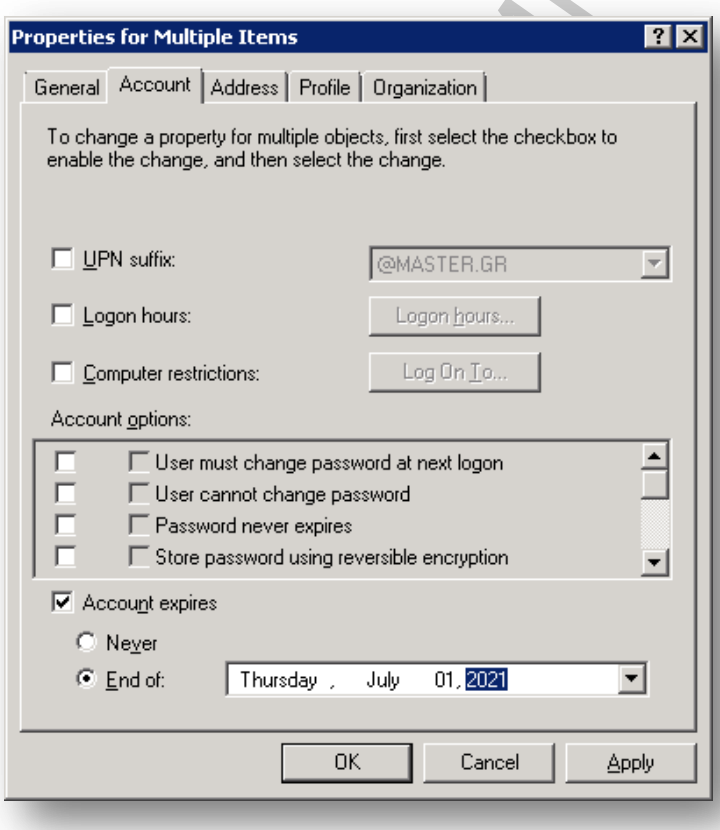
Αναθέτουμε στις ομάδες των μαθητών να μπορούν να συνδέονται στο δίκτυο μόνο τις εργάσιμες μέρες και από τις 8 το πρωί μέχρι τις 4 το απόγευμα.



Εικόνα 9.8.2: Ώρες σύνδεσης μαθητών

9.9 Λήξη λογαριασμού χρήστη

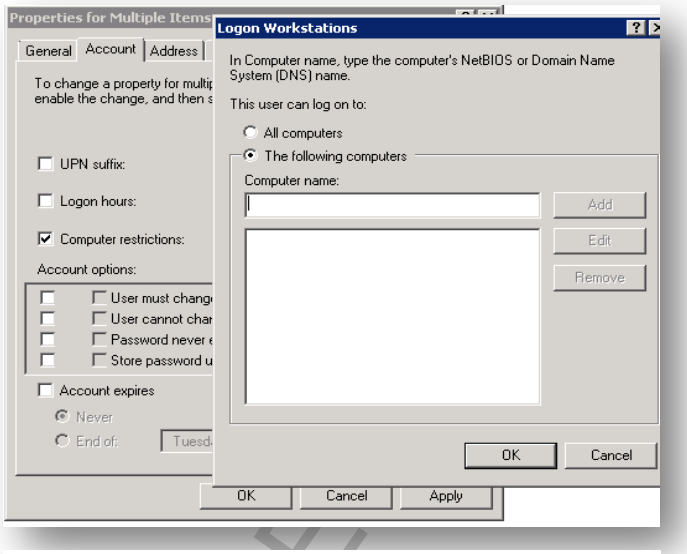
Δημιουργώντας κάθε χρονιά τους μαθητές της πρώτης δημοτικού δηλώνουμε εξαρχής τον χρόνο λήξης του λογαριασμού σε 12 χρόνια.



Εικόνα 9.9: Λήξη λογαριασμού χρηστών

9.10 Περιορισμός πρόσβασης σε υπολογιστές

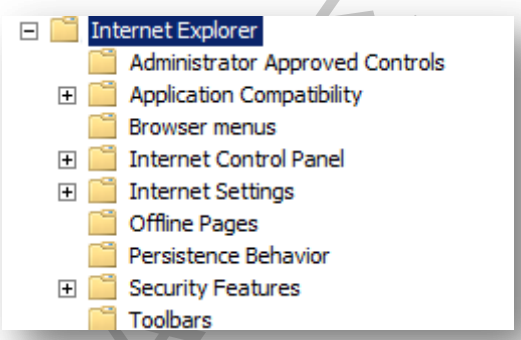
Οι μαθητές, οι καθηγητές και οι δάσκαλοι δεν θα πρέπει να έχουν καμία πρόσβαση στους υπολογιστές της γραμματείας του λογιστηρίου και της διοίκησης. Επιλέγουμε λοιπόν αυτούς τους χρήστες. Με δεξί κλικ στις ιδιότητες τσεκάρουμε την επιλογή Computer Restrictions και στη συνέχεια επιλέγουμε τους υπολογιστές στους οποίους δεν πρέπει να συνδέονται.



Εικόνα 9.10: Computer Restriction

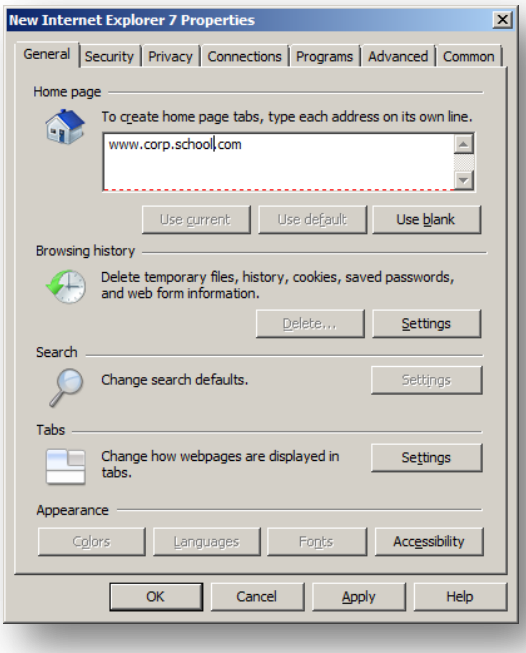
9.11 Ρυθμίσεις Internet Explorer

Για να ρυθμίσουμε παραμέτρους στον Internet Explorer στα Windows server 2008 έχουμε τρεις επιλογές. Το εργαλείο Internet Explorer Maintenance (IEM) που βρίσκεται στο User configuration\Windows Settings, στο User Configuration\Administrative Templates\Windows Componets και στα Preferences. Το IEM δεν μπορεί να επεμβαίνει στις ρυθμίσεις του χρήστη αλλά δεν απαγορεύει στον χρήστη να επέμβει και αυτός. Απλά όταν ξανασυνδεθεί ο χρήστης εμφανίζονται οι ρυθμίσεις που έχουν γίνει με το IEM. Αν θέλουμε οι ρυθμίσεις του internet explorer να είναι υποχρεωτικές θα πρέπει να εργαστούμε στο Administrative templates. Στη συνέχεια βλέπουμε τις επιλογές του internet explorer .



Εικόνα 9.10.1: Επιλογές internet Explorer ανά κατηγορία

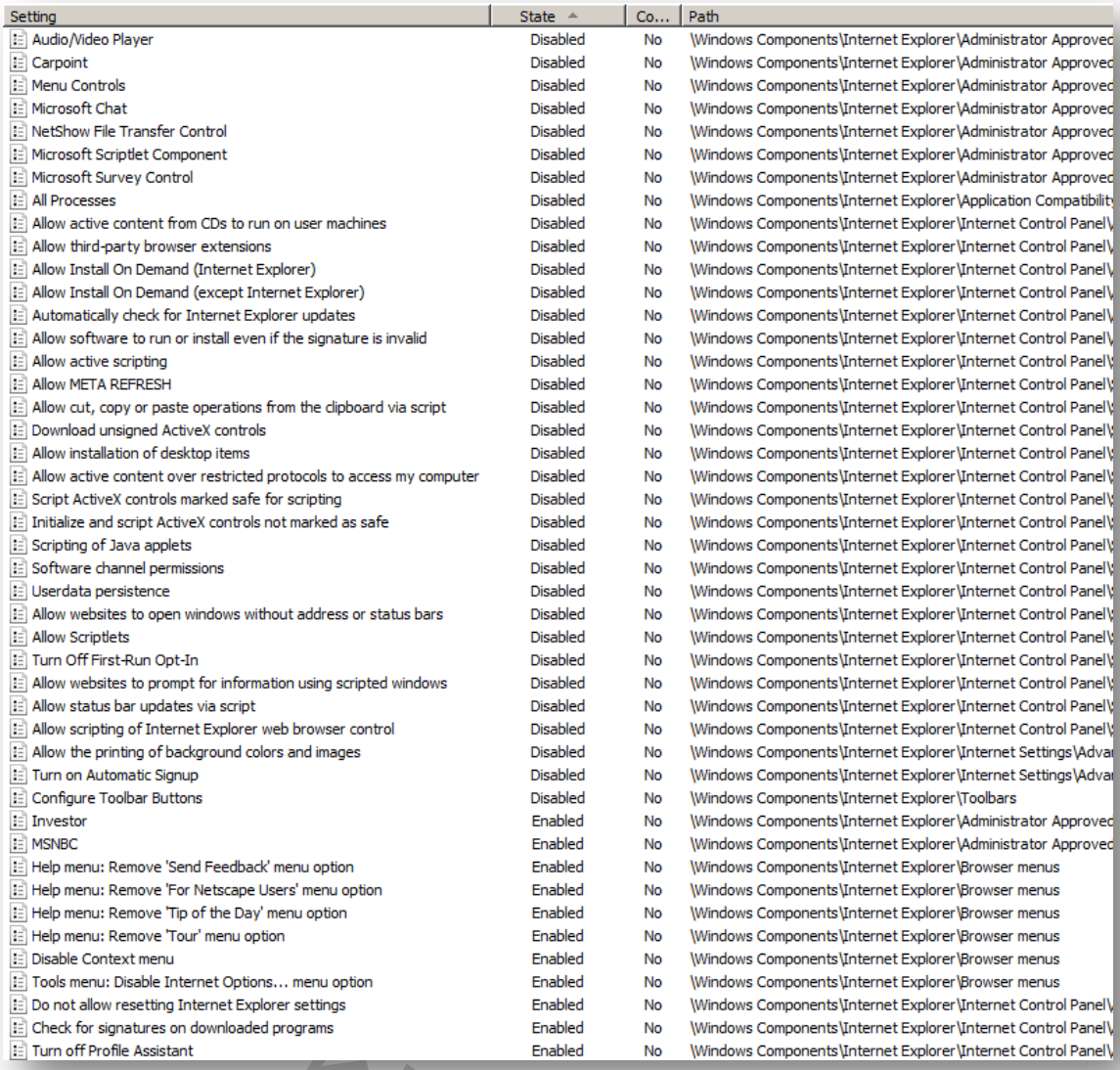
Στα Preferences του User Configuration ορίζουμε τις ιδιότητες του internet explorer όπως φαίνεται και στην εικόνα 9.10.2. Θα ορίσουμε για όλες τις ομάδες χρηστών σαν αρχική σελίδα την σελίδα του σχολείου.



Εικόνα 9.10.2: Ιδιότητες internet explorer

Για τους μαθητές του γυμνασίου και του λυκείου ορίζουμε τις πολιτικές που εμφανίζονται στην εικόνα 9.10.3. Οι μαθητές του δημοτικού δεν έχουν καθόλου πρόσβαση ενώ όλοι οι άλλοι χρήστες έχουν πλήρη πρόσβαση.

Ρυθμίσεις όπως απενεργοποίηση της δημοσίευσης στο internet αρχείων και φακέλων, απενεργοποίηση του download αρχείων από web publishing τοποθεσίες, απενεργοποίηση messenger, απενεργοποίηση του automatic download και πολλές άλλες αυξάνουν την ασφάλεια του δικτύου.



Setting	State	Co...	Path
Audio/Video Player	Disabled	No	\Windows Components\Internet Explorer\Administrator Approved
Carpoint	Disabled	No	\Windows Components\Internet Explorer\Administrator Approved
Menu Controls	Disabled	No	\Windows Components\Internet Explorer\Administrator Approved
Microsoft Chat	Disabled	No	\Windows Components\Internet Explorer\Administrator Approved
NetShow File Transfer Control	Disabled	No	\Windows Components\Internet Explorer\Administrator Approved
Microsoft Scriptlet Component	Disabled	No	\Windows Components\Internet Explorer\Administrator Approved
Microsoft Survey Control	Disabled	No	\Windows Components\Internet Explorer\Administrator Approved
All Processes	Disabled	No	\Windows Components\Internet Explorer\Application Compatibility
Allow active content from CDs to run on user machines	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow third-party browser extensions	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow Install On Demand (Internet Explorer)	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow Install On Demand (except Internet Explorer)	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Automatically check for Internet Explorer updates	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow software to run or install even if the signature is invalid	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow active scripting	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow META REFRESH	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow cut, copy or paste operations from the clipboard via script	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Download unsigned ActiveX controls	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow installation of desktop items	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow active content over restricted protocols to access my computer	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Script ActiveX controls marked safe for scripting	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Initialize and script ActiveX controls not marked as safe	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Scripting of Java applets	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Software channel permissions	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Userdata persistence	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow websites to open windows without address or status bars	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow Scriptlets	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Turn Off First-Run Opt-In	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow websites to prompt for information using scripted windows	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow status bar updates via script	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow scripting of Internet Explorer web browser control	Disabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Allow the printing of background colors and images	Disabled	No	\Windows Components\Internet Explorer\Internet Settings\Advar
Turn on Automatic Signup	Disabled	No	\Windows Components\Internet Explorer\Internet Settings\Advar
Configure Toolbar Buttons	Disabled	No	\Windows Components\Internet Explorer\Toolbars
Investor	Enabled	No	\Windows Components\Internet Explorer\Administrator Approved
MSNBC	Enabled	No	\Windows Components\Internet Explorer\Administrator Approved
Help menu: Remove 'Send Feedback' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Help menu: Remove 'For Netscape Users' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Help menu: Remove 'Tip of the Day' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Help menu: Remove 'Tour' menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Disable Context menu	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Tools menu: Disable Internet Options... menu option	Enabled	No	\Windows Components\Internet Explorer\Browser menus
Do not allow resetting Internet Explorer settings	Enabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Check for signatures on downloaded programs	Enabled	No	\Windows Components\Internet Explorer\Internet Control Panel\
Turn off Profile Assistant	Enabled	No	\Windows Components\Internet Explorer\Internet Control Panel\

Εικόνα 9.10.3. Ρυθμίσεις internet explorer

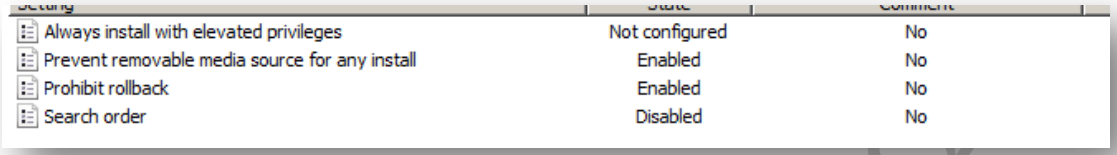
9.12 Απενεργοποίηση δεξί κλικ

Στα Windows με την χρήση του δεξιού κλικ του ποντικιού μας βλέπουμε ιδιότητες φακέλων, αρχείων και λειτουργιών. Για να μη μπορεί ο χρήστης να επέμβει απενεργοποιούμε την λειτουργία του δεξιού κλικ ενεργοποιώντας την επιλογή Remove Windows Explorer's default context menu στο User Configuration\Administrative Templates\Windows Components\Windows Explorer.

