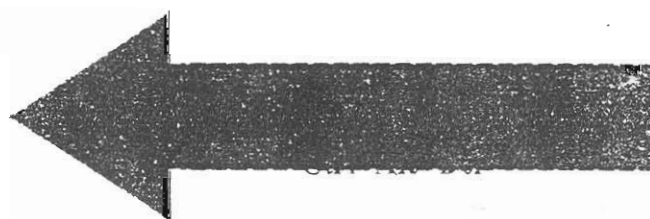
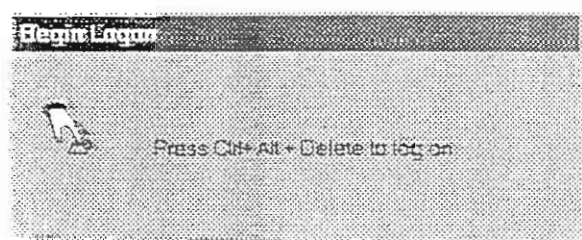
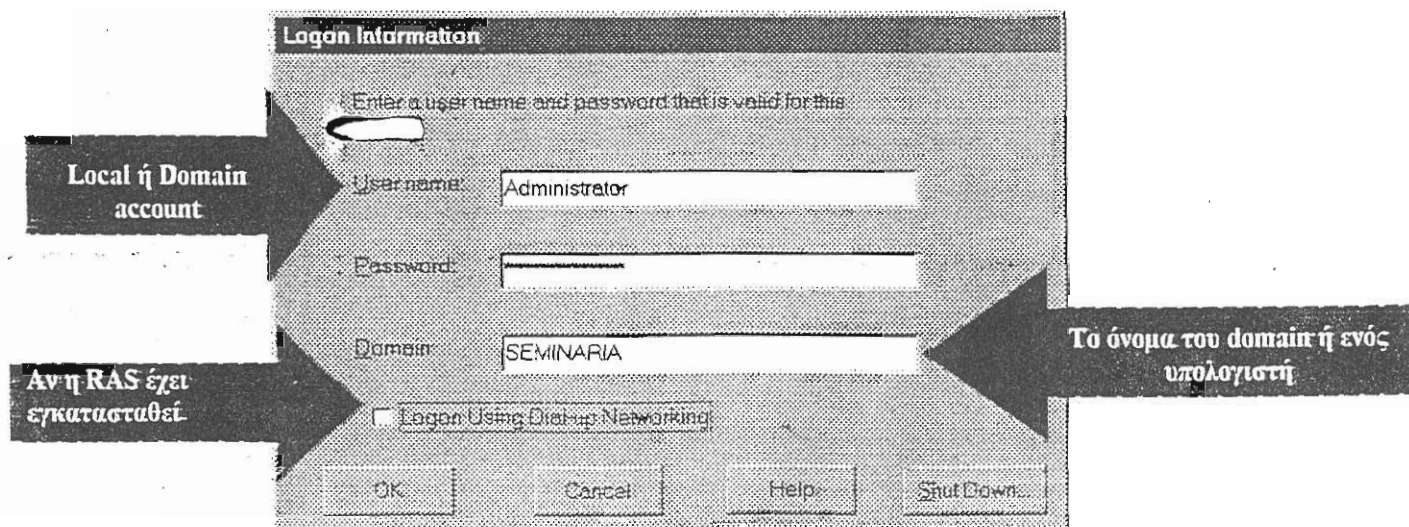


A.2 ΚΑΝΟΝΤΑΣ LOGIN ΣΕ ΕΝΑΝ ΥΠΟΛΟΓΙΣΤΗ Η DOMAIN

Κάθε φορά που εκκινούμε τον υπολογιστή μας (θεωρώντας ότι αυτός είναι μέλος ενός network domain), το σύστημα μας εμφανίζει ένα μήνυμα με το οποίο μας προτρέπεται να πατήσουμε Ctrl+Alt+Delete για να κάνουμε login. Πατώντας αυτή την ακολουθία πληκτρών εμφανίζεται στην οθόνη το Login Information Box στο οποίο πρέπει εμείς να εισάγουμε τις απαραίτητες πληροφορίες έτσι ώστε να μας επιτραπεί η πρόσβαση στο σύστημα. Πιο συγκεκριμένα:



Μεταβαίνουμε
εδώ



Στον παρακάτω πίνακα περιγράφονται οι επιλογές του πλαισίου διαλόγου

Επιλογή	Περιγραφή επιλογής
User Name	Εδώ πρέπει να εισάγετε το όνομα χρήστη που σας έχει ανατεθεί από το διαχειριστή του συστήματος (System Administrator). Το όνομα χρήστη είναι μοναδικό και δεν μπορούν να έχουν δύο χρήστες το ίδιο. Μπορεί να είναι οποιοδήποτε όνομα που να σας αρέσει και δεν αναγκαστικά το όνομά σας.
Password	Σε αυτό το πεδίο θα πρέπει να δώσετε την κωδική σας λέξη. Προσοχή όμως: η μορφή με την οποία θα δώσετε την κωδική λέξη έχει σημασία. Δηλαδή, τα κεφαλαία με τα μικρά γράμματα στο password (κωδική λέξη) διαφέρουν μεταξύ τους και δε θεωρούνται ίδια. Για παράδειγμα, οι κωδικές λέξεις User01 και useR01 δεν είναι ίδιες. Εσείς θα πρέπει να εισάγετε τον κωδικό σας όπως ακριβώς έχει αυτή οριστεί.
Domain	Εδώ εισάγουμε είτε το όνομα του domain στο οποίο θέλουμε να κάνουμε login, είτε το όνομα του υπολογιστή. Στην πρώτη περίπτωση, όταν εισάγουμε το username & password, ελέγχεται η βάση δεδομένων ασφαλείας του Primary domain controller έτσι ώστε να ελεγχθεί η εγκυρότητα των στοιχείων σας. Στη δεύτερη περίπτωση ελέγχεται η τοπική βάση ασφαλείας του υπολογιστή στον οποίο κάνετε login.
Logon Using Dial-up Networking	Στην περίπτωση όπου έχει εγκατασταθεί η Remote Access Service (RAS), μας επιτρέπεται να κάνουμε login σε ένα απομακρυσμένο δίκτυο με τη χρήση της RAS.
Shut Down	Κλείνει όλα τα αρχεία, αποθηκεύει τυχόν πληροφορίες του λειτουργικού συστήματος και τέλος προετοιμάζει τον υπολογιστή ώστε να μπορέσει να τερματιστεί η λειτουργία του με ασφάλεια. Στα Windows NT Server, το πλήκτρο αυτό είναι απενεργοποιημένο, για να αποτρέψει κάποιον μη εξουσιοδοτημένο χρήστη να κλείσει τον server.

