ΕΠ ΚτΠ
Χρηματοδότηση:
Ευρωπαϊκό Κοινωνικό Ταμείο: 75%
Εθνικοί Πόροι: 25%

# Εκπαιδευτικό Υλικό για την

# «Εγκατάσταση και Διαμόρφωση ΣΕΠΕΗΥ με Windows Server 2003 και Windows XP»

Ανάδοχος: Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών

Ιούνιος 2008

Αναπτύχθηκε στο πλαίσιο υλοποίησης του Υποέργου 2
«Πρακτική Εκπαίδευση Εκπαιδευτικών Πληροφορικής»

της Πράξης «Δράσεις Επιμόρφωσης Εκπαιδευτικών Πληροφορικής»
της Κατηγορίας Πράξεων 1.2.2
«Επιμόρφωση εκπαιδευτικών και Πιστοποίηση»
του Μέτρου 1.2
«Εισαγωγή και Αξιοποίηση των Νέων Τεχνολογιών στην Εκπαίδευση»

Περιεχόμενα

## Κατάλογος Πινάκων



## Κατάλογος Εικόνων

# 1 Εισαγωγή

Ένας μεγάλος αριθμός σχολικών εργαστηρίων είναι διαμορφωμένος γύρω από έναν εξυπηρετητή στον οποίο είναι αναπτυγμένο ένα MS-Windows 2003 domain. Οι σταθμοί εργασίας του εργαστηρίου λειτουργούν με βάση το λειτουργικό σύστημα MS-Windows XP Professional Greek. Κατά την εγκατάσταση των λειτουργικών συστημάτων του εξυπηρετητή και των σταθμών εργασίας καλείται κανείς να πραγματοποιήσει ορισμένες ρυθμίσεις προκειμένου να ολοκληρωθεί με επιτυχία η διαδικασία.

Το παρόν κείμενο αποτελεί μια πρόταση για την αρχική εγκατάσταση σχολικών εργαστηρίων αυτής της αρχιτεκτονικής. Διατυπώνεται μια άποψη για τον τρόπο λήψης αποφάσεων κατά την αρχική ρύθμιση των πληροφοριακών συστημάτων, ώστε να επιτυγχάνεται ομοιόμορφη διαμόρφωση των σχολικών εργαστηρίων με στόχο τη βέλτιστη απόδοση και την ασφάλεια από εξωτερικούς και εσωτερικούς κινδύνους, ενώ επιτυγχάνεται η επιθυμητή λειτουργικότητα και διευκολύνεται η διαχείριση. Δεν αποτελεί απαραίτητα και οδηγό επανεγκατάστασης, καθώς στην πλειονότητα των περιπτώσεων η επανεγκατάσταση των υπολογιστικών συστημάτων πραγματοποιείται αυτόματα με χρήση υπαρχόντων αντιγράφων ασφαλείας (images). Μπορεί όμως να χρησιμεύσει ως οδηγός ρύθμισης των υπολογιστικών συστημάτων και αντιμετώπισης προβλημάτων.

Γίνεται αναφορά με αναλυτικό τρόπο στα λειτουργικά συστήματα εξυπηρετητή και σταθμών εργασίας και στις αποφάσεις που πρέπει να ληφθούν κατά την εγκατάσταση και ρύθμιση αυτών. Ακολουθούν αναλυτικές οδηγίες σχετικά με τη δημιουργία του domain του σχολικού εργαστηρίου και την ένταξη των σταθμών εργασίας σε αυτό, ενώ γίνεται αναφορά και στην οργάνωση και διαχείρισή του.

# 2 Εγκατάσταση Windows 2003 Server στον εξυπηρετητή του σχολικού εργαστηρίου

Ο τρόπος με τον οποίο γίνεται η διάταξη των κατατμήσεων (partitioning) εξαρτάται από πολλές παραμέτρους, όπως η ύπαρξη περισσότερων σκληρών δίσκων στον εξυπηρετητή, καθώς και η χωρητικότητα αυτών ή η ανάγκη για εγκατάσταση άλλων λειτουργικών συστημάτων στον ίδιο υπολογιστή (π.χ. Linux). Οι γενικές οδηγίες που μπορούν να εφαρμοστούν σε κάθε περίπτωση είναι οι ακόλουθες:

- Να πραγματοποιείται διαχωρισμός κάθε σκληρού δίσκου σε περισσότερες από μία κατατμήσεις, ώστε να είναι δυνατή η υποστήριξη λειτουργιών όπως η λήψη αντιγράφων ασφαλείας των κατατμήσεων και η βελτιστοποίηση της απόδοσης με χρήση των κατατμήσεων με κατάλληλο τρόπο (π.χ. μεταφορά αρχείου σελιδοποίησης – pagefile).
- Ο σκληρός δίσκος (ή η διαμόρφωση δύο δίσκων σε συστοιχία RAID0 ή RAID1) που περιέχει την πρωτεύουσα κατάτμηση να διαχωρίζεται ως εξής:
    - Η κύρια κατάτμηση που περιλαμβάνει το λειτουργικό σύστημα και τις εγκατεστημένες εφαρμογές να καταλαμβάνει το 30% του σκληρού δίσκου. Η λήψη αντιγράφου ασφαλείας αυτής της κατάτμησης επαρκεί για έκτακτες περιπτώσεις αντιμετώπισης καταστροφών (disaster recovery). Το όνομα (volume label) της κατάτμησης προτείνεται να είναι ‘system’.
    - Η δεύτερη κατάτμηση να καταλαμβάνει το 20% της διαθέσιμης χωρητικότητας. Σε αυτή θα αποθηκεύονται τα αρχεία χρηστών, συνεπώς η λήψη αντιγράφου ασφαλείας αυτής της κατάτμησης θα εξασφαλίζει τη φύλαξη της πλειοψηφίας των δεδομένων των χρηστών (data backup). Το όνομα (volume label) της κατάτμησης προτείνεται να είναι ‘data’.
    - Ο χώρος που απομένει και αποτελεί το 50% της χωρητικότητας του σκληρού δίσκου προτείνεται να χρησιμοποιείται για τη λήψη αντιγράφων ασφαλείας αν δεν υπάρχει δεύτερος σκληρός δίσκος. Το όνομα (volume label) της κατάτμησης προτείνεται να είναι ‘backup’. Αν υπάρχει δεύτερος σκληρός δίσκος τότε οι δύο κατατμήσεις ‘system’ & ‘data’ προτείνεται να καταλαμβάνουν το 60 & 40% του σκληρού δίσκου αντίστοιχα.
- Αν είναι διαθέσιμος και δεύτερος σκληρός δίσκος που δεν συμμετέχει σε κάποια διαμόρφωση RAID0 ή RAID1, προτείνεται ο διαχωρισμός του σε 2 κατατμήσεις ως εξής:

  - Η πρώτη κατάτμηση καταλαμβάνει το 50% της χωρητικότητας του σκληρού δίσκου. Σε αυτή αποθηκεύονται συχνά προσπελάσιμα αρχεία του λειτουργικού συστήματος και των εφαρμογών για βελτιστοποίηση της απόδοσης (αρχεία σελιδοποίησης [pagefile], προσωρινής αποθήκευσης [caching, temporary folders] κλπ). Το όνομα (volume label) της κατάτμησης προτείνεται να είναι 'temp'.
  - Η δεύτερη κατάτμηση καταλαμβάνει το υπόλοιπο 50% και προτείνεται να χρησιμοποιείται για τη λήψη αντιγράφων ασφαλείας. Το όνομα (volume label) της κατάτμησης προτείνεται να είναι 'backup'.
- Η διαμόρφωση των κατατμήσεων να πραγματοποιείται με χρήση του συστήματος αρχείων NTFS.

Κατά την αρχική εγκατάσταση ζητείται η ρύθμιση των 'Regional and Language options'. Προφανώς, λόγω της χρήσης του εξυπηρετητή του σχολικού εργαστηρίου θα πρέπει να επιλεγούν τα ελληνικά (Greek) όπου υποστηρίζονται (χρήση και επεξεργασία αριθμών, νομίσματος, ημερομηνίας, ώρας και λειτουργία πληκτρολογίου).

Στη συνέχεια ζητείται ένα όνομα και ένας οργανισμός (Name & Organization), που δεν έχουν ιδιαίτερη βαρύτητα και μπορούν να επιλεχθούν με τυχαίο τρόπο. Για λόγους ομοιομορφίας μόνο προτείνεται να δίνονται τα ακόλουθα ονόματα:

- Name: SCHOOL
- Organization: ΥΡΕΡΤΗ

Ανάλογα με τις άδειες που έχουν αγοραστεί (το σχολείο διαθέτει το αντίστοιχο CAL) συμπληρώνεται και το Licensing mode.

Σε ότι αφορά το όνομα του υπολογιστή (computer name) είναι δυνατές διάφορες προσεγγίσεις. Προτείνεται απλώς να δίνεται το όνομα 'Server' ώστε να είναι ξεκάθαρος ο ρόλος του υπολογιστή. Δεν υπάρχει λόγος εφαρμογής πιο πολύπλοκων σχημάτων ονοματολογίας, που π.χ. εμπλέκουν το DNS όνομα που έχει δοθεί από το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ). Μόνο αν στη σχολική μονάδα συνυπάρχουν δύο διαφορετικά εργαστήρια με ανεξάρτητο domain προτείνεται να δίνονται διαφορετικά ονόματα στους εξυπηρετητές για την αποφυγή προβλημάτων (π.χ. 'Server1', 'Server2' κλπ).

Στη συνέχεια ζητείται ο κωδικός ασφαλείας του διαχειριστή του συστήματος (administrator password). Η πρακτική χρήσης προφανούς ή κοινού κωδικού ασφαλείας δεν προτείνεται. Είναι επιθυμητό κατά την αρχική εγκατάσταση να

ορίζεται προσωρινός κωδικός ασφαλείας, που πρέπει στη συνέχεια να αλλαχθεί από το διαχειριστή (π.χ. password: Changeme!).

Στις ρυθμίσεις δικτύου μπορούν να επιλεγούν 'Network typical settings' και η ένταξη του υπολογιστή σε workgroup. Η δημιουργία του domain προτείνεται να πραγματοποιηθεί σε μεταγενέστερη φάση, όταν έχει επιβεβαιωθεί η καλή λειτουργία του υπολογιστή. Οι TCP/IP ρυθμίσεις μπορούν να πραγματοποιηθούν σύμφωνα με τις οδηγίες που έχουν εκδοθεί για τη διασύνδεση σχολικών εργαστηρίων στο ΠΣΔ.

Συνοπτικά αναφέρεται ότι κάθε εξυπηρετητής έχει IP διεύθυνση της μορφής 10.x.y.z όπου οι τιμές x & y εξαρτώνται από τη σχολική μονάδα και λαμβάνονται μετά από επικοινωνία με το helpdesk του ΠΣΔ (8011180181) και η τιμή z είναι 10 για τον πρώτο εξυπηρετητή της σχολικής μονάδας, 11 για τον δεύτερο εξυπηρετητή κ.ο.κ. Το subnet mask είναι της μορφής 255.255.255.0 και το default gateway έχει τιμή 10.x.y.1 όπου οι τιμές x & y παραμένουν ίδιες με αυτές της IP διεύθυνσης. Ως DNS Server ορίζεται η IP διεύθυνση του ίδιου του εξυπηρετητή (10.x.y.z).

Δεν ενεργοποιούμε το πρωτόκολλο WINS ούτε τη ρύθμιση "Enable LMHOSTS lookup", ενώ επιλέγουμε "Disable NetBIOS over TCP/IP".

Η τυπική εγκατάσταση των Windows 2003 Server περιλαμβάνει σχεδόν όλες τις απαραίτητες συνιστώσες (Windows components). Μόνο για την ενεργοποίηση της δυνατότητας απομακρυσμένης διαχείρισης του εξυπηρετητή, πρέπει να γίνει επιπλέον επιλογή της εγκατάστασης των Terminal Services σε administration mode. Η υπηρεσία DNS εγκαθίσταται αυτόματα και ρυθμίζεται κατά τη δημιουργία του domain σύμφωνα με τις σχετικές οδηγίες που ακολουθούν.

Μετά την εγκατάσταση του λειτουργικού συστήματος είναι πιθανό να απαιτείται η ενεργοποίησή του μέσα σε κάποιο χρονικό διάστημα για να είναι δυνατή η περαιτέρω χρήση του (product activation). Η άδεια χρήσης καθορίζει αν είναι απαραίτητο κάτι τέτοιο καθώς και το διάστημα που μπορεί να χρησιμοποιηθούν τα Windows 2003 Server χωρίς ενεργοποίηση. Η βέλτιστη μέθοδος για τους εξυπηρετητές των σχολικών εργαστηρίων είναι να πραγματοποιείται η διαδικασία μέσω διαδικτύου (Start / Programs / Accessories / System tools / Activate Windows ή μέσω του εικονιδίου που εμφανίζεται στην μπάρα εργασιών). Δεν χρειάζεται να γίνεται δήλωση (registration) του λειτουργικού συστήματος.

Απαραίτητη προϋπόθεση για την εύρυθμη λειτουργία του λειτουργικού συστήματος είναι η εγκατάσταση όλων των κρίσιμων ενημερώσεων. Αρχικά

εγκαθίσταται το τελευταίο service pack του λειτουργικού συστήματος (SP1) αν δεν περιεχόταν στο cd εγκατάστασης που χρησιμοποιήθηκε. Στη συνέχεια εγκαθίστανται όλες οι νεότερες κρίσιμες εκδόσεις, καθώς και ανανεώσεις που αφορούν το εγκατεστημένο υλικό και λογισμικό από την ιστοσελίδα http://windowsupdate.microsoft.com.

Τμήμα της εγκατάστασης του λειτουργικού συστήματος θεωρείται και η εγκατάσταση των οδηγών συσκευών (system drivers) της μητρικής, των καρτών επέκτασης και των περιφερειακών συσκευών. Μπορεί να γίνει χρήση των μέσων (cd's, δισκέτες κλπ) που παρασχέθηκαν μαζί με το υπολογιστικό σύστημα. Προτείνεται όμως να εγκαθίστανται οι τελευταίες εκδόσεις των οδηγών, που στην πλειονότητα των περιπτώσεων μπορούν να ληφθούν από το διαδίκτυο.

Η εγκατάσταση του εκτυπωτή, που συνήθως είναι συνδεδεμένος στον εξυπηρετητή μπορεί να γίνει σε αυτό το σημείο σύμφωνα με τις οδηγίες του εκάστοτε μοντέλου. Για τη χρήση της υπηρεσίας εκτύπωσης από όλους τους χρήστες του εργαστηρίου ο εκτυπωτής πρέπει να διαμοιραστεί, οπότε ο εξυπηρετητής αναλαμβάνει και το ρόλο του διακομιστή εκτυπώσεων.

# 3 Εγκατάσταση Windows XP στους σταθμούς εργασίας του σχολικού εργαστηρίου

Η φιλοσοφία που διέπει την εγκατάσταση του λειτουργικού συστήματος στους σταθμούς εργασίας είναι ανάλογη με την προαναφερόμενη του εξυπηρετητή του εργαστηρίου. Συνεπώς σε πολλά σημεία ακολουθείται κοινή πρακτική.

Ο τρόπος με τον οποίο γίνεται η διάταξη των κατατμήσεων (partitioning) εξαρτάται από πολλές παραμέτρους, όπως η ύπαρξη περισσοτέρων σκληρών δίσκων, καθώς και η χωρητικότητα αυτών ή η ανάγκη για εγκατάσταση άλλων λειτουργικών συστημάτων στον ίδιο υπολογιστή (π.χ. Linux). Οι γενικές οδηγίες που μπορούν να εφαρμοστούν στη συνηθισμένη περίπτωση ύπαρξης ενός μόνο σκληρού δίσκου είναι οι ακόλουθες:

- Να πραγματοποιείται διαχωρισμός του σκληρού δίσκου σε περισσότερες από μία κατατμήσεις, ως εξής:

  - Η κύρια κατάτμηση που περιλαμβάνει το λειτουργικό σύστημα και τις εγκατεστημένες εφαρμογές να καταλαμβάνει το 30% του σκληρού δίσκου. Η λήψη αντιγράφου ασφαλείας αυτής της κατάτμησης επαρκεί για έκτακτες περιπτώσεις αντιμετώπισης καταστροφών (disaster recovery). Το όνομα (volume label) της κατάτμησης προτείνεται να είναι ‘system’.

  - Η δεύτερη κατάτμηση να καταλαμβάνει το 30% της διαθέσιμης χωρητικότητας και να χρησιμοποιείται αν είναι επιθυμητό για την εγκατάσταση δεύτερου λειτουργικού συστήματος. Το όνομα (volume label) της κατάτμησης προτείνεται να είναι ομώνυμο του λειτουργικού συστήματος που έχει εγκατασταθεί (π.χ. ‘linux’).

  - Ο χώρος που απομένει και αποτελεί το 40% της χωρητικότητας του σκληρού δίσκου προτείνεται να χρησιμοποιείται για τη λήψη αντιγράφων ασφαλείας. Το όνομα (volume label) της κατάτμησης προτείνεται να είναι ‘backup’.

- Η διαμόρφωση της κατάτμησης system να πραγματοποιείται με χρήση του συστήματος αρχείων NTFS, ενώ της κατάτμησης backup με χρήση του συστήματος αρχείων FAT32.

Κατά την αρχική εγκατάσταση ζητείται η ρύθμιση των ‘Regional and Language options’. Προφανώς, λόγω της χρήσης των σταθμών εργασίας του σχολικού εργαστηρίου θα πρέπει να επιλεγούν τα ελληνικά (Greek) όπου υποστηρίζονται (χρήση και επεξεργασία αριθμών, νομίσματος, ημερομηνίας, ώρας και

λειτουργία πληκτρολογίου). Όταν εγκαθίστανται ελληνικές εκδόσεις του λειτουργικού συστήματος – όπως συμβαίνει στην πλειονότητα των εργαστηρίων – η ρύθμιση είναι εξ' αρχής ενεργοποιημένη.

Στη συνέχεια ζητείται ένα όνομα και ένας οργανισμός (Name & Organization), που δεν έχουν ιδιαίτερη βαρύτητα και μπορούν να επιλεχθούν με τυχαίο τρόπο. Για λόγους ομοιομορφίας μόνο προτείνεται να δίνονται τα ακόλουθα ονόματα:

- Name: SCHOOL
- Organization: ΥΡΕΡΤΗ

Σε ότι αφορά το όνομα του υπολογιστή (computer name) είναι δυνατές διάφορες προσεγγίσεις. Προτείνεται να δίνεται το όνομα 'ClientXY' και η αρίθμηση να ακολουθεί την τοποθέτηση των σταθμών εργασίας στο χώρο του εργαστηρίου.

Στη συνέχεια ζητείται ο κωδικός ασφαλείας του διαχειριστή του συστήματος (administrator password). Η πρακτική χρήσης προφανούς ή κοινού κωδικού ασφαλείας δεν προτείνεται. Είναι επιθυμητό κατά την αρχική εγκατάσταση να ορίζεται προσωρινός κωδικός ασφαλείας, που πρέπει στη συνέχεια να αλλαχθεί από το διαχειριστή (π.χ. password: Changeme!).

Στις ρυθμίσεις δικτύου μπορούν να επιλεγούν 'Network typical settings' και η ένταξη του υπολογιστή σε workgroup. Η εισαγωγή του σταθμού εργασίας στο domain προτείνεται να πραγματοποιηθεί σε μεταγενέστερη φάση, όταν έχει επιβεβαιωθεί η καλή λειτουργία του υπολογιστή. Στις TCP/IP ρυθμίσεις δεν απαιτείται οποιαδήποτε επέμβαση, αφού υπάρχει στο εργαστήριο υπηρεσία DHCP. Δεν ενεργοποιούμε το πρωτόκολλο WINS ούτε τη ρύθμιση "Enable LMHOSTS lookup", ενώ επιλέγουμε "Disable NetBIOS over TCP/IP".

Μετά την εγκατάσταση του λειτουργικού συστήματος είναι πιθανό να απαιτείται η ενεργοποίησή του μέσα σε κάποιο χρονικό διάστημα για να είναι δυνατή η περαιτέρω χρήση του (product activation). Η άδεια χρήσης καθορίζει αν είναι απαραίτητο κάτι τέτοιο καθώς και το διάστημα που μπορεί να χρησιμοποιηθούν τα Windows XP Professional χωρίς ενεργοποίηση. Η βέλτιστη μέθοδος για τους σταθμούς εργασίας των σχολικών εργαστηρίων είναι να πραγματοποιείται η διαδικασία μέσω διαδικτύου (Start / Programs / Accessories / System tools / Activate Windows ή μέσω του εικονιδίου που εμφανίζεται στην μπάρα εργασιών). Δεν χρειάζεται να γίνεται δήλωση (registration) του λειτουργικού συστήματος.

Απαραίτητη προϋπόθεση για την εύρυθμη λειτουργία του λειτουργικού συστήματος είναι η εγκατάσταση όλων των κρίσιμων ενημερώσεων. Αρχικά

εγκαθίσταται το τελευταίο service pack του λειτουργικού συστήματος (SP2) αν δεν περιεχόταν στο cd εγκατάστασης που χρησιμοποιήθηκε. Στη συνέχεια εγκαθίστανται όλες οι νεότερες κρίσιμες εκδόσεις, καθώς και ανανεώσεις που αφορούν το εγκατεστημένο υλικό και λογισμικό από την ιστοσελίδα http://windowsupdate.microsoft.com.

Τμήμα της εγκατάστασης του λειτουργικού συστήματος θεωρείται και η εγκατάσταση των οδηγών συσκευών (system drivers) της μητρικής, των καρτών επέκτασης και των περιφερειακών συσκευών. Μπορεί να γίνει χρήση των μέσων (cd's, δισκέτες κλπ) που παρασχέθηκαν μαζί με το υπολογιστικό σύστημα. Προτείνεται όμως να εγκαθίστανται οι τελευταίες εκδόσεις των οδηγών, που στην πλειονότητα των περιπτώσεων μπορούν να ληφθούν από το διαδίκτυο. Η εγκατάσταση του εκτυπωτή που διαμοιράζεται από τον εξυπηρετητή του εργαστηρίου μπορεί να πραγματοποιηθεί σε αυτή τη φάση.

# 4 Διαμόρφωση domain σχολικού εργαστηρίου

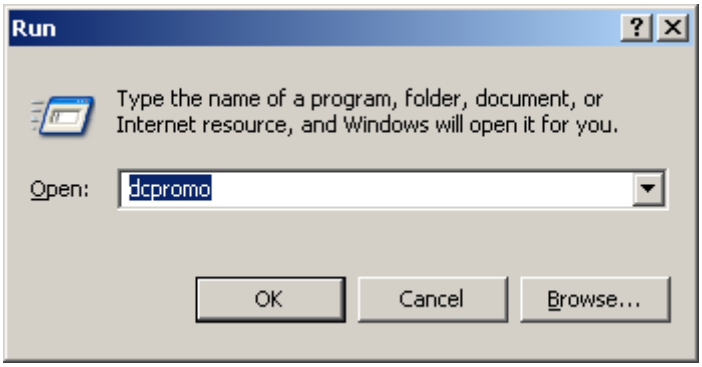
Σε κάθε σχολική μονάδα είναι ανεπτυγμένη υποδομή σε ανεξάρτητο δέντρο και δάσος του ενεργού καταλόγου σε σχέση με τα υπόλοιπα σχολεία. Η διαδικασία δημιουργίας του παραπάνω σχήματος περιγράφεται στη συνέχεια.

## 4.1 Εγκατάσταση domain

Μετά την εγκατάσταση των λειτουργικών συστημάτων στον εξυπηρετητή και στους σταθμούς εργασίας του σχολικού εργαστηρίου, είναι δυνατή η δημιουργία του domain και η ένταξη όλων των υπολογιστών σε αυτό. Η διαδικασία στον εξυπηρετητή γίνεται με χρήση του ενσωματωμένου οδηγού, που μπορεί να κληθεί με δύο τρόπους. Είτε εκτελείται από τη γραμμή εντολών η εντολή 'dcpromo', είτε μέσα από το γραφικό περιβάλλον (εφαρμογή 'Manage your server') επιλέγεται η αναβάθμιση του εξυπηρετητή σε domain controller. Και στις δύο περιπτώσεις η υπόλοιπη διαδικασία είναι κοινή.