9.13 Δυνατότητες εγκατάστασης απεγκατάστασης λογισμικών.

Συχνά οι χρήστες θέλουν να κάνουν εγκατάσταση ένα λογισμικό είτε μέσω cd ή usb είτε κατεβάζοντάς το από το διαδίκτυο. Πολλές φορές αυτά τα λογισμικά είναι επιβλαβή για το δίκτυο (ιοί) ενώ άλλες φορές δημιουργούν καθυστερήσεις. Η πολιτική για τους μαθητές είναι να μη μπορεί κανείς να κάνει εγκατάσταση ή απεγκατάσταση ενός λογισμικού. Όλοι οι μαθητές λοιπόν ανήκουν στους Domains Users οι οποίοι δεν έχουν δικαίωμα εγκατάστασης\απεγκατάστασης.

Όλοι οι υπόλοιποι χρήστες εκτός των administrator ανήκουν στους Power Users. Για να απενεργοποιήσουμε την δυνατότητα εγκατάστασης - απεγκατάστασης λογισμικού δίνουμε επιπλέον πολιτικές σε αυτούς τους χρήστες. Ανοίγοντας τον διορθωτή πολιτικών επιλέγουμε Computer Configuration\Policies\AdministrativeTemplates\WindowsComponents\Windows installer.

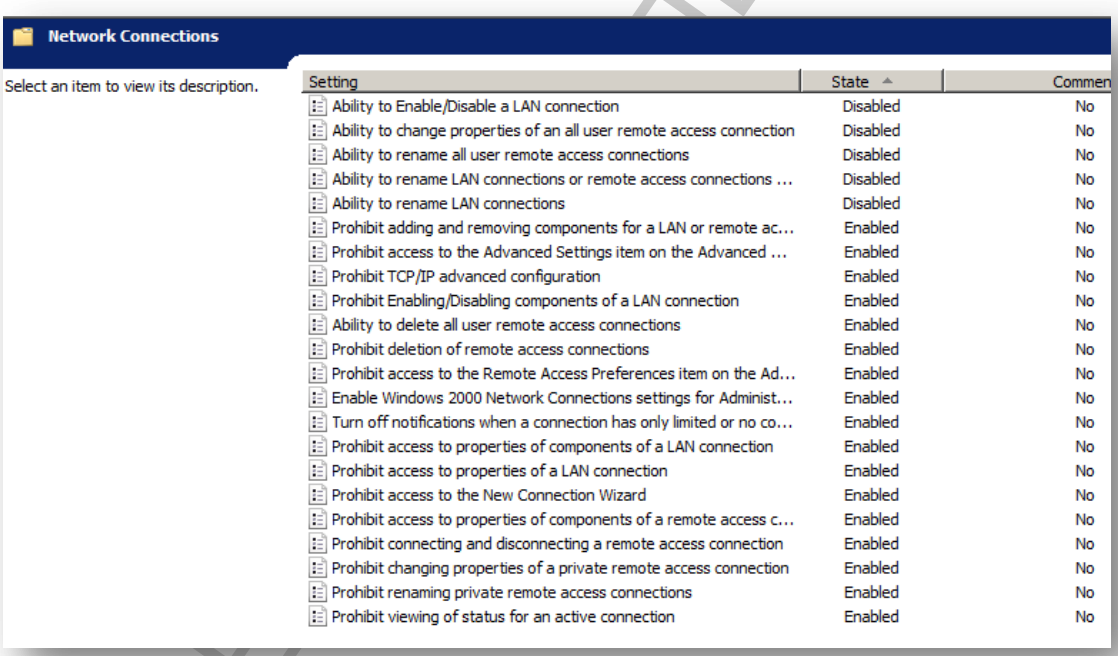


Setting	State	Comment
Always install with elevated privileges	Not configured	No
Prevent removable media source for any install	Enabled	No
Prohibit rollback	Enabled	No
Search order	Disabled	No

Εικόνα 9.12: Windows installer

9.14 Δεν μπορούν να αλλάξουν τις ιδιότητες του δικτύου.

Οι ρυθμίσεις που μπορούν να γίνουν για τις ιδιότητες του δικτύου είναι αρκετές. Για να μη μπορεί ο χρήστης να επέμβει οπουδήποτε στο δίκτυο δεν εμφανίζουμε το εικονίδιο του δικτύου, δεν επιτρέπουμε αλλαγές στο δίκτυο και άλλες επιλογές όπως φαίνεται και στην εικόνα 9.13.



Network Connections

Select an item to view its description.

Setting	State	Comment
Ability to Enable/Disable a LAN connection	Disabled	No
Ability to change properties of an all user remote access connection	Disabled	No
Ability to rename all user remote access connections	Disabled	No
Ability to rename LAN connections or remote access connections ...	Disabled	No
Ability to rename LAN connections	Disabled	No
Prohibit adding and removing components for a LAN or remote ac...	Enabled	No
Prohibit access to the Advanced Settings item on the Advanced ...	Enabled	No
Prohibit TCP/IP advanced configuration	Enabled	No
Prohibit Enabling/Disabling components of a LAN connection	Enabled	No
Ability to delete all user remote access connections	Enabled	No
Prohibit deletion of remote access connections	Enabled	No
Prohibit access to the Remote Access Preferences item on the Ad...	Enabled	No
Enable Windows 2000 Network Connections settings for Administ...	Enabled	No
Turn off notifications when a connection has only limited or no co...	Enabled	No
Prohibit access to properties of components of a LAN connection	Enabled	No
Prohibit access to properties of a LAN connection	Enabled	No
Prohibit access to the New Connection Wizard	Enabled	No
Prohibit access to properties of components of a remote access c...	Enabled	No
Prohibit connecting and disconnecting a remote access connection	Enabled	No
Prohibit changing properties of a private remote access connection	Enabled	No
Prohibit renaming private remote access connections	Enabled	No
Prohibit viewing of status for an active connection	Enabled	No

Εικόνα 9.16. Ρυθμίσεις δικτύου

Οι παραπάνω πολιτικές εφαρμόζονται σε όλους τους χρήστες του δικτύου εκτός από τους διαχειριστές και βρίσκονται στο User Configuration\AdministrativeTemplates\Network.

9.15 Δεν λειτουργεί η γραμμή εντολών.

Αφαιρούμε την εντολή run από όλους τους χρήστες εκτός από τους διαχειριστές μη δίνοντάς τους την δυνατότητα να εργαστούν σε περιβάλλον γραμμής εντολών. Η επιλογή Remove Run menu from Start Menu βρίσκεται στο User Configuration\Administrative Templates\Start Menu and Taskbar.

ΚΕΦΑΛΑΙΟ 10 - Συμπεράσματα μέσω εργαστηριακών μετρήσεων

Με τη δημιουργία του Ενεργού Καταλόγου η Microsoft θέτει τους παρακάτω στόχους:
- Μείωση του κόστους λειτουργίας του τμήματος μηχανογράφησης
- Βελτίωση υπηρεσιών
- Ταχύτητα
- Αποτελεσματικότερη εξειδίκευση και εκπαίδευση προσωπικού

Θα συνδυάσουμε τώρα την θεωρία με την πράξη. Στις εργαστηριακές μετρήσεις χρησιμοποιήσαμε 30 υπολογιστές με Windows 7 και δύο εκτυπωτές δικτύου. Και οι 30 υπολογιστές έχουν το ίδιο υλικό (hardware) και βρίσκονται στο ίδιο φυσικό χώρο (δεν υπάρχουν καθυστερήσεις μετακίνησης). Θα συγκρίνουμε τον χρόνο και την αποτελεσματικότητα ενός δικτύου τομέα και ενός δικτύου ομάδας εργασίας (workgroup). Βέβαια θα δούμε ότι υπάρχουν πάρα πολλές εργασίες τις οποίες δεν υποστηρίζει ένα δίκτυο εργασίας. Κάποιες από αυτές τις είδαμε και θα αναλύσουμε τα πλεονεκτήματά τους. Θα συγκρίνουμε τα δύο δίκτυα σε σχέση με το κόστος που χρειάζεται για να ολοκληρωθούν, σε σχέση με το χρόνο και σε σχέση με την ασφάλεια υπηρεσιών.

10.1 Ενεργός Κατάλογος και χρόνος

Με τις τελευταίες τεχνολογίες και σε συνεργασία με τον ενεργό κατάλογο έχει μειωθεί αισθητά ο χρόνος εγκατάστασης και συντήρησης ενός δικτύου. Ας δούμε όμως τι έδειξαν οι εργαστηριακές μετρήσεις.

DHCP SERVER:

Οι λειτουργίες ενός DHCP server είναι οι εξής :

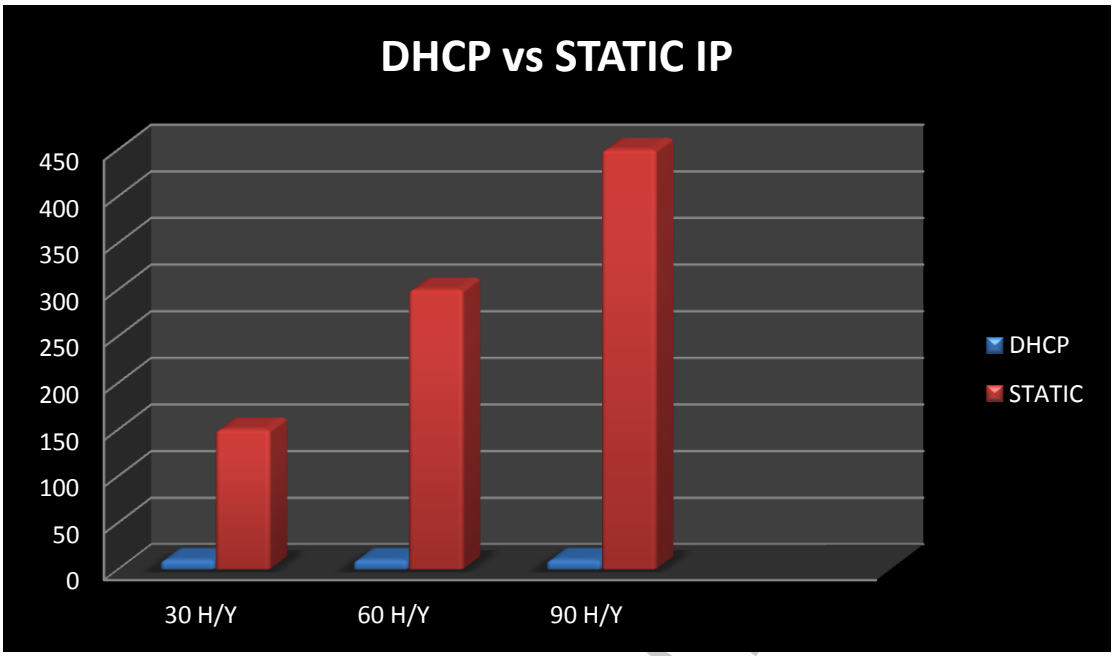
- Δυναμική ανάθεση IP σε ένα DHCP πελάτη.
    - Κατανομή των παρακάτω πληροφοριών
    - Πληροφορία μάσκα υποδικτύου (subnet mask)
    - IP διεύθυνση προεπιλεγμένης πύλης (Default gateway IP addresses)
    - Διεύθυνση IP Domain Name System (DNS)

Οι παραπάνω διευθύνσεις είναι της μορφής:
- IP διεύθυνση: 192.168.1.79
- Μάσκα Υποδικτύου: 255.255.255.0
- Προεπιλεγμένη πύλη: 192.168.1.254
- DNS: 192.168.1.1
- DNS : 192.168.1.2

Αρχικά χτίσαμε ένα δίκτυο σταθμού εργασίας. Θα έπρεπε να δηλώσουμε σε κάθε υπολογιστή ξεχωριστά τις παραπάνω διευθύνσεις και το όνομα του σταθμού εργασίας. Μαζί με την επανεκκίνηση του υπολογιστή χρειαζόμαστε 150 λεπτά για την ολοκλήρωση ενός δικτύου 30 υπολογιστών (5 λεπτά ανά υπολογιστή). Θα πρέπει δε να τονίσουμε ότι δεν λαμβάνονται υπόψη καθυστερήσεις λόγω ανθρωπίνων λαθών (διενέξεις IP, λάθος πληκτρολόγηση).

Στη συνέχεια ενεργοποιήσαμε στον ελεγκτή τομέα τον DHCP server, ορίσαμε σε όλους τους υπολογιστές αυτόματες IP διευθύνσεις και DNS και συνδεόμαστε στον τομέα των windows 2008 server. Στους υπολογιστές εκχωρήθηκαν οι διευθύνσεις σε δευτερόλεπτα. Ο μόνος μετρήσιμος χρόνος προς σύγκριση είναι ο χρόνος ενεργοποίησης του DHCP server ο οποίος είναι 10 λεπτά.

Όπως βλέπουμε και στο παρακάτω γράφημα χρειαζόμαστε 15 φορές περισσότερο χρόνο για να εγκαταστήσουμε στατικές IP διευθύνσεις σε 30 υπολογιστές. Θα πρέπει να τονίσουμε δε ότι για κάθε νέο υπολογιστή θα χρειαζόμαστε επιπλέον χρόνο εγκατάστασης για στατική IP διεύθυνση ενώ με τον DHCP server είτε έναν υπολογιστή έχουμε είτε 100 ο χρόνος εγκατάστασης είναι σταθερός.