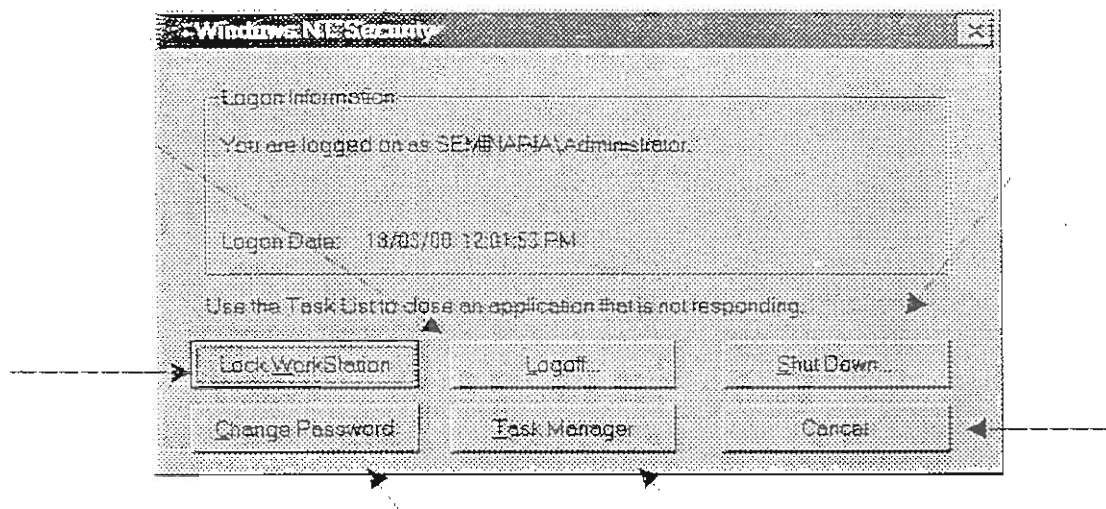
A.3 TO SECURITY DIALOG BOX ΤΩΝ WINDOWS NT

Με το πάτημα των πλήκτρων Alt+Ctrl+Del από τη στιγμή που έχουμε κάνει login στο σύστημα μας εμφανίζεται στην οθόνη το Windows NT Security Dialog box, με το οποίο μπορούμε να επιτελέσουμε τις παρακάτω λειτουργίες



Με το πλήκτρο αυτό μπορούμε να κάνουμε log-off από το σύστημα

Με το πλήκτρο αυτό μπορούμε να τερματίσουμε τη λειτουργία του υπολογιστή



Με το πλήκτρο αυτό κλειδώνουμε το σταθμό

Με τη λειτουργία αυτή, αλλάζουμε τον κωδικό ασφαλείας μας

Από εδώ μπορούμε να εκκινήσουμε τον Task manager

Κλείνουμε το πλαίσιο διαλόγου

<u>Επιλογή</u>	<u>Λειτουργία που επιτελείται</u>
Lock workstation	Ασφαλίζει τον υπολογιστή από μη εξουσιοδοτημένη χρήση, χωρίς να είναι απαραίτητο να κάνουμε log-off. Όλες οι εφαρμογές που βρίσκονται σε λειτουργία συνεχίζουν να εκτελούνται. Ένας κλειδωμένος σταθμός εργασίας, μπορεί να ξεκλειδωθεί μόνο από το χρήστη εκείνο που τον κλειδωσε ή από κάποιον διαχειριστή δικτύου (system administrator). Αν η λειτουργία του ξεκλειδώματος γίνει από έναν διαχειριστή δικτύου, τότε το μόνο που μπορεί να κάνει ο διαχειριστής είναι log-off.
Change Password	Επιτρέπει στο χρήστη να αλλάξει τον κωδικό πρόσβασης του. Βασική προϋπόθεση για την επιτυχή αλλαγή του κωδικού ασφαλείας, είναι ο χρήστης να γνωρίζει τον παλιό κωδικό. Αυτό γίνεται για να αποτρεπεί άλλους χρήστες να αλλάζουν το password ενός άλλου χρήστη.
Logoff	Κάνει log-off στον χρήστη, αφήνοντας όλες τις υπηρεσίες να συνεχίζουν να τρέχουν κανονικά. Συνιστάται να κάνετε πάντα log-off όταν δε χρειάζεστε άλλο τον υπολογιστή.
Task Manager	Εμφανίζει μια λίστα με τις διεργασίες και τα προγράμματα που τρέχουν εκείνη τη στιγμή. Ο Task manager χρησιμοποιείται για να εναλλασσόμαστε μεταξύ εφαρμογών και για να τερματίσουμε «με το χέρι» κάποια εφαρμογή που δεν αποκρίνεται.
Shut Down	Κλείνει όλα τα ανοικτά αρχεία, τερματίζει όλες τις εφαρμογές, και τερματίζει τη λειτουργία του υπολογιστή.
Cancel	Κλείνει το πλαίσιο διαλόγου NT security dialog box.

B. ΛΟΓΑΡΙΑΣΜΟΙ ΧΡΗΣΤΩΝ (USER ACCOUNTS)

Στο τμήμα αυτό θα μελετήσουμε θέματα σχετικά με τη διαχείριση των χρηστών του δικτύου μας. Μεταξύ άλλων, θα αναφερθούμε στον τρόπο με τον οποίο μπορούμε να δημιουργήσουμε και να διαγράψουμε έναν χρήστη, πώς να του αναθέσουμε περισσότερες ή λιγότερες άδειες χρήσης, για τον τρόπο εκείνο με τον οποίο μπορούμε να διαχειριστούμε το περιβάλλον εργασίας του χρήστη (User Work environment), ή το User-Profile όπως άλλως λέγεται κ.α.