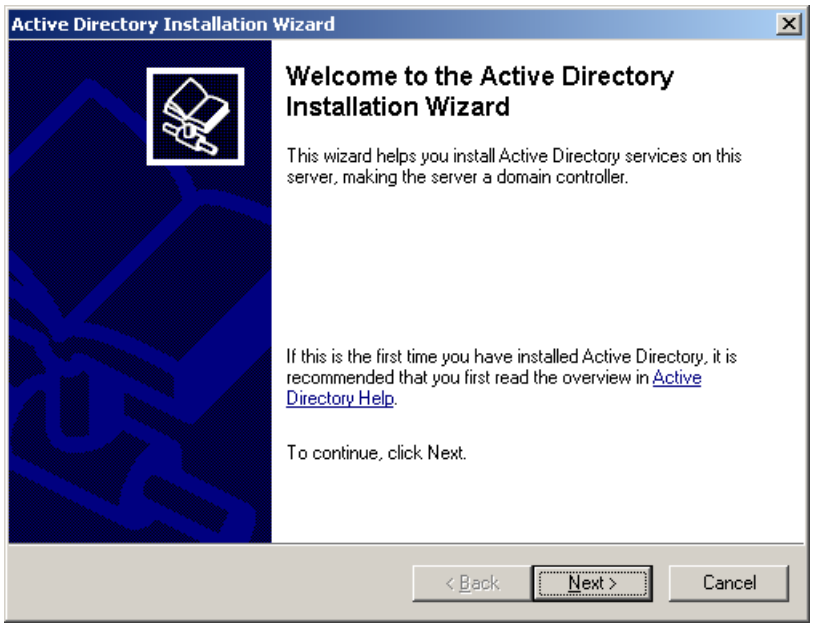
Σε περίπτωση ύπαρξης δεύτερου ΣΕ στο ίδιο τοπικό δίκτυο, υπάρχουν δύο επιλογές:

- τα δύο εργαστήρια ανήκουν σε διαφορετικά domains. Βασική υπηρεσία για τη λειτουργία του domain είναι το DNS. Οι σταθμοί εργασίας και των δύο εργαστηρίων λαμβάνουν από το δρομολογητή μέσω του πρωτοκόλλου DHCP ενιαία λίστα DNS εξυπηρετητών. Σε αυτήν την περίπτωση απαιτείται ο ένας εξυπηρετητής να είναι δευτερεύων για την υπηρεσία DNS του άλλου εργαστηρίου. Οπότε οι σταθμοί εργασίας όποιον και αν λάβουν ως πρωτεύων εξυπηρετητή DNS, θα βρουν τα κατάλληλα στοιχεία – DNS records – για τη σύνδεση στο domain.
- όλα τα εργαστήρια να ενταχθούν στο ίδιο domain. Το συγκεκριμένο σχήμα είναι αρκετά πολύπλοκο και προϋποθέτει την ύπαρξη κοινής αρχής διαχείρισης των εργαστηρίων.
- Εκτελείται η εντολή 'dcpromo' από τη γραμμή εντολών.



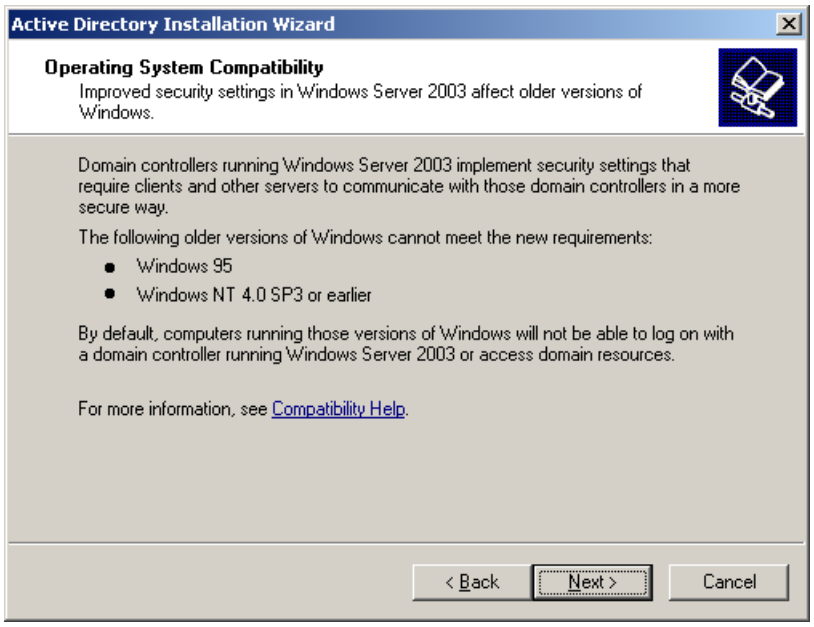
Εικόνα 1 – Active Directory: Εκτέλεση 'dcpromo'

- Ξεκινά η διαδικασία εγκατάστασης του Active Directory.



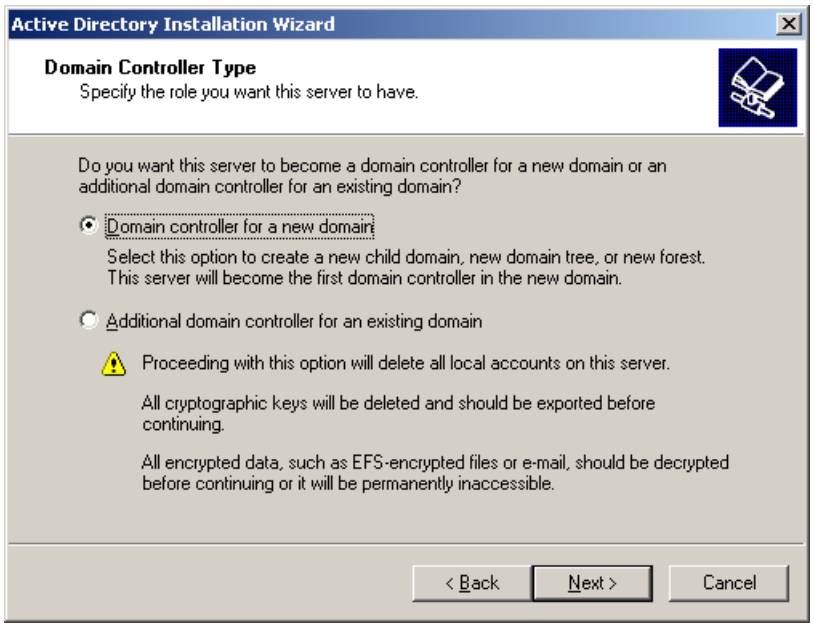

Εικόνα 2 – Active Directory: Οδηγός εγκατάστασης Active Directory

- Γίνεται αποδεκτό το ενημερωτικό μήνυμα, καθώς στα σχολικά εργαστήρια δεν αναμένεται να συνυπάρχουν Windows 2003 Server domain controllers με σταθμούς εργασίας με παλιότερα λειτουργικά συστήματα της Microsoft.



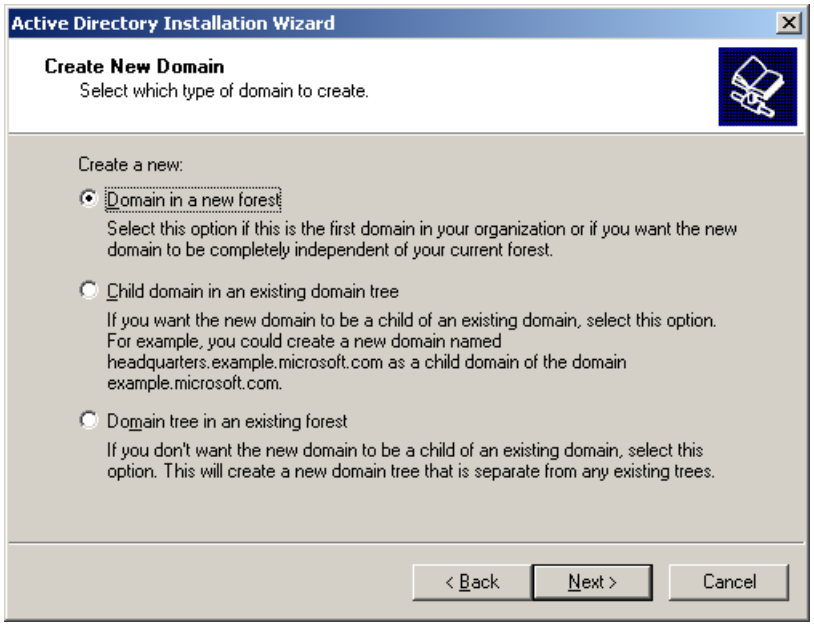
Εικόνα 3 – Active Directory: Operating system compatibility

- Ο domain controller επιλέγεται να είναι ο πρώτος σε ένα νέο domain.



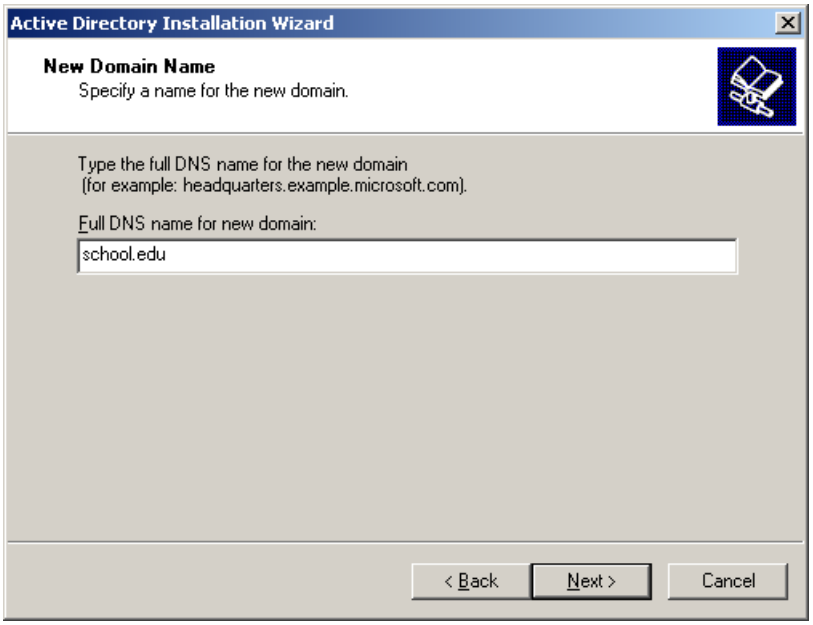

Εικόνα 4 – Active Directory: Domain controller type

- Επιλέγεται να δημιουργηθεί το domain μέσα σε ένα νέο forest, αφού σε κάθε σχολείο είναι ανεπτυγμένη υποδομή σε ανεξάρτητο δάσος και δέντρο του ενεργού καταλόγου.



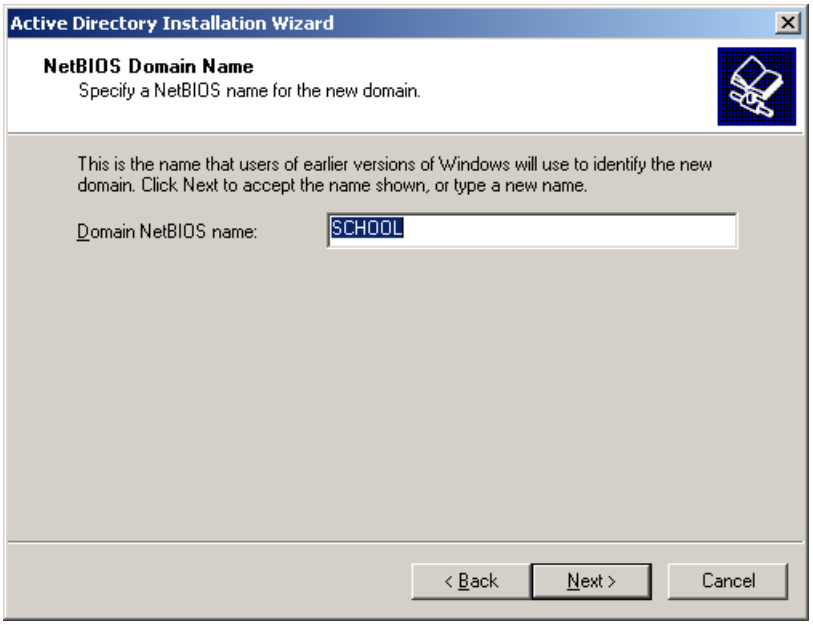

Εικόνα 5 – Active Directory: Domain type

- Ορίζεται όνομα για το domain. Δεν υπάρχει λόγος εφαρμογής της εξωτερικής DNS ονοματολογίας, που έχει οριστεί από το ΠΣΔ, ούτε χρειάζεται να χρησιμοποιηθεί ένα καταχωρημένο στην InterNIC όνομα. Το όνομα του domain κάθε σχολικού εργαστηρίου μπορεί να είναι τυχαίο (π.χ. 'school.edu'). Τα σχολικά εργαστήρια που βρίσκονται στο ίδιο τοπικό δίκτυο πρέπει να έχουν διαφορετικό domain.



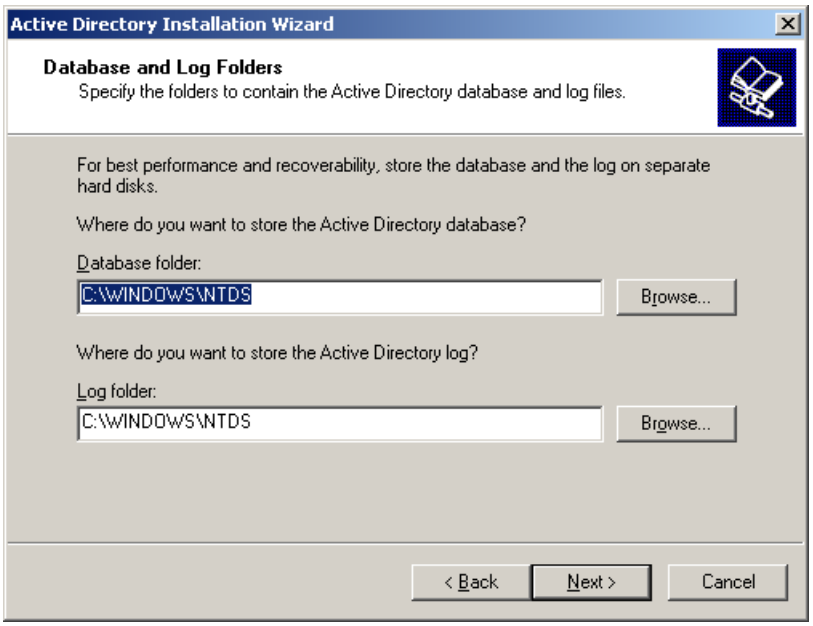

Εικόνα 6 – Active Directory: Domain name

- Ο ορισμός του NetBIOS name αφήνεται στην προεπιλεγμένη τιμή του.



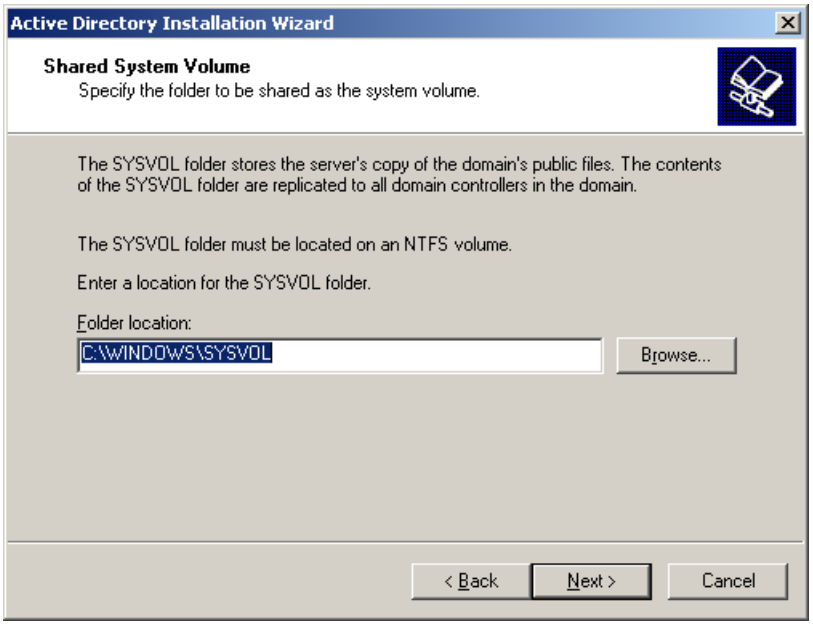
Εικόνα 7 – Active Directory: NetBIOS domain name

- Ορίζονται οι φάκελοι αποθήκευσης της βάσης δεδομένων και των αρχείων καταγραφής του ενεργού καταλόγου (database and log folders). Καθώς το μέγεθος του Active Directory δεν είναι αυξημένο στα σχολικά εργαστήρια δεν κρίνεται σκόπιμη η αποθήκευση των συγκεκριμένων αρχείων σε πιθανό δεύτερο σκληρό δίσκο για βελτιστοποίηση της απόδοσης. Με αυτόν τον τρόπο γίνεται πιο εύκολη και η λήψη αντιγράφων ασφαλείας για επαναφορά του συστήματος.



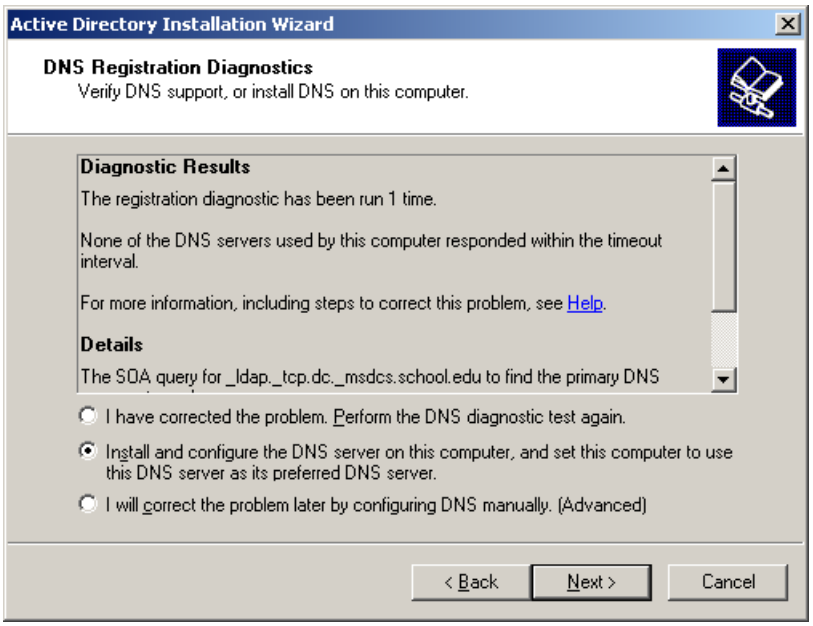

Εικόνα 8 – Active Directory: Database and log folders

- Ορίζεται το μονοπάτι του διαμοιραζόμενου φακέλου ‘sysvol’. Προτείνεται να γίνεται αποδεκτή η προεπιλεγμένη επιλογή φακέλου.



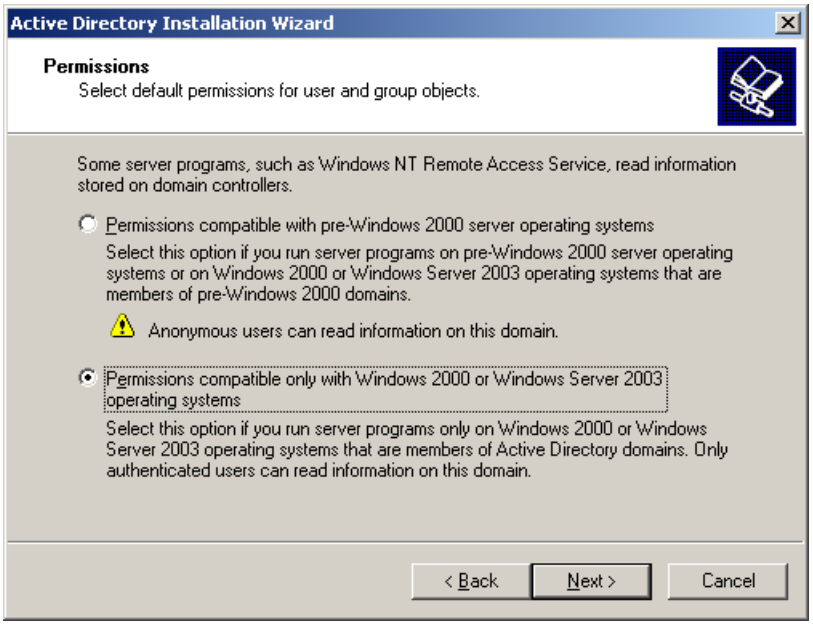

Εικόνα 9 – Active Directory: Shared system volume

- Στη συνέχεια πραγματοποιείται διαγνωστικός έλεγχος σχετικά με την υπηρεσία DNS. Αν δεν είναι εγκατεστημένη, τότε ο οδηγός της εγκατάστασης προχωρά στην άμεση εγκατάσταση και ρύθμισή της.



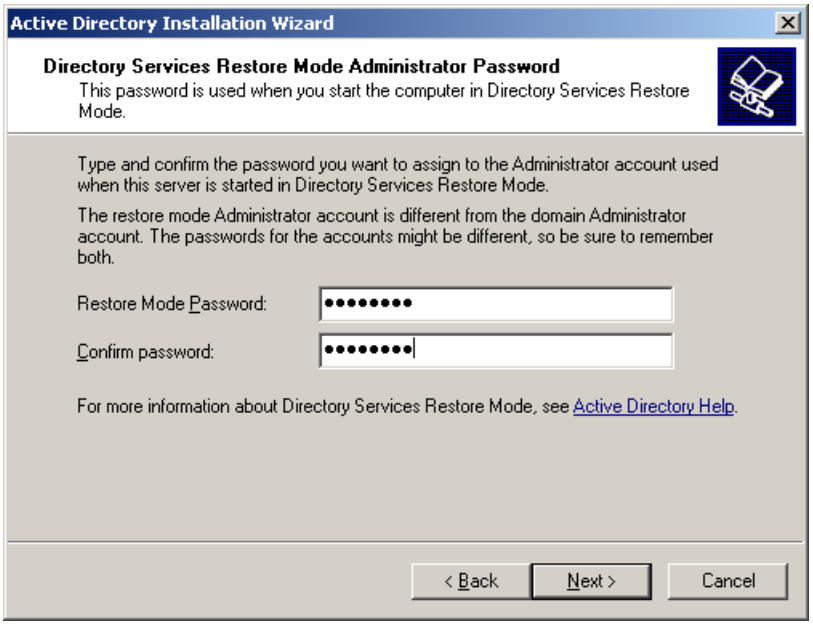

Εικόνα 10 – Active Directory: DNS registration diagnostics

- Για λόγους ασφαλείας επιλέγεται η δυνατότητα πρόσβασης στο domain μόνο από πιστοποιημένους χρήστες.



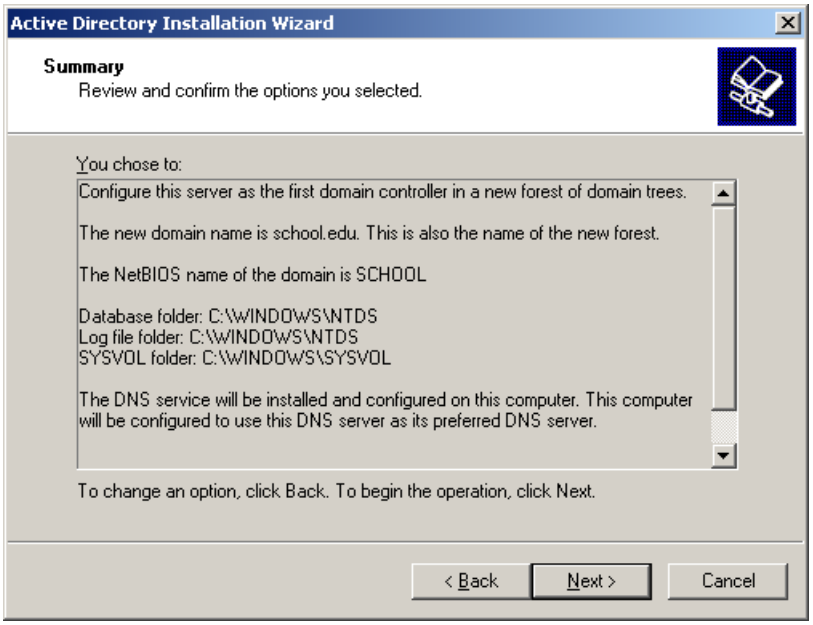

Εικόνα 11 – Active Directory: Permissions

- Ορίζεται ο κωδικός ασφαλείας για το λογαριασμό διαχειριστή, όταν ο εξυπηρετητής λειτουργεί σε 'directory services restore mode'. Για λόγους ευκολίας διαχείρισης προτείνεται να επιλέγεται ίδιος κωδικός με αυτόν που έχει οριστεί για κάποιον από τους διαχειριστές του domain.



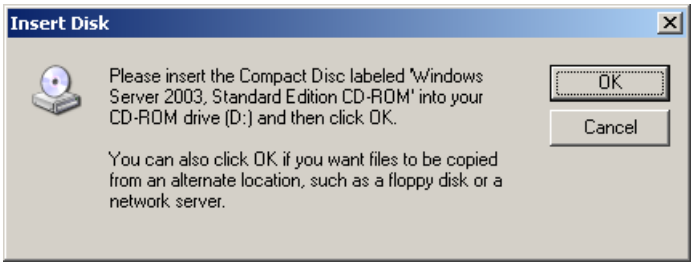

Εικόνα 12 – Active Directory: Directory services restore mode administrator password

- Ελέγχεται η σύνοψη των επιλογών διαμόρφωσης του domain.



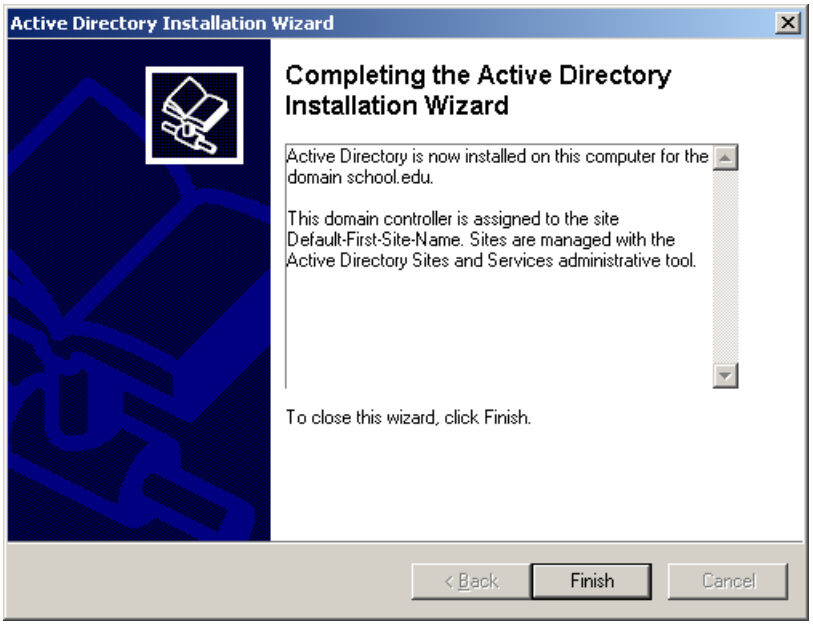

Εικόνα 13 – Active Directory: Summary

- Αν απαιτηθεί εισάγεται το μέσο εγκατάστασης των Windows 2003 Server.