Εικόνα 10.1.1: Χρόνος εγκατάστασης DHCP vs Static IP

PRINT SERVER:

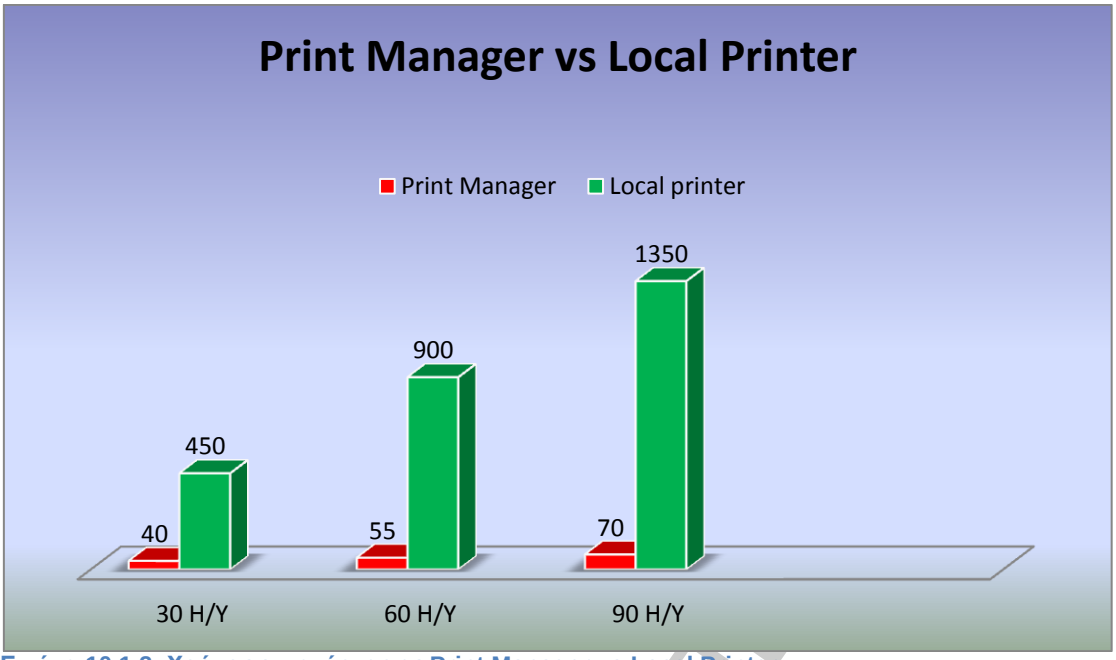
Σε ένα δίκτυο σταθμού εργασίας με 30 υπολογιστές εγκαταστήσαμε έναν δικτυακό εκτυπωτή σε ένα προφίλ χρήστη για κάθε υπολογιστή. Η εγκατάσταση ολοκληρώθηκε σε 7,5 ώρες (450 λεπτά). Η εγκατάσταση ενός εκτυπωτή εξαρτάται και από τον οδηγό εγκατάστασης του εκτυπωτή. Με τις νέες τεχνολογίες και τις δυνατότητες των εκτυπωτών οι οδηγοί εγκατάστασης είναι ένα ‘’βαρύ’’ λογισμικό. Ένας μέσος χρόνος εγκατάστασης ανά υπολογιστή είναι 15 λεπτά. Αν προστεθεί μελλοντικά και άλλος χρήστης θα προστεθούν άλλα 15 λεπτά για την εγκατάσταση του εκτυπωτή.

Στη συνέχεια εγκαταστήσαμε τον ίδιο εκτυπωτή στον τομέα μας με την βοήθεια του Print Manager. Η διαδικασία έχει ως εξής:

- Εγκατάσταση ρόλου Print Server
- Εγκατάσταση εκτυπωτή στην κονσόλα του Print Management
- Τοποθέτηση αρχείων εγκατάστασης στην κονσόλα του Print Management.
- Δημιουργία ομάδας χρηστών που θα χρησιμοποιούν τον συγκεκριμένο εκτυπωτή.
- Ανάθεση μέσω πολιτικών ομάδας τον εκτυπωτή στους 30 χρήστες.

Η όλη διαδικασία ολοκληρώθηκε σε 40 λεπτά. Να σημειώσουμε δε ότι για νέους χρήστες το μόνο που χρειάζεται είναι να προσθέτουμε τον αντίστοιχο χρήστη στην ομάδα που δημιουργήσαμε (χρονικά 20 δευτερόλεπτα).

Όπως παρατηρούμε και στο παρακάτω γράφημα με την χρήση Print Manager και πολιτικών ομάδων η εγκατάσταση είναι κατά 11,25 φορές πιο γρήγορη.



Εικόνα 10.1.2: Χρόνος εγκατάστασης Print Manager vs Local Printer

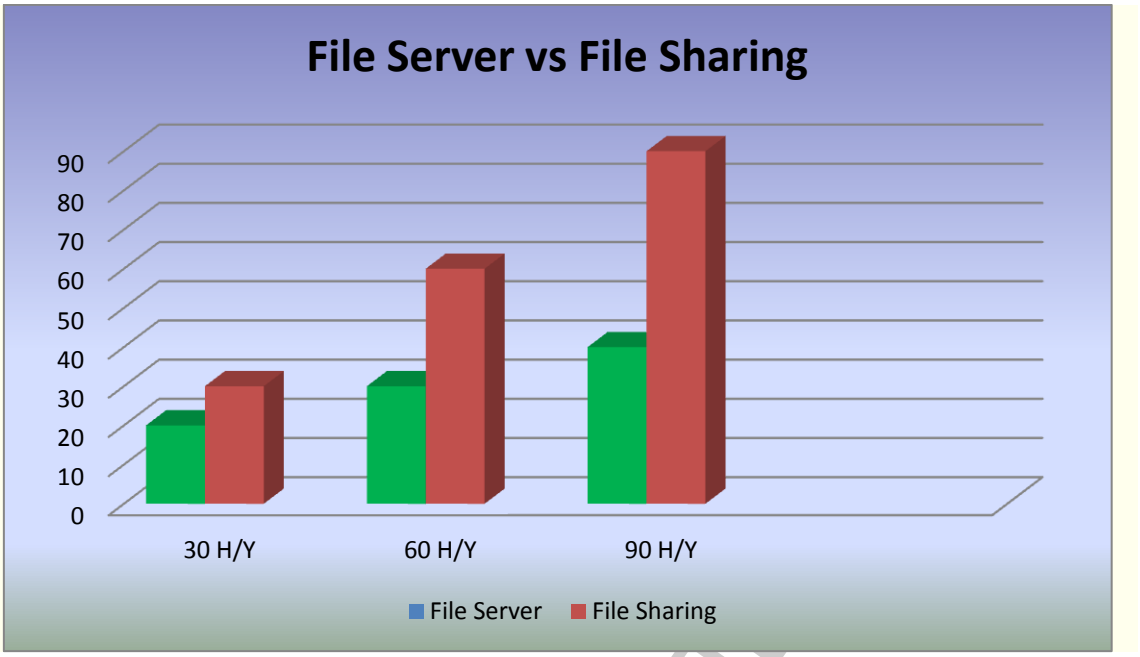
FILE SERVER:

Δημιουργήσαμε σε ένα υπολογιστή ενός δικτύου εργασίας με 30 υπολογιστές ένα φάκελο και τον κάναμε κοινόχρηστο στους υπόλοιπους 29. Στη συνέχεια πήγαμε σε κάθε υπολογιστή για να συνδέσουμε με συντόμευση τον συγκεκριμένο φάκελο στην επιφάνεια εργασίας ενός χρήστη. Για την ολοκλήρωση χρειαστήκαμε 30 λεπτά.

Σε ένα δίκτυο τομέα ακολουθήσαμε την εξής διαδικασία:

- Εγκατάσταση ρόλου File Server
- Δημιουργία φακέλου και κοινή χρήση σε όλους (everyone)
- Δημιουργία πολιτικής στο User Configuration\Preferences\Windows Settings\Shortcuts με την οποία τοποθετούμε στην επιφάνεια εργασίας του κάθε χρήστη μία συντόμευση του κοινόχρηστου φακέλου.
- Ανάθεση πολιτικής σε όλους τους χρήστες.

Η διαδικασία με τομέα είχε διάρκεια 20 λεπτά. Όπως παρατηρούμε και από το παρακάτω γράφημα με την χρήση του File Server κερδίζουμε αρχικά με την πρώτη εγκατάσταση 10 λεπτά. Στη συνέχεια όμως αν προσθέσουμε υπολογιστές στο δίκτυο στο μεν σταθμό εργασίας θέλουμε 1 λεπτό για κάθε χρήστη ενώ στο δίκτυο τομέα 20 δευτερόλεπτα ανά χρήστη.

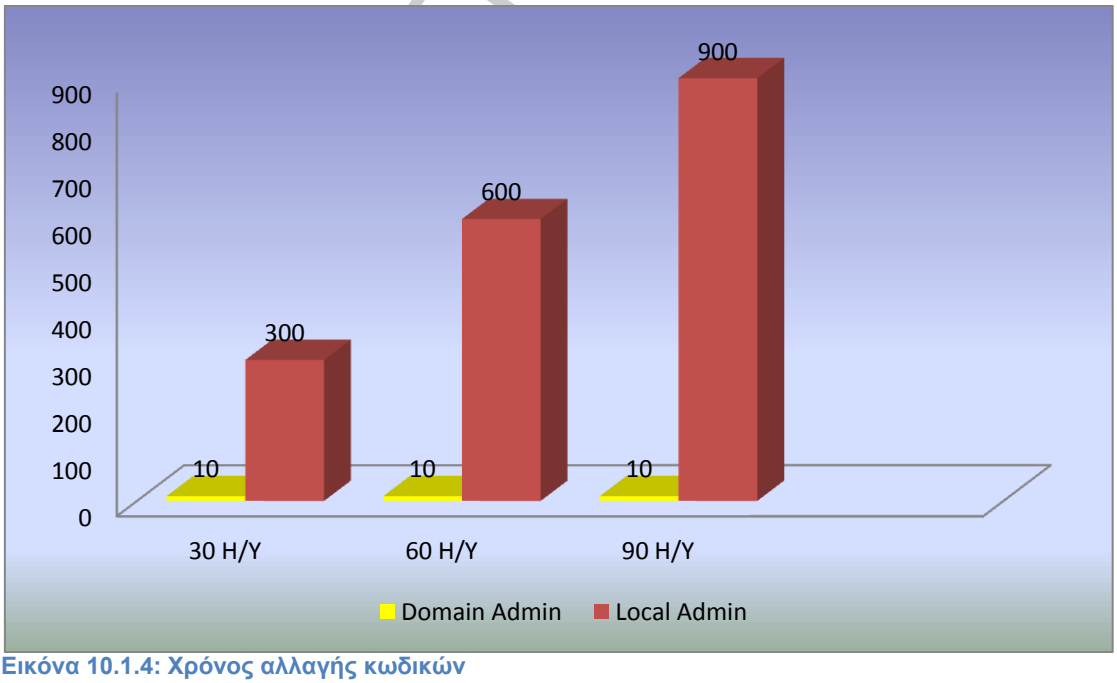


Εικόνα 10.1.3: Χρόνος εγκατάστασης File Server vs File Sharing

Αλλαγή κωδικού πρόσβασης τοπικού διαχειριστή:

Σε μια ομάδα εργασίας δεν υπάρχει η έννοια του γενικού διαχειριστή. Κάθε υπολογιστής έχει τα προφίλ του διαχειριστή και των χρηστών που συνδέονται σε αυτών. Για να είναι πιο ασφαλείς οι υπολογιστές θα πρέπει να αλλαχτεί ο κωδικός του διαχειριστή. Η διαδικασία αυτή θα πρέπει να γίνει σε κάθε υπολογιστή. Κάθε υπολογιστής θέλει 10 λεπτά άρα χρειαζόμαστε συνολικά 300 λεπτά για να αλλάξουμε όλους τους κωδικούς. Για κάθε νέο υπολογιστή που συνδέεται θα πρέπει να γίνεται η ίδια διαδικασία.

Σε ένα δίκτυο τομέα υπάρχει ένας λογαριασμός διαχειριστή και η αλλαγή κωδικού γίνεται μέσα σε 10 λεπτά.

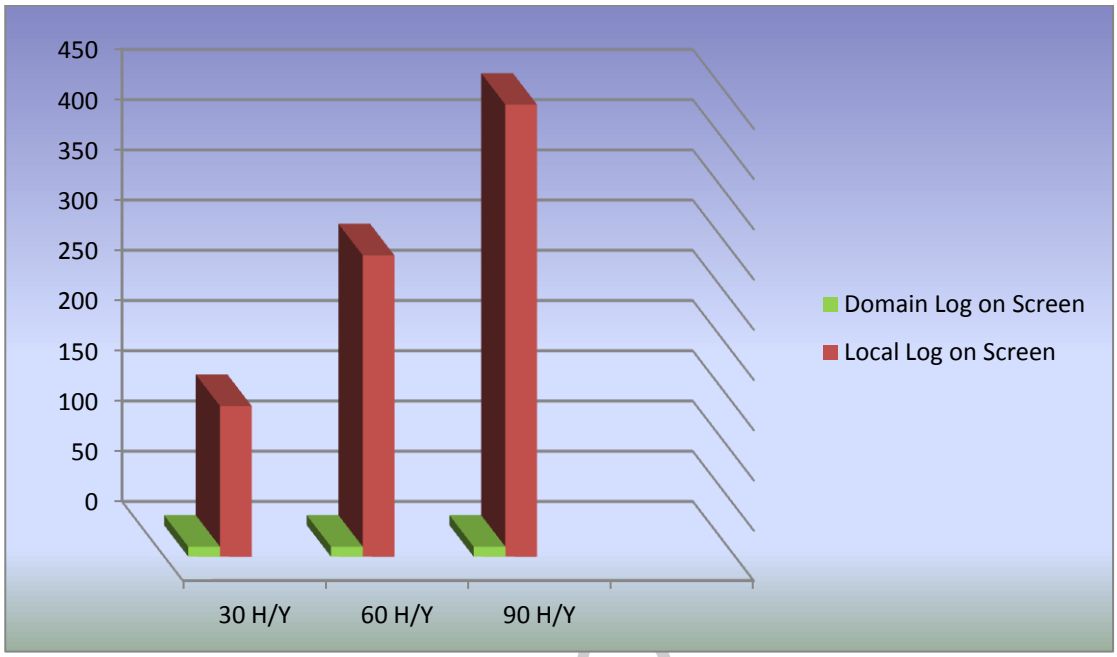


Εικόνα 10.1.4: Χρόνος αλλαγής κωδικών

Log on screen:

Για την παραμετροποίηση της οθόνης σύνδεσης σε 30 υπολογιστές σε ένα δίκτυο εργασίας χρειαζόμαστε 150 λεπτά.

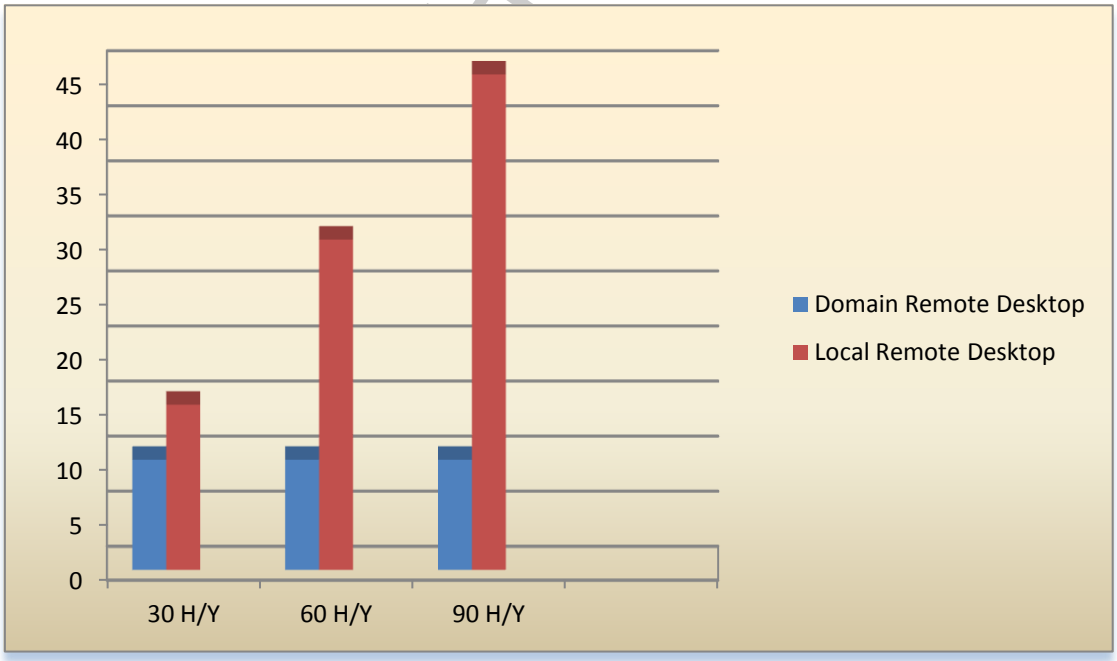
Η αντίστοιχη εργασία σε δίκτυο τομέα γίνεται με πολιτική ομάδων σε 10 λεπτά.