B.1 ΕΙΣΑΓΩΓΙΚΑ

Τί είναι ένα User Account:

Ένα user-account, ή ένας λογαριασμός χρήστη είναι τα χαρακτηριστικά που έχει ένας χρήστης σε ένα δικτυακό σύστημα και τα οποία είναι μοναδικά. Με ένα user-account, δίνεται η δυνατότητα σε έναν χρήστη να κάνει login είτε σε ένα domain και να προσπελάσει τους δικτυακούς πόρους (network – resources), είτε σε έναν υπολογιστή (ο οποίος τρέχει NT server, ή Workstation) και να προσπελάσει πόρους που βρίσκονται συνδεδεμένοι επάνω στον υπολογιστή και μόνο (τοπικούς πόρους – local resources). Ως πόρους (resources), εννοούμε οτιδήποτε μπορεί να χρησιμοποιηθεί από έναν χρήστη που κάθεται σε ένα υπολογιστικό σύστημα όπως π.χ. ο εκτυπωτής, ο σκληρός δίσκος, η μονάδα δισκέτας, ένας σαρωτής (scanner), ακόμη και προγράμματα. Το κάθε άτομο που κάνει χρήση του δικτύου, θα πρέπει να έχει ένα λογαριασμό. Η χρήση και ο λόγος ύπαρξης των λογαριασμών χρηστών έγκειται στο γεγονός, του να υπάρχει έλεγχος σχετικά με το ποιος και το πόσο χρησιμοποιεί το δίκτυο. Για παράδειγμα ο διαχειριστής του δικτύου, μπορεί να περιορίσει το χρόνο που κάποιος χρήστης θα επιτρέπεται να είναι logged-on.

Τύποι Λογαριασμών χρηστών

Υπάρχουν δύο γενικές κατηγορίες λογαριασμών, όπου η κάθε μία χωρίζεται σε υποκατηγορίες: λογαριασμοί που δημιουργούνται από το διαχειριστή του δικτύου και λογαριασμοί built-in.

Λογαριασμός	Περιγραφή
Λογαριασμοί δημιουργούμενοι από το διαχειριστή	Τέτοιου είδους λογαριασμοί, δίνουν τη δυνατότητα σε ένα χρήστη να μπορεί να έχει πρόσβαση σε ένα δικτυακό σύστημα και να μπορεί να προσπελάσει δικτυακούς πόρους. Δημιουργούνται από ένα διαχειριστή δικτύου και περιέχουν πληροφορίες σχετικά με το χρήστη, όπως π.χ. το όνομα του και τον κωδικό ασφαλείας του.
Guest Account	Ο λογαριασμός αυτός είναι built-in και υπάρχει σε κάθε σύστημα NT. Έχει περιορισμένες δυνατότητες και δίνει τη δυνατότητα πρόσβασης στο σύστημα σε περιστασιακούς χρήστες, έτσι ώστε αυτοί να μπορούν να περιηγηθούν, προσπελώνοντας πόρους που βρίσκονται στον τοπικό υπολογιστή. Για παράδειγμα, αν ένας υπάλληλος χρειάζεται να έχει πρόσβαση σε έναν υπολογιστή για λίγο, ώρα, μπορεί να χρησιμοποιήσει το λογαριασμό guest. Ο guest account είναι εξ' ορισμού απενεργοποιημένος.
Administrator	Ο built-in administrator account (User name administrator), χρησιμοποιείται για να μπορούμε να διαχειριστούμε καθολικά τις ρυθμίσεις του υπολογιστή και του όλου δικτύου. Ο λογαριασμός αυτός χρησιμοποιείται για να επιτελούνται πολλών ειδών εργασίες, όπως για παράδειγμα η δημιουργία και η αφαίρεση χρηστών από το σύστημα ή διαχείριση πολιτικών ασφαλείας, κλπ.

Συνοπτικά, ένας *built-in account* προϋπάρχει στο σύστημα από τη στιγμή της εγκατάστασης των Windows NT server και μετά, ενώ ένας λογαριασμός που δημιουργείται από το διαχειριστή του δικτύου, δεν υπάρχει από πριν στο σύστημα.

Βασικές Έννοιες

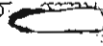
Στο τμήμα αυτό θα εξηγήσουμε μερικούς όρους που χρησιμοποιούνται στη δικτύωση των υπολογιστών με NT. Καταρχήν, υπάρχουν δύο τρόποι για να εγκαταστήσουμε ένα δίκτυο:

Peer-to-Peer:

Στην περίπτωση αυτή οι υπολογιστές είναι συνδεδεμένοι ο ένας με τον άλλο, χωρίς να υπάρχει κάποιος κεντρικός υπολογιστής που να ελέγχει κωδικούς ασφαλείας (περίπτωση DOMAIN Controller – βλέπε παρακάτω). Οι κωδικοί ασφαλείας των χρηστών ελέγχονται από τον κάθε υπολογιστή χωριστά.

Domain:

Ένα Domain αποτελείται από ένα σύνολο υπολογιστών, οι οποίοι θεωρούνται ως ομάδα στην οποία έχει ανατεθεί ένα όνομα. Για παράδειγμα, το microsoft.com είναι το όνομα του domain της Microsoft, στο Internet. Ένα domain, στη συνέχεια, μπορεί να αποτελεί από μόνο του μια ομάδα εργασίας (*Workgroup* – βλέπε παρακάτω) ή να περιέχει περισσότερα από ένα workgroups τα οποία λέμε ότι ανήκουν στο Domain.

Οι υπολογιστές που είναι μέρος του δικτύου, ανήκουν όλοι σε κάποιο Domain, το οποίο μπορεί να έχει ένα οποιοδήποτε όνομα, π.χ. SEMINARIADOMAIN κλπ. Σε αυτή τη μορφή δικτύωσης, ένας από τους υπολογιστές του δικτύου επιτελεί ρόλο *ελεγκτή*, ελέγχοντας τους κωδικούς όλων των χρηστών του δικτύου. Ο υπολογιστής αυτός ονομάζεται *Primary Domain Controller (PDC)*. Όταν κάποιος χρήστης κάνει login στο δίκτυο, τότε το όνομα-χρήστη και ο κωδικός ασφαλείας που δίνει θα πρέπει να βρίσκονται αποθηκευμένα στη *βάση δεδομένων ασφαλείας (security database)*, του PDC, έτσι ώστε να μπορεί να ελεγχθεί η εγκυρότητά τους. Για να αποτελούν μέρος της security database, βέβαια, θα πρέπει προηγουμένως ο διαχειριστής του δικτύου να έχει δημιουργήσει μία αντίστοιχη καταχώρησ  security database του PDC. Θα πρέπει, δηλαδή, να έχει δημιουργηθεί ένας *λογαριασμός χρήστη (user account)* από τον διαχειριστή του δικτύου, ώστε ο πρώτος να μπορεί να κάνει login στο δίκτυο.

Ο PDC πρέπει να έχει Windows NT, ενώ οι υπόλοιποι υπολογιστές του δικτύου, μπορούν να τρέχουν Windows 9x, Windows NT Server, Windows NT Workstation,

UNIX (συνοδευόμενο πάντα από τους κατάλληλους προσομοιωτές συστημάτων αρχείων). Σε ένα domain, μπορεί να υπάρχει μόνο ένας PDC.