Εικόνα 14 – Active Directory: Μήνυμα εισαγωγής cd-rom

- Ολοκληρώνεται ο οδηγός εγκατάστασης.




Εικόνα 15 – Active Directory: Ολοκλήρωση εγκατάστασης

- Πραγματοποιείται επανεκκίνηση του συστήματος για την ενσωμάτωση των αλλαγών σε αυτό.


Εικόνα 16 – Active Directory: Επανεκκίνηση συστήματος

## 4.2 Ρύθμιση υπηρεσίας DNS

Στον εξυπηρετητή του εργαστηρίου υπάρχει υπηρεσία ονοματολογίας DNS, που συνήθως εγκαθίσταται κατά τη δημιουργία του Active Directory. Η υπηρεσία είναι υπεύθυνη μόνο για το εσωτερικό ιδιωτικό υποδίκτυο (10.x.y.z) του σχολικού εργαστηρίου, ενώ προωθεί τα υπόλοιπα αιτήματα στους εξυπηρετητές ονοματολογίας του ΠΣΔ. Η ρύθμιση της υπηρεσίας μπορεί να πραγματοποιηθεί σύμφωνα με τη διαδικασία που περιγράφεται στη συνέχεια.

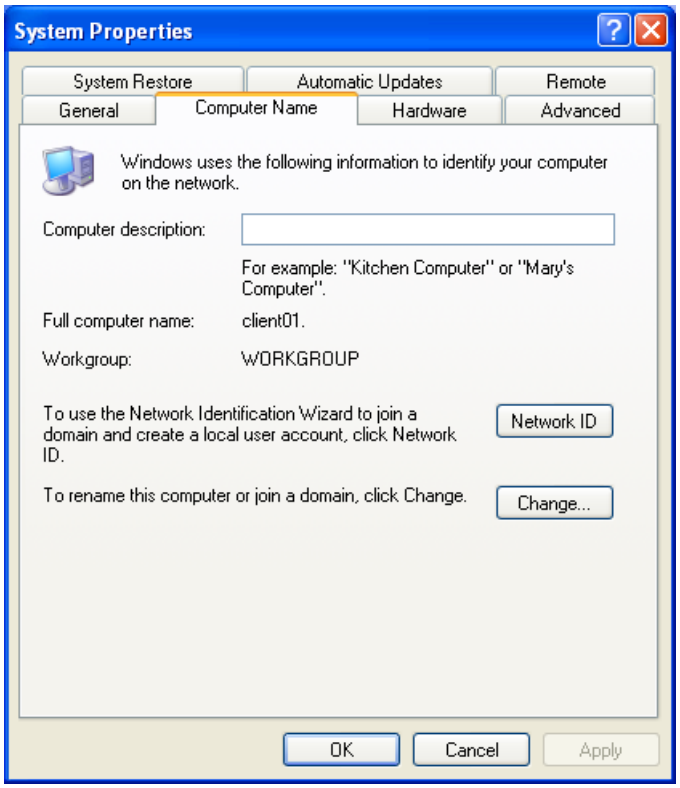
Από την κονσόλα διαχείρισης της υπηρεσίας DNS (Start → Programs → Administrative tools → DNS) διαγράφεται η ζώνη '.' από τις forward lookup ζώνες και πραγματοποιείται επανεκκίνηση της υπηρεσίας DNS (δεξί κλικ στο εικονίδιο του εξυπηρετητή, all tasks & restart). Στη συνέχεια επιλέγονται οι

ιδιότητες (properties) του εξυπηρετητή και στην καρτέλα forwarders ορίζεται ότι για όλα τα ερωτήματα που δεν αφορούν το domain θα απαντούν διαδοχικά οι πλησιέστεροι εξυπηρετητές ονοματολογίας του ΠΣΔ. εξαρτώνται από τη γεωγραφική τοποθεσία της σχολικής μονάδας και λαμβάνονται μετά από επικοινωνία με το helpdesk του ΠΣΔ (8011180181). Τέλος, δημιουργείται μια reverse lookup primary ζώνη που καλύπτει το εύρος του ιδιωτικού υποδικτύου της σχολικής μονάδας (network_ID:10.x.y).

## 4.3 Σύνδεση σταθμών εργασίας στο domain

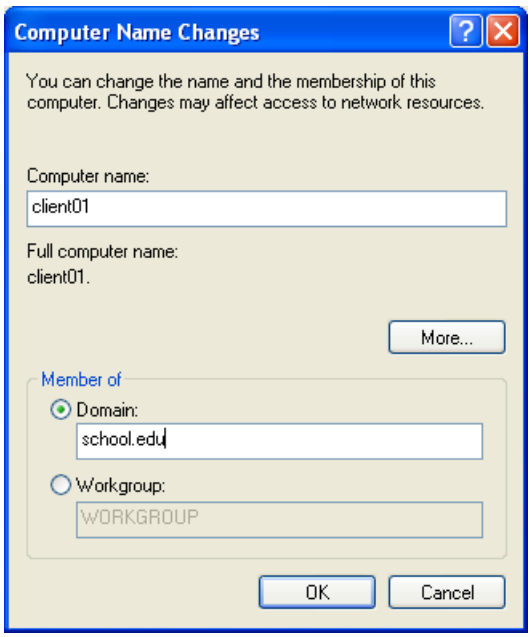
Η ένταξη ενός σταθμού εργασίας στο domain μπορεί να πραγματοποιηθεί σύμφωνα με τη διαδικασία που περιγράφεται στη συνέχεια.

- Από τις ιδιότητες συστήματος (system properties) και την καρτέλα 'Computer name' είναι δυνατή η εισαγωγή ενός σταθμού εργασίας στο domain του σχολικού εργαστηρίου. Επιλέγεται το κουμπί 'change'.



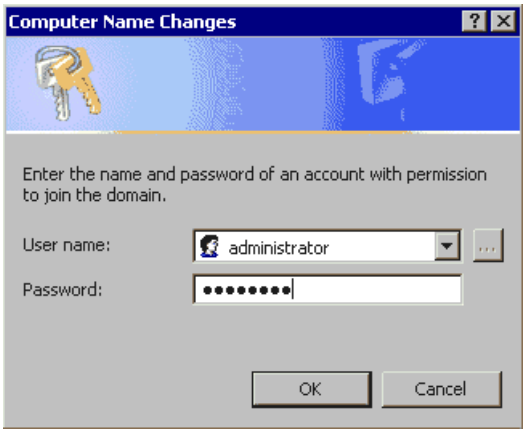

Εικόνα 17 – Active Directory: Ιδιότητες σταθμού εργασίας

- Εισάγεται το σωστό όνομα του domain προκειμένου να ολοκληρωθεί η διαδικασία.




Εικόνα 18 – Active Directory: Αλλαγή membership σταθμού εργασίας

- Απαιτείται το όνομα και ο κωδικός ασφαλείας ενός λογαριασμού με δικαιώματα εισαγωγής ενός υπολογιστή στο domain. Εισάγονται τα στοιχεία του διαχειριστή του domain.



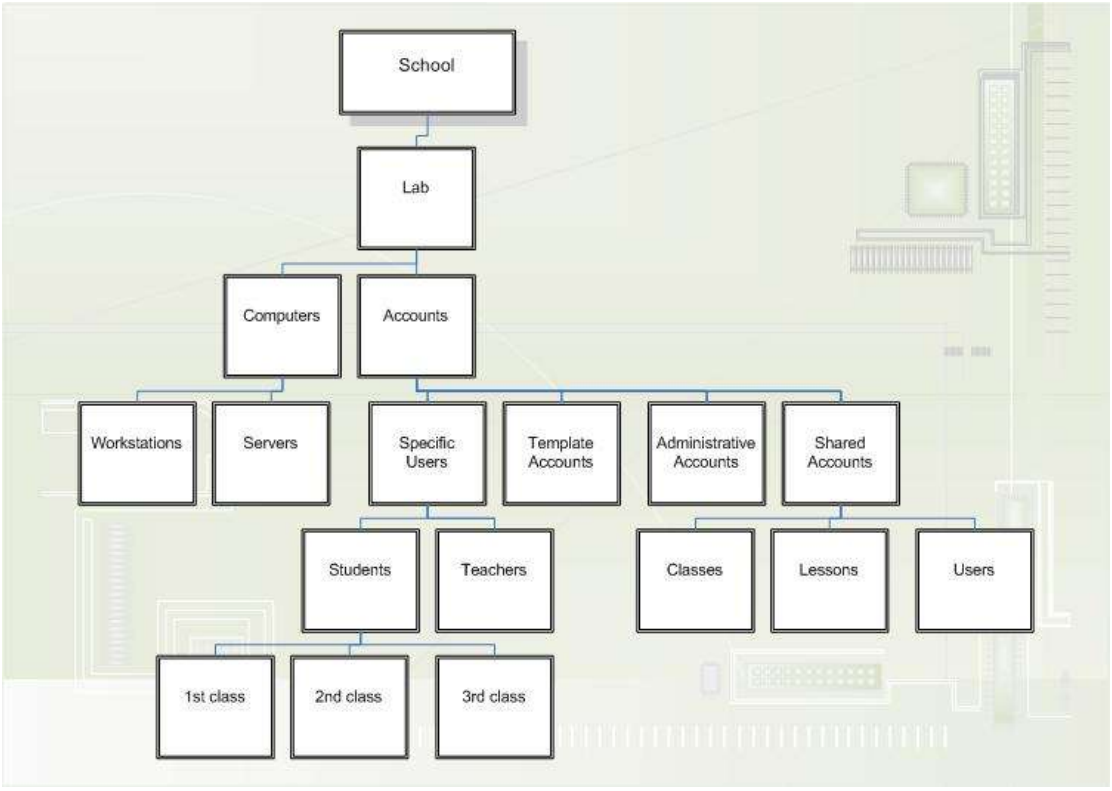

Εικόνα 19 – Active Directory: Εισαγωγή λογαριασμού με κατάλληλα δικαιώματα

Μετά από την επανεκκίνησή του ο σταθμός εργασίας ανήκει στο domain και μπορεί να συνδέεται σε αυτό αν είναι γνωστός κάποιος λογαριασμός χρήστη. Έχει δημιουργηθεί στο Active Directory ένα αντικείμενο υπολογιστή που ανήκει στο default container 'computers' (εκτός και είχε δημιουργηθεί το αντικείμενο εκ των προτέρων στην επιθυμητή οργανωτική μονάδα). Είναι δυνατή η μετακίνηση του αντικειμένου στο κατάλληλο OU για την πιθανή εφαρμογή πολιτικών ομάδας.

## 4.4 Δόμηση domain (organizational units)

Η οργάνωση των αντικειμένων του domain (υπολογιστές και λογαριασμοί χρηστών) γίνεται ώστε να υπάρχει μια **λογική αναπαράσταση του πραγματικού κόσμου με στόχο να είναι δυνατή η εφαρμογή πολιτικών ομάδας (group policies)**. Με αυτό το τρόπο επιτυγχάνεται η χρήση του domain με διαφορετικούς τρόπους, ενώ διασφαλίζονται η επιθυμητή λειτουργικότητα, ασφάλεια και απόδοση.

Στο διάγραμμα που ακολουθεί απεικονίζεται η προτεινόμενη δόμηση του Active Directory σε οργανωτικές μονάδες (OU's). Στη συνέχεια αναλύεται κάθε τμήμα του, ώστε να γίνει κατανοητός ο τρόπος με τον οποίο μπορεί να αξιοποιηθεί η εν λόγω δομή.




Εικόνα 20 – Δόμηση του Active Directory σε οργανωτικές μονάδες (OU's)

Το κορυφαίο OU με τίτλο 'School' περιέχει μόνο το OU 'Lab', που περιλαμβάνει τους υπολογιστές και τους λογαριασμούς του σχολικού εργαστηρίου. Μπορεί μελλοντικά να ενσωματώσει επιπλέον OUs (π.χ. δεύτερο εργαστήριο, υπολογιστές και χρήστες γραφείων σχολείου) αν είναι επιθυμητή η επέκταση του domain σε όλο το σχολείο.

Κάτω από το OU 'Computers' αποθηκεύονται μόνο οι υπολογιστές που ανήκουν στο σχολικό εργαστήριο και εφαρμόζονται μόνο τα τμήματα των group policies που αφορούν υπολογιστές (όπως και στα OU's που βρίσκονται πιο χαμηλά στο δέντρο).

Κάτω από το OU 'Accounts' αποθηκεύονται μόνο οι λογαριασμοί χρηστών του σχολικού εργαστηρίου και εφαρμόζονται μόνο τα τμήματα των group policies που αφορούν χρήστες (όπως και στα OU's που βρίσκονται πιο χαμηλά στο δέντρο).

Κάτω από το OU 'Servers' αποθηκεύονται όλα τα υπολογιστικά συστήματα που παρέχουν κάποιο είδος υπηρεσίας στο εργαστήριο (π.χ. proxy server). Στην παρούσα μορφή των εργαστηρίων αυτό το OU δεν έχει μέλη, καθώς ο domain controller εξ' ορισμού ανήκει σε ομώνυμο OU που βρίσκεται εκτός του δέντρου. Το OU 'Workstations' περιέχει όλους τους σταθμούς εργασίας του σχολικού εργαστηρίου.

Σε ότι αφορά τους λογαριασμούς χρηστών υπάρχει ένα OU με τίτλο 'Administrative accounts' με χρήστες με διαχειριστικά δικαιώματα, που μπορούν να χρησιμοποιηθούν από τον υπεύθυνο εργαστηρίου, τους τεχνικούς της ΤΣ ή οποιονδήποτε άλλο απαιτήσει τέτοιας μορφής πρόσβαση στο μέλλον. Στο OU 'Template accounts' αποθηκεύονται πρότυποι λογαριασμοί, που μπορούν να χρησιμοποιηθούν για τη γρήγορη δημιουργία λογαριασμών που ανήκουν σε οποιαδήποτε άλλη κατηγορία (π.χ. μαθητών).

Το OU 'Shared accounts' περιέχει τρία OUs. Στο 'Classes' μπορούν να δημιουργηθούν κοινόχρηστοι λογαριασμοί για τους μαθητές ανάλογα με την τάξη ή το τμήμα στο οποίο ανήκουν (1st class, 2nd class κλπ). Στο 'Lessons' είναι δυνατή με αντίστοιχο τρόπο η δημιουργία κοινόχρηστων λογαριασμών ανάλογα με το μάθημα για το οποίο γίνεται χρήση του εργαστηρίου (Physics, English κλπ). Τέλος, το OU 'Users' περιέχει κοινόχρηστους λογαριασμούς μαθητών, χωρίς κάποια ιδιαίτερη εξειδίκευση (User01, User02 κλπ). Το πλήθος αυτών των λογαριασμών είναι ίδιο με τον αριθμό των σταθμών εργασίας. Με εφαρμογή κατάλληλων group policies μπορούν οι μαθητές να εισάγονται σε ένα περιβάλλον σχετικό με τον κοινόχρηστο λογαριασμό που έχουν επιλέξει.

Το OU 'Specific Users' μπορεί να χρησιμοποιηθεί για τη δημιουργία προσωπικών λογαριασμών για καθηγητές ('Teachers') και μαθητές συγκεκριμένης τάξης ('Students'). Η αξιοποίησή του πολλαπλασιάζει τις παρεχόμενες δυνατότητες από το σχολικό εργαστήριο (π.χ. κάθε μαθητής μπορεί να έχει το δικό του χώρο αποθήκευσης αρχείων). Απαιτείται όμως να αφιερωθεί πολύ μεγαλύτερος χρόνος για τη διαχείριση του Active Directory από τον υπεύθυνο εργαστηρίου.

Είναι ευνόητο πως κάποιο μέρος του ανωτέρω δέντρου μπορεί να μην χρησιμοποιείται, ανάλογα με τη μέθοδο αξιοποίησης του Active Directory που θα επιλέξει ο υπεύθυνος εργαστηρίου. Η ύπαρξη ενός τέτοιου υποδέντρου δεν επηρεάζει με κάποιο τρόπο τη λειτουργικότητα ή την ασφάλεια των πληροφοριακών συστημάτων. Για την σωστή αξιοποίηση του εργαστηρίου κρίνεται καταρχήν αναγκαία η χρήση των OU's 'Workstations', 'Administrative accounts' & 'Shared accounts'.

Η προτεινόμενη ιεραρχία των OUs μπορεί να δημιουργηθεί με τη χρήση της εντολής dsadd ou. Συγκεκριμένα:

```
dsadd ou "ou=School, dc=school, dc=edu" -desc "Οι οντότητες της Σχολικής/Διοικητικής Μονάδας"

dsadd ou "ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Οι οντότητες του 1ου Σχολικού Εργαστηρίου Πληροφορικής και Εφαρμογών Η/Υ"

dsadd ou "ou=Computers, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Το σύνολο των υπολογιστών του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Servers, ou=Computers, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Οι εξυπηρετητές του ΣΕΠΕΗΥ πλέον του Domain Controller"

dsadd ou "ou=Workstations, ou=Computers, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Οι σταθμοί εργασίας του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Το σύνολο των χρηστών του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Administrative Accounts, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Οι διαχειριστικοί λογαριασμοί του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Shared Accounts, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Οι διαμοιραζόμενοι λογαριασμοί του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Classes, ou=Shared Accounts, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Διαμοιραζόμενοι λογαριασμοί τάξεων του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Lessons, ou=Shared Accounts, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Διαμοιραζόμενοι λογαριασμοί μαθημάτων του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Users, ou=Shared Accounts, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Διαμοιραζόμενοι λογαριασμοί μαθητών του 1ου ΣΕΠΕΗΥ (π.χ. user1, user2, κλπ"

dsadd ou "ou=Specific Users, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Προσωπικοί λογαριασμοί χρηστών του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Students, ou=Specific Users, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -desc "Προσωπικοί λογαριασμοί μαθητών του 1ου ΣΕΠΕΗΥ"
```

```
dsadd ou "ou=1st Class, ou=Students, ou=Specific Users, ou=Accounts, ou=SEPEHY_1,
ou=School, dc=school, dc=edu" -desc "Προσωπικοί λογαριασμοί μαθητών 1ης τάξης του
1ου ΣΕΠΕΗΥ"

dsadd ou "ou=2nd Class, ou=Students, ou=Specific Users, ou=Accounts, ou=SEPEHY_1,
ou=School, dc=school, dc=edu" -desc "Προσωπικοί λογαριασμοί μαθητών 2ης τάξης του
1ου ΣΕΠΕΗΥ"

dsadd ou "ou=3rd Class, ou=Students, ou=Specific Users, ou=Accounts, ou=SEPEHY_1,
ou=School, dc=school, dc=edu" -desc "Προσωπικοί λογαριασμοί μαθητών 3ης τάξης του
1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Teachers, ou=Specific Users, ou=Accounts, ou=SEPEHY_1, ou=School,
dc=school, dc=edu" -desc "Προσωπικοί λογαριασμοί καθηγητών του 1ου ΣΕΠΕΗΥ"

dsadd ou "ou=Template Accounts, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school,
dc=edu" -desc "Προσωπικοί λογαριασμοί μαθητών 1ης τάξης του 1ου ΣΕΠΕΗΥ"
```

Οι ανωτέρω εντολές βρίσκονται στο αρχείο CreateOUs.bat, στη Βιβλιοθήκη του Ενημερωτικού Κόμβου http://ts.sch.gr, μετά από login με τα στοιχεία χρήστη του ΠΣΔ.

## 4.5 Πολιτικές ομάδας (group policies)

Σύμφωνα με τη ανωτέρω δόμηση του Active Directory σε OU's είναι δυνατή η εφαρμογή πολιτικών ομάδας (group policies). Στη συνέχεια αναφέρονται συνοπτικά οι κύριες ρυθμίσεις που μπορούν να εφαρμοστούν στα OU's 'Workstations' & 'Shared accounts'. Για το OU "Workstations" δημιουργούμε την πολιτική "SEPEHY-Workstations policy", ενώ για το OU "Shared accounts", δημιουργούμε την πολιτική "SEPEHY-Shared accounts policy". Το πρόθεμα "SEPEHY-" ορίζεται ως πρώτο συνθετικό των ονομάτων των πολιτικών, για να είναι περισσότερο εύκολος ο διαχωρισμός τους από τις πολιτικές που υπάρχουν εξ αρχής σε κάθε δομή Active Directory. Όλες οι διαχειριστικές εργασίες θα πραγματοποιούνται στις πολιτικές "SEPEHY-…", μειώνοντας τους κινδύνους να αλλοιώσουν τις πολιτικές που εγγενώς έχει το Active Directory και να προκαλέσουν αστάθεια του συστήματος.

Επισημαίνεται πως οι πολιτικές ομάδας επηρεάζουν σε μεγάλο βαθμό το περιβάλλον εργασίας του χρήστη. Γι' αυτό θα πρέπει να γνωρίζει ο υπεύθυνος εργαστηρίου τον τρόπο λειτουργίας τους και να είναι σε θέση να τροποποιήσει τις εφαρμοζόμενες πολιτικές, προκειμένου να διαμορφώσει το εργαστήριο σύμφωνα και με τις απαιτήσεις των χρηστών.

- Στο OU 'Workstations' δημιουργείται από τις ιδιότητες του OU αντικείμενο πολιτικής ομάδας με όνομα 'SEPEHY-Workstations policy'. Σε αυτό το αντικείμενο είναι ενεργοποιημένο μόνο το τμήμα των ρυθμίσεων

σε υπολογιστές για βελτιστοποίηση της απόδοσης. Επιλέγεται μέσα από τις ιδιότητες του αντικειμένου η ιδιότητα 'Disable User Configuration Settings'. Το αντικείμενο πολιτικής ομάδας διαμορφώνεται σύμφωνα με τον πίνακα που ακολουθεί.

| **Policy Path (Machine)** | **Full Policy Name** | **Setting** |
|---|---|---|
| Administrative Templates\System | Turn off Autoplay | Enabled (CD Drives) |
| Administrative Templates\System\User Profiles | Slow network connection timeout for user profiles | Enabled (default) |
| Administrative Templates\System\Logon | Don't display the Getting Started welcome screen at logon | Enabled |
| Administrative Templates\System\Remote Assistance | Solicited Remote Assistance | Enabled |
| Administrative Templates\System\Remote Assistance | Offer Remote Assistance | Enabled (Domain Admins) |
| Administrative Templates\System\System Restore | Turn off System Restore | Enabled |
| Administrative Templates\System\Error Reporting | Display Error Notification | Enabled |
| Administrative Templates\System\Windows Time Service\Time Providers | Enable Windows NTP Client | Enabled |
| Administrative Templates\Network\Offline Files | Allow or Disallow use of the Offline Files feature | Disabled |
| Administrative Templates\Network\Network Connections | Prohibit use of Internet Connection Sharing on your DNS domain network | Enabled |
| Administrative Templates\Network\Network Connections | Prohibit use of Internet Connection Firewall on your DNS domain network | Enabled |
| Administrative Templates\Network\Network Connections | Prohibit installation and configuration of Network Bridge on your DNS domain network | Enabled |
| Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile | Windows Firewall: Protect all network connections | Disabled |
| Administrative Templates\Windows Components\Security Center | Turn on Security Center (Domain PCs only) | Enabled |
| Administrative Templates\Windows Components\Terminal Services | Allow users to connect remotely using Terminal Services | Enabled |
| Administrative Templates\Windows Components\Windows Installer | Allow admin to install from Terminal Services session | Enabled |
| Administrative Templates\Windows Components\Windows Messenger | Do not allow Windows Messenger to be run | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Security Zones: Do not allow users to change policies | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Security Zones: Do not allow users to add/delete sites | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Make proxy settings per-machine (rather than per-user) | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable Periodic Check for Internet Explorer software updates | Enabled |

| | | |
|---|---|---|
| Administrative Templates\Windows Components\Internet Explorer | Disable showing the splash screen | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Do not allow users to enable or disable add-ons | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the General page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Security page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Content page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Connections page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Programs page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Privacy page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Advanced page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page | Allow software to run or install even if the signature is invalid | Disabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page | Allow active content from CDs to run on user machines | Disabled |
| Administrative Templates\Windows Components\Windows Update | Configure Automatic Updates | Enabled (4) |
| Administrative Templates\Windows Components\Windows Update | Allow Automatic Updates immediate installation | Enabled |
| Administrative Templates\Windows Components\Windows Media Player | Do Not Show First Use Dialog Boxes | Enabled |
| Administrative Templates\Windows Components\Windows Media Player | Prevent Desktop Shortcut Creation | Enabled |

Πίνακας 1 Ρυθμίσεις πολιτικής "SEPEHY-Workstations policy"

- Στο OU 'Shared accounts' δημιουργείται αντικείμενο πολιτικής ομάδας με όνομα '**SEPEHY-Shared accounts policy**'. Σε αυτό το αντικείμενο είναι ενεργοποιημένο μόνο το τμήμα των ρυθμίσεων σε λογαριασμούς χρηστών για βελτιστοποίηση της απόδοσης. Επιλέγεται μέσα από τις ιδιότητες του αντικειμένου η ιδιότητα 'Disable Computer Configuration Settings'. Το αντικείμενο πολιτικής ομάδας διαμορφώνεται σύμφωνα με τον πίνακα που ακολουθεί.