Εικόνα 10.1.5: Χρόνος εγκατάστασης Log on screen

Enable remote desktop:

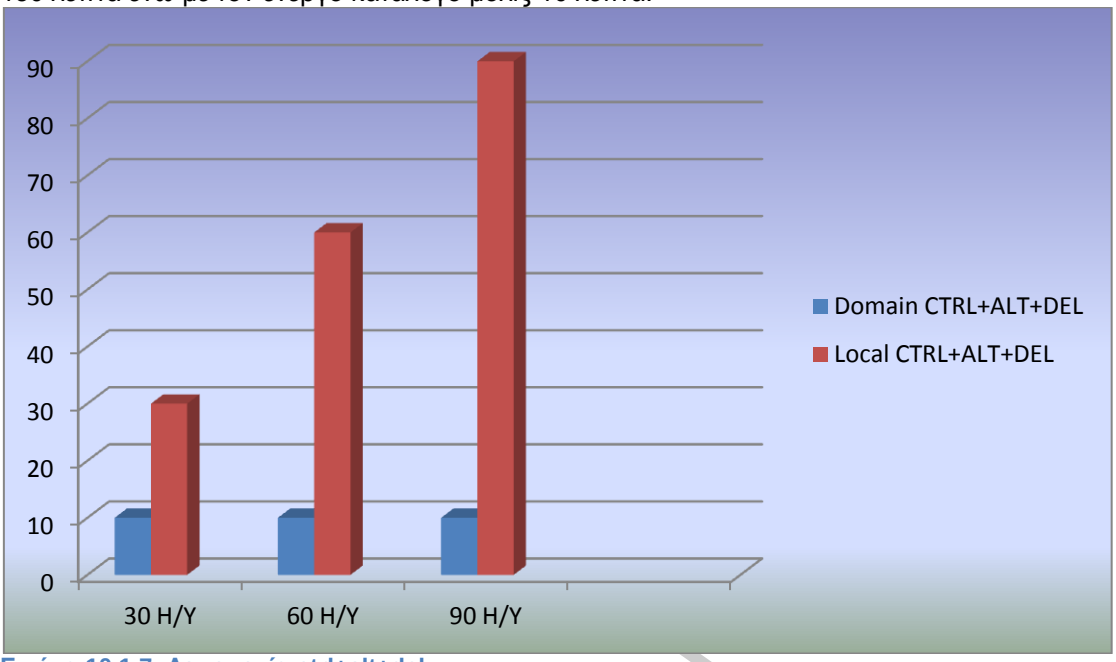
Για την ενεργοποίηση της απομακρυσμένης σύνδεσης σε 30 υπολογιστές χρειαζόμαστε15 λεπτά σε ένα δίκτυο σταθμού εργασίας, ενώ με τον ενεργό κατάλογο 10 λεπτά.



Εικόνα 10.1.6: Ενεργοποίηση Απομακρυσμένης λειτουργίας

CTRL+ALT+DEL:

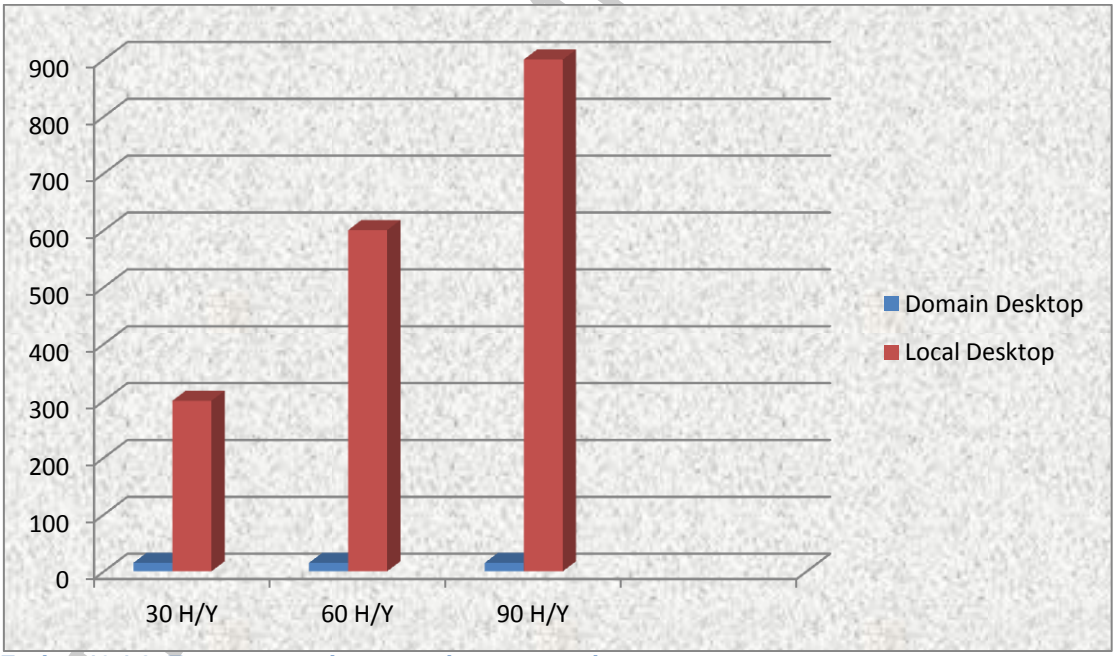
Για να ρυθμίσουμε τις λειτουργίες των πλήκτρων CTRL+ALT+DEL σε 30 υπολογιστές θέλουμε 150 λεπτά ενώ με τον ενεργό κατάλογο μόλις 10 λεπτά.



Εικόνα 10.1.7: Λειτουργία ctrl+alt+del

DESKTOP CUSTOMIZATION:

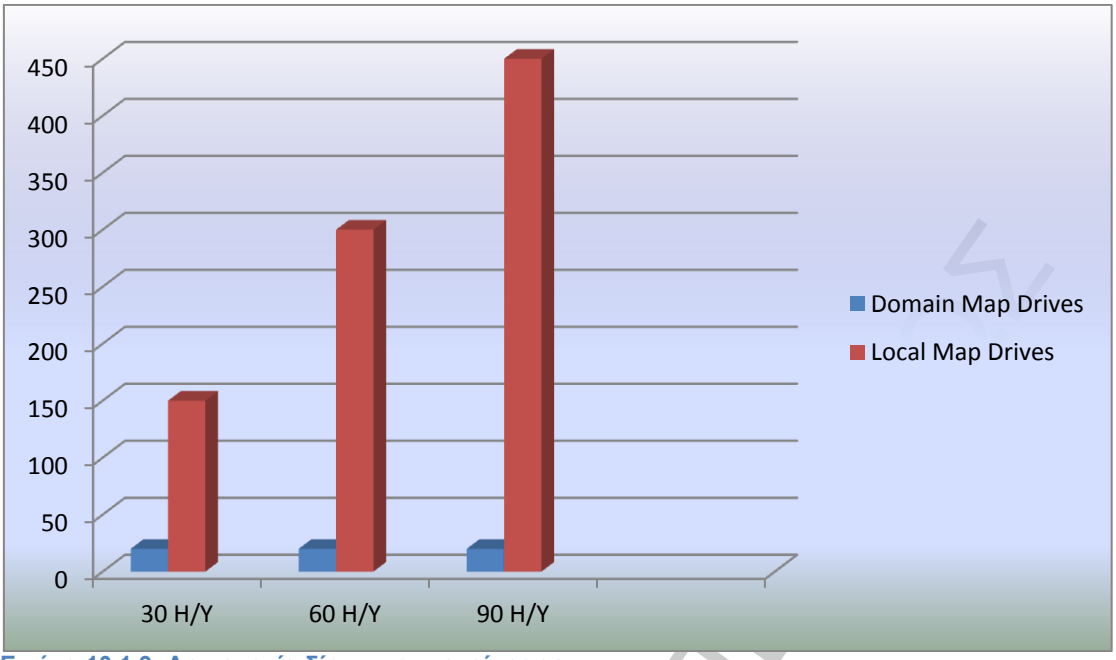
Η παραμετροποίηση της επιφάνειας εργασίας θέλει 300 λεπτά ενώ με τον ενεργό κατάλογο 15 λεπτά.



Εικόνα 10.1.8: Παραμετροποίηση επιφάνειας εργασίας

MAP DRIVES:

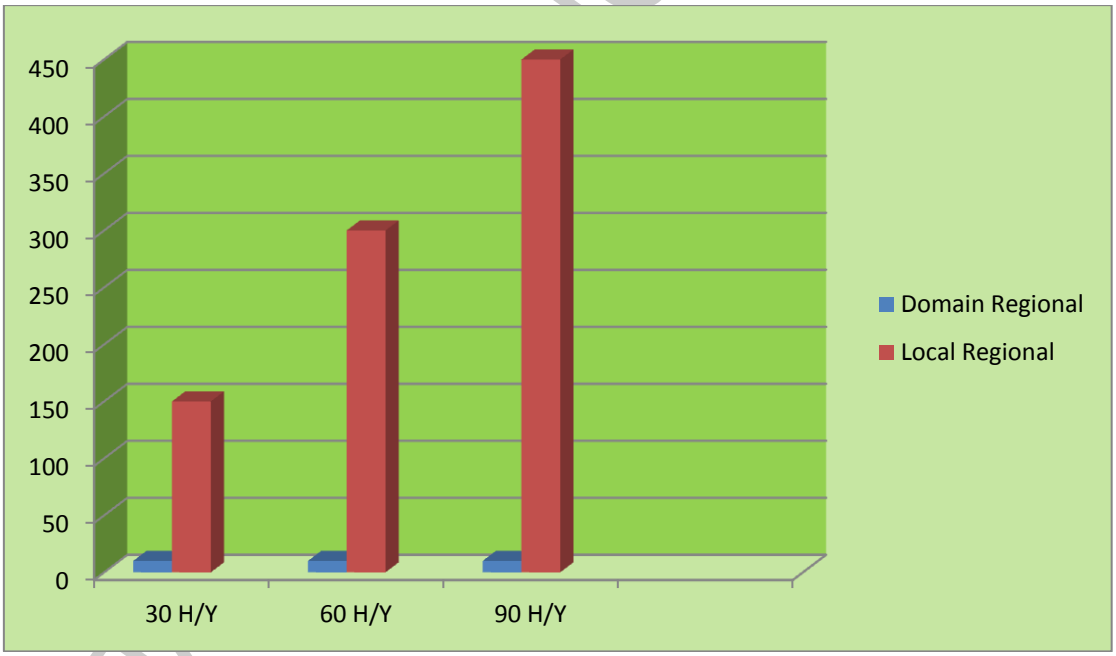
Η δημιουργία αντιστοίχιση δίσκων για μία αντιστοίχηση ανά υπολογιστή χρειάζεται 150 λεπτά ενώ με τον ενεργό κατάλογο 20 λεπτά.



Εικόνα 10.1.9: Δημιουργία δίσκων αντιστοίχησης

REGIONAL SETTINGS:

Οι τοπικές ρυθμίσεις χρειάζονται 150 λεπτά για να ολοκληρωθούν σε 30 υπολογιστές ενώ μέσω του ενεργού καταλόγου 10 λεπτά.



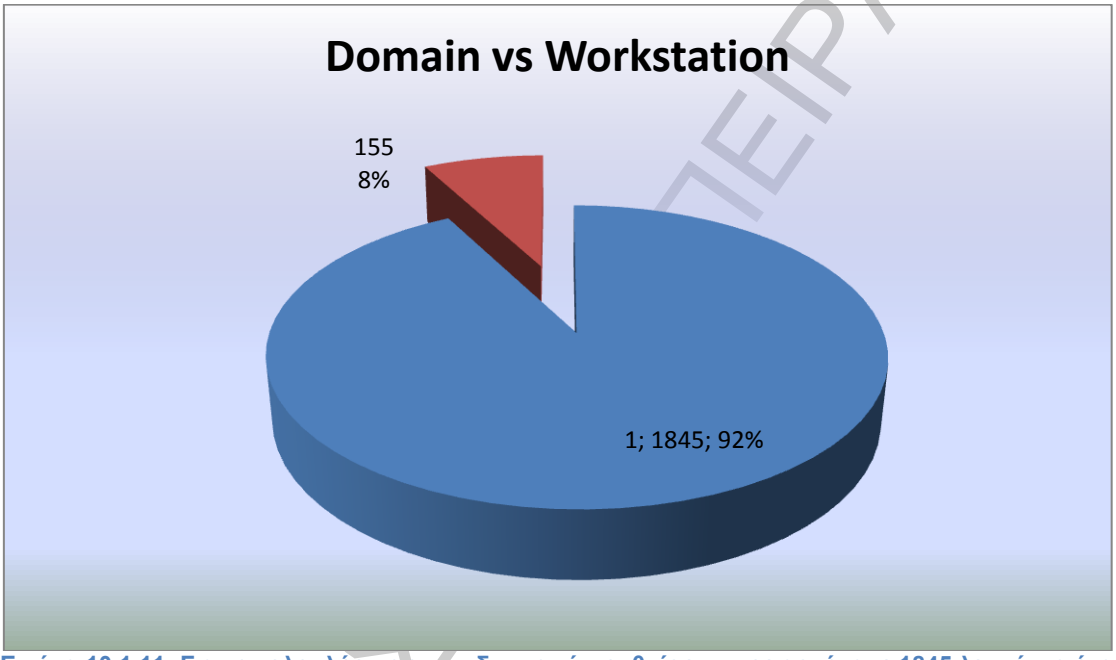
Εικόνα 10.1.10: Τοπικές Ρυθμίσεις

	Δίκτυο Σταθμού Εργασίας (λεπτά)	Δίκτυο Τομέα (λεπτά)
DHCP SERVER	150	10
PRINT SERVER	450	40
FILE SERVER	30	20

Αλλαγή κωδικού πρόσβασης	300	10
Log on screen	150	10
Enable remote desktop	15	10
CTRL+ALT+DEL	150	10
DESKTOP CUSTOMIZATION	300	15
MAP DRIVES	150	20
REGIONAL SETTINGS	150	10

Πίνακας 10.1: Συνολικός χρόνος εγκατάστασης (Workgroup vs Domain)

Παρατηρούμε ότι ένα δίκτυο τομέα με την βοήθεια του ενεργού καταλόγου και των πολιτικών ομάδων ολοκληρώνεται 12 φορές πιο γρήγορα από ένα δίκτυο σταθμού εργασίας. Χρησιμοποιήσαμε μόλις 8% του χρόνου μας για να ρυθμίσουμε ένα δίκτυο τομέα σε αντίθεση με ένα δίκτυο σταθμού εργασίας που χρειαστήκαμε το 92% του χρόνου μας.



Εικόνα 10.1.11: Για την ολοκλήρωση των δικτυακών ρυθμίσεων χρειαστήκαμε 1845 λεπτά για ένα σταθμό εργασίας ενώ για ένα τομέα με ενεργό κατάλογο χρειαστήκαμε μόλις 155 λεπτά.

Στην εικόνα 10.1.12 παρατηρούμε ότι σε ένα σταθμό εργασίας κάθε υπολογιστή που προσθέτουμε αυξάνεται ο χρόνος εργασίας, ενώ σε ένα δίκτυο τομέα παραμένει σχεδόν ίδιος.