Ταυτόχρονα με τον primary controller, είναι δυνατό να υπάρχουν και ένας ή περισσότεροι ακόμη *backup domain controllers*, (BDCs). Οι τελευταίοι επικοινωνούν σε τακτά χρονικά διαστήματα με τον PDC και *αντιγράφουν τη βάση δεδομένων ασφαλείας (security database)*, έτσι ώστε να υπάρχουν περισσότερα από ένα αντίγραφα της στο δίκτυο. Εδώ θα πρέπει να σημειωθεί ότι οι BDCs δεν μπορούν να κάνουν έλεγχο των κωδικών ασφαλείας των χρηστών. Το μόνο πράγμα για το οποίο είναι υπεύθυνοι είναι να κρατούν αντίγραφο ασφαλείας της βάσης σε περίπτωση που ο PDC τεθεί εκτός λειτουργίας.

Στην τελευταία περίπτωση, θα πρέπει ένας από τους διαθέσιμους BDCs να προαχθεί σε primary domain controller, θέτοντας αυτοματα τον προηγούμενο PDC να εκτελεί ρόλο BDC. Η προαγωγή γίνεται πάντα από το διαχειριστή του δικτύου. Αν από την άλλη, ο PDC τεθεί εκτός λειτουργίας και δεν υπάρχει διαθέσιμος backup domain controller, οι χρήστες μπορούν πάλι να κάνουν login στο δίκτυο, αλλά δεν μπορούν να επιτελεστούν διαχειριστικές λειτουργίες (ούτε και από τον διαχειριστή), μέχρις ότου επανέλθει σε λειτουργία ο Domain Controller.

ΣΗΜΕΙΩΣΗ: Για να μπορεί ένας υπολογιστής να εκτελεί ρόλο *Domain Controller*, είτε *Primary*, είτε *Backup*, θα πρέπει να εκτελεί είτε *Windows NT Server*, είτε *Windows NT Workstation*.

Workgroup:

Ένα workgroup γενικά αποτελείται από τους υπολογιστές εκείνους, οι οποίοι είναι περισσότερο πιθανό ότι θα επικοινωνούν μεταξύ τους και είναι αυτοί που περιέχουν τους περισσότερους δικτυακούς πόρους, όπως εκτυπωτές, αρχεία, κλπ. Ένα workgroup, θα μπορούσαμε να πούμε ότι είναι μια γενικότερη μορφή αναφοράς σε ένα σύνολο δικτυωμένων υπολογιστών. Αντίθετα, ο όρος *Domain*, χρησιμοποιείται περισσότερο για να περιγράψει ένα σύνολο υπολογιστικών οντοτήτων, οι οποίες έχουν δικτυωθεί σε μια ομάδα, στην οποία έχει ανατεθεί κάποιο όνομα και στην οποία γίνεται έλεγχος των κωδικών ασφαλείας και των ονομάτων των χρηστών. Ένα Domain, επομένως, είναι εύκολο να καταλάβετε ότι αποτελεί από μόνο του και ένα Workgroup.

Στην περίπτωση που έχουμε δικτύωση peer-to-peer, όλοι οι υπολογιστές ανήκουν στο ίδιο workgroup και ο έλεγχος των κωδικών γίνεται από τον κάθε υπολογιστή χωριστά και όχι από κάποιο domain controller.

B.2 ΣΧΕΤΙΚΑ ΜΕ ΛΟΓΑΡΙΑΣΜΟΥΣ ΧΡΗΣΤΩΝ

Στο τμήμα αυτό θα αναφερθούμε στη σειρά εκείνη των διαδικασιών που είναι απαραίτητες για τη δημιουργία λογαριασμών χρηστών σε ένα domain. Καταρχήν, οι μόνοι που έχουν άδεια να δημιουργούν νέους λογαριασμούς χρηστών είναι οι διαχειριστές του δικτύου (*System Administrators*) καθώς και οι διαχειριστές λογαριασμών των χρηστών (*Account Operators*). Οι μεν πρώτοι έχουν την ιδιότητα να επεμβαίνουν στις ιδιότητες του κάθε χρήστη στο σύστημα (ακύρωση και στους λογαριασμούς των άλλων διαχειριστών), οι δε διαχειριστές λογαριασμών μπορούν να επεμβαίνουν (και να δημιουργούν), μόνο σε λογαριασμούς χρηστών. Δε μπορούν, δηλαδή, να σβήσουν, να αλλάξουν τις ιδιότητες ή και να δημιουργήσουν νέους λογαριασμούς διαχειριστών του συστήματος (*administrative accounts*).

Που Δημιουργούνται

Οι λογαριασμοί των χρηστών ενός Domain όταν δημιουργούνται αποθηκεύονται στην master directory database του PDC και στη συνέχεια ένα αντίγραφο της βάσης αποθηκεύεται στον κάθε BDC. Από τη στιγμή που έχει δημιουργηθεί ένας λογαριασμός χρήστη στον PDC ο χρήστης αυτός μπορεί να κάνει κανονικά login στο δίκτυο.

ΣΗΜΕΙΩΣΗ: Μερικές φορές, μπορεί να περάσει λίγος χρόνος προτού ενημερωθούν οι BDCs με τις αλλαγές που έγιναν στη βάση. Σε αυτό το χρονικό διάστημα, είναι πιθανό μερικοί νέοι χρήστες να μη μπορούν να κάνουν login από οποιονδήποτε σταθμό του δικτύου. Παρόλα αυτά ο διαχειριστής του δικτύου μπορεί να επιβάλλει την ενημέρωση της βάσης σε όλους τους BDCs (να κάνει το λεγόμενο *συγχρονισμό – synchronization*) παρακάμπτοντας την αυτόματη λειτουργία. Αυτό μπορεί να επιτευχθεί μέσω του Server Manager, ή μέσω της γραμμής εντολών πληκτρολογώντας την εντολή `net accounts /sync`.

Είδη Λογαριασμών

Domain User Accounts

Ένα Domain User Account δημιουργείται με τη βοήθεια του User Manager for Domains. Όταν δημιουργούμε ένα λογαριασμό χρήστη σε ένα Domain, τότε ο χρήστης αυτός μπορεί να κάνει login στο δίκτυο από οποιονδήποτε υπολογιστή που ανήκει στο ίδιο Domain, μιας και θα διαθέτει λογαριασμό *εμβέλειας Domain*. Τα επιμέρους στοιχεία του Domain user account (π.χ. User-name, password, directory permissions, κλπ) αποθηκεύονται στην κύρια βάση δεδομένων του PDC (master security database). Ένα αντίγραφο της βάσης αυτής αποθηκεύεται στη συνέχεια σε όλους τους Backup Domain Controllers.