| Policy Path (User) | Full Policy Name | Setting |
|---|---|---|
| Administrative Templates\Start Menu and Taskbar | Remove user's folders from the Start Menu | Enabled |
| Administrative Templates\Start Menu and Taskbar | Remove links and access to Windows Update | Enabled |

| | | |
|---|---|---|
| Administrative Templates\Start Menu and Taskbar | Remove programs on Settings menu | Enabled |
| Administrative Templates\Start Menu and Taskbar | Remove Network Connections from Start Menu | Enabled |
| Administrative Templates\Start Menu and Taskbar | Remove My Pictures icon from Start Menu | Enabled |
| Administrative Templates\Start Menu and Taskbar | Remove My Music icon from Start Menu | Enabled |
| Administrative Templates\Start Menu and Taskbar | Add Logoff to the Start Menu | Enabled |
| Administrative Templates\Start Menu and Taskbar | Remove Drag-and-drop context menus on the Start Menu | Enabled |
| Administrative Templates\Start Menu and Taskbar | Prevent changes to Taskbar and Start Menu Settings | Enabled |
| Administrative Templates\Start Menu and Taskbar | Remove access to the context menus for the taskbar | Enabled |
| Administrative Templates\Start Menu and Taskbar | Turn off personalized menus | Enabled |
| Administrative Templates\Start Menu and Taskbar | Turn off user tracking | Enabled |
| Administrative Templates\Start Menu and Taskbar | Turn off notification area cleanup | Enabled |
| Administrative Templates\Start Menu and Taskbar | Lock the Taskbar | Enabled |
| Administrative Templates\Start Menu and Taskbar | Remove Set Program Access and Defaults from Start menu | Enabled |
| Administrative Templates\Desktop | Remove Properties from the My Documents context menu | Enabled |
| Administrative Templates\Desktop | Remove Properties from the My Computer context menu | Enabled |
| Administrative Templates\Desktop | Remove Properties from the Recycle Bin context menu | Enabled |
| Administrative Templates\Desktop | Prohibit user from changing My Documents path | Enabled |
| Administrative Templates\Control Panel | Prohibit access to the Control Panel | Enabled |
| Administrative Templates\Control Panel\Printers | Prevent deletion of printers | Enabled |
| Administrative Templates\Network\Network Connections | Prohibit access to properties of a LAN connection | Enabled |
| Administrative Templates\Network\Network Connections | Prohibit access to the New Connection Wizard | Enabled |
| Administrative Templates\System | Don't display the Getting Started welcome screen at logon | Enabled |
| Administrative Templates\System | Prevent access to the command prompt | Enabled |
| Administrative Templates\System | Prevent access to registry editing tools | Enabled |
| Administrative Templates\System\User Profiles | Limit profile size | Enabled (default) |
| Administrative Templates\System\Ctrl+Alt+Del Options | Remove Task Manager | Enabled |

| | | |
|---|---|---|
| Administrative Templates\System\Ctrl+Alt+Del Options | Remove Lock Computer | Enabled |
| Administrative Templates\System\Ctrl+Alt+Del Options | Remove Change Password | Enabled |
| Administrative Templates\Windows Components\Windows Explorer | Removes the Folder Options menu item from the Tools menu | Enabled |
| Administrative Templates\Windows Components\Windows Explorer | Remove Map Network Drive and Disconnect Network Drive | Enabled |
| Administrative Templates\Windows Components\Windows Explorer | Hides the Manage item on the Windows Explorer context menu | Enabled |
| Administrative Templates\Windows Components\Windows Explorer | Remove Hardware tab | Enabled |
| Administrative Templates\Windows Components\Windows Explorer | Remove Security tab | Enabled |
| Administrative Templates\Windows Components\Windows Explorer | Remove CD Burning features | Enabled |
| Administrative Templates\Windows Components\Microsoft Management Console | Restrict users to the explicitly permitted list of snap-ins | Enabled |
| Administrative Templates\Windows Components\Task Scheduler | Hide Property Pages | Enabled |
| Administrative Templates\Windows Components\Task Scheduler | Prevent Task Run or End | Enabled |
| Administrative Templates\Windows Components\Task Scheduler | Prohibit Drag-and-Drop | Enabled |
| Administrative Templates\Windows Components\Task Scheduler | Prohibit New Task Creation | Enabled |
| Administrative Templates\Windows Components\Task Scheduler | Prohibit Task Deletion | Enabled |
| Administrative Templates\Windows Components\Task Scheduler | Hide Advanced Properties Checkbox in Add Scheduled Task Wizard | Enabled |
| Administrative Templates\Windows Components\Task Scheduler | Prohibit Browse | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Search: Disable Search Customization | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable external branding of Internet Explorer | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the General page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Security page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Content page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Connections page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Programs page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Privacy page | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel | Disable the Advanced page | Enabled |

| | | |
|---|---|---|
| Administrative Templates\Windows Components\Internet Explorer | Disable changing Advanced page settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing home page settings | Enabled<br>(about:blank) |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing Temporary Internet files settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing history settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing color settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing link color settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing font settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing language settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing accessibility settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable Internet Connection wizard | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing connection settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing proxy settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing Automatic Configuration settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing ratings settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing certificate settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing Profile Assistant settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable AutoComplete for forms | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Do not allow AutoComplete to save passwords | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing Messaging settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing Calendar and Contact settings | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable the Reset Web Settings feature | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Disable changing default browser check | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Do not allow users to enable or disable add-ons | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Identity Manager: Prevent users from using Identities | Enabled |
| Administrative Templates\Windows Components\Internet Explorer | Configure Outlook Express | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Browser menus | Tools menu: Disable Internet Options... menu option | Enabled |

| | | |
|---|---|---|
| Administrative Templates\Windows Components\Internet Explorer\Browser menus | Help menu: Remove 'Tip of the Day' menu option | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Browser menus | Help menu: Remove 'For Netscape Users' menu option | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Browser menus | Help menu: Remove 'Tour' menu option | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Browser menus | Help menu: Remove 'Send Feedback' menu option | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Toolbars | Disable customizing browser toolbar buttons | Enabled |
| Administrative Templates\Windows Components\Internet Explorer\Toolbars | Disable customizing browser toolbars | Enabled |
| Administrative Templates\Windows Components\NetMeeting | Disable Directory services | Enabled |
| Administrative Templates\Windows Components\NetMeeting | Prevent adding Directory servers | Enabled |
| Administrative Templates\Windows Components\NetMeeting | Prevent viewing Web directory | Enabled |
| Administrative Templates\Windows Components\NetMeeting | Prevent changing Call placement method | Enabled |
| Administrative Templates\Windows Components\NetMeeting | Prevent automatic acceptance of Calls | Enabled |
| Administrative Templates\Windows Components\Windows Media Player | Prevent CD and DVD Media Information Retrieval | Enabled |
| Administrative Templates\Windows Components\Windows Media Player | Prevent Music File Media Information Retrieval | Enabled |
| Administrative Templates\Windows Components\Windows Media Player | Prevent Radio Station Preset Retrieval | Enabled |
| Administrative Templates\Windows Components\Windows Media Player\User Interface | Hide Privacy Tab | Enabled |
| Administrative Templates\Windows Components\Windows Media Player\User Interface | Hide Security Tab | Enabled |
| Administrative Templates\Windows Components\Windows Media Player\Networking | Hide Network Tab | Enabled |

Πίνακας 2 Ρυθμίσεις πολιτικής "SEPEHY-Shared accounts policy"

Οι ανωτέρω πολιτικές προτείνεται να εφαρμόζονται σε κάθε σχολικό εργαστήριο, ώστε να παρέχεται η επιθυμητή λειτουργικότητα, ενώ ταυτόχρονα διασφαλίζεται το εργαστήριο από εξωτερικούς κινδύνους και κυρίως από την πιθανότητα απορύθμισης του λόγω κακής χρήσης. Κύριος στόχος τους είναι να αποτρέπουν την πρόσβαση των απλών χρηστών σε 'επικίνδυνες' λειτουργίες. Στη συνέχεια είναι δυνατή η περαιτέρω χρήση των πολιτικών ομάδας (στα ίδια ή σε άλλα OU's που μπορεί να χρησιμοποιηθούν) ανάλογα με τις ανάγκες του εργαστηρίου.

Για τη βέλτιστη διαχείριση των πολιτικών ομάδας προτείνεται να γίνεται χρήση κατάλληλων εργαλείων, που επιτρέπουν τη μέγιστη αξιοποίηση των παρεχόμενων δυνατοτήτων με τον ευκολότερο δυνατό τρόπο. Το δωρεάν

προσφερόμενο Group Policy Management Console (GPMC) μπορεί να εγκατασταθεί στον εξυπηρετητή του εργαστηρίου και παρέχει χρήσιμες λειτουργικότητες όπως η εισαγωγή/εξαγωγή (import/export) αντικειμένων πολιτικών ομάδας, η λήψη αντιγράφων ασφαλείας αντικειμένων πολιτικών ομάδας και η δημιουργία αναφορών.

### 4.5.1 Αντίγραφα Πολιτικών Ομάδων και επαναφορά

Είναι δυνατό να λάβουμε αντίγραφα ασφαλείας των πολιτικών ομάδων και να τις επαναφέρουμε στον εξυπηρετητή σε περίπτωση που αυτές καταστραφούν. Τα αντίγραφα ασφαλείας τα λαμβάνουμε με την ακόλουθη διαδικασία: Από την κονσόλα Group Policy Management ανοίγουμε τα Group Policy Objects και από το δεξί παράθυρο επιλέγουμε αυτά για τα οποία θέλουμε να δημιουργήσουμε αντίγραφα ασφαλείας. Με δεξί κουμπί του ποντικιού επιλέγουμε “Back Up …”. Ορίζουμε το φάκελο στον οποίο θα αποθηκευτούν τα αντίγραφα και δίνουμε μία περιγραφή για αυτά. Η δημιουργία των αντιγράφων ολοκληρώνεται με επιβεβαίωση της επιτυχούς ολοκλήρωσης. Σε ένα φάκελο μπορούμε να αποθηκεύσουμε πολλά αντίγραφα, από τα οποία μπορούμε να επιλέξουμε ποια θα επαναφέρουμε με το επόμενο βήμα.

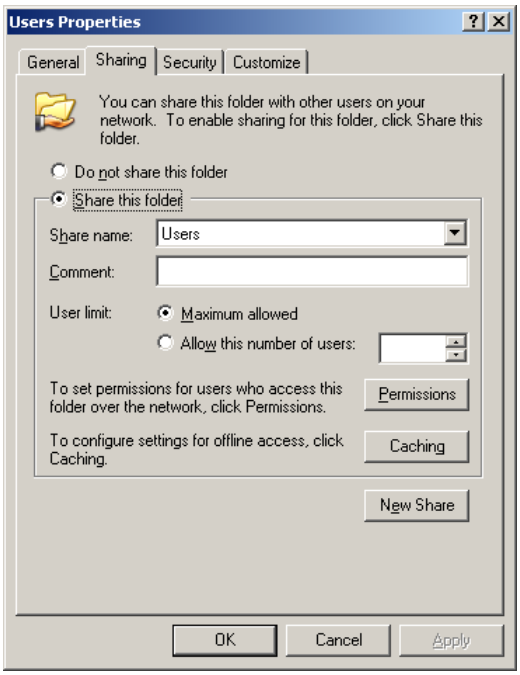
Για την επαναφορά των πολιτικών ομάδων από το αντίγραφό τους στον ίδιο εξυπηρετητή, πραγματοποιούμε την ακόλουθη διαδικασία: από το domain school.edu και τα Group Policy Objects επιλέγουμε με δεξί κουμπί του ποντικιού Manage Backups. Επιλέγουμε τη θέση στην οποία βρίσκονται τα GPO Backups, επιλέγουμε το επιθυμητό GPO και κάνουμε Restore. Στη συνέχεια από το OU στο οποίο θέλουμε να ενεργοποιήσουμε κάποιο GPO δημιουργούμε ένα Link προς το συγκεκριμένο GPO.

### 4.5.2 Εισαγωγή έτοιμων ρυθμίσεων

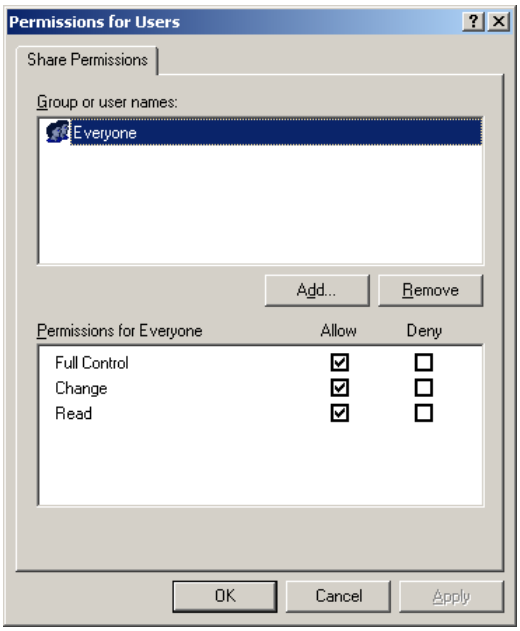
Είναι δυνατό να εισάγουμε μία πολιτική ομάδας από υπόδειγμα που υπάρχει στον Ενημερωτικό Κόμβο της Τεχνικής Στήριξης http://ts.sch.gr με την ακόλουθη διαδικασία: Αποθηκεύουμε τα αντίγραφα σε κάποιο φάκελο του εξυπηρετητή. Από το Group Policy Management δημιουργούμε στα Group Policy Objects μία νέα πολιτική με το όνομα που επιθυμούμε. Με δεξί κουμπί του ποντικιού σε αυτήν επιλέγουμε “Import Settings …”, ορίζουμε το φάκελο στον οποίο βρίσκεται η πολιτική που θέλουμε να εισάγουμε και επιλέγουμε τη συγκεκριμένη πολιτική. Στη συνέχεια από το OU στο οποίο θέλουμε να ενεργοποιήσουμε κάποιο GPO δημιουργούμε ένα Link προς το συγκεκριμένο GPO.

## 4.6 Ρύθμιση πολιτικών για «Τα έγγραφα μου» και την «Επιφάνεια Εργασίας»

Στον εξυπηρετητή δημιουργούμε το φάκελο users στην κατάτμηση με το όνομα DATA που βρίσκεται στον πρώτο σκληρό δίσκο. Το φάκελο αυτό τον κάνουμε share ορίζοντας στην επιλογή Permissions "Everyone" "Full Control".




Εικόνα 21 – Διαμοιρασμός του καταλόγου Users

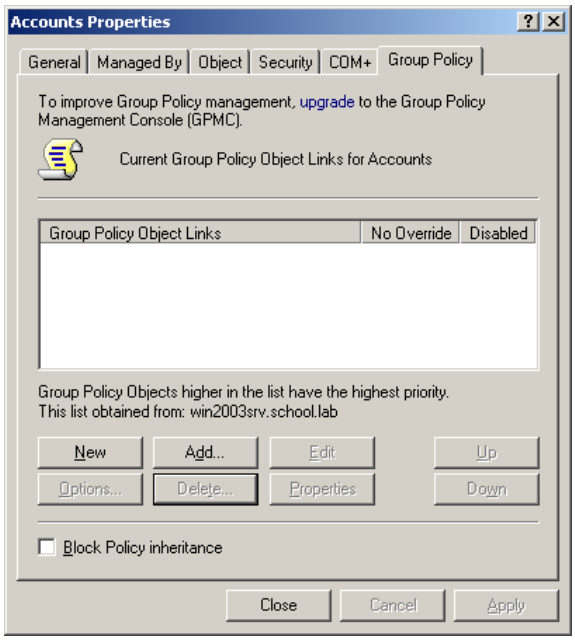



Εικόνα 22 – Ρύθμιση Ιδιοτήτων διαμοιρασμού του καταλόγου Users

ΔΕΝ αλλάζουμε τις ρυθμίσεις στο φύλλο «Security».

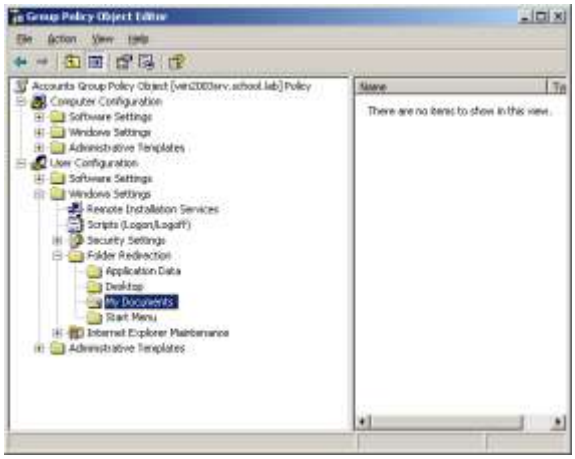
Με τον ίδιο τρόπο που δημιουργήθηκε ο φάκελος Users δημιουργούμε και διαμοιράζουμε το φάκελο "Profiles"στην ίδια πάντα κατάτμηση.

Στη συνέχεια μέσα από την κονσόλα διαχείρισης "Active Directory Users and Computers" επιλέγουμε το OU Accounts και με δεξί click και "Properties" πηγαίνουμε στο φύλλο Group Policy.



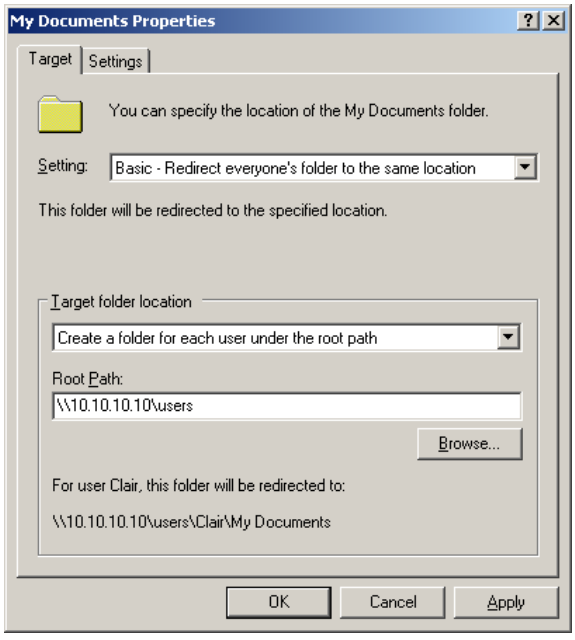

Εικόνα 23 – Δημιουργία Account Group Policy

Δημιουργούμε μία νέα πολιτική επιλέγοντας New και την ονομάζουμε «SEPEHY-Accounts Group Policy Object». Στην συνέχεια επιλέγουμε Edit οπότε και εμφανίζεται ένα νέο παράθυρο όπου μας δίνει τη δυνατότητα να κάνουμε τις επιθυμητές ρυθμίσεις.




Εικόνα 24 – Ρύθμιση της ανακατεύθυνσης των MyDocuments

Πηγαίνουμε στο "User Configuration" ➔ "Windows Settings" ➔ "Folders Redirections" και κάνουμε δεξί click και Properties στο "My Documents". Κάνουμε τις επιλογές όπως φαίνονται στην ακόλουθη εικόνα βάζοντας προφανώς την IP διεύθυνση του εξυπηρετητή του εργαστηρίου που είναι της μορφή 10.X.Y.Z . Στο παράδειγμα που εικονίζεται είναι 10.10.10.10 .




Εικόνα 25 – Ρύθμιση του path των MyDocuments

Επιλέγουμε OK.

Στο ίδιο Policy με παρόμοιο τρόπο κάνουμε redirect την επιφάνεια εργασίας (Desktop) κάθε χρήστη στο path \\<Server-IP>\Users (δεξί click στο φάκελο "Desktop" ακριβώς «πάνω» από τον "My Documents")

Στο τέλος κλείνουμε με τη σειρά τις κονσόλες Group Policy Editor και Active Directory Users and Computers. Οι ρυθμίσεις αυτές θα εμφανιστούν την πρώτη φορά που ο χρήστης θα κάνει logon σε ένα σταθμό εργασίας. Δηλαδή τότε μέσα στον φάκελο Users θα δημιουργηθεί αυτόματα ένας φάκελος με το όνομα του χρήστη και μέσα σε αυτό θα υπάρχουν δύο φάκελοι, My Documents και Desktop.

## 4.7 Λογαριασμοί Διαχείρισης Σχολικού Εργαστηρίου

Για τη διαχείριση του εξυπηρετητή και των σταθμών εργασίας έχει δημιουργηθεί ένας αριθμός λογαριασμών με τα ανάλογα δικαιώματα (domain administrators). Οι υπόλοιποι λογαριασμοί του domain δεν έχουν καταρχήν κανένα διαχειριστικό δικαίωμα σε κανένα από τα υπολογιστικά συστήματα του εργαστηρίου. Υπάρχει πάντα η δυνατότητα να εξουσιοδοτηθούν οι απλοί χρήστες από κάποιον με διαχειριστικά δικαιώματα να πραγματοποιούν συγκεκριμένες διαχειριστικές εργασίες στο domain.

Όλοι οι διαχειριστικοί λογαριασμοί είναι τοποθετημένοι στο OU 'Administrative accounts', έτσι ώστε να εφαρμόζονται σε αυτούς οι κατάλληλες πολιτικές ομάδας. Αυτοί οι λογαριασμοί είναι οι μόνοι που έχουν **δικαίωμα πρόσβασης στον εξυπηρετητή του εργαστηρίου**, τοπικά ή με χρήση εργαλείων απομακρυσμένης διαχείρισης. Το ελάχιστο πλήθος διαχειριστικών λογαριασμών σε επίπεδο domain είναι το ακόλουθο.

1. Λογαριασμός διαχείρισης του domain από τον **υπεύθυνο του εργαστηρίου**. Αυτός ο λογαριασμός έχει πλήρη διαχειριστικά δικαιώματα και επιτρέπει στον καθηγητή, που έχει οριστεί υπεύθυνος στο σχολικό εργαστήριο να πραγματοποιήσει οποιαδήποτε διαχειριστική εργασία (προληπτική συντήρηση, δημιουργία λογαριασμών, εγκατάσταση λογισμικού κλπ). Σημειώνεται πως για λόγους ασφαλείας δεν προτείνεται η χρήση του λογαριασμού κατά την καθημερινή λειτουργία του εργαστηρίου. Ο κωδικός ασφαλείας του λογαριασμού είναι γνωστός μόνο στον υπεύθυνο εργαστηρίου. [Προτεινόμενο όνομα: 'yper']
2. Λογαριασμός διαχείρισης του domain, που δεν χρησιμοποιείται τακτικά, αλλά μπορεί να χρησιμεύσει σε **έκτακτη περίπτωση**. Αν π.χ. για κάποιο λόγο (απώλεια κωδικού ασφαλείας ή κλείδωμα κύριου διαχειριστικού λογαριασμού) δεν είναι δυνατή άμεσα η πρόσβαση στον εξυπηρετητή του εργαστηρίου. Ο λογαριασμός αυτός έχει ανάλογα δικαιώματα με τον προηγούμενο. Ο κωδικός ασφαλείας του λογαριασμού φυλάσσεται από τη σχολική μονάδα. [Προτεινόμενο όνομα: 'bdmn']
3. Λογαριασμός διαχείρισης του domain για τους **Τεχνικούς Υπεύθυνους ΚΕΠΛΗΝΕΤ**, που χρησιμοποιείται επιτόπια ή απομακρυσμένα. Παρέχει

στον τεχνικό πλήρη διαχειριστικά δικαιώματα για την ικανοποίηση οποιουδήποτε αιτήματος έχει τεθεί και κυρίως για την αντιμετώπιση προβλημάτων. Ο κωδικός ασφαλείας του λογαριασμού είναι γνωστός μόνο στους τεχνικούς ΚΕΠΛΗΝΕΤ της περιοχής. [Προτεινόμενο όνομα: 'tstech']

4. Λογαριασμός διαχείρισης του domain για **μηχανικούς και τεχνικούς της Τεχνικής Στήριξης**, που ανήκουν σε υψηλότερο επίπεδο από τους τεχνικούς ΚΕΠΛΗΝΕΤ. Ο λογαριασμός αυτός έχει πλήρη διαχειριστικά δικαιώματα και επιτρέπει τον χειρισμό οποιουδήποτε ζητήματος κυρίως με χρήση απομακρυσμένης διαχείρισης. Ο κωδικός ασφαλείας του λογαριασμού είναι γνωστός μόνο στους τεχνικούς – μηχανικούς της κεντρικής υπηρεσίας αρωγής χρηστών της Τεχνικής Στήριξης στην περιοχή. [Προτεινόμενο όνομα: 'tsremote']

Ανάλογα με τις ανάγκες που θα προκύψουν σε κάθε σχολικό εργαστήριο, **το σχήμα διαχείρισης που περιγράφεται μπορεί να τροποποιηθεί**. Νέοι λογαριασμοί ίσως δημιουργηθούν για τη διαχείριση του εργαστηρίου, ενώ θα μπορούσε να γίνει χρήση και της δυνατότητας εξουσιοδότησης απλών χρηστών με διαχειριστικά δικαιώματα (delegation). Σε κάθε περίπτωση πρέπει να τηρούνται οι εξής βασικοί κανόνες:

- Θα πρέπει **να μην υπάρχει λογαριασμός διαχειριστή με όνομα 'administrator'** στο domain. Οι υπάρχοντες εξ' ορισμού λογαριασμοί στον εξυπηρετητή και στους σταθμούς εργασίας θα πρέπει να μετονομάζονται και να δημιουργούνται ομώνυμοι λογαριασμοί χωρίς προνόμια για λόγους ασφαλείας.
- Δεν υπάρχει **κανένας τοπικός λογαριασμός με διαχειριστικά δικαιώματα** σε κάποιον από τους σταθμούς εργασίας του εργαστηρίου. Οι built-in λογαριασμοί 'administrator' παραμένουν απενεργοποιημένοι (disabled) με χρήση της Group Policy επιλογής *Computer Configuration* | *Windows Settings* | *Security Settings* | *Local Policies* | *Security Options* | *Accounts: Administrator account status.* Η διαχείριση στους σταθμούς εργασίας πραγματοποιείται με χρήση των λογαριασμών του domain.
- **Κατά την καθημερινή χρήση του εργαστηρίου για εκπαιδευτικούς σκοπούς δεν θα πρέπει να γίνεται χρήση κανενός λογαριασμού με διαχειριστικά δικαιώματα**. Οι λογαριασμοί απλών χρηστών (για μαθητές και καθηγητές) επαρκούν για την πλειονότητα των περιπτώσεων χρήσης των πληροφοριακών συστημάτων.