Εικόνα 10.1.12: Όσο μεγαλώνει ένα δίκτυο σταθμού εργασίας τόσο αυξάνει και ο χρόνος παραμετροποίησης του. Αντίθετα ο χρόνος σε ένα δίκτυο τομέα παραμένει σταθερός.

10.2 Ενεργός Κατάλογος και κόστος

Το κόστος ενός δικτυακού εξοπλισμού ενός οργανισμού εξαρτάται από τα εξής χαρακτηριστικά:

Αγορά υλικού – λογισμικού τερματικών:

Το κόστος αγοράς υλικού και λογισμικού των τερματικών είναι ίδιο είτε χρησιμοποιήσουμε δίκτυο σταθμού εργασίας είτε δίκτυο τομέα.

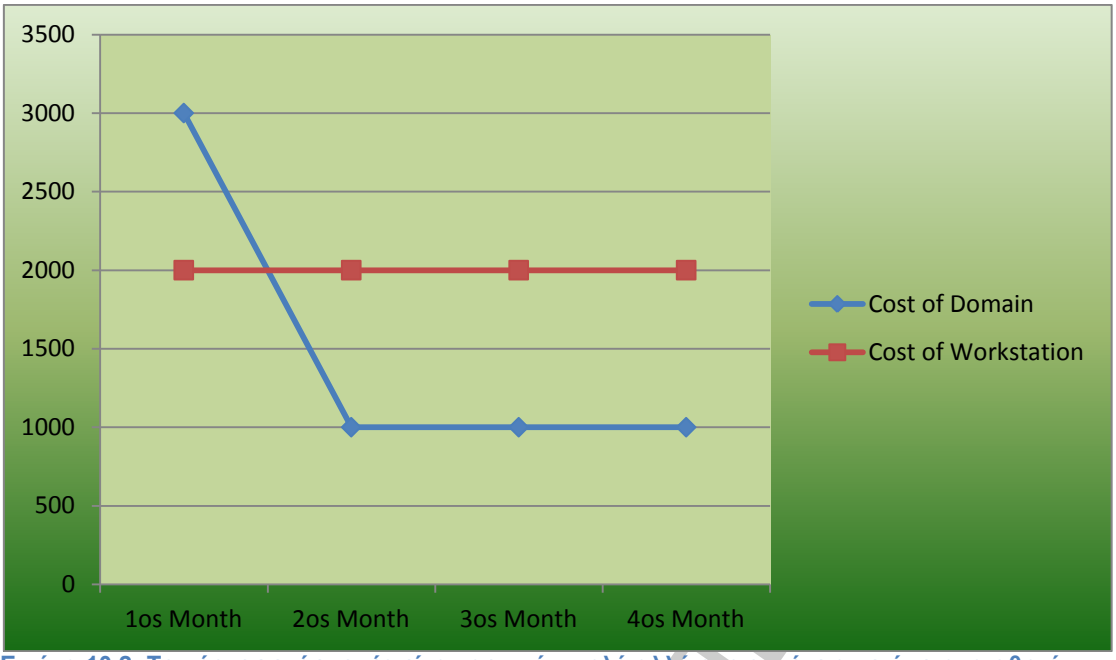
Αγορά υλικού – λογισμικού διακομιστών:

Ένας σταθμός εργασίας δεν έχει διακομιστή άρα δεν επιβαρύνεται οικονομικά. Ένα δίκτυο τομέα έχει τουλάχιστον ένα ελεγκτή τομέα. Για ένα περιβάλλον εργασίας 30 υπολογιστών το κόστος ενός επώνυμου διακομιστή ξεκινάει από 2000 €. Μαζί με τις άδειες χρήσης των Windows για 30 χρήστες το κόστος ανεβαίνει περίπου στα 3000. Άρα ένα δίκτυο τομέα είναι ακριβότερο τουλάχιστον κατά 3000€ σαν αρχική εγκατάσταση.

Μισθοδοσία Διαχειριστών δικτύου.

Ένα δίκτυο σταθμού εργασίας με 30 υπολογιστές χρειάζεται τουλάχιστον δύο διαχειριστές. Αν υποθέσουμε ότι ο καθένας αμείβεται με 1000€ μηνιαίως τότε έχουμε πάγια κάθε μήνα 2000€.

Ένα δίκτυο τομέα με 30 υπολογιστές συντηρείται και με έναν μόνο διαχειριστή. Από την μισθοδοσία του έχουμε ένα πάγιο των 1000 € μηνιαίως. Μόνο από της μισθοδοσίες έχει γίνει απόσβεση του αρχικού κόστους εγκατάστασης σε τρεις μήνες.



Εικόνα 10.2: Το κόστος ενός τομέα είναι αρχικά υψηλό αλλά στη συνέχεια μειώνεται αισθητά

10.3 Ενεργός Κατάλογος και Υπηρεσίες ασφάλειας

Η ασφάλεια ενός δικτύου υπολογιστών είναι ένα ολόκληρο κεφάλαιο στην τεχνολογία της πληροφορικής και στηρίζεται σε τρεις βασικές ιδέες.

- Ακεραιότητα δεδομένων. Με την περιορισμένη πρόσβαση σε φακέλους (read only, read –write, deny) περιορίζουμε την λάθος χρήση από κακόβουλους ή άπειρους χρήστες.
- Η διαθεσιμότητα. Με υπηρεσίες όπως το redundancy, hot spare, backup domain controller, ups εξασφαλίζουμε την συνεχή λειτουργία του δικτύου.
- Η εμπιστευτικότητα. Με την επικύρωση των χρηστών στον ενεργό κατάλογο αποφεύγουμε την σύνδεση στο δίκτυο μη εξουσιοδοτημένου χρήστη.

Με την χρήση του ενεργού καταλόγου αυξάνεται η ασφάλεια ενός δικτύου. Η πιστοποίηση των χρηστών και οι πολιτικές που αναθέτουμε σε κάθε οργανωτική ομάδα στοχεύουν στην ασφάλεια του δικτύου.

- Δημιουργήσαμε πολιτικές με πολύπλοκους κωδικούς.
- Δημιουργήσαμε δικαιώματα σε δεδομένα - φακέλους ανά χρήστη.
- Προσαρμόσαμε τις λειτουργίες των Windows έτσι ώστε να μην έχουν πρόσβαση σε καταλόγους όπου μπορούν να βλάψουν (σκόπιμα ή μη) το δίκτυο.
- Προσαρμόσαμε τις λειτουργίες του internet explorer.

Δεν μπορούμε να μιλήσουμε με ποσοστά για το αν υπάρχει μεγαλύτερη ασφάλεια σήμερα από ότι παλιότερα. Δεν μπορούμε να συγκρίνουμε δυο ανόμοιες καταστάσεις. Πριν 10 χρόνια η χρήση του διαδικτύου δεν ήταν τόσο διαδεδομένη όσο σήμερα άρα και οι επιθέσεις και οι κακόβουλοι χρήστες λιγότεροι και όσο η τεχνολογία εξελίσσεται τόσο και οι κακόβουλοι χρήστες αυξάνονται και εξελίσσονται.

10.4 Ενεργός Κατάλογος και Σενάρια

Θα παρατηρήσουμε ότι με τη χρήση των πολιτικών ομάδων στα Windows 2008 server έχουμε περιορίσει πολύ την χρήση των σεναρίων (scripts). Η Microsoft ενσωμάτωσε σε γραφικό περιβάλλον τον διορθωτή πολιτικών. Έτσι αντί να γράφουμε κώδικα για να ορίσουμε πολιτικές και ομάδες τώρα πια αρκεί να ψάξουμε στον διορθωτή πολιτικών. Με αυτόν τον τρόπο η διαχείριση γίνεται πιο εύκολη και πιο γρήγορη. Δεν χρειάζεται πια να γνωρίζουμε κάποια γλώσσα και να προγραμματίζουμε εντολές.

Φυσικά δεν καταργείται πλήρως η λειτουργία των σεναρίων μιας και κάθε δίκτυο είναι διαφορετικό και δεν είναι δυνατόν να καλυφθούν όλα τα σενάρια με τον διορθωτή πολιτικών. Άλλωστε ένα σενάριο μπορούμε να το διαμορφώσουμε ακριβώς όπως θέλουμε εμείς ενώ στα Preferences έχουμε πολλές μεν αλλά συγκεκριμένες επιλογές.

Θα δώσουμε τώρα ένα παράδειγμα σύγκρισης. Είδαμε παραπάνω ότι για να δημιουργήσουμε ένα δίσκο αντιστοίχησης σε 30 υπολογιστές χρειαστήκαμε περίπου 20 λεπτά.

Δημιουργήσαμε ένα σενάρια το οποίο δημιουργεί δίσκο αντιστοίχησης σε 30 υπολογιστές και το αναθέσαμε μέσω πολιτικής στην σύνδεση (log on) του κάθε χρήστη. Το σενάριο είναι το παρακάτω:

MapNetworkDrive.vbs

```
' ----------------------------------------------------'
Option Explicit
Dim objNetwork
Dim strDriveLetter, strRemotePath
strDriveLetter = "J:"
strRemotePath = "\\master\map"

' Purpose of script to create a network object. (objNetwork)
' Then to apply the MapNetworkDrive method.  Result J: drive
Set objNetwork = CreateObject("WScript.Network")

objNetwork.MapNetworkDrive strDriveLetter, strRemotePath
WScript.Quit

' End of Example VBScript.
```

Η διαδικασία δημιουργίας δίσκου αντιστοίχησης ήταν 10 λεπτά πιο αργή και αυτό γιατί κατά την πληκτρολόγηση έγιναν και λάθη. Αν θέλουμε λοιπόν να συγκρίνουμε τους δύο τρόπους θα λέγαμε ότι η διαφορά σε ταχύτητα δεν είναι μεγάλη αλλά για την δημιουργία σεναρίων θα πρέπει να γνωρίζουμε κάποια γλώσσα προγραμματισμού και να γνωρίζουμε καλή πληκτρολόγηση.

Το συγκεκριμένο παράδειγμα δεν μας δίνει το πραγματικό αποτέλεσμα. Υπάρχουν σενάρια που για να γραφτούν είναι σελίδες και χρειάζονται πολύ χρόνο. Αντίθετα με τις ρυθμίσεις των Preferences αποφεύγουμε πλέον με ένα κλικ όλο αυτό το χρόνο.

10.5 Συμπεράσματα εργαστηριακών μετρήσεων

Λαμβάνοντας υπόψη τα αποτελέσματα των εργαστηριακών μετρήσεων καταλήγουμε στα παρακάτω συμπεράσματα:

- Ένα δίκτυο τομέων με την χρήση ενεργού καταλόγου ολοκληρώνεται τουλάχιστον 11 φορές πιο γρήγορα από ένα δίκτυο σταθμού εργασίας.
- Το κόστος υλοποίησης είναι αρχικά υψηλό αλλά γίνεται άμεσα απόσβεση και δεν έχει υψηλό κόστος συντήρησης.
- Είναι πιο ασφαλές από ότι ένα απλό σταθμό εργασίας γιατί μπορούμε να επέμβουμε σε ιδιότητες του χρήστη.
- Σε ένα δίκτυο τομέα η διαχείριση και η συντήρηση είναι κεντρική από τον διαχειριστή και φυσικά πολύ πιο εύκολη.
- Ένα δίκτυο τομέα απαιτεί λιγότερο προγραμματισμό.

Θα πρέπει να σημειώσουμε ότι κατά την υλοποίηση του δικτύου αντιμετωπίσαμε αρκετά προβλήματα και αυτά γιατί η Microsoft αρχικά έδινε ελλιπείς πληροφορίες. Όμως η βιβλιογραφία και το Knowledge base των Windows είναι διαθέσιμη παντού στο διαδίκτυο οπότε τα προβλήματα ξεπεράστηκαν άμεσα.

ΚΕΦΑΛΑΙΟ 11 - Το μέλλον

Η Microsoft εισάγει μια νέα τεχνολογία καταλόγου που στηρίζεται σε μια βάση δεδομένων. Ο σχεδιασμός της στηρίζεται σε ένα νέο API το οποίο παρέχει στους προγραμματιστές ένα ενιαίο πρότυπο το οποίο στηρίζεται στην αρχή claims-based access control, στις εφαρμογές που τρέχουν στο σύννεφο (cloud).

Ο κώδικας είναι στο αρχικό στάδιο και δεν έχει ακόμα ένα επίσημο όνομα, αν και εσωτερικά η Microsoft το αποκαλεί Επόμενη Γενιά Ενεργού Καταλόγου (NGAD). Το NGAD, εντούτοις, δεν είναι μια αντικατάσταση του Ενεργού Καταλόγου αλλά “clip-on” που παρέχει στους προγραμματιστές ένα ενιαίο προγραμματισμό API για την οικοδόμηση του ελέγχου πρόσβασης στις εφαρμογές που μπορούν να τρέξουν είτε εσωτερικά, στις συσκευές είτε στο Azure (λειτουργικό σύστημα που έχει η Microsoft στο σύννεφο). Οι χρήστες δεν θα πρέπει να αλλάξουν τους υπάρχοντες καταλόγους τους αλλά πρέπει να έχουν την επιλογή να αντιγραφούν (replicate) στο NGAD.

Το NGAD αποθηκεύει δεδομένα καταλόγου σε μια SQL-based βάση δεδομένων και χρησιμοποιεί την επίπεδη δομή του, για να απαντήσει ή να θέσει ερωτήσεις ή ισχυρισμούς όπως «είμαι πάνω από 21». Για να εξασφαλιστεί η ασφάλεια, κάθε ισχυρισμός υπογράφεται από μια πηγή έκδοσης, όπως μια επιχείρηση.

“Μπορείτε να απαντήσετε ερωτήσεις στον κατάλογό σας που ήταν αδύνατον ακόμα και να διατυπωθούν” λέει ο Kim Cameron, προγραμματιστής στη Microsoft. “Μπορείτε να ανακαλύψετε ποιος είχε πρόσβαση σε ένα αρχείο τον περασμένο Σεπτέμβριο”. Λέει ότι το NGAD είναι μια αναδιαμόρφωση του προτύπου προγραμματισμού για τον ενεργό κατάλογο.

Επιπλέον, ο σχεδιασμός του καταλόγου σημαίνει πολλά νέα σύννεφα ή άλλες εφαρμογές. Αυτό όμως δεν θα επιβαρύνει τον κεντρικό ενεργό κατάλογο με τα αιτήματα και ο διαχειριστής δεν χρειάζεται να επεμβαίνει συχνά για υποστήριξη εφαρμογών.

Η πρόθεση είναι η δημιουργία ενός «λογικού καταλόγου» που μοιράζεται τα στοιχεία αρχιτεκτονικής όπως το σχήμα (schema) και τα APIs.

Το πιο σημαντικό χαρακτηριστικό του NGAD είναι η δημιουργία βάσεων δεδομένων SQL. Περιλαμβάνει μια SQL-based “αποθήκη”, μια κεντρική διαχειριστική βάση δεδομένων για τα μεταδεδομένα εφαρμογής το οποίο περιλαμβάνει ένα πρότυπο επέκτασης ταυτότητας (identity deployment model). Το NGAD εισάγει επίσης ένα σχήμα αποκαλούμενο System.Identity και System.Identity API. Το API εκθέτει το σχήμα στους υπεύθυνους για την ανάπτυξη μέσω LINQ. Ο κατάλογος ενσωματώνει επίσης τη γλώσσα διαμόρφωσης “M”.