Local User Account


Αντίθετα από την παραπάνω περίπτωση, ένα Local User account, αφορά *μόνο τον υπολογιστή στον οποίο δημιουργήθηκε*. Ένας χρήστης που διαθέτει ένα τέτοιου τύπου λογαριασμό, μπορεί να κάνει login μόνο στον υπολογιστή, στον οποίου την τοπική βάση ασφαλείας βρίσκονται αποθηκευμένα τα επί μέρους στοιχεία του λογαριασμού του (username, password, directory permissions, κλπ). Στην περίπτωση που ο συγκεκριμένος υπολογιστής ανήκει σε κάποιο domain και ένας χρήστης έχει κάνει login με τον *τοπικό του λογαριασμό* στον υπολογιστή αυτόν, τότε μπορεί να δει τους υπόλοιπους υπολογιστές του δικτύου, αλλά για να συνδεθεί σε κάποιον από αυτούς μέσω του Network neighborhood, θα πρέπει πρώτα να δώσει ένα username και password που να ανήκουν στο Domain. Αν δε διαθέτει ένα domain user account, τότε μπορεί να προσπελάσει τους πόρους του συγκεκριμένου υπολογιστή.

ΣΧΕΔΙΑΖΟΝΤΑΣ ΛΟΓΑΡΙΑΣΜΟΥΣ ΧΡΗΣΤΩΝ

Είναι γενικά καλό να υπάρχει κάποια στοιχειώδης οργάνωση και μελέτη προτού δημιουργήσουμε νέους λογαριασμούς χρηστών στο δίκτυό μας. Για να μπορέσουμε να οργανώσουμε τη διαδικασία αυτή θα πρέπει να καθοριστεί:

- Ένα σύνολο κανόνων σχετικό με την ονοματολογία των usernames των χρηστών. Τα ονόματα των χρηστών στο δίκτυο, θα πρέπει να είναι μοναδικά, έτσι ώστε να μην έχουν δύο χρήστες το ίδιο username, και επίσης θα πρέπει να είναι εύκολο για τους χρήστες να μπορούν να το θυμηθούν.
- Αν ο κωδικός ασφαλείας θα καθορίζεται από το διαχειριστή μια και εξω, ή οι χρήστες θα έχουν τη δυνατότητα να τον αλλάζουν.
- Οι ώρες κατά τις οποίες θα μπορούν οι χρήστες να χρησιμοποιούν το δίκτυο. Για παράδειγμα είναι δυνατόν να ορίσετε ότι οι απλοί χρήστες δε θα μπορούν να χρησιμοποιούν το δίκτυο στις βραδινές ώρες.
- Οι υπολογιστές (Workstations) από τους οποίους θα μπορούν οι χρήστες να προσπελάσουν το δίκτυο, έτσι ώστε να μπορείτε να ελέγχετε ποιοι υπολογιστές έχουν πρόσβαση στους δικτυακούς πόρους.
- Το αν τα home directories, θα βρίσκονται στον local Workstation, ή σε κάποιον server, έτσι ώστε να υπάρχει ένας κεντρικοποιημένος έλεγχος και διαχείρισή τους.

ΟΝΟΜΑΤΟΛΟΓΙΑ

Οι κανόνες που θέτουμε στα ονόματα των χρηστών του δικτύου μας, καθορίζει το πως οι χρήστες αυτοί θα αναγνωρίζονται στο δίκτυο. Ένα συνεπές σύνολο κανόνων, βοηθά πάντοτε και στην εύκολη απομνημόνευση των ονομάτων αλλά και στην εύκολη  γρήση και εύρεση αυτών σε λίστες.

Προκειμένου, βέβαια, να μπορέσετε να καθορίσετε τους κανόνες της ονοματολογίας των χρηστών θα πρέπει πρώτα να έχετε υπόψη σας τα παρακάτω:

- Τα ονόματα των χρηστών θα πρέπει να είναι μοναδικά. Τα Domain User Accounts, θα πρέπει να είναι μοναδικά στο Domain στο οποίο ανήκουν, ενώ τα Local User Accounts θα πρέπει να είναι μοναδικά στον υπολογιστή στον οποίο ανήκουν.

- Τα ονόματα των χρηστών μπορούν να αποτελούνται από το πολύ μέχρι 20 χαρακτήρες (κεφαλαία ή μικρά), εκτός από τους παρακάτω: «/ \ [] : ; | = , - * ? < > ». Μπορείτε να χρησιμοποιήσετε συνδυασμούς από γράμματα και αριθμούς, έτσι ώστε να βοηθήσετε τους χρήστες να θυμούνται τα ονόματά τους.
- Σε περίπτωση που ο αριθμός των χρηστών είναι μεγάλος, τότε είναι πολύ πιθανό να έχετε χρήστες με ίδια ονοματεπώνυμα. Μερικές συμβουλές, για να μπορέσετε να χειριστείτε τα διπλά ονόματα είναι οι εξής:
 - Θα μπορούσατε να χρησιμοποιήσετε το μικρό όνομα σε συνδυασμό με γράμματα από το επώνυμο του χρήστη για το username. Για παράδειγμα σε περίπτωση που έχετε δύο χρήστες με το ίδιο όνομα π.χ. Γεώργιος Κωνσταντίνου, θα μπορούσατε να ονομάσετε τον πρώτο χρήστη ως GeorgeK και το δεύτερο ως GeorgeKon.
 - Θα μπορούσατε επίσης, να αναθέσετε αριθμούς στα usernames. Για παράδειγμα στην παραπάνω περίπτωση θα μπορούσατε να δημιουργήσετε τα ακόλουθα usernames: GeorgeK1 και GeorgeK2.
- Τέλος, σε μεγάλες επιχειρήσεις, είναι καλό να μπορείτε να αναγνωρίζετε τους προσωρινούς χρήστες από τους μόνιμους. Μια καλή πρακτική γι' αυτό είναι να προσθέτετε ένα «T-» μπροστά από τα usernames των προσωρινών χρηστών. Για παράδειγμα αν ο Γεώργιος Κωνσταντίνου άνηκε στους εποχικούς υπαλλήλους της επιχείρησής μας, θα μπορούσαμε να τον ονομάσουμε T-GeorgeK.