Για τη μετονομασία του λογαριασμού Administrator και του λογαριασμού Guest πραγματοποιούμε τα ακόλουθα βήματα:

- Με την Group Policy Management Console δημιουργούμε στο domain school.edu το GPO "SEPEHY-Rename Administrator and Guest Accounts".
- Κάνουμε Edit το GPO που δημιουργήσαμε στο προηγούμενο βήμα και στην ομάδα επιλογών: Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options, τροποποιούμε τη ρύθμιση: "Accounts: Rename administrator account".
- Ενεργοποιούμε την επιλογή "Define this policy setting" και εισάγουμε το νέο όνομα 'yper'.
- Με παρόμοιο τρόπο υπάρχει η δυνατότητα τροποποίησης του ονόματος του λογαριασμού Guest, από τη ρύθμιση "Accounts: Rename guest account".

## 4.8 Διαδικασία εισαγωγής λογαριασμών χρηστών

Η διαδικασία εισαγωγής χρηστών μπορεί να επιταχυνθεί με τη χρήση του αντίστοιχου εργαλείου της γραμμής εντολών dsadd user. Ακολουθεί παράδειγμα δημιουργίας κοινόχρηστου λογαριασμού:

```
dsadd user "cn=user10, ou=Users, ou=Shared Accounts, ou=Accounts, ou=SEPEHY_1, ou=School, dc=school, dc=edu" -pwd Changeme! -canchpwd no -pwdneverexpires yes -profile "\10.10.10.10\Profiles\user10"
```

Στην περίπτωση που πρέπει να γίνει μαζικά εισαγωγή μεγάλου αριθμού προσωπικών λογαριασμών χρηστών, μπορούμε με τη βοήθεια ενός φύλλου εργασίας να δημιουργήσουμε μία γραμμή εντολών δημιουργίας λογαριασμού ανά χρήστη με τη βοήθεια του υποδείγματος που υπάρχει στον Ενημερωτικό Κόμβο http://ts.sch.gr (πρόσβαση για κάθε χρήστη με τα στοιχεία του προσωπικού του λογαριασμού στο ΠΣΔ).

Τα ονόματα των λογαριασμών δημιουργούνται αυτόματα από το όνομα και το επώνυμο του χρήστη, εκτός από τους κοινόχρηστους λογαριασμούς, όπου μπορούμε να επιλέξουμε ονοματολογία του τύπου user1, user2, κλπ. Στην περίπτωση που με την αυτόματη δημιουργία γραμμής εντολών προκύπτουν κοινά ονόματα λογαριασμών, τότε πρέπει να τροποποιήσουμε κατ' ελάχιστο τα κοινά ονόματα, ώστε να μην προκύψουν προβλήματα στη δημιουργία των λογαριασμών.

Όταν τα στοιχεία του φύλλου εργασίας είναι σωστά επιλέγουμε τα κελιά με τις εντολές dsadd user και τα αντιγράφουμε σε παράθυρο της γραμμής εντολών, αφού προηγουμένως έχουν δημιουργηθεί τα OUs, που ορίζονται στην στήλη OU.

# 5 Άλλες υπηρεσίες και ρυθμίσεις

## 5.1 Ενεργοποίηση απομακρυσμένης πρόσβασης (Remote Desktop) & αυτόματων ενημερώσεων (Automatic Updates)

Προκειμένου να είναι εφικτή η απομακρυσμένη διαχείριση του εξυπηρετητή πρέπει να είναι ενεργοποιημένη η προσφερόμενη υπηρεσία των Windows. Στις ιδιότητες συστήματος (system properties) ενεργοποιείται η δυνατότητα Remote Desktop που επιτρέπει εξ' ορισμού την πρόσβαση σε όσους ανήκουν στο group 'Administrators'.

Ενεργοποιείται επίσης η καθημερινή αυτόματη λήψη και εγκατάσταση των νέων κρίσιμων ενημερώσεων. Ορίζεται κάποια ώρα κατά την οποία δεν γίνεται χρήση του εργαστηρίου και είναι ο εξυπηρετητής σε λειτουργία. Προτείνεται να γίνεται αποδεκτή η τυπική ώρα (3:00 π.μ.) αν δεν υπάρχουν ιδιαιτερότητες που καθιστούν αναγκαίο κάποιο διαφορετικό χειρισμό.

## 5.2 Ενεργοποίηση υπηρεσίας shadow copies

Η έκδοση 2003 της σειράς λειτουργικών συστημάτων Microsoft Server ενσωματώνει μια νέα πολύ χρήσιμη λειτουργικότητα με το όνομα 'shadow copies of shared folders'. Αυτή η δυνατότητα επιτρέπει την αντιμετώπιση του φαινομένου της απώλειας δεδομένων από διαμοιραζόμενους φακέλους μετά από εσφαλμένη διαγραφή ή τροποποίηση αρχείων από τους χρήστες. Αυτό επιτυγχάνεται με τη δημιουργία κρυμμένων αντιγράφων (shadow copies) των αρχείων που ανήκουν σε διαμοιραζόμενους φακέλους ανά τακτά χρονικά διαστήματα.

Προτείνεται η ενεργοποίηση της δυνατότητας τουλάχιστον στην κατάτμηση που περιέχει τα αρχεία των χρηστών, αλλά και σε οποιαδήποτε άλλη κατάτμηση υπάρχουν διαμοιραζόμενοι φάκελοι που χρειάζονται προστασία. Από το εργαλείο διαχείρισης Computer Management και το τμήμα που αφορά τους διαμοιραζόμενους φακέλους (shared folders) μπορεί να ρυθμιστεί η υπηρεσία (με δεξί κλικ → all tasks → configure shadow copies). Σε κάθε κατάτμηση που ενεργοποιείται η δυνατότητα επιλέγεται χώρος ίσος με το 10% του μεγέθους της και τροποποιείται το υπάρχον χρονοδιάγραμμα ώστε καθημερινά να λαμβάνονται αντίγραφα στις 11:00, αν δεν υπάρχουν ιδιαιτερότητες στο ωράριο λειτουργίας του εργαστηρίου που καθιστούν αναγκαίο κάποιο διαφορετικό χειρισμό.

Η ανάκτηση προηγούμενων εκδόσεων αρχείων από τα ληφθέντα shadow copies πραγματοποιείται:

- από την κονσόλα του εξυπηρετητή μέσω του '\\<server-name>\<drive-letter>$, όπου <drive-letter> η κατάτμηση όπου βρίσκεται ο διαμοιραζόμενος φάκελος από τον οποίο θέλουμε να ανακτήσουμε αρχεία.
- από το σταθμό εργασίας μετά την εγκατάσταση του "shadow copy client" (από το http://www.microsoft.com/downloads/, αναζήτηση του "shadow copy client"), \\<server-name>\, καρτέλα "Previous Versions" στα Properties του Shared Folder.

## 5.3 Αρχείο σελιδοποίησης (paging file)

Η ταχύτητα προσπέλασης στο αρχείο σελιδοποίησης είναι κρίσιμη για την αποδοτική λειτουργία του εξυπηρετητή και την παροχή υπηρεσιών στο εργαστήριο. Όταν υπάρχει δεύτερος σκληρός δίσκος είναι δυνατή η χρήση του για αυτό το σκοπό και συγκεκριμένα η αξιοποίηση της κατάτμησης που έχει διαμορφωθεί για αυτό το σκοπό.

Στις ιδιότητες συστήματος (system properties) και στις επιλογές που έχουν σχέση με την απόδοση (performance options) είναι εφικτή η ρύθμιση του αρχείου εικονικής μνήμης (virtual memory). Προτείνεται η διαγραφή του αρχείου σελιδοποίησης από την πρωτεύουσα κατάτμηση που περιέχει το λειτουργικό σύστημα και τις εφαρμογές και η δημιουργία νέου αρχείου στην πρώτη κατάτμηση του δεύτερου σκληρού δίσκου. Το αρχικό μέγεθος του αρχείου (initial size) προτείνεται να είναι ίσο με το μέγιστο μέγεθος (maximum size) και να έχει τιμή 1.5 φορά μεγαλύτερη από το μέγεθος της διαθέσιμης μνήμης RAM (π.χ. για συστήματα με 512 MB μνήμη RAM ισχύει ότι 'initial size = maximum size = 764 MB'). Αν η μνήμη έχει περιορισμένο μέγεθος ο παραπάνω κανόνας μπορεί να τροποποιείται ώστε το pagefile να έχει μέγεθος τουλάχιστον 768 MB (π.χ. για 256 MB μνήμη RAM η αναλογία μπορεί να πάρει την τιμή 3 ώστε 'initial size = maximum size = 768 MB').

Κατά την εφαρμογή της ανωτέρω οδηγίας πρέπει να αγνοηθεί οποιοδήποτε μήνυμα αφορά τη διαγραφή του αρχείου σελιδοποίησης από την πρωτεύουσα κατάτμηση και να πραγματοποιηθεί επανεκκίνηση του συστήματος όταν ζητηθεί.

## 5.4 Θέση αρχείου εκτυπώσεων (spooler file)

Η μεταφορά του βοηθητικού αρχείου εκτυπώσεων (spooler) στο δεύτερο σκληρό δίσκο του εξυπηρετητή μπορεί να συμβάλει στην ταχύτερη απόκρισή του, καθώς στο σχολικό περιβάλλον χρησιμοποιείται συχνά ως διακομιστής εκτυπώσεων από όλους τους σταθμούς εργασίας του εργαστηρίου.

Η επιθυμητή ρύθμιση μπορεί να πραγματοποιηθεί από το παράθυρο επισκόπησης των εγκατεστημένων εκτυπωτών (Control Panel – Printers), όπου από το μενού 'File – Server Properties' και τις προηγμένες ρυθμίσεις (advanced) μπορεί να οριστεί η τοποθεσία (spool folder) του βοηθητικού αρχείου σε οποιοδήποτε φάκελο της πρώτης κατάτμησης του δεύτερου σκληρού δίσκου (π.χ. *<DriveLetter>:\spool*)

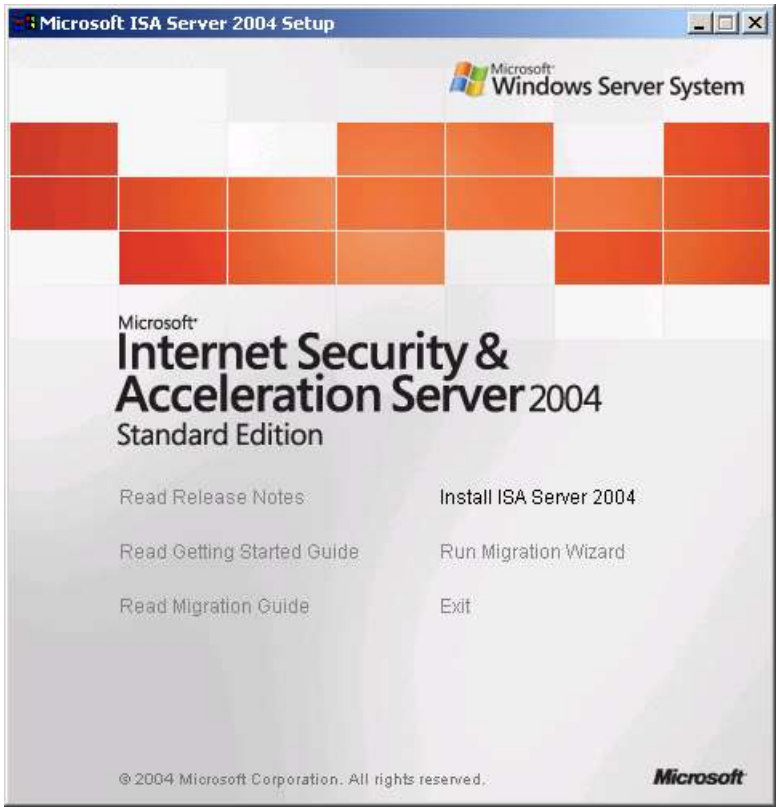
# 6 MS ISA Server 2004

Σε ορισμένα σχολικά εργαστήρια εγκαθίσταται η νεότερη έκδοση του proxy server της Microsoft για επιτάχυνση της πρόσβασης στον παγκόσμιο ιστό. Με την υπηρεσία προσωρινής αποθήκευσης που παρέχεται από την εφαρμογή, είναι δυνατή η προσπέλαση ιστοσελίδων από τους χρήστες του σχολικού εργαστηρίου, χωρίς να καταναλώνεται πολύτιμο εύρος ζώνης.

Η διαδικασία εγκατάστασης του MS ISA Server 2004 και η προτεινόμενη ρύθμισή του για βέλτιστη λειτουργία περιγράφεται στη συνέχεια. Το ενσωματωμένο φράγμα ασφαλείας (firewall) εγκαθίσταται εξ' ορισμού και δεν είναι δυνατή η απενεργοποίησή του κατά την εγκατάσταση. Λόγω της λειτουργίας του ISA Server 2004 ως φράγμα ασφαλείας απαιτούνται ορισμένες ειδικές ενέργειες για την ορθή ρύθμιση της εφαρμογής στο σχολικό περιβάλλον.

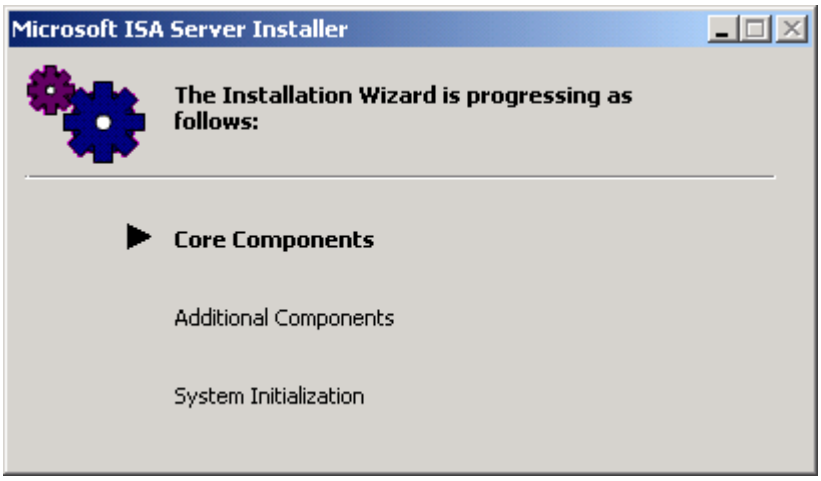
## 6.1 Ρύθμιση MS ISA Server 2004

Εμφανίζεται η αρχική οθόνη εγκατάστασης. Επιλέγεται 'Install ISA Server 2004'.



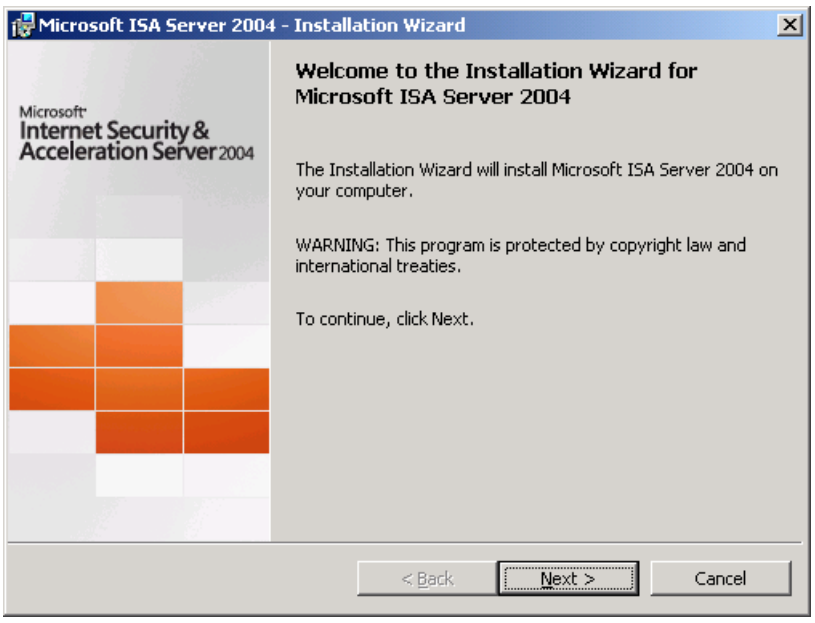

Εικόνα 26 – MS ISA Server 2004: Αρχική οθόνη εγκατάστασης

- Εμφανίζεται ενημερωτικό μήνυμα σχετικά με τη διαδικασία βημάτων που θα ακολουθήσει ο οδηγός εγκατάστασης.




Εικόνα 27 – MS ISA Server 2004: Ενημερωτικό μήνυμα

- Πραγματοποιείται εκκίνηση του οδηγού εγκατάστασης.

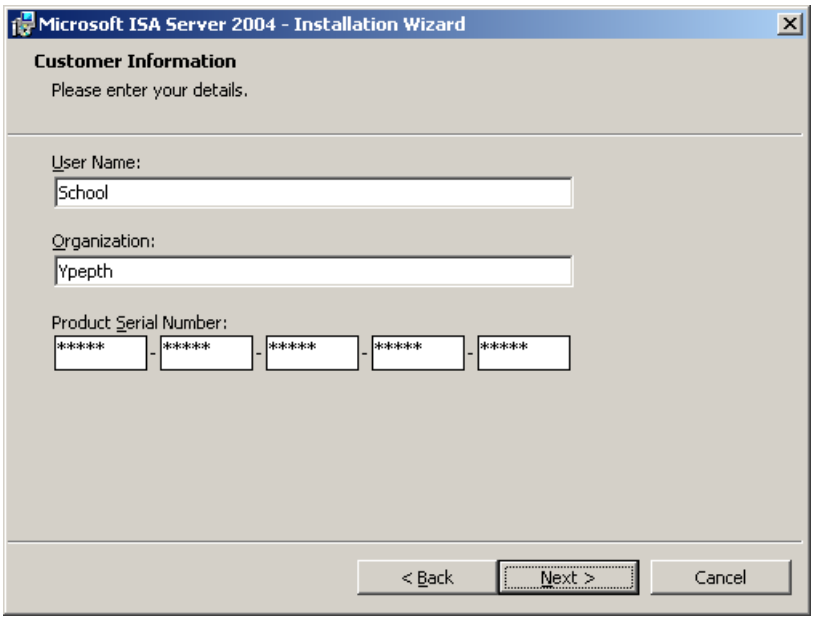



Εικόνα 28 – MS ISA Server 2004: Εκκίνηση οδηγού εγκατάστασης

- Γίνεται αποδεκτή η άδεια χρήσης του προϊόντος.

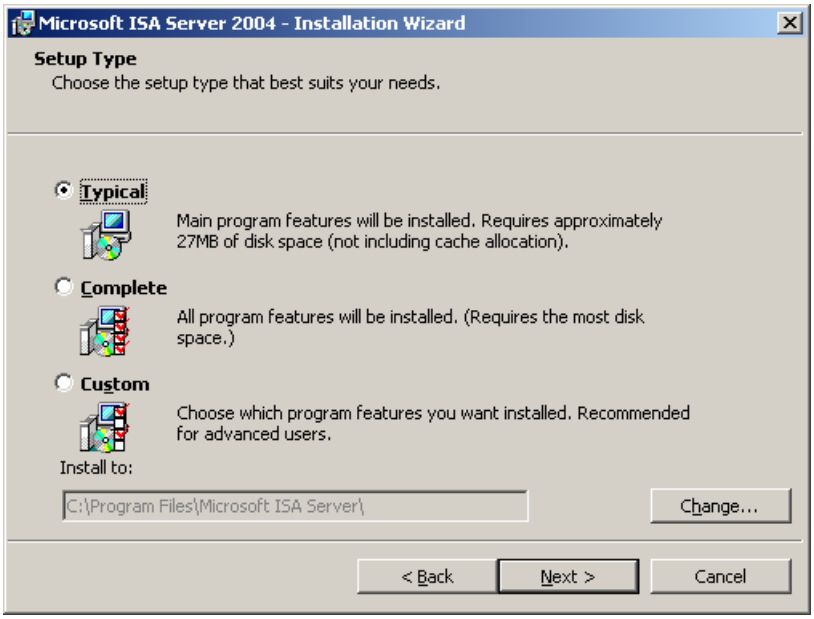

Εικόνα 29 – MS ISA Server 2004: Αποδοχή όρων άδειας χρήσης

- Εισάγονται τα στοιχεία χρήστη. Προτείνεται να διατηρηθούν οι προεπιλεγμένες τιμές, που προκύπτουν από τις αντίστοιχες τιμές των Windows. Επίσης γίνεται εισαγωγή του αριθμού-κλειδιού του προϊόντος (product key).



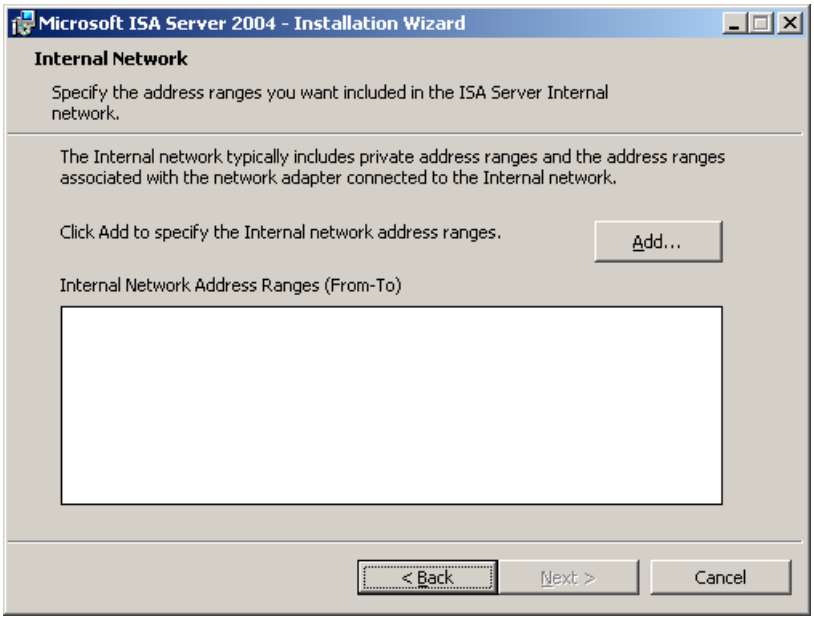

Εικόνα 30 – MS ISA Server 2004: Εισαγωγή στοιχείων χρήστη & αριθμού-κλειδιού

- Επιλέγεται τυπική εγκατάσταση. Η πλήρης εγκατάσταση δεν είναι εφαρμόσιμη σε αυτή την περίπτωση, καθώς περιλαμβάνει τον message screener που απαιτεί τη λειτουργία της υπηρεσίας snmp.



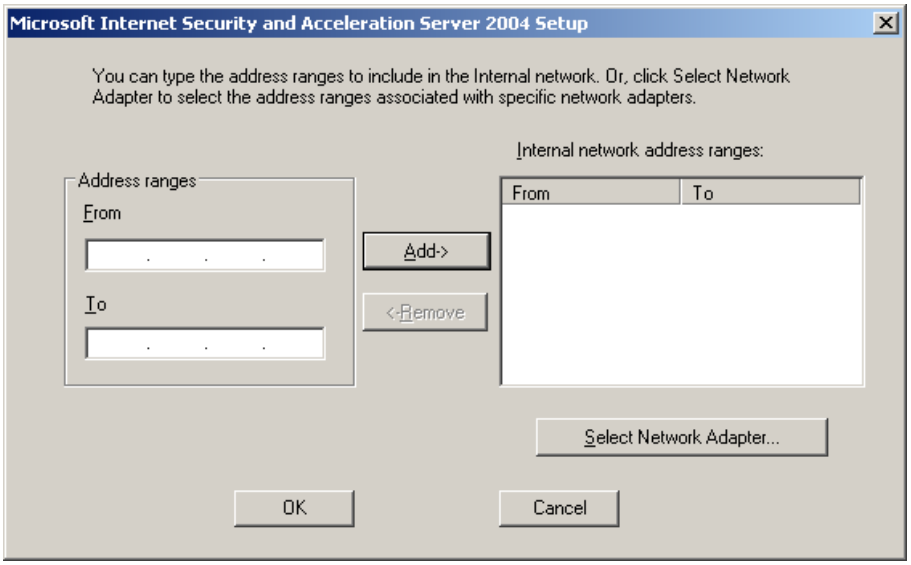

Εικόνα 31 – MS ISA Server 2004: Ορισμός παραμέτρων εγκατάστασης

- Εμφανίζεται ο οδηγός καθορισμού των διευθύνσεων που απαρτίζουν το εσωτερικό υποδίκτυο, όπως το εκλαμβάνει ο ISA Server 2004.