Δεδομένου ότι το NGAD είναι ένα add on είναι παρόμοιο στην έννοια με τις ενεργές υπηρεσίες ομοσπονδίας καταλόγου (AD FS), μια ενότητα για τη διανομή της επικύρωσης, και τον ενεργό τρόπο εφαρμογής καταλόγου (ADAM), τα οποία θα αντικατασταθούν τελικά από το NGAD.

Το NGAD αφήνει τους χρήστες να δημιουργήσουν σύνθετες σχέσεις μεταξύ των στοιχείων που αποθηκεύουν όπως οι φίλοι, οι συνάδελφοι, οι ρόλοι, οι αναθέσεις υπηρεσιών και τα σύνολα μηχανών. Εκείνες οι σχέσεις μπορούν να χρησιμοποιηθούν για να δημιουργήσουν λεπτομερείς ισχυρισμούς που διοικούν τον έλεγχο πρόσβασης.

Με τον Ενεργό Κατάλογο η μόνη σχέση που έχουμε είναι η ομάδα.

Ένα άλλο εξελικτικό στοιχείο είναι η υποστήριξη για τις νεώτερες τεχνολογίες Ιστού όπως RSS και το REST.

Η Microsoft δεν σχεδίασε ένα πρόσθετο χρονικό πλαίσιο για τον κατάλογο NGAD, αλλά εάν ακολουθεί τις προηγούμενες καινοτομίες καταλόγου από την επιχείρηση θα μπορούσε να απελευθερωθεί ως αυτόνομο προϊόν ή να ενσωματωθεί στην επόμενη έκδοση των παραθύρων. (http://conklintechnology.com/site/2009/11/18/microsofts-next-generation-active-directory/), (http://www.networkworld.com/news/2010/021710-active-directory-turns-10.html?page=2)

ΚΕΦΑΛΑΙΟ 12- Συμπεράσματα

Πολύ νωρίς με την δημιουργία των πρώτων δικτύων υπολογιστών δημιουργήθηκε η ανάγκη απλοποίησης στη διαχείρισή τους. Η Microsoft προέβλεψε αυτήν την ανάγκη και από πολύ

νωρίς (1996) προσπάθησε με διάφορες τεχνολογίες να επιτύχει το Zero Administration for Windows. Ο Ενεργός Κατάλογος κάνει την εμφάνισή του το 2000 και εδώ και μια δεκαετία έχει επικρατήσει στην παγκόσμια αγορά. Ο παραθυρικός τρόπος διαχείρισης ενός λειτουργικού διακομιστή με στόχο την πιο εύκολη διαχείριση ενός δικτύου γίνεται πιο ελκυστικός στους διαχειριστές αυτού.

Η δημιουργία δασών, τομέων, οργανωτικών μονάδων μαζί με την κεντρική διαχείριση (πολιτικές ομάδων) και επικύρωση των χρηστών καθιστά τον Ενεργό Κατάλογο ένα εργαλείο σύμμαχο του διαχειριστή.

Η δημιουργία ενός δικτύου υπολογιστών ενός οργανισμού προϋποθέτει αρχικά ανάλυση. Ένα σχολικό δίκτυο απαρτίζεται από πολλά τμήματα με διαφορετικές ανάγκες. Διαφορετικές ανάγκες ανά τμήμα αλλά και ανά χρήστη. Η συλλογή πληροφοριών δεν ήταν εύκολη. Σε ερωτήσεις όπως “τι εφαρμογές θα πρέπει να εγκατασταθούν στον υπολογιστή σας” η απάντηση από απλούς χρήστες δεν ήταν σαφής πάντα “ότι εσύ νομίζεις καλύτερο”. Τελικά συνεργαστήκαμε με τον διαχειριστή του δικτύου για να κάνουμε μια σωστή καταγραφή και ανάλυση αναγκών τόσο σε επίπεδο λογισμικού όσο και σε επίπεδο υλικού.

Σχεδιάζοντας το δίκτυό μας καθιστούμε επιτακτική την ανάγκη διαχωρισμού των διακομιστών ανάλογα με το πεδίο λειτουργικότητάς τους. Η ανάγκη αυτή δημιουργείται από τον όγκο και την ταχύτητα εργασίας. Για παράδειγμα σε ένα σχολικό δίκτυο όπου ο όγκος των δεδομένων είναι μεγάλος (σημειώσεις, εργασίες..) προτείνεται ο διακομιστής δεδομένων να είναι ξεχωριστός από τον διακομιστή που διαχειρίζεται τα ηλεκτρονικά ταχυδρομεία των χρηστών.

Με τις τεχνολογίες redundancy και replication που υποστηρίζει και η Microsoft επιτυγχάνεται η συνεχή λειτουργία του δικτύου ακόμα και σε περίπτωση φυσικής καταστροφής του computer room.

Κατά την υλοποίηση του δικτύου χρησιμοποιήσαμε τις πολιτικές του Ενεργού Καταλόγου της Microsoft για να διαχειριστούμε ένα δίκτυο 30 υπολογιστών και να εξάγουμε συμπεράσματα. Στην εικόνα 10.1.12 βλέπουμε ότι ο στόχος της Microsoft για μηδενισμό του χρόνου διαχείρισης έχει επιτευχθεί κατά 90%.

Το κόστος υλοποίησης είναι αρχικά υψηλό. Θα πρέπει βέβαια να τονίσουμε σε μεγάλα δίκτυα το κόστος είναι πάρα πολύ υψηλό. Αυτό εξαρτάται από το μέγεθος του δικτύου (πόσους υπολογιστές – χρήστες εξυπηρετεί και ποιους ρόλους έχουμε προσθέσει). Για ένα δίκτυο 30 υπολογιστών αρκεί ένας διακομιστής με κόστος περίπου 3000€. Για ένα δίκτυο 300 υπολογιστών όμως, το κόστος είναι πάρα πολύ υψηλό για έναν οργανισμό. Μια ενδεικτική τιμή είναι από 150.000€ και πάνω.

Η ασφάλεια ενός δικτύου είναι μεγαλύτερη με την χρήση πολιτικών τόσο σε επίπεδο χρήστη όσο και σε επίπεδο υπολογιστή. Με πολιτικές επικύρωσης, και περιορισμένων προσβάσεων σε υπολογιστές, σε πόρους στο δίκτυο και σε διαδίκτυα ελαχιστοποιούμε τις πιθανότητες κακόβουλης ή μη (λόγω απειρίας) επίθεσης στο δίκτυό μας.

Με τα Windows server 2008 R2 και την χρήση πολιτικών έχει ελαχιστοποιηθεί η χρήση σεναρίων. Η χρήση σεναρίων αυξάνει τον χρόνο και την πολυπλοκότητα της διαχείρισης.

Η επόμενη γενιά του Ενεργού καταλόγου είναι το NGAD (next generation active directory). Το NGAD έρχεται να προστεθεί στον Ενεργό κατάλογο δίνοντας την δυνατότητα προγραμματισμού σε API. Θα είναι ενδιαφέρον να δούμε πώς η Microsoft σχεδιάζει να παντρέψει αυτές τις δύο τεχνολογίες και ποιο είναι το πραγματικό όφελος για τους τελικούς χρήστες και τους προγραμματιστές.

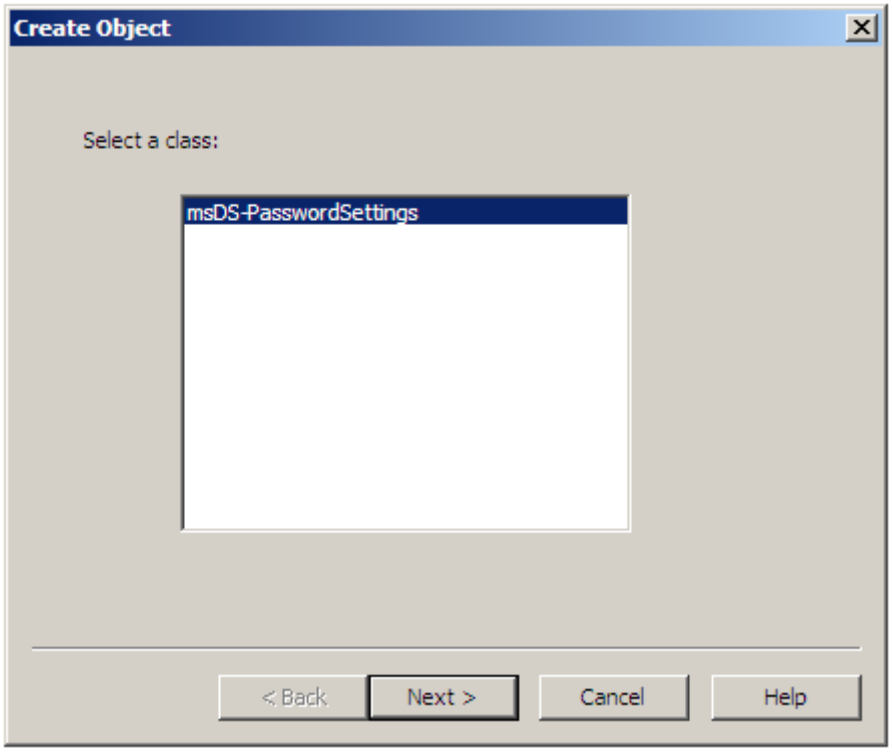
ΠΑΡΑΡΤΗΜΑ

Δημιουργία κωδικών πρόσβασης ανά ομάδα εργασίας.

1. Κάνουμε κλικ στο start και πληκτρολογούμε στο run adsiedit.msc.
2. Στη κονσόλα που εμφανίζεται κάνουμε διπλό κλικ στον τομέα και διπλό κλικ στο CN=System.
3. Κάνουμε δεξί κλικ στο CN=Password Settings Container και New object. Σε αυτό το σημείο αρχίζει η διαδικασία δημιουργίας νέου αντικειμένου με πολιτικές που θα καθορίσουμε εμείς.

Ας δούμε όμως τις επιλογές που έχουμε.

Όταν δημιουργούμε ένα αντικείμενο αυτό ανήκει σε κάποια κλάση. Έτσι το νέο αντικείμενο δημιουργείται στην κλάση msDS-Password Settings.



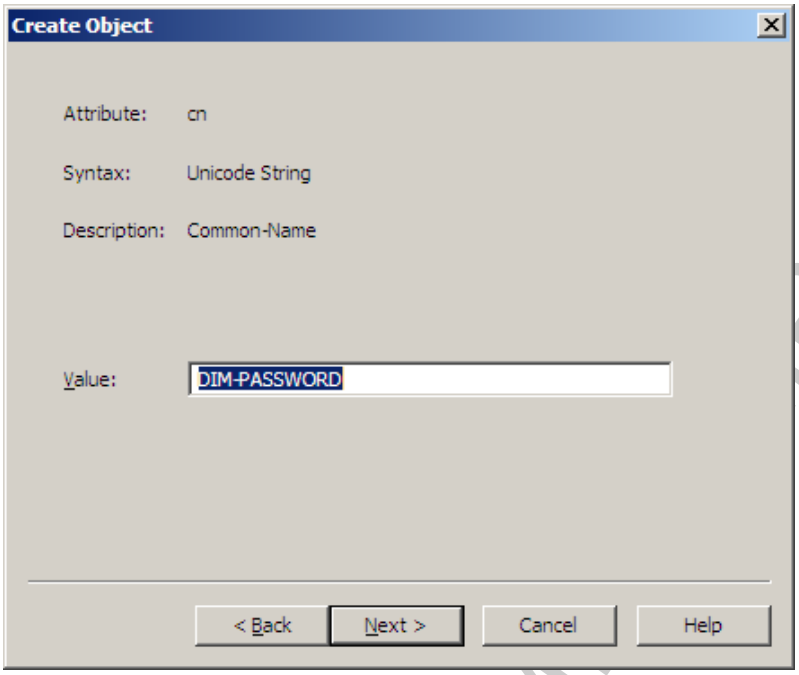
Εικόνα 1: Δημιουργία κωδικών

Δημιουργούμε τρία PSO. Για το δημοτικό με το όνομα DIM-PASSWORD,για το γυμνάσιο και το λύκειο GL-PASSWORD και AUSERS-PASSWORD για τους υπόλοιπους χρήστες). Οι μαθητές του δημοτικού θα έχουν πολύ λίγα δικαιώματα-επιλογές στον τρόπο χρήσης του υπολογιστή. Οι πιθανότητες να δημιουργήσουν άθελα τους κάποιο πρόβλημα είναι μηδενικές. Επίσης ένα από τα χαρακτηριστικά γνωρίσματα της ηλικίας τους είναι το ότι ξεχνάνε εύκολα. Για αυτό το λόγω δεν θα βάλουμε κωδικούς πρόσβασης. Το όνομα χρήστη είναι εύκολο να το θυμούνται γιατί είναι το δικό τους.

Οι μαθητές του γυμνασίου και του λυκείου και έχουν περισσότερα δικαιώματα και προσβάσεις στο ενδοδίκτυο αλλά και στο διαδίκτυο αλλά θα πρέπει να μάθουν και να προστατεύονται με κωδικούς. Εδώ η πολιτική που ακολουθείται είναι το μήκος του κωδικού να είναι το λιγότερο με 7 χαρακτήρες. Συνηθίζονταν ο κωδικός να είναι η ημερομηνία γέννησης. Κάτι που είναι γνωστό σε πολλούς άρα δεν υπήρχε και μεγάλη προστασία.

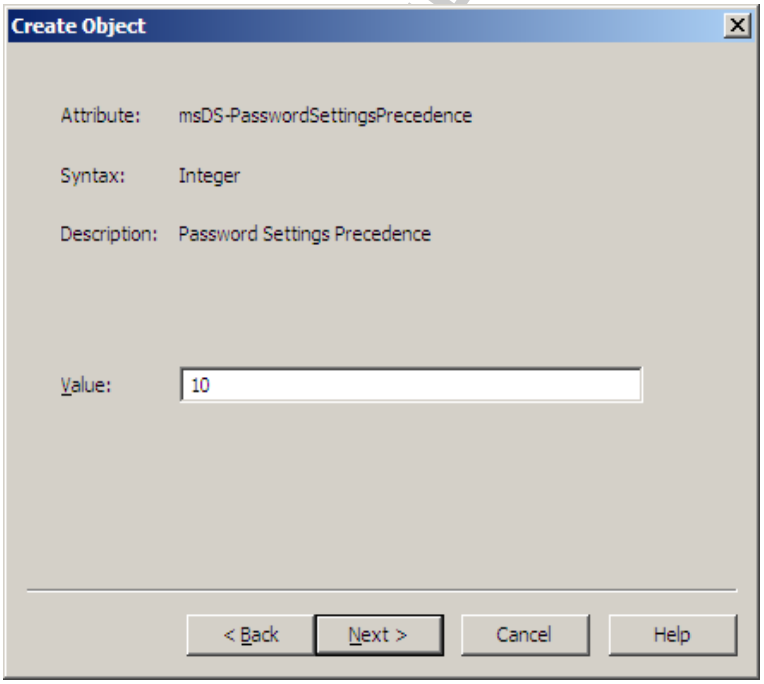
Τέλος όλοι οι υπόλοιποι χρήστες του δικτύου (AUSER) είναι χρήστες οι οποίοι χειρίζονται πολύ το ενδοδίκτυο και το διαδίκτυο. Αποθηκεύουν προσωπικά δεδομένα στο δίκτυο ή οικονομικά στοιχεία (λογιστήριο) του σχολείου. Για την μεγαλύτερη ασφάλεια των δεδομένων υιοθετούμε την πολιτική κωδικών με τα εξής χαρακτηριστικά:

- Ελάχιστο μήκος κωδικού : 7 χαρακτήρες
- Ενεργοποίηση της πολυπλοκότητας κωδικού
- Ο λογαριασμός του χρήστη να κλειδώνει στην τέταρτη αποτυχημένη προσπάθεια και να ξεκλειδώνει μόνο από τον διαχειριστή. (Σε μεγάλους οργανισμούς η Microsoft προτείνει και ταυτοποίηση στοιχείων του χρήστη).