Κωδικοί Ασφαλείας, Logon Hours, Logon Hours, Περιορισμοί Σταθμών εργασίας

Κωδικοί Ασφαλείας

Για να προστατευθεί η πρόσβαση σε ένα Domain ή σε ένα υπολογιστή, ο κάθε χρήστης θα πρέπει να έχει μαζί με το username του και ένα κωδικό ασφαλείας, ή αλλιώς password. Προτού αρχίσετε να αναθέτετε κωδικούς ασφαλείας στους χρήστες θα πρέπει να λάβετε υπόψη σας τα παρακάτω:

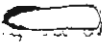
- Θα πρέπει πάντοτε να αναθέτετε ένα password στο λογαριασμό του Administrator, έτσι ώστε να αποτρέπεται μη-εξουσιοδοτημένους χρήστες από τη χρήση του.
- Θα πρέπει να καθορίσετε ποιος θα ελέγχει τον κωδικό. Μπορείτε να καθορίσετε ότι ο κάθε χρήστης θα έχει έναν κωδικό ασφαλείας, τον οποίο είτε δε θα μπορεί να αλλάξει, οπότε και θα καθορίζεται από το σύστημα (το διαχειριστή) το πότε θα αλλάξει, είτε θα μπορεί να τον ελέγχει πλήρως. Αυτό που συνηθίζεται είναι ο κάθε χρήστης να μπορεί να ελέγχει τον κωδικό του πλήρως.
- Θα πρέπει να καθορίσετε το αν κάποιος (κάποιοι) λογαριασμοί χρηστών θα έχουν ημερομηνία λήξεως. Τέτοιου είδους λογαριασμοί χρησιμοποιούνται σε περιπτώσεις, όπου έχουμε εποχιακούς υπαλλήλους, των οποίων τα accounts θα λήγουν με το τέλος του συμβολαίου τους.
- Τέλος θα πρέπει να «εκπαιδεύσετε» τους χρήστες σας σχετικά με τους τρόπους με τους οποίους μπορούν να καθορίζουν τους κωδικούς ασφαλείας τους:
 - Θα πρέπει να αποφεύγουν να χρησιμοποιούν στο password κωδικούς οι οποίοι να περιέχουν ονόματα από μέλη της οικογένειάς τους
 - Θα πρέπει να μάθουν να χρησιμοποιούν μεγάλα passwords, όχι 2 και 3 χαρακτήρων, αλλά 8 – 10 ή και παραπάνω, με μέγιστο καθορισμένο μήκος τους 14 χαρακτήρες.
 - Θα πρέπει να κάνουν χρήση και μικρών και κεφαλαίων γραμμάτων. Όσον αφορά τα Windows NT, οι κωδικοί ασφαλείας είναι *case sensitive*, που σημαίνει ότι το A είναι διαφορετικό από το a. Οπότε, το password BledaR21 είναι διαφορετικό από το blEdaR21.

Επιτρεπτές ώρες χρήσης του δικτύου (Logon Hours) και περιορισμοί σταθμών εργασίας (Workstation Restrictions)

Θα πρέπει να καθορίζετε τις ώρες κατά τις οποίες ένας χρήστης θα μπορεί να έχει πρόσβαση στο δίκτυο και επίσης από ποιους σταθμούς εργασίας θα μπορεί να κάνει login στο δίκτυο. Για να υπορέσετε να καθορίσετε logon hours & Workstation Restrictions, θα πρέπει να έχετε υπόψη σας τα παρακάτω:

- Οι επιτρεπτες ώρες χρήσης του δικτύου, θα πρέπει να ανατίθενται σε χρήστες οι οποίοι επιβάλλεται να κάνουν χρήση του δικτύου μόνο στις ώρες εργασίας τους. Για παράδειγμα, θα μπορούσατε να καθορίσετε ότι οι νυκτοφύλακες θα πρέπει να μπορούν να κάνουν login, μόνο τις ώρες 0:00 – 07:00.
- Επίσης, στην περίπτωση που ο κάθε χρήστης έχει και ένα προσωπικό υπολογιστή στην εταιρεία, θα πρέπει να μπορεί να κάνει login μόνο από το δικό του υπολογιστή, ειδικά στην περίπτωση όπου τα δεδομένα που βρίσκονται αποθηκευμένα στους υπολογιστές των χρηστών είναι σημαντικά και κρίσιμα.

Κατάλογοι Εργασίας (Home Folders)

Αυτό που συνηθίζεται στα δίκτυα υπολογιστών, είναι οι απλοί χρήστες να μην έχουν δικαίωμα πρόσβασης σε ένα μεγάλο μέρος του σκληρού δίσκου (ή των σκληρών δίσκων), έτσι ώστε να μην προκληθεί κάποια ζημιά από λάθος. Οι άδειες που συνήθως έχουν είναι απλή ανάγνωση και εκτέλεση των περιεχομένων των αρχείων των δίσκων. Παρόλα αυτά είναι αναγκαίο ο κάθε χρήστης να έχει ένα προσωπικό κατάλογο (*home folder*), στον οποίο θα έχει πλήρη πρόσβαση και στον οποίο θα έχει δικαίωμα να κάνει ό,τι θέλει (να δημιουργήσει ή να σβήσει αρχεία/καταλόγους, κλπ). Το τελευταίο είναι απαραίτητο, γιατί υπάρχουν πολλά προγράμματα,  οποία για να μπορέσουν να εκτελεστούν σωστά θα πρέπει να υπάρχει ένας χώρος στο δίσκο στον οποίο να μπορούν να αποθηκεύουν δεδομένα. Για παράδειγμα, σε ένα πρόγραμμα επεξεργαστή κειμένου, σε περίπτωση που ο χρήστης χρειάζεται να αποθηκεύσει το αρχείο του στο δίσκο, θα πρέπει να έχει τέτοιου είδους άδεια. Οπότε, ο *προσωπικός κατάλογος*, αποτελεί ένα σημείο, όπου τα δεδομένα του εκάστοτε χρήστη αποθηκεύονται. Φυσικά, είναι φανερό ότι ο κάθε χρήστης έχει διαφορετικό κατάλογο εργασίας από τους άλλους χρήστες του δικτύου. Τέλος, οι home

folders, μπορούν να βρίσκονται είτε τοπικά στον υπολογιστή (Workstation), από τον οποίο γίνεται το login, είτε στο server του δικτύου, ώστε να υπάρχει κεντρικός έλεγχος, των δεδομένων των χρηστών.

ΔΗΜΙΟΥΡΓΩΝΤΑΣ ΛΟΓΑΡΙΑΣΜΟΥΣ ΧΡΗΣΤΩΝ

Παρακάτω βλέπουμε ένα πλαίσιο διαλόγου με το οποίο έχουμε τη δυνατότητα να δημιουργούμε νέους χρήστες στο σύστημα μας. Με βάση το πλαίσιο αυτό θα εξηγήσουμε τη διαδικασία με την οποία δημιουργούμε νέους λογαριασμούς χρηστών, καθώς επίσης και τα βήματα που θα πρέπει να ακολουθήσουμε στη διαδικασία αυτή.