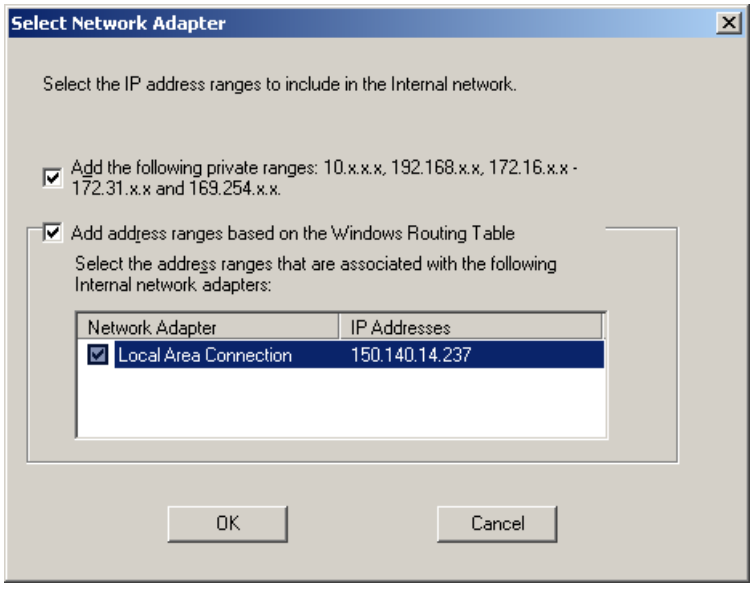

Εικόνα 32 – MS ISA Server 2004: Οδηγός ορισμού εσωτερικού υποδικτύου

- Εμφανίζεται το παράθυρο εισαγωγής του εύρους διευθύνσεων του εσωτερικού υποδικτύου. Επιλέγεται 'Select Network Adapter'.



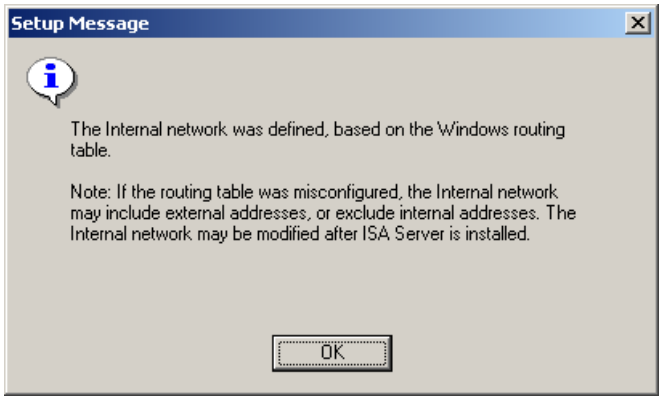

Εικόνα 33 – MS ISA Server 2004: Επιλογή εύρους εσωτερικού υποδικτύου

- Επιλέγεται ο προσαρμογέας δικτύου (network adapter) στον οποίο είναι συνδεδεμένο το τοπικό δίκτυο και ενεργοποιείται κάθε δυνατό εύρος (private ranges & ranges based on the Windows Routing Table).



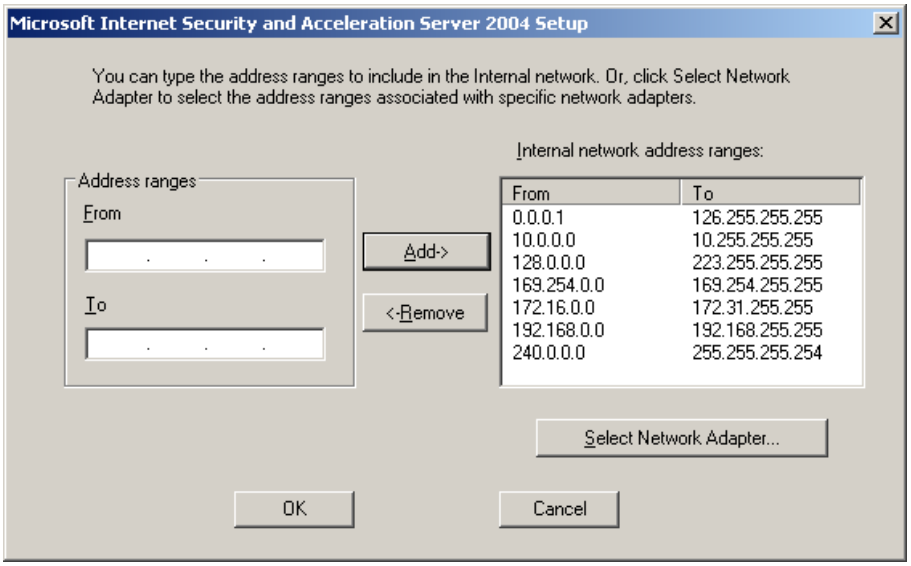

Εικόνα 34 – MS ISA Server 2004: Επιλογή προσαρμογέα δικτύου

- Εμφανίζεται ενημερωτικό μήνυμα σχετικά με την σημασία της ορθής ρύθμισης του εσωτερικού υποδικτύου.



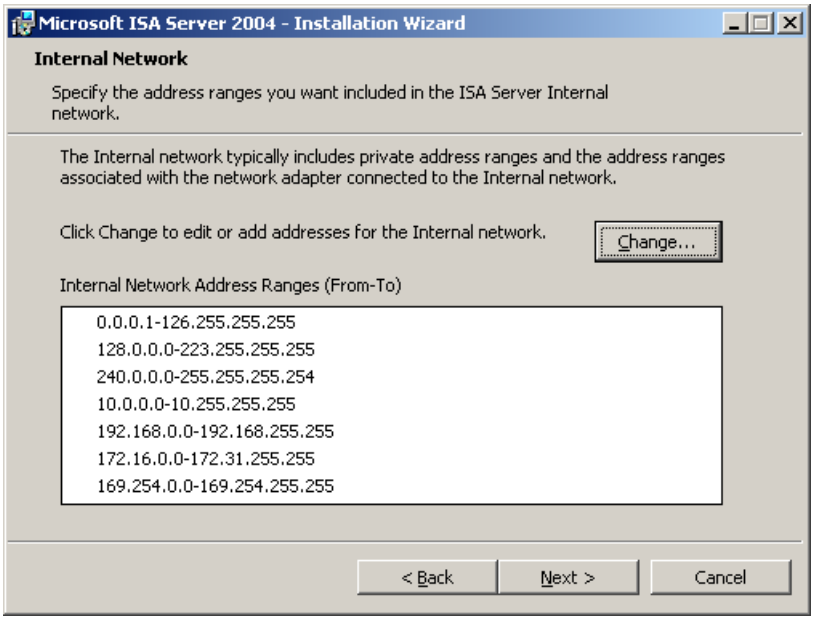

Εικόνα 35 – MS ISA Server 2004: Ενημερωτικό μήνυμα

- Εμφανίζεται η λίστα των διευθύνσεων που επιλέχθηκαν.



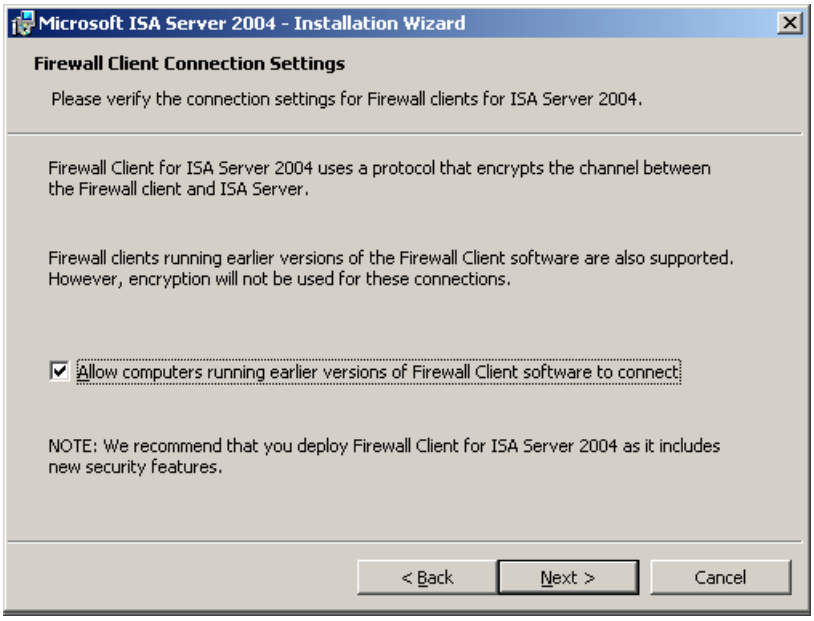

Εικόνα 36 – MS ISA Server 2004: Εύρος διευθύνσεων εσωτερικού υποδικτύου

- Εμφανίζεται το εύρος διευθύνσεων που έχει επιλεγεί και δίνεται δυνατότητα για πραγματοποίηση αλλαγών, που δεν χρειάζεται να αξιοποιηθεί.



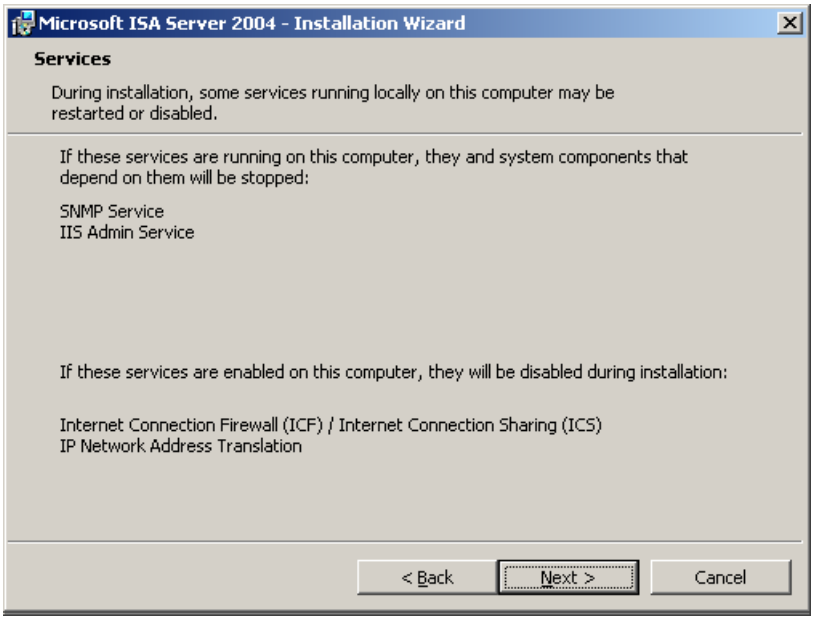

Εικόνα 37 – MS ISA Server 2004: Αλλαγή εύρους διευθύνσεων εσωτερικού υποδικτύου

- Επιλέγεται να είναι δυνατή η χρήση του ISA Server από σταθμούς εργασίας που δεν έχουν την τελευταία έκδοση του Firewall Client.



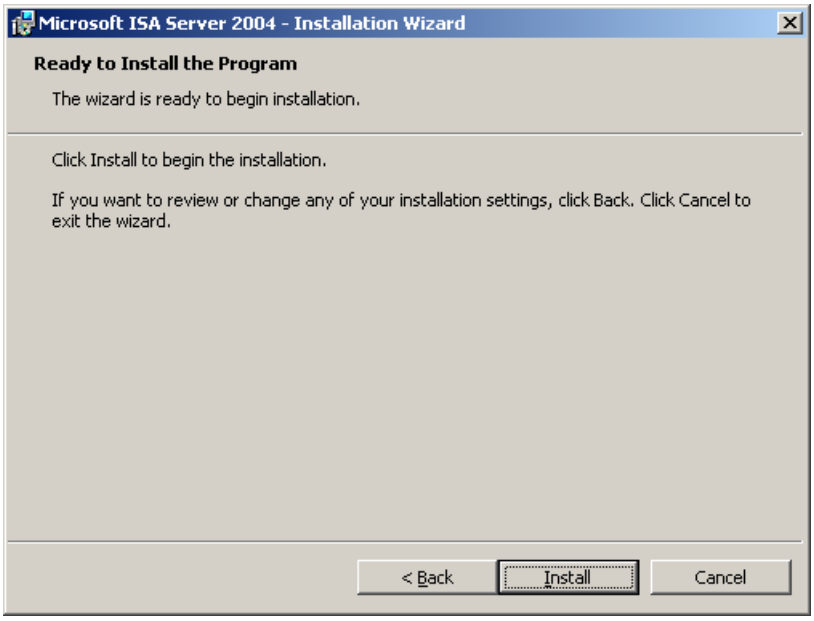

Εικόνα 38 – MS ISA Server 2004: Ρυθμίσεις firewall client

- Εμφανίζεται ενημερωτικό μήνυμα σχετικά με την προσωρινή παύση – απενεργοποίηση ορισμένων υπηρεσιών, που δεν συνηθίζεται να είναι σε λειτουργία στο σχολικό εργαστήριο.




Εικόνα 39 – MS ISA Server 2004: Παύση – απενεργοποίηση υπηρεσιών

- Πραγματοποιείται εκκίνηση της διαδικασίας εγκατάστασης με βάση τις επιλογές που έγιναν στα προηγούμενα βήματα.

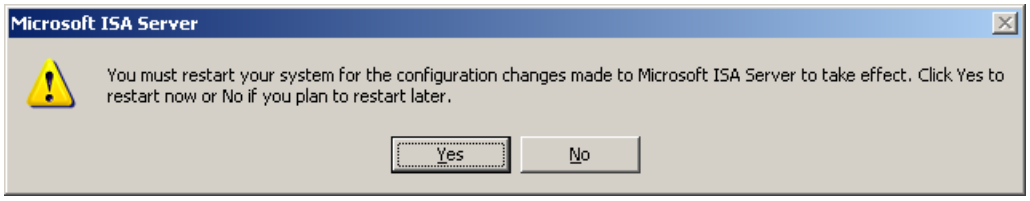



Εικόνα 40 – MS ISA Server 2004: Εκκίνηση εγκατάστασης

- Μετά από σημαντικό χρονικό διάστημα η εγκατάσταση ολοκληρώνεται.


Εικόνα 41 – MS ISA Server 2004: Ολοκλήρωση εγκατάστασης

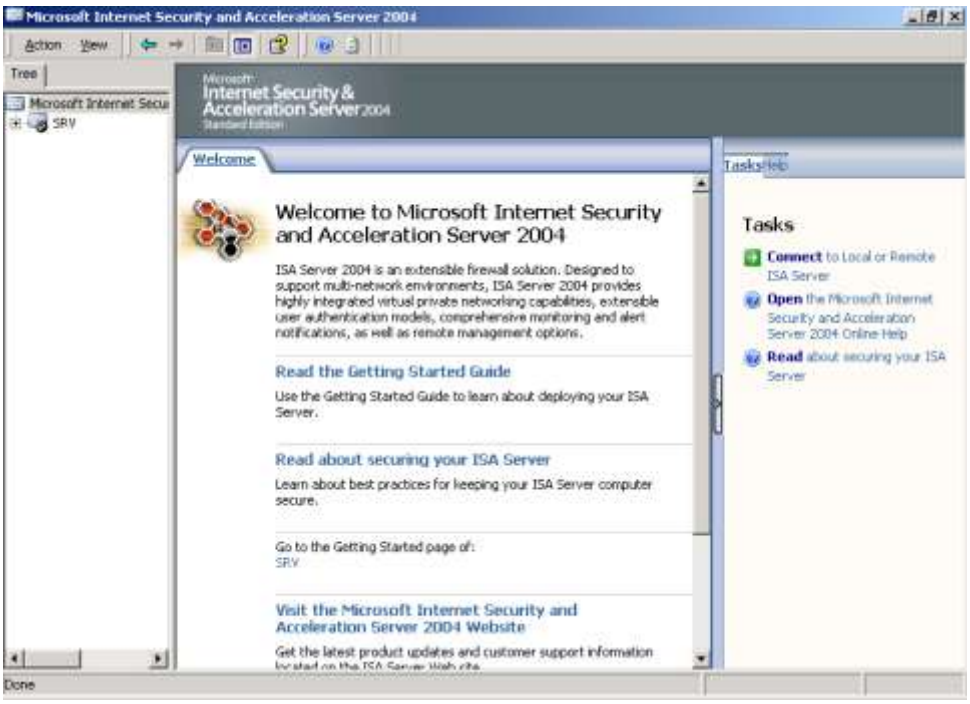
- Ζητείται επανεκκίνηση του συστήματος για την επιτυχή ολοκλήρωση της διαδικασίας.




Εικόνα 42 – MS ISA Server 2004: Επανεκκίνηση συστήματος

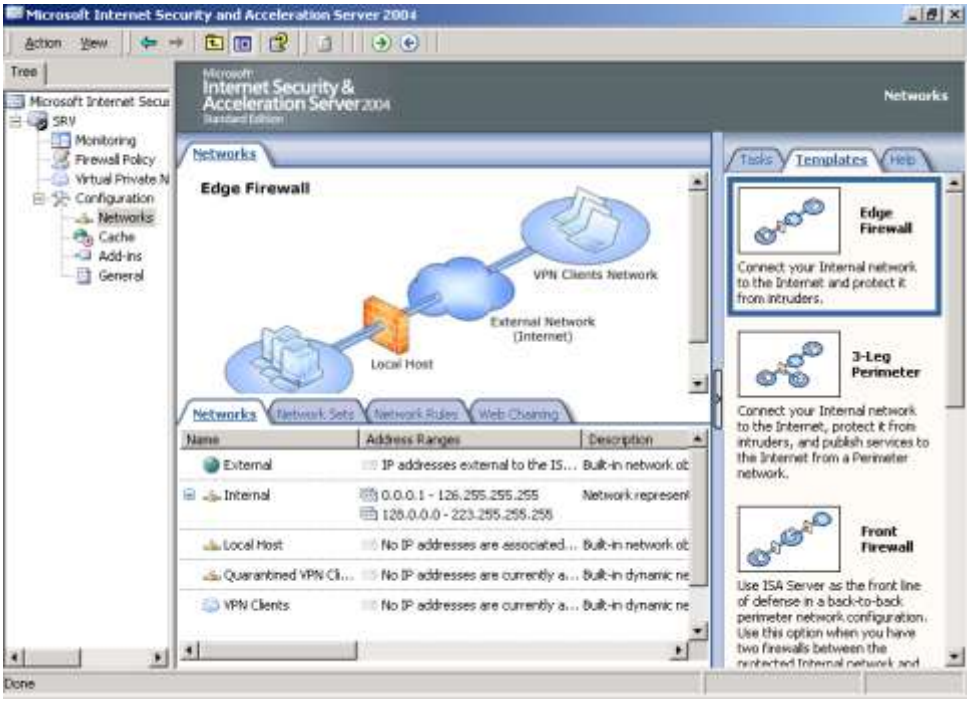
## 6.2 Ρύθμιση ISA Server για την απενεργοποίηση του firewall

- Γίνεται εκκίνηση του περιβάλλοντος διαχείρισης του ISA Server (Start → Programs → Microsoft ISA Server → ISA Management).



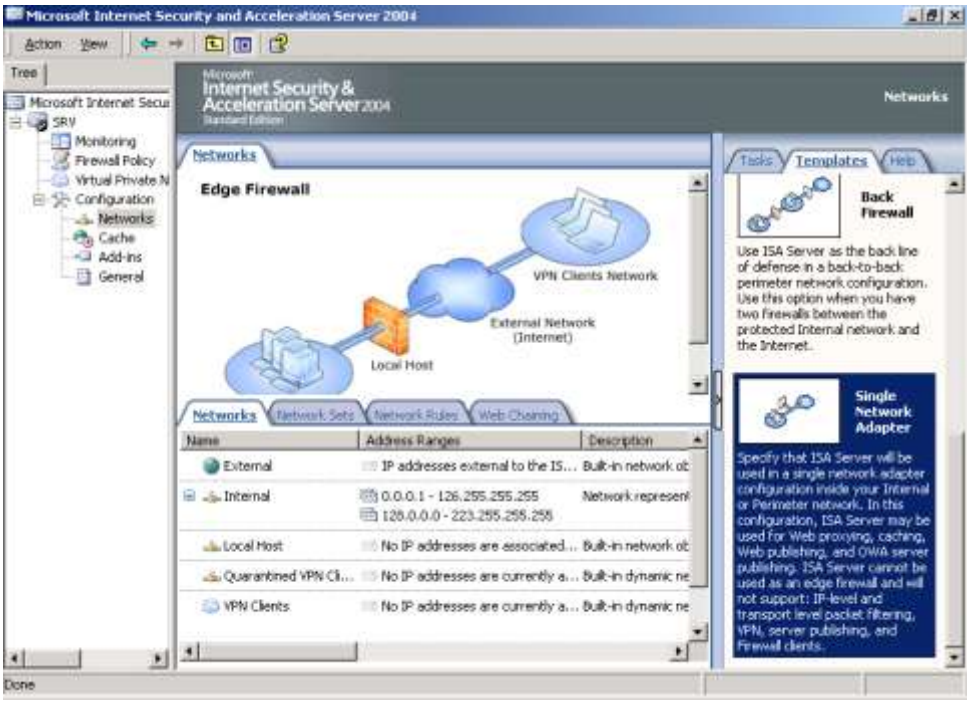

Εικόνα 43 – MS ISA Server 2004: ISA Management

- Επιλέγεται η ρύθμιση των δικτύων (configuration – networks) από την δενδρική δομή του αριστερού παραθύρου.



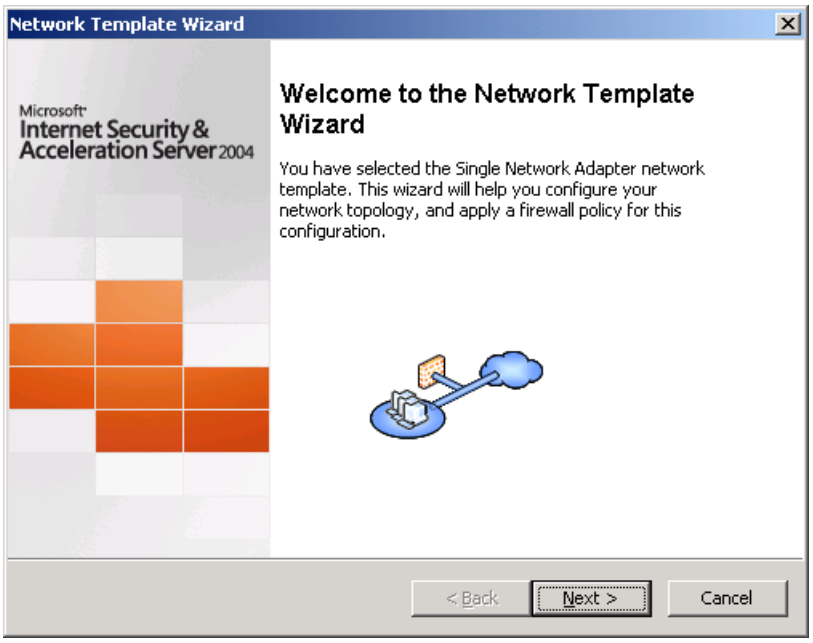

Εικόνα 44 – MS ISA Server 2004: Ρύθμιση δικτύων

- Επιλέγονται τα πρότυπα (templates) από το δεξί παράθυρο επιλέγουμε το και συγκεκριμένα η λειτουργία του ISA Server ως 'single network adapter'.



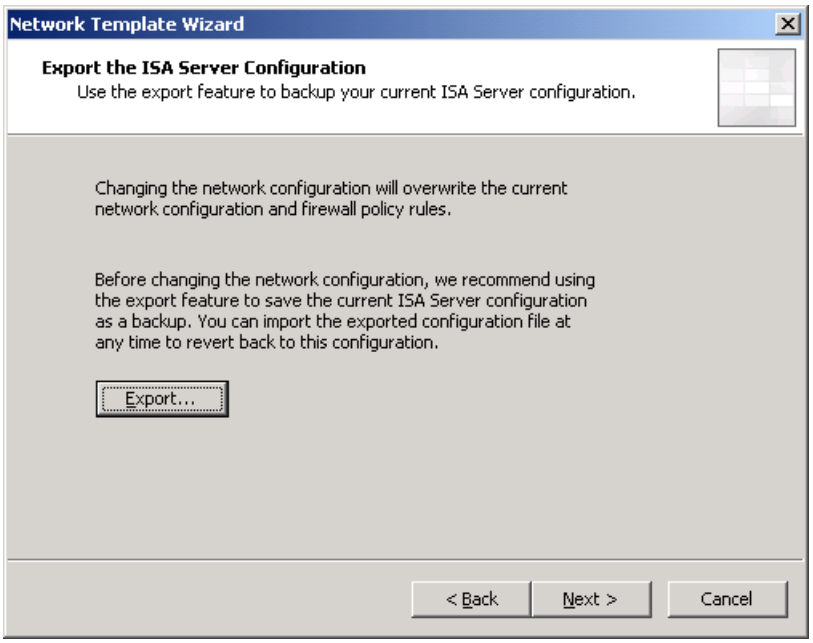

Εικόνα 45 – MS ISA Server 2004: Single Network Adapter

- Γίνεται εκκίνηση ενός οδηγού ρύθμισης του ISA Server 2004.