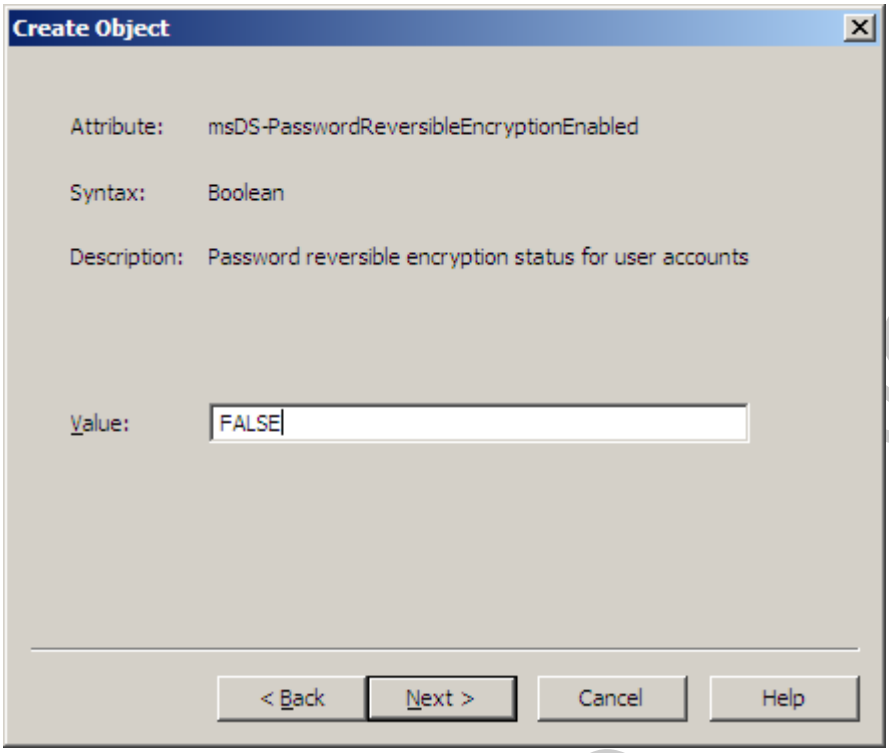
Εικόνα 2: Όνομα Πολιτικής

Για την αποφυγή των συγκρούσεων (conflict) των PSO δίνουμε την τιμή 10 στο Password Settings Precedence.

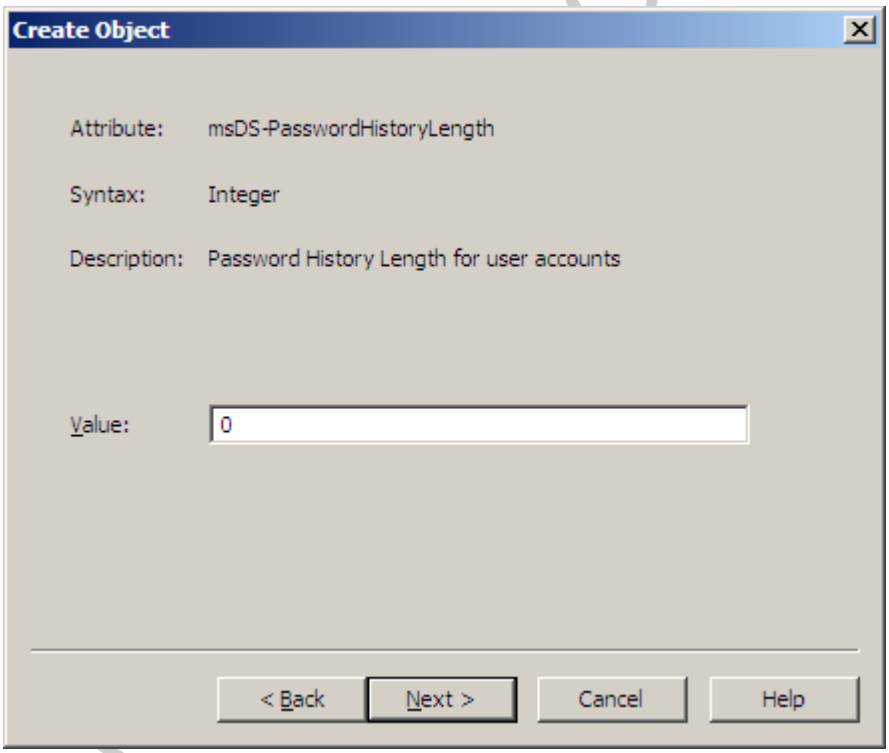


Εικόνα 3: Password Settings Precedence

Δεν θέλουμε κρυπτογράφηση του κωδικού οπότε επιλέγουμε FALSE.

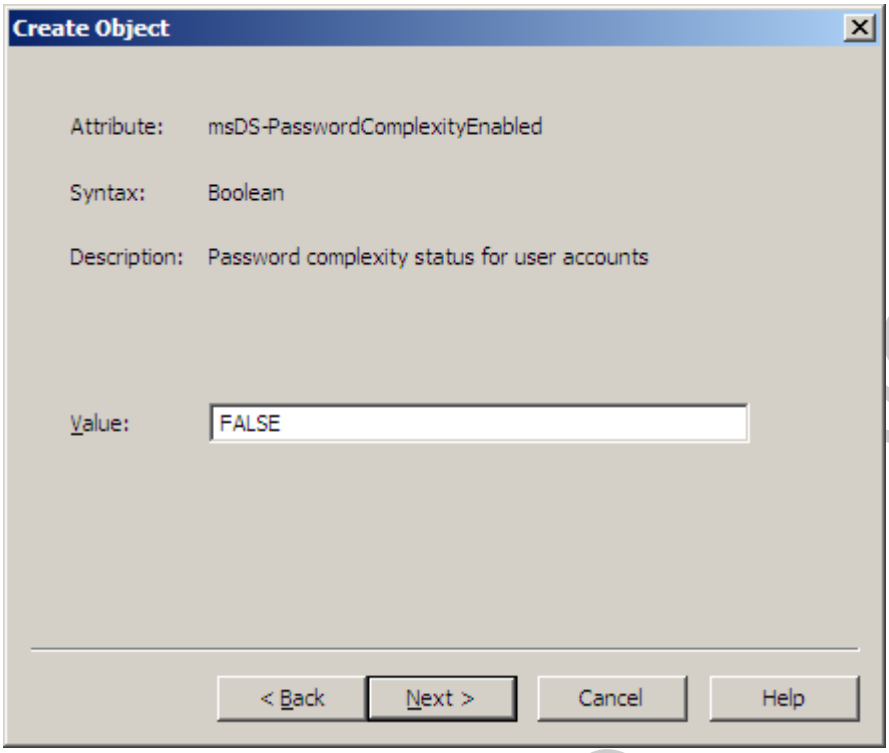


Εικόνα 4: Κρυπτογράφηση κωδικού



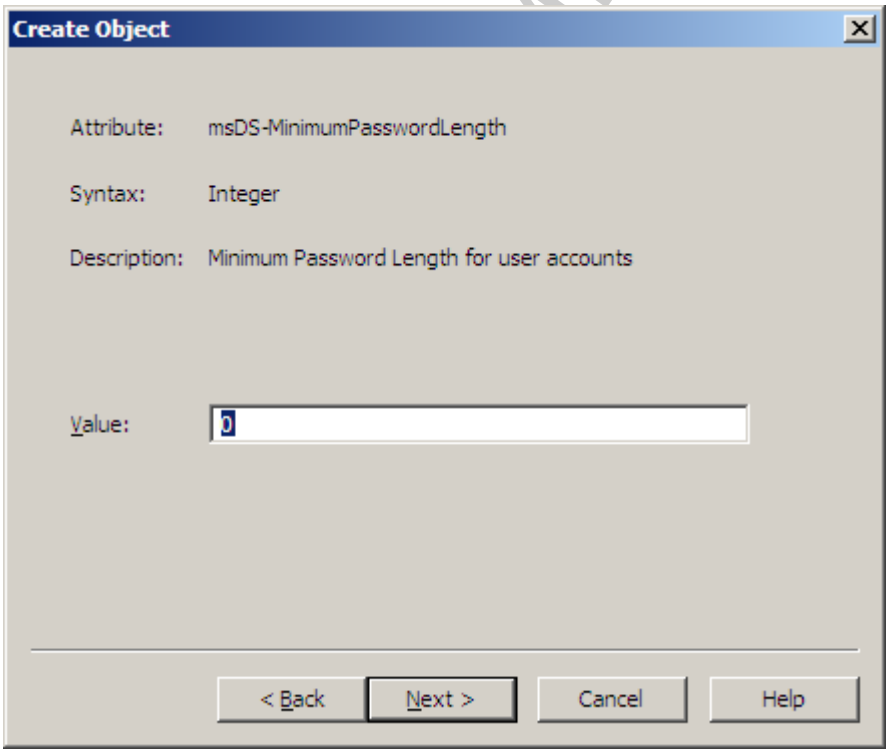
Εικόνα 5: Ιστορικό κωδικού

Δεν θέλουμε πολύπλοκο κωδικό για τους μαθητές. Η τιμή γίνεται TRUE για τους υπόλοιπους χρήστες.



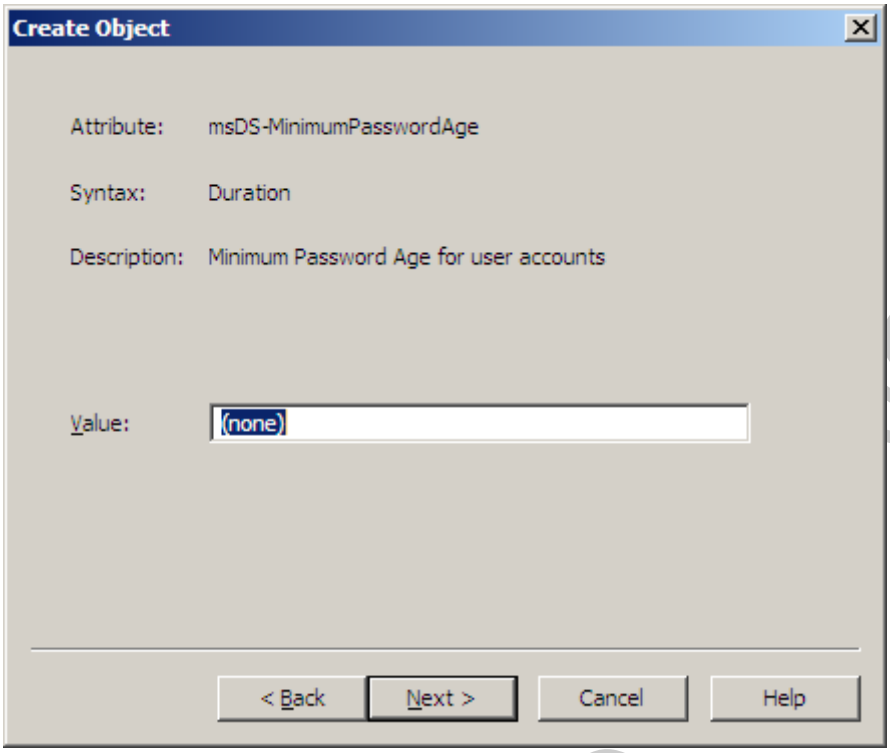
Εικόνα 6: Πολυπλοκότητα κωδικού

Ορίζουμε ελάχιστο μήκος κωδικού για τους μαθητές του δημοτικού 0 και για τους υπόλοιπους χρήστες 7.

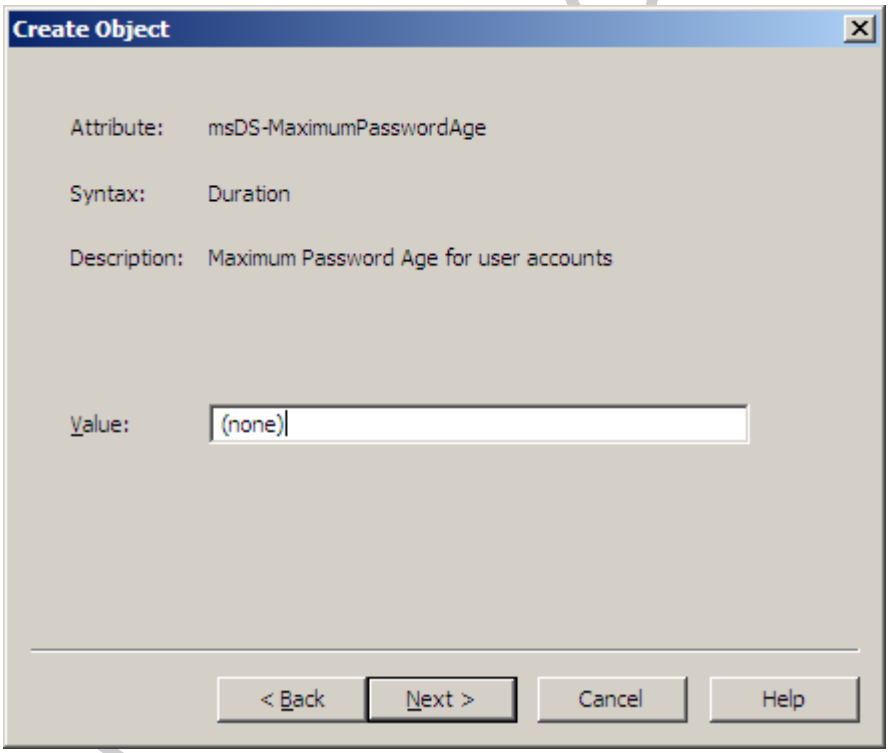


Εικόνα 7: Ελάχιστο μήκος κωδικού

Δεν μας ενδιαφέρει ούτε η ελάχιστη ούτε η μέγιστη ηλικία του κωδικού.