Εδώ εισάγουμε μια περιγραφή σχετικά με το χρήστη, π.χ. αν είναι ordinary user, super user κλπ

Τα πεδία αυτά περιέχουν τον κωδικοποιημένο κωδικό ασφαλείας μας (password). Στο δεύτερο πεδίο ξαναεισαγούμε το password έτσι ώστε να βεβαιωθούμε ότι εισήχθη σωστά

Διάφορες άλλες ιδιότητες που αφορούν το χρήστη μας

Εδώ εισάγουμε το πλήρες όνομα του χρήστη μας, π.χ. Γεώργιος Αναστασίου

Εδώ εισάγουμε το username του νέου μας χρήστη, π.χ. George. Αυτό το όνομα θα χρησιμοποιείται κατά το

Με τα κουμπιά αυτά μεταβαίνουμε σε άλλα πλαίσια διαλόγου με τα οποία μπορούμε να ρυθμίσουμε κάποιες άλλες ιδιότητες του χρήστη (θα αναφερθούμε σε αυτά παρακάτω)

Στο παραπάνω πλαίσιο διαλόγου, πέρα από τα text boxes στα οποία εισάγουμε τα διάφορα προσωπικά στοιχεία του χρήστη, υπάρχουν και τέσσερα checkboxes, τα οποία μπορεί να είναι τσεκαρισμένα ή όχι. Πιο συγκεκριμένα:

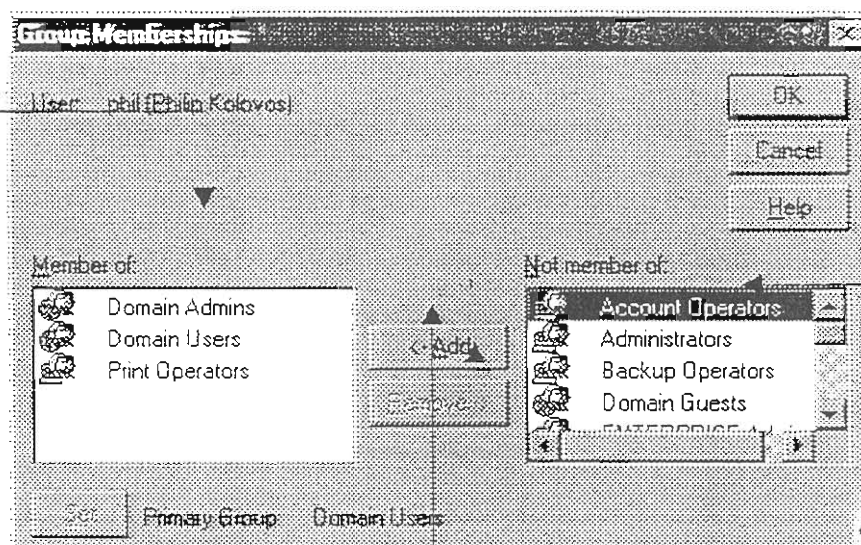
- Το checkbox *User Must Change Password at Next Logon* καθορίζει ότι από την επόμενη φορά που ο συγκεκριμένος χρήστης θα κάνει login, θα του επιβληθεί από το σύστημα να αλλάξει τον κωδικό ασφαλείας του.
- Το checkbox *User Cannot Change Password*, αντίθετα σε περίπτωση που είναι επιλεγμένο δε θα επιτραπεί στο χρήστη να αλλάξει τον κωδικό ασφαλείας. Αυτό το checkbox το ενεργοποιούμε μόνο σε περιπτώσεις λογαριασμών που είναι κοινόχρηστοι όπως π.χ. λογαριασμοί με username guest, inv, κλπ. Στην περίπτωση αυτή, υπάρχει ένα στάνταρ password το οποίο το γνωρίζουν οι χρήστες και το οποίο είναι κοινοχρηστο, όπως π.χ. public, inv, κλπ. Επομένως, δεν είναι επιθυμητό ο κάθε χρήστης να μπορεί να αλλάξει τον κωδικό αυτό, γιατί έτσι οι υπόλοιποι χρήστες δε θα μπορούν να χρησιμοποιήσουν το account αυτό.
- Αυτό που συνηθίζεται στις πολιτικές των διαφόρων συστημάτων δικτύων, είναι οι κωδικοί ασφαλείας που τίθενται από τον χρήστη να έχουν *ημερομηνία λήξης*. Αυτό σημαίνει ότι μετά από κάποιο καιρό (π.χ. 6 μήνες), το password του χρήστη λήγει οπότε και θα πρέπει να το αλλάξει. Αυτό γίνεται για να ισχυροποιηθεί η ασφάλεια επάνω στα δεδομένα των χρηστών του δικτύου. Είναι γενικά καλό οι κωδικοί ασφαλείας να αλλάζουν σε τακτά χρονικά διαστήματα, έτσι ώστε να είναι πιο δύσκολο για έναν κακόβουλο χρήστη (π.χ. hacker) να μπορεί να το μαντέψει ή να το αποκρυπτογραφήσει. Αν, τώρα, το checkbox *Password Never expires* είναι ενεργοποιημένο (τσεκαρισμένο), τότε ο κωδικός ασφαλείας του χρήστη δε λήγει ποτέ και ποτέ δεν επιβάλλεται από το σύστημα να αλλάχθει ο κωδικός.
- Τέλος, το checkbox *Account Disabled*, το ενεργοποιούμε μόνο στην περίπτωση όπου θέλουμε να «κλειδώσουμε» έξω από το σύστημα κάποιον χρήστη για κάποιον λόγο.

ΟΜΑΔΕΣ ΧΡΗΣΤΩΝ (USER GROUPS)

Είναι κανόνας ότι ο κάθε χρήστης του δικτύου, θα πρέπει να αποτελεί μέλος μιας ομάδας χρηστών. Δε μπορεί να υπάρξει αυτόνομα μέσα στο δίκτυο. Για παράδειγμα ο χρήστης με username Administrator, ανήκει στην ομάδα χρηστών Domain Admins, η οποία είναι υπεύθυνη για τη διαχείριση ολόκληρου του domain. Άλλοι χρήστες είναι πιθανόν να ανήκουν στην ίδια ομάδα (στην Domain Admins), οπότε και αυτοί θα έχουν τη δυνατότητα να διαχειριστούν πλήρως το Domain. Επιπρόσθετα οι απλοί χρήστες του δικτύου μπορεί να ανήκουν στην ομάδα χρηστών Domain Users. Είναι επίσης δυνατό κάποιος χρήστης να ανήκει σε δύο ή και περισσότερες ομάδες χρηστών. Οπότε, είναι δυνατό ένας χρήστης που ανήκει στην ομάδα Domain users, να ανήκει ταυτόχρονα και στην ομάδα Account Operators, όπου έχει δικαίωμα να δημιουργεί και να παρεμβαίνει στις ιδιότητες των άλλων απλών χρηστών. Η ομάδα στην οποία ανήκει κάποιος χρήστης ονομάζεται group.