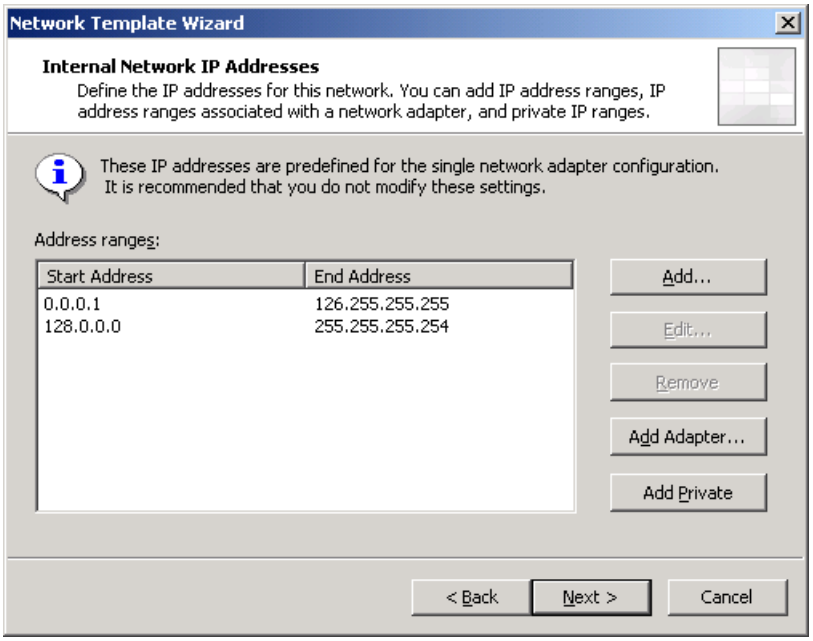

Εικόνα 46 – MS ISA Server 2004: Εκκίνηση οδηγού ρύθμισης

- Δεν γίνεται χρήση της δυνατότητας λήψης αντιγράφων ασφαλείας (export) της ισχύουσας ρύθμισης του ISA Server.



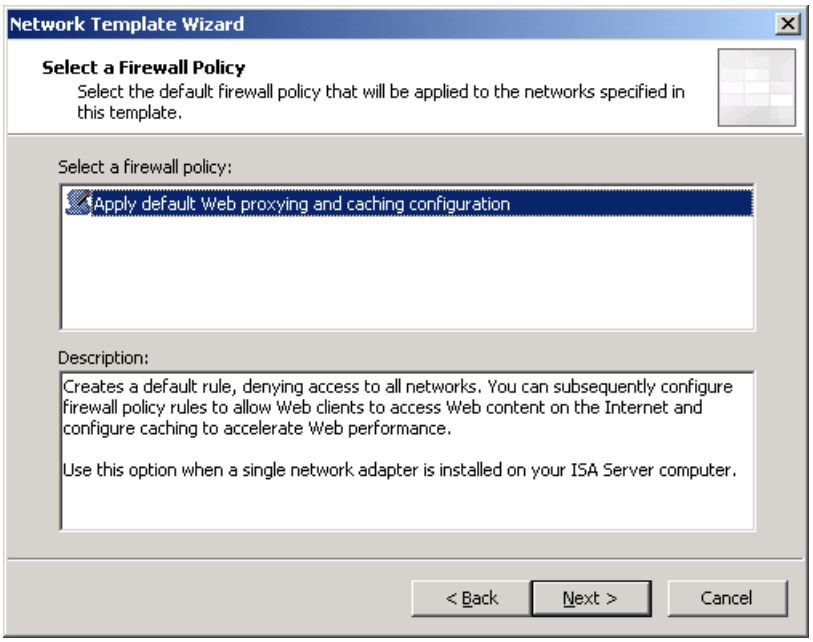

Εικόνα 47 – MS ISA Server 2004: Οθόνη αποθήκευσης ρυθμίσεων

- Γίνονται αποδεκτές οι προεπιλεγμένες ρυθμίσεις.



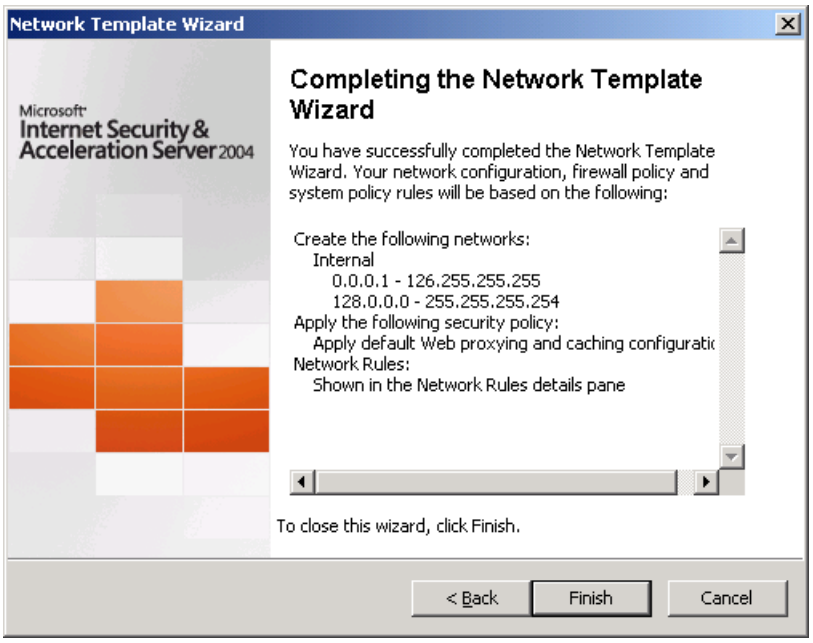

Εικόνα 48 – MS ISA Server 2004: Ορισμός IP διευθύνσεων

- Επιλέγεται η εφαρμογή των τυπικών ρυθμίσεων ('apply default Web proxying and caching configuration').



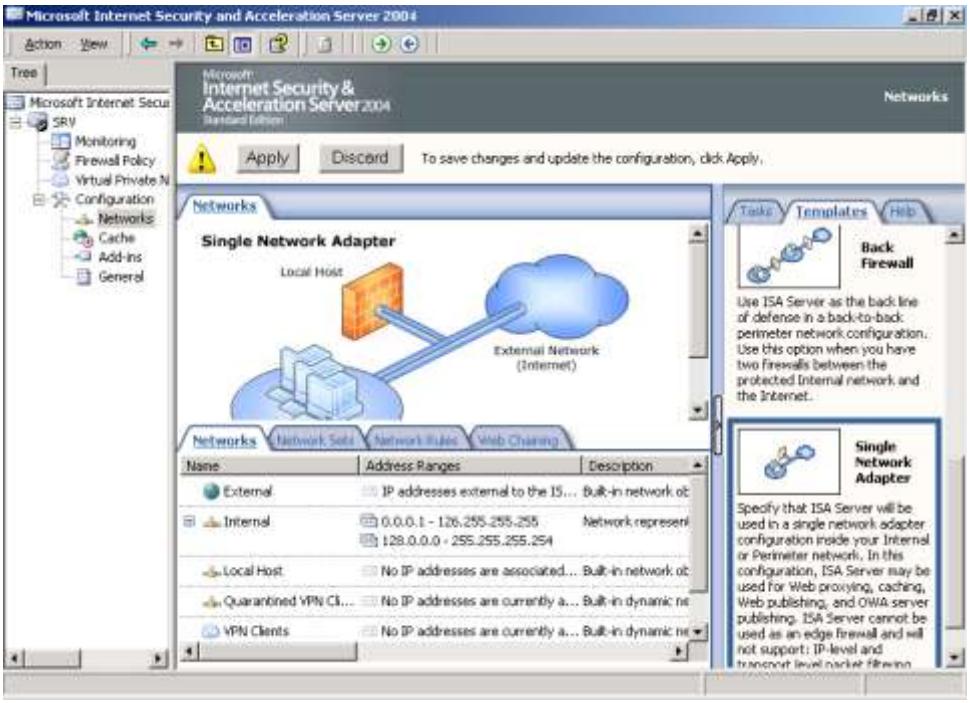

Εικόνα 49 – MS ISA Server 2004: Εφαρμογή τυπικών ρυθμίσεων

- Ολοκληρώνεται ο οδηγός ρύθμισης του ISA Server.



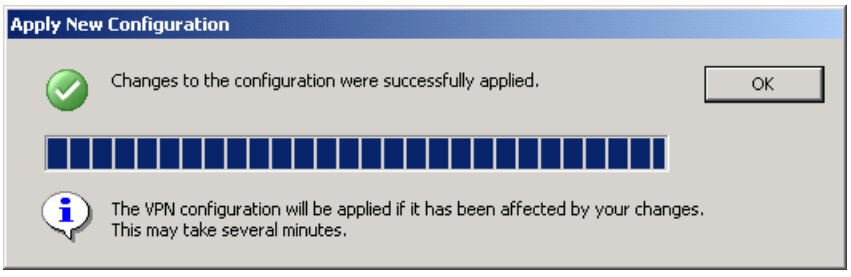

Εικόνα 50 – MS ISA Server 2004: Ολοκλήρωση οδηγού ρύθμισης

- Γίνεται αποθήκευση και εφαρμογή των ρυθμίσεων που επιλέχθηκαν (πλήκτρο 'apply').



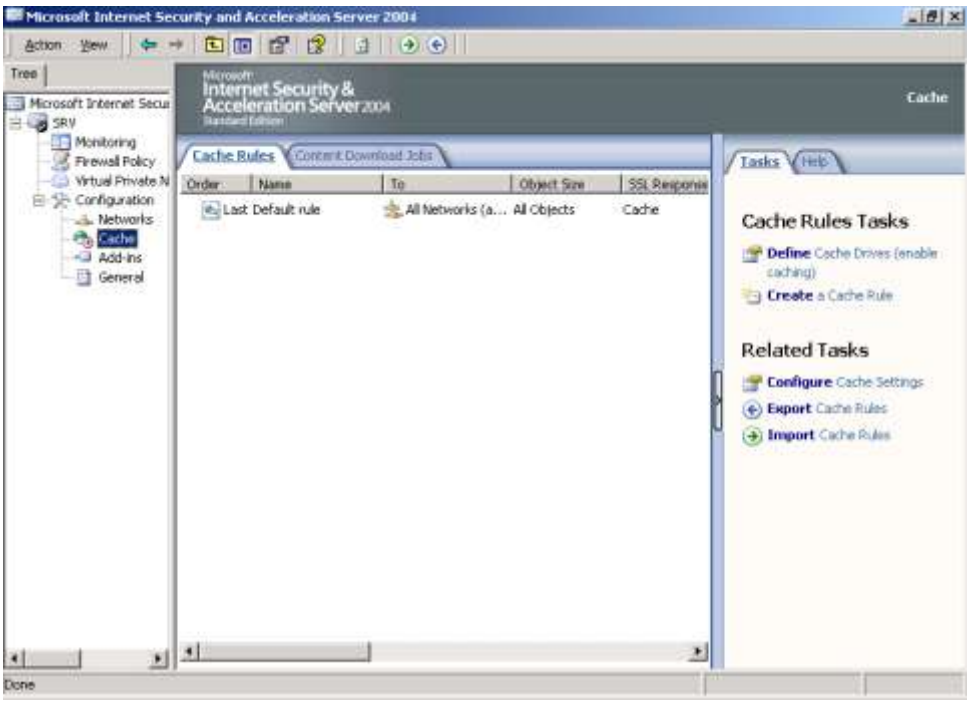

Εικόνα 51 – MS ISA Server 2004: Εφαρμογή ρυθμίσεων

- Εμφανίζεται μήνυμα σχετικά με την επιτυχή εφαρμογή των ρυθμίσεων.



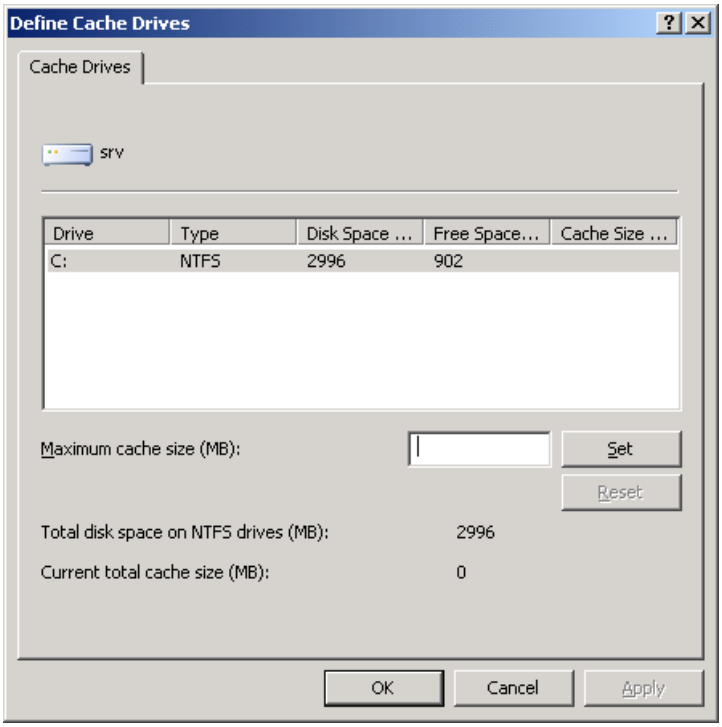

Εικόνα 52 – MS ISA Server 2004: Ενημερωτικό μήνυμα

- Στη συνέχεια ρυθμίζεται η προσωρινή μνήμη αποθήκευσης (cache) του ISA Server. Επιλέγεται 'cache' από τη δενδρική δομή του αριστερού παραθύρου και 'define cache drives' από το δεξί τμήμα της κονσόλας διαχείρισης.



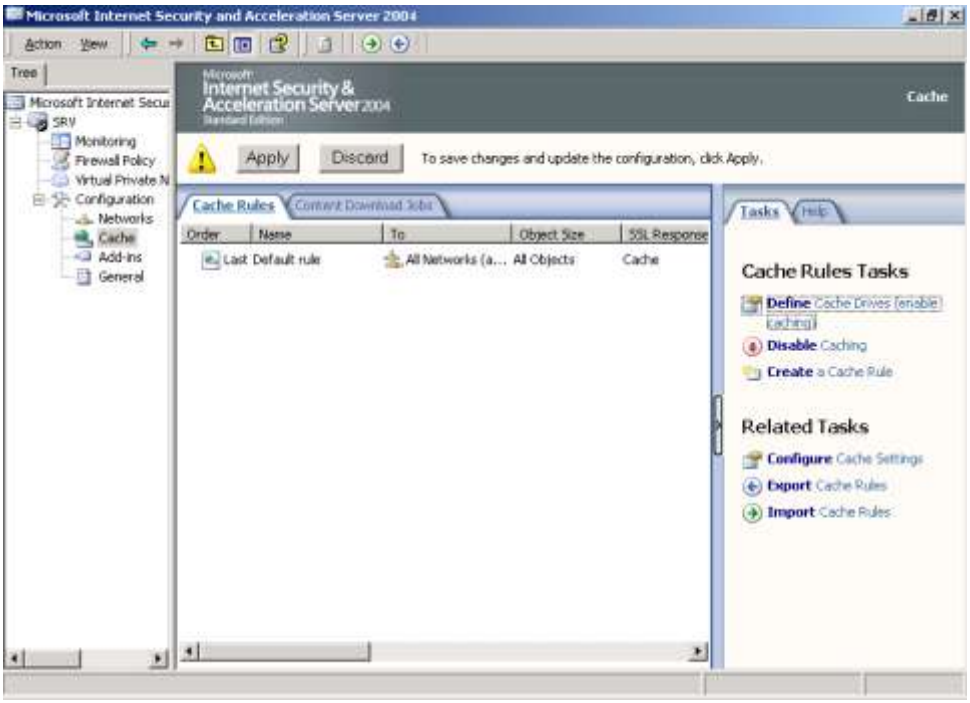

Εικόνα 53 – MS ISA Server 2004: Ρύθμιση cache

- Επιλέγεται η κατάτμηση που θα χρησιμοποιηθεί για την αποθήκευση των προσωρινών αρχείων και ορίζεται το μέγεθός της. Γίνεται εκμετάλλευση της κατάτμησης που έχει δημιουργηθεί για αυτό το σκοπό (πρώτη κατάτμηση δεύτερου σκληρού δίσκου με volume label 'temp') και καταλαμβάνεται το 20% του διαθέσιμου χώρου.



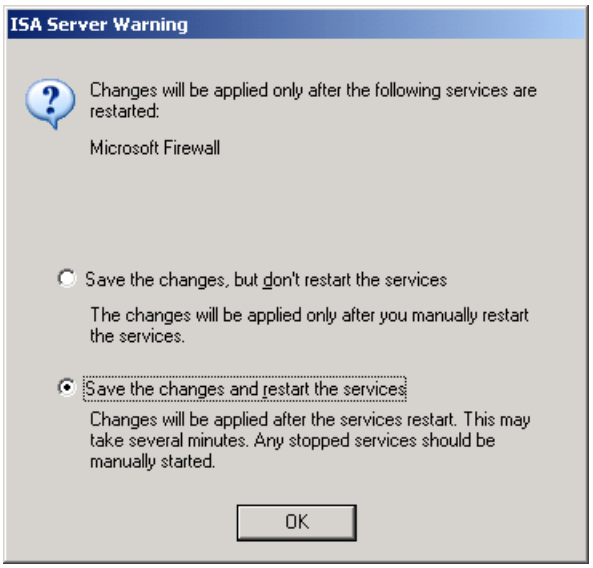

Εικόνα 54 – MS ISA Server 2004: Ορισμός cache drive

- Γίνεται αποθήκευση και εφαρμογή των ρυθμίσεων που επιλέχθηκαν (πλήκτρο 'apply').



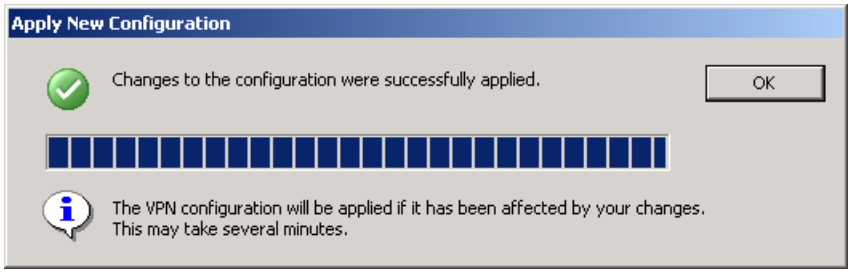

Εικόνα 55 – MS ISA Server 2004: Εφαρμογή ρυθμίσεων

- Πραγματοποιείται επανεκκίνηση των σχετικών υπηρεσιών για την ορθή ολοκλήρωση της διαδικασίας.



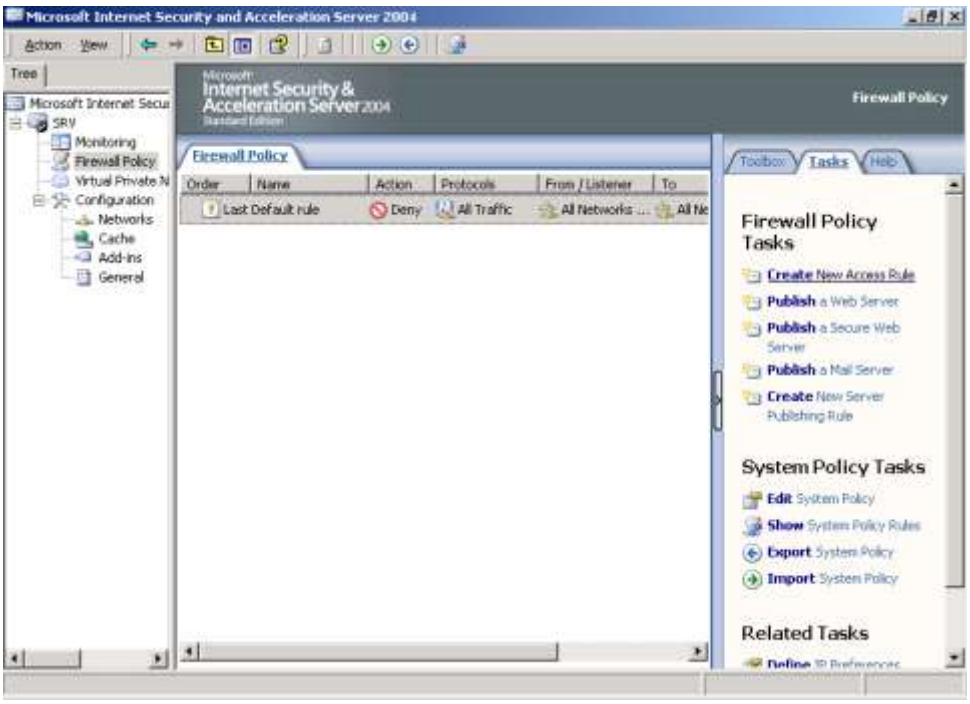

Εικόνα 56 – MS ISA Server 2004: Επανεκκίνηση υπηρεσιών

- Εμφανίζεται μήνυμα σχετικά με την επιτυχή εφαρμογή των ρυθμίσεων.




Εικόνα 57 – MS ISA Server 2004: Ενημερωτικό μήνυμα

- Από τη δενδρική δομή του αριστερού παραθύρου επιλέγεται 'firewall policy' και από το δεξί τμήμα 'create new access rule'.

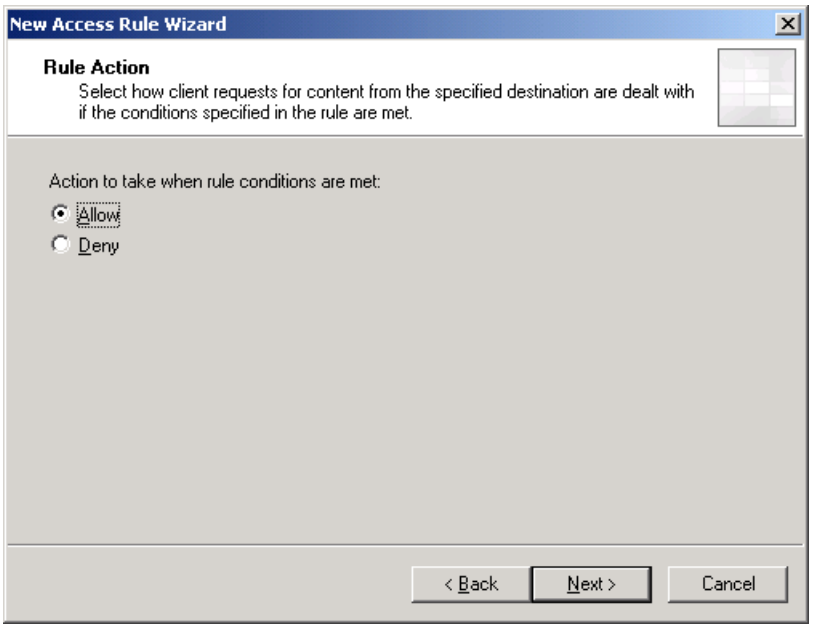



Εικόνα 58 – MS ISA Server 2004: Ρύθμιση firewall

- Ξεκινά νέος οδηγός ρύθμισης του ISA Server. Δίνεται ως όνομα 'Allow All (Disable any firewall options) προκειμένου να είναι σαφής η λειτουργία του κανόνα.

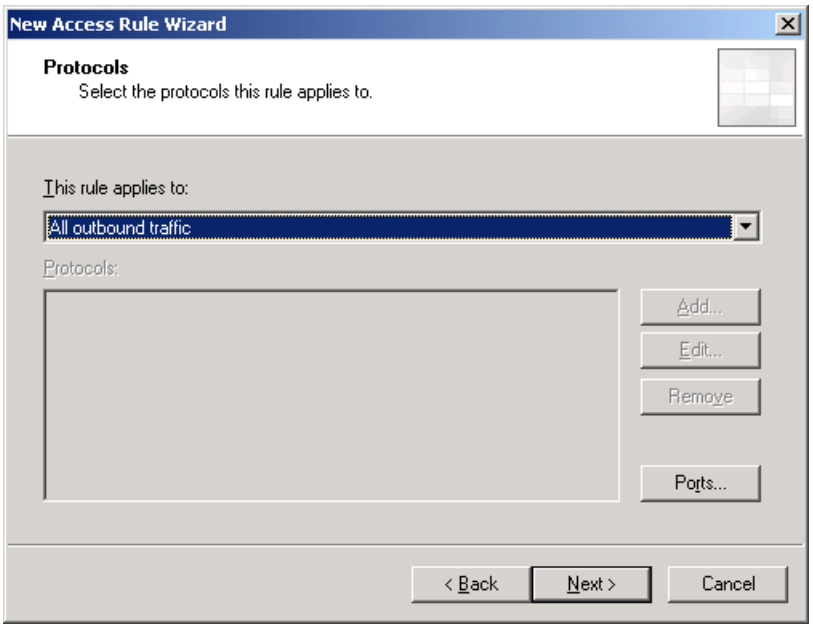

Εικόνα 59 – MS ISA Server 2004: Εκκίνηση οδηγού ρύθμισης

- Επιλέγεται η εφαρμογή του κανόνα όταν έχει ισχύ η συνθήκη που θα οριστεί ('allow').



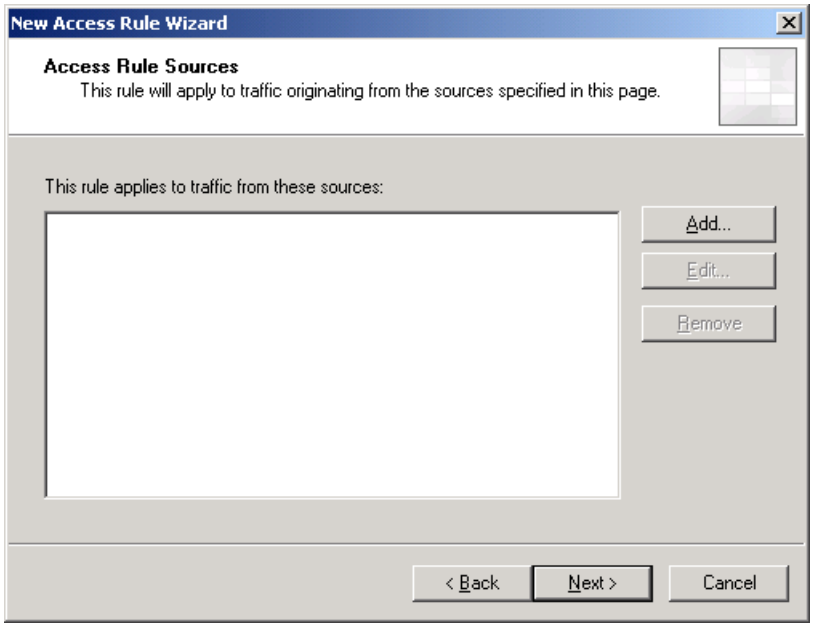

Εικόνα 60 – MS ISA Server 2004: Ορισμός τύπου κανόνα

- Ο κανόνας αφορά όλη την εξερχόμενη κυκλοφορία ('all outbound traffic').