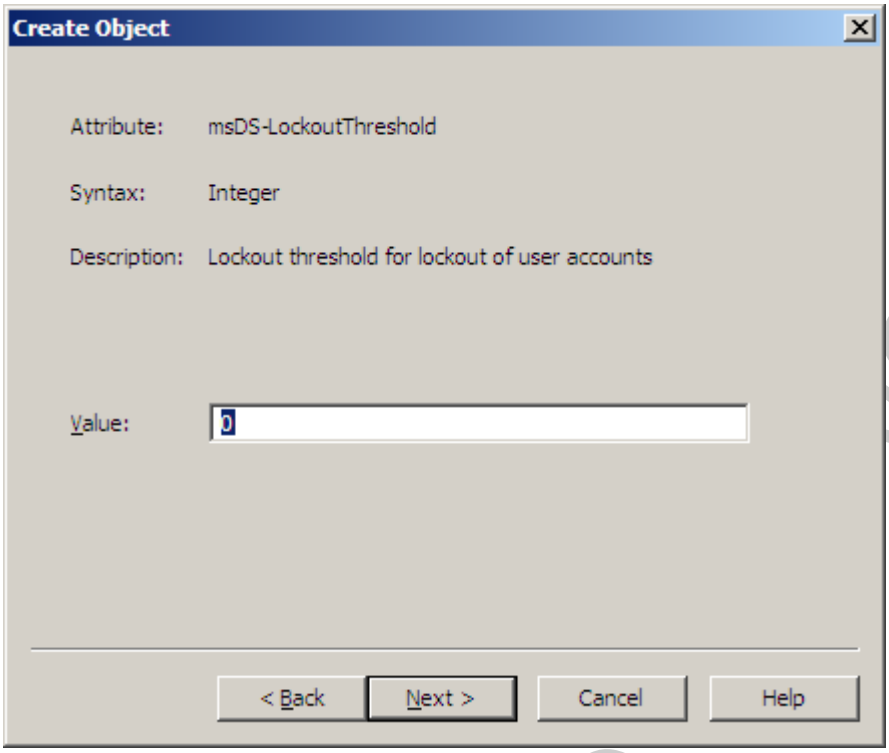


Εικόνα 8: Ελάχιστη ηλικία κωδικού



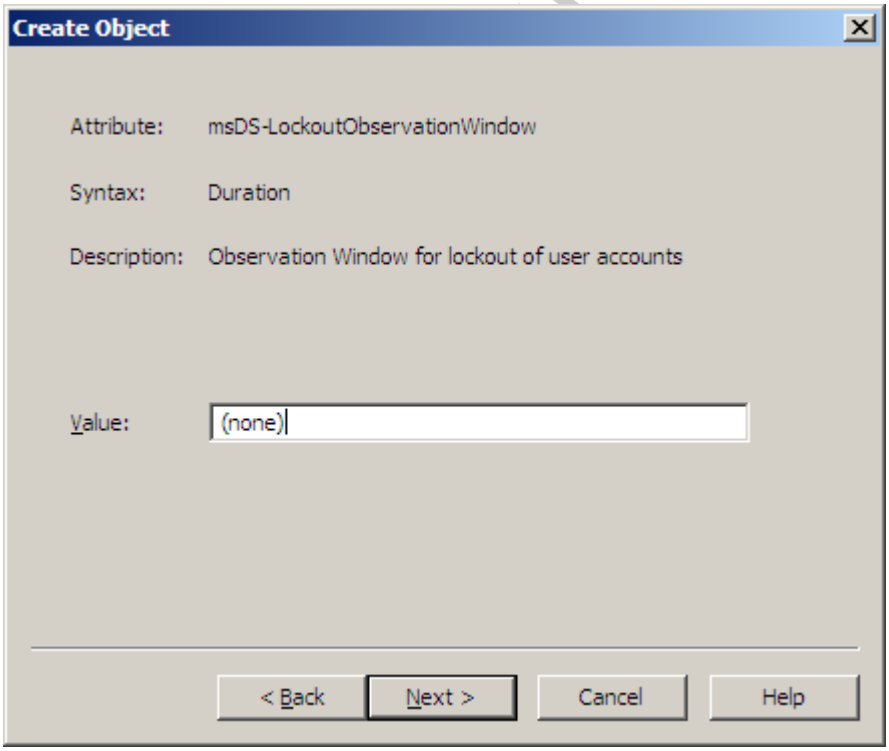
Εικόνα 9: Μέγιστη ηλικία κωδικού

Ο λογαριασμός των μαθητών δεν θα κλειδώνει ποτέ. Αντίθετα για τους υπόλοιπους χρήστες εδώ μπαίνει η τιμή 4.

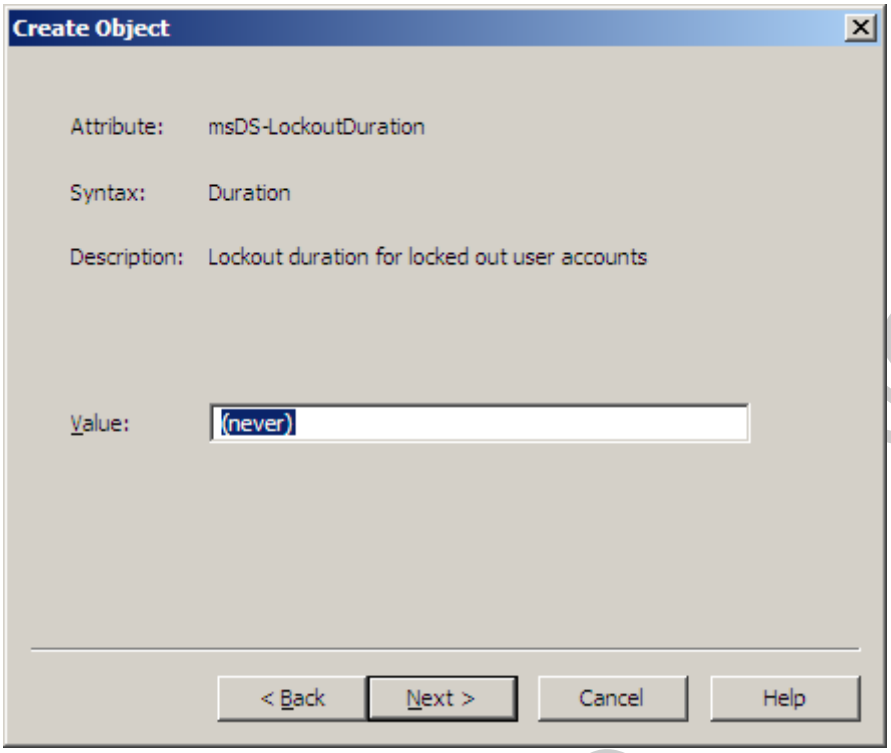


Εικόνα 10: Κλείδωμα χρήστη

Η διάρκεια κλειδώματος ενός λογαριασμού δεν ορίζεται.

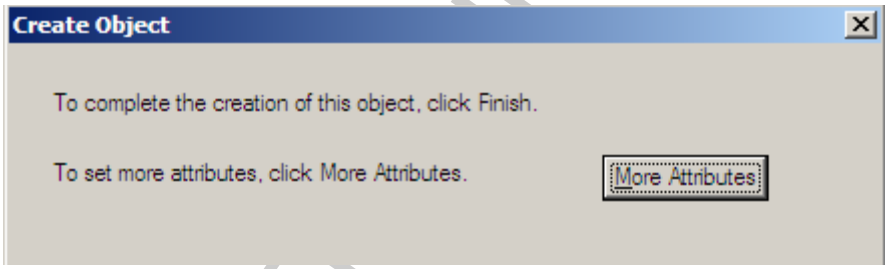


Εικόνα 11: Κλείδωμα χρήστη

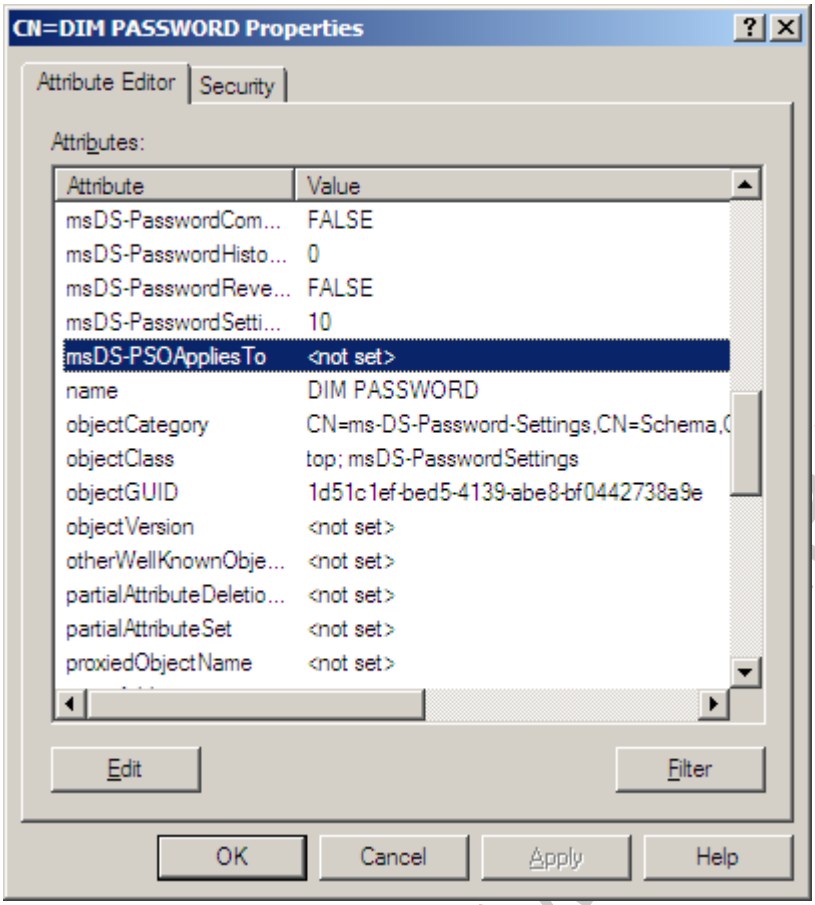


Εικόνα 12: Διάρκεια κλειδώματος

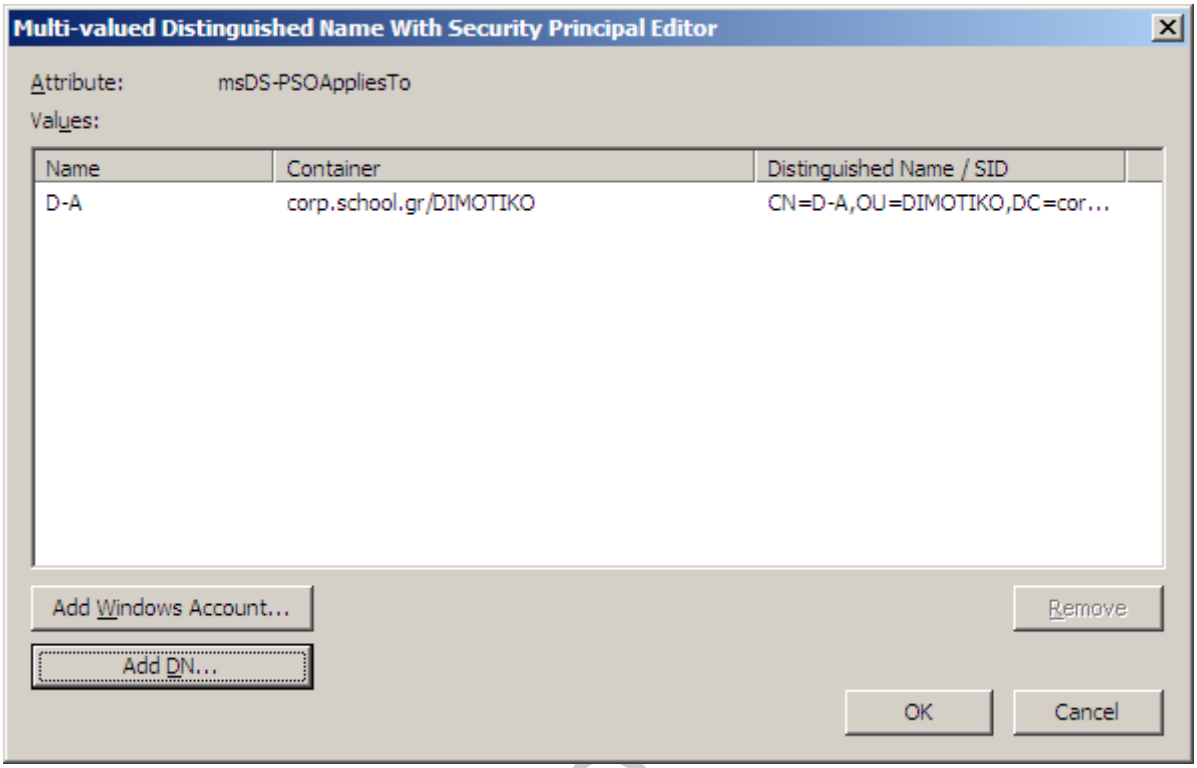
Τέλος στην επιλογή More Attributes πέρα του ότι μπορούμε να διορθώσουμε ή να αλλάζουμε τις ιδιότητες που θέλουμε, το πιο βασικό είναι ότι δηλώνουμε με την επιλογή msDS –PSOApliesTo την ομάδα στην οποία έχουμε εφαρμόσει την αντίστοιχη πολιτική για κωδικούς.



Εικόνα 13: More Attributes



Εικόνα 14: Ιδιότητες



Εικόνα 15: Διορθωτής πολιτικής

Εκτός από το γραφικό περιβάλλον μπορούμε να δημιουργήσουμε PSO δημιουργώντας σενάριο (script) όπως το παρακάτω, το οποίο το εισάγουμε στο αντίστοιχο container.

- dn: CN=corp, CN=Password Settings Container,CN=System,DC=D-A
- changetype: add
- objectClass: msDS-PasswordSettings
- msDS-MaximumPasswordAge:-1728000000000
- msDS-MinimumPasswordAge:-864000000000
- msDS-MinimumPasswordLength:8
- msDS-PasswordHistoryLength:24
- msDS-PasswordComplexityEnabled:TRUE
- msDS-PasswordReversibleEncryptionEnabled:FALSE
- msDS-LockoutObservationWindow:-18000000000
- msDS-LockoutDuration:-18000000000
- msDS-LockoutThreshold:0
- msDS-PasswordSettingsPrecedence:20
- msDS-PSOAppliesTo:CN=user1,CN=Users,DC=dc1,DC=contoso,DC=com

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Πληροφοριακά Συστήματα. Ν. Αλωνιστιώτη, Β. Γαζής Πανεπιστήμιο Πειραιά.
2. http://el.wikipedia.org/wiki/%CE%9B%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B9%CE%BA%CF%8C_%CF%83%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1
3. http://el.wikipedia.org/wiki/Unix
4. http://www.mhpcc.edu/training/vitecbids/UnixIntro/Overview.html#Whatis
5. http://www.doc.ic.ac.uk/~wjk/UnixIntro/Lecture1.html
6. http://ph150.edu.physics.uoc.gr/view.php?s=3&b=1&p=1
7. http://windows.microsoft.com/el-GR/windows/history
8. http://www.computerhope.com/issues/ch000575.htm
9. http://www.doecirc.energy.gov/documents/MS_Active_Directory_Design_Guide.pdf (John Dias 2002)
10. http://www.williamstanek.com/windows/ (William R. Stanek)
11. http://searchwinit.techtarget.com/definition/Zero-Administration
12. Help των Windows server 2008 R2
13. http://en.wikipedia.org/wiki/RAID
14. http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx
15. http://www.tech-faq.com/understanding-dhcp.html
16. http://www.microsoft.com/windowsserver2008/en/us/file-print.aspx
17. http://www.petri.co.il/windows-2008-print-server-management.htm
18. http://serverfault.com/questions/218686/server-2008-print-server-vs-network-printer
19. http://www.networkworld.com/news/2010/021710-active-directory-turns-10.html?page=2
20. http://conklintechnology.com/site/2009/11/18/microsofts-next-generation-active-directory/
21. Help των Windows server 2008 R2