Έτσι λοιπόν, με το πάτημα του πλήκτρου *Groups* εμφανίζεται ένα πλαίσιο διαλόγου με το οποίο μπορούμε να ρυθμίσουμε σε ποιες ομάδες χρηστών ανήκει ο χρήστης.

Εδώ βλέπουμε σε ποιες ομάδες χρηστών είναι μέλος ο χρήστης



Εδώ βλέπουμε σε ποιες ομάδες ο χρήστης μας δεν είναι μέλος

Με τα πλήκτρα αυτά μπορούμε να αφαιρέσουμε και να προσθέσουμε ένα χρήστη από μια ομάδα

Ρυθμίζοντας τα Profiles & τους καταλόγους εργασίας (Home Folders) των χρηστών

Profiles

Το profile ενός χρήστη δεν είναι τίποτε άλλο από τις ρυθμίσεις που έχει το desktop του. Δηλαδή, τι εικονίδια θα υπάρχουν στην επιφάνεια εργασίας του χρήστη, ποιες εντολές εμφανίζονται στο start menu κλπ. Στα Windows NT οι ρυθμίσεις αυτές αποτελούν ένα σύνολο καταλόγων, οι οποίοι εμπεριέχονται μέσα σε έναν άλλο κατάλογο, ξεχωριστό για τον κάθε χρήστη. Το σύνολο αυτό των καταλόγων, ή απλά το profile του χρήστη μπορεί να είναι αποθηκευμένο είτε τοπικά, είτε στον κεντρικό server του domain. Στην πρώτη περίπτωση λέγεται ότι ο χρήστης έχει *τοπικό (local)* profile, ενώ στη δεύτερη περίπτωση το profile του είναι *roaming*. Το local profile, αποθηκεύεται στον υπολογιστή από τον οποίο κάνει login ο χρήστης και φορτώνεται κάθε φορά που κάνει ξανά login, από το δίσκο του τοπικού υπολογιστή. Είναι κατανοητό, ότι αν ο χρήστης κάνει login από άλλο υπολογιστή και δεν έχει roaming profile, τότε υπάρχει περίπτωση οι ρυθμίσεις της επιφάνειας εργασίας του να είναι διαφορετικές στον υπολογιστή εκείνο.

Το *roaming* profile, αποθηκεύεται στον κεντρικό εξυπηρετή του δικτύου και «φορτώνεται» κάθε φορά που κάνει ο χρήστης login στον τοπικό υπολογιστή. Ότι αλλαγές επιτελεστούν από το χρήστη στην επιφάνεια εργασίας, αποθηκεύονται στο «φορτωμένο από τον server(loaded)» τοπικό profile και μόλις ο χρήστης αποχωρήσει από το δίκτυο (logout), τότε ενημερώνεται και το αντίγραφο του profile του στον server.

Τέλος, υπάρχει και ένας τρίτος τύπος profile, το *mandatory*. Η περίπτωση αυτή αναφέρεται σε profiles που είναι υποχρεωτικά και δε μπορούν να αλλάξουν από το χρήστη. Τα profiles των χρηστών αποθηκεύονται στον domain server. Ο χρήστης, κατά τη διάρκεια που είναι logged on μπορεί να επιτελέσει αλλαγές στο desktop, αλλά όταν κάνει logout, το αντίγραφο που βρίσκεται στον server δε θα ενημερωθεί. Η κατηγορία αυτή είναι όμοια με την προηγούμενη, με τη μόνη διαφορά ότι όταν ο χρήστης κάνει logout, το αντίγραφο του profile στο server, δεν ενημερώνεται, οπότε και αυτόματα αναπαύονται και οι οποιεσδήποτε αλλαγές.

Δημιουργώντας Roaming User Profiles

Για να δημιουργήσουμε Roaming User Profiles, θα πρέπει να ακολουθήσουμε δύο βήματα να δημιουργήσουμε ένα test user profile¹⁰ και στη συνέχεια να αντιγράψουμε το user profile αυτό σε έναν network server. Για να δημιουργήσουμε ένα test user profile ακολουθούμε τα εξής βήματα:

Για να δημιουργήσετε ένα test user account

1. Δημιουργήστε ένα λογαριασμό χρήστη με το username test και μη βάλετε τίποτα για το profile & home folder του χρήστη αυτού.
2. Κάντε login με το username αυτό. Ένα profile για το χρήστη test δημιουργείται αυτόματα στον τοπικό υπολογιστή στον κατάλογο C:\Windows\Profiles
3. Ρυθμίστε την επιφάνεια εργασίας του χρήστη test, κάνοντας τις απαραίτητες αλλαγές στο desktop, start menu κλπ.
4. Κάντε logoff και μετά logon πάλι ως Administrator.

Για να αντιγράψετε το test user profile σε ένα network server

1. Δημιουργήστε έναν κατάλογο σε ένα drive στον server, ο οποίος θα κρατά τα profiles των χρηστών, π.χ. \\servername\Users\Profiles\user_name
2. Στο control Panel κάντε διπλό κλικ στο System και μετά κάντε κλικ στην καρτέλα User Profiles.
3. Κάτω από την ετικέτα Profiles Stored On This Computer κάντε κλικ στο profile το οποίο θέλετε να αντιγράψετε (στην περίπτωση μας το profile του χρήστη test), και μετά κάντε κλικ στο πλήκτρο Copy To.
4. Στο πλαίσιο διαλόγου Copy Profile To, γράψτε το μονοπάτι στο δίκτυο προς το server
5. Κάτω από το Permitted to Use, κάντε κλικ στο Change.
6. Προσθέστε τον κατάλληλο χρήστη και πατήστε OK¹¹
7. Στον κατάλογο στον οποίο δημιουργήσατε στο δίκτυο, αλλάζτε το αρχείο Ntuser.dat, σε Ntuser.man, μόνο στην περίπτωση όπου το profile είναι mandatory.

¹⁰ Βλέπε παρακάτω για τον τρόπο με τον οποίο μπορούμε να δημιουργήσουμε ένα νέο user account

¹¹ Εξηγήσεις σχετικά με το πλαίσιο διαλόγου για το πως μπορούμε να προσθέτουμε νέους χρήστες δίδονται παρακάτω