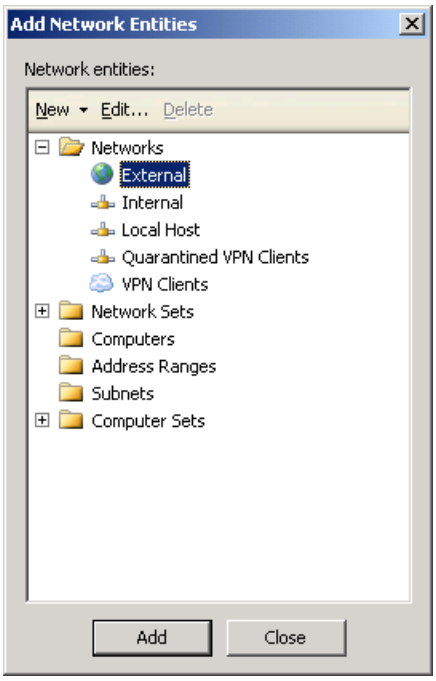

Εικόνα 61 – MS ISA Server 2004: Ρύθμιση κανόνα (outbound traffic)

- Με το πλήκτρο 'add' γίνεται προσθήκη πηγών.



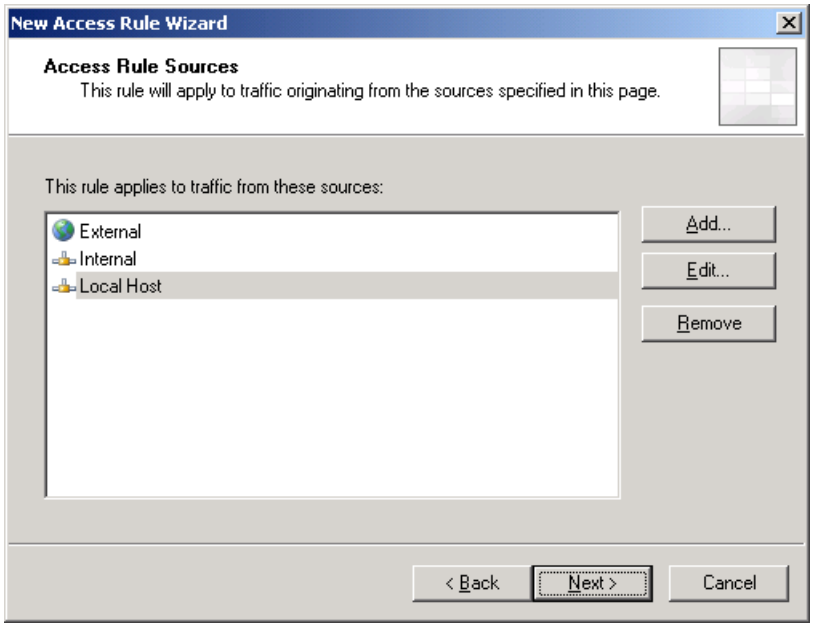

Εικόνα 62 – MS ISA Server 2004: Ρύθμιση κανόνα (sources)

- Γίνεται προσθήκη των πηγών 'local host', 'internal' & external' που βρίσκονται στο φάκελο 'networks'.



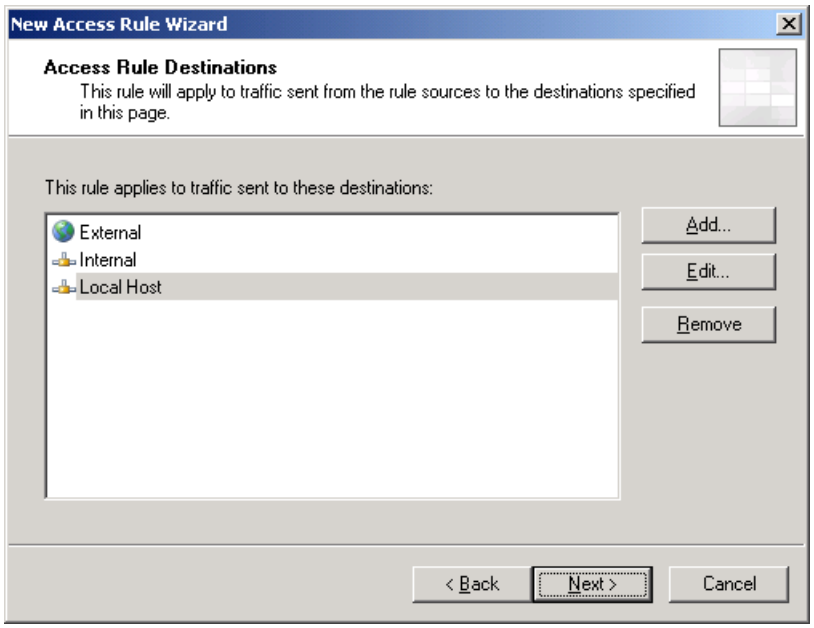

Εικόνα 63 – MS ISA Server 2004: Ρύθμιση κανόνα (sources)

- Ελέγχεται αν επιλέχθηκαν ορθά οι πηγές.



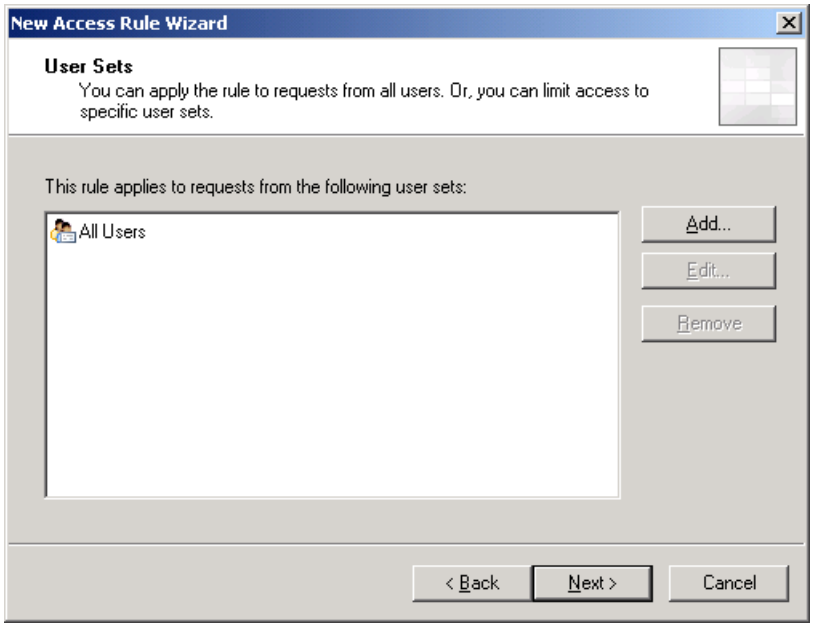

Εικόνα 64 – MS ISA Server 2004: Ρύθμιση κανόνα (sources)

- Με τον ίδιο τρόπο επιλέγονται οι ίδιοι προορισμοί.




Εικόνα 65 – MS ISA Server 2004: Ρύθμιση κανόνα (destinations)

- Γίνεται αποδεκτή το προεπιλεγμένο user set 'all users'.

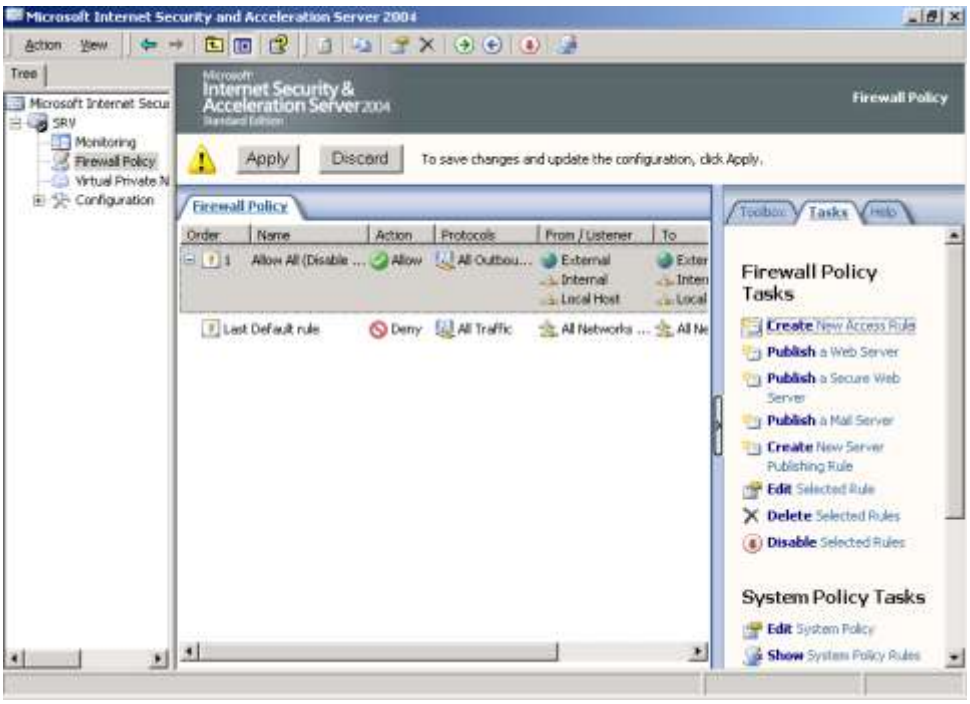



Εικόνα 66 – MS ISA Server 2004: Ρύθμιση κανόνα (user sets)

- Ολοκληρώνεται ο οδηγός ρύθμισης του ISA Server 2004.

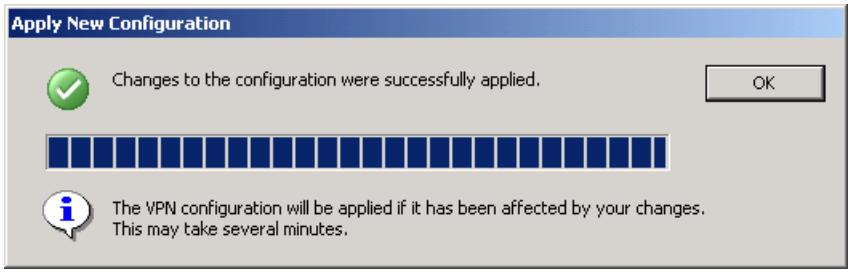

Εικόνα 67 – MS ISA Server 2004: Ολοκλήρωση οδηγού ρύθμισης

- Γίνεται αποθήκευση και εφαρμογή των ρυθμίσεων που επιλέχθηκαν (πλήκτρο 'apply').




Εικόνα 68 – MS ISA Server 2004: Εφαρμογή ρυθμίσεων

- Εμφανίζεται μήνυμα σχετικά με την επιτυχή εφαρμογή των ρυθμίσεων.




Εικόνα 69 – MS ISA Server 2004: Ενημερωτικό μήνυμα

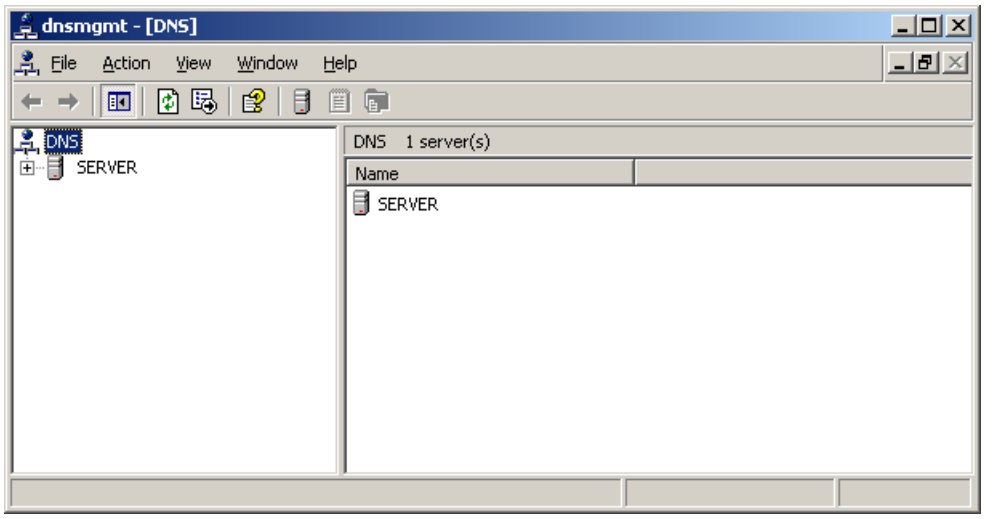
## 6.3 Αυτοματοποιημένη ρύθμιση σταθμών εργασίας

Όπως και στην προηγούμενη έκδοση του ISA Server μπορούν να γίνουν ρυθμίσεις ώστε:

1. Να είναι δυνατή η αυτόματη ρύθμιση του Internet Explorer των σταθμών εργασίας ώστε να χρησιμοποιούν τον ISA Server.
2. Να είναι δυνατή η απευθείας σύνδεση των σταθμών εργασίας με το διαδίκτυο σε περιπτώσεις που δεν παρέχεται η συγκεκριμένη υπηρεσία (π.χ. καταστροφή του εξυπηρετητή).

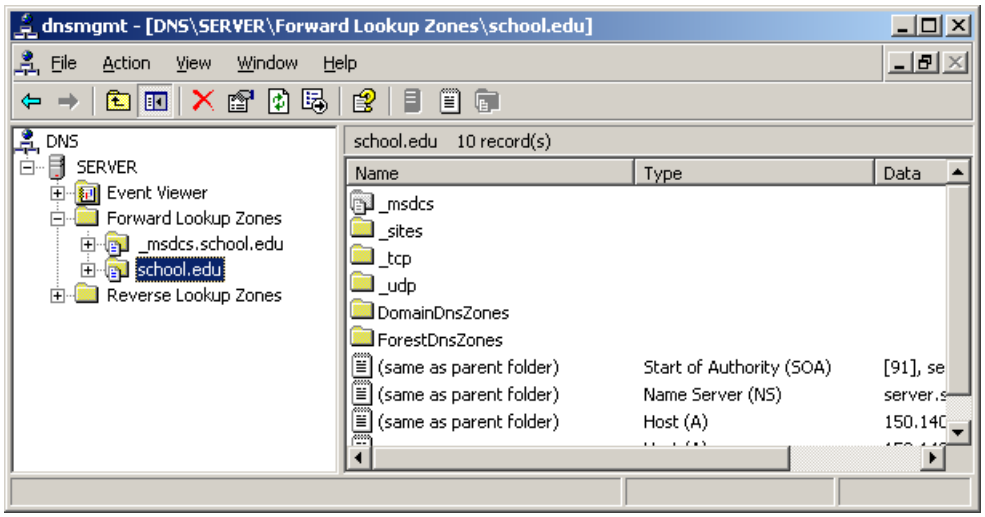
Οι ζητούμενες ρυθμίσεις μπορούν να ενεργοποιηθούν με χρήση του Web Proxy Autodiscovery Protocol (WPAD) και ρύθμιση της υπάρχουσας υπηρεσίας DNS ως ακολούθως:

- Γίνεται εκκίνηση της κονσόλας διαχείρισης της υπηρεσίας DNS (Start → Programs → Administrative tools → DNS).



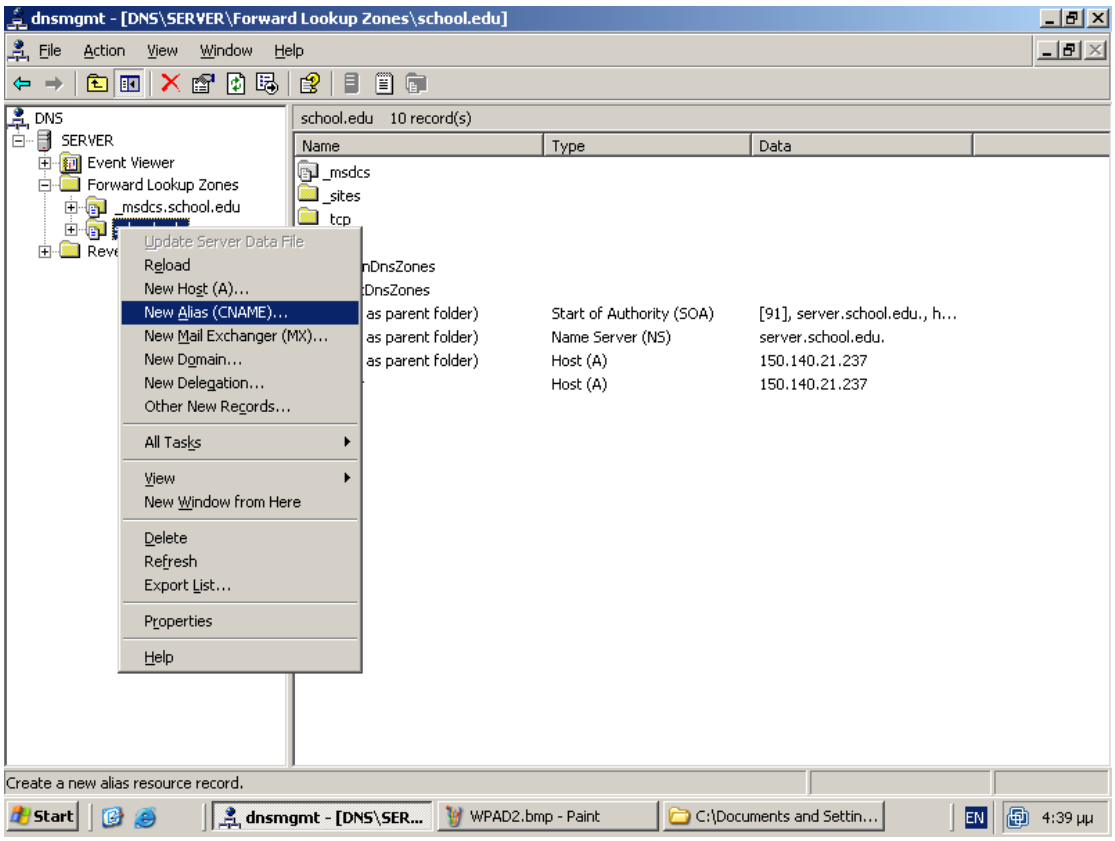

Εικόνα 70 – MS ISA Server 2000: Ρύθμιση υπηρεσίας DNS

- Επιλέγεται η forward lookup zone στην οποία είναι επιθυμητή η αυτόματη ρύθμιση της υπηρεσίας proxy.



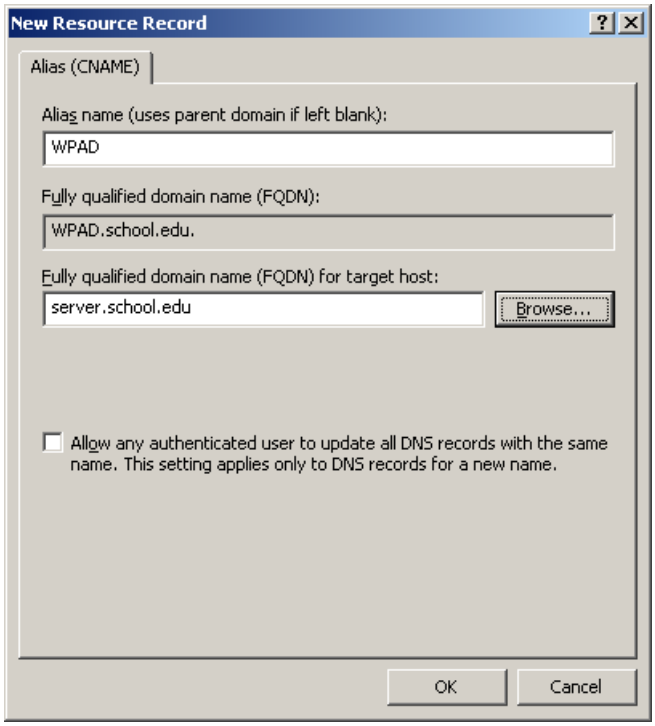

Εικόνα 71 – MS ISA Server 2000: Ρύθμιση υπηρεσίας DNS

- Δημιουργείται νέο Alias (New Alias [CNAME]).




Εικόνα 72 – MS ISA Server 2000: Ρύθμιση υπηρεσίας DNS

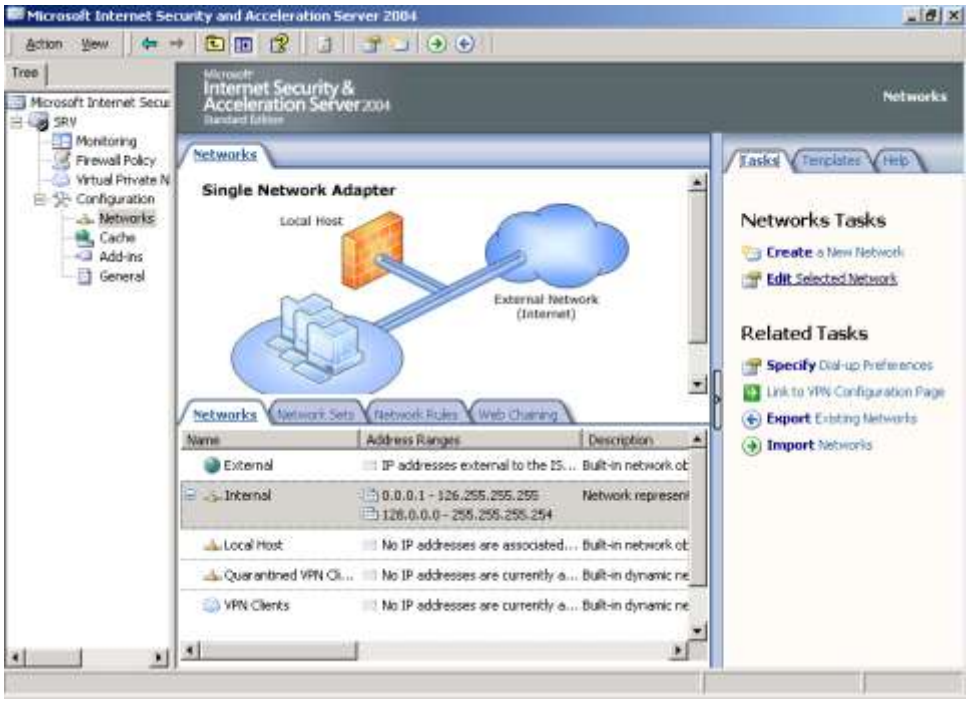
- Ορίζονται το όνομα του alias και το πλήρες όνομα του εξυπηρετητή.



Εικόνα 73 – MS ISA Server 2000: Ρύθμιση υπηρεσίας DNS

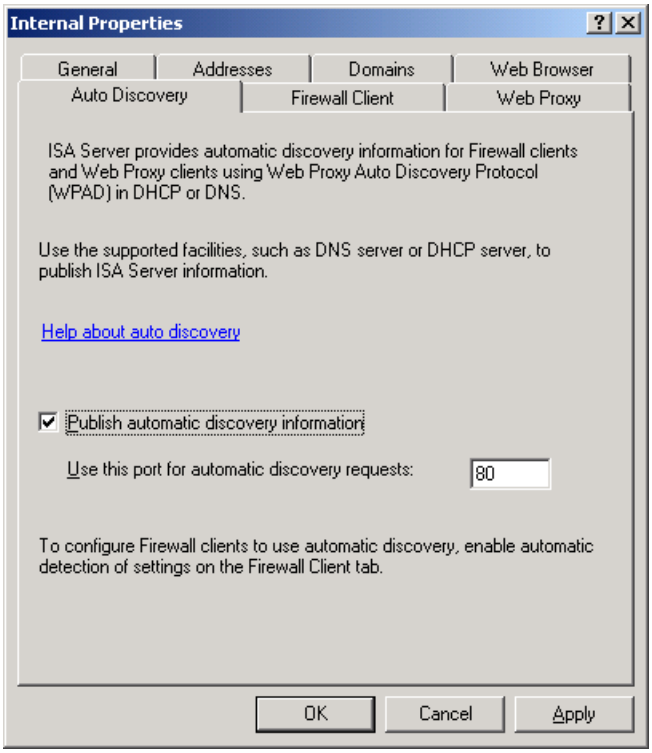
Στη συνέχεια από το εργαλείο ISA Management εφαρμόζονται οι ακόλουθες οδηγίες:

- Από τη δενδρική δομή επιλέγονται οι δικτυακές ρυθμίσεις (configuration – network) και για το εσωτερικό υποδίκτυο (internal) επιλέγεται 'edit selected network'.




Εικόνα 74 – MS ISA Server 2004: Ρύθμιση ιδιοτήτων εσωτερικού υποδικτύου

- Ενεργοποιείται η χρήση του WPAD πρωτοκόλλου στη συνήθη θύρα 80 για το εσωτερικό υποδίκτυο.




Εικόνα 75 – MS ISA Server 2004: Ρύθμιση WPAD

Στους σταθμούς εργασίας που χρησιμοποιούν το Firefox ως εφαρμογή πλοήγησης στο Διαδίκτυο πρέπει στα «Εργαλεία/Επιλογές/Για προχωρημένους/Δίκτυο/Σύνδεση/Ρυθμίσεις» να ενεργοποιηθεί η επιλογή «Αυτόματος εντοπισμός ρυθμίσεων διαμεσολαβητή για αυτό το δίκτυο» και να γίνει επανεκκίνηση του Firefox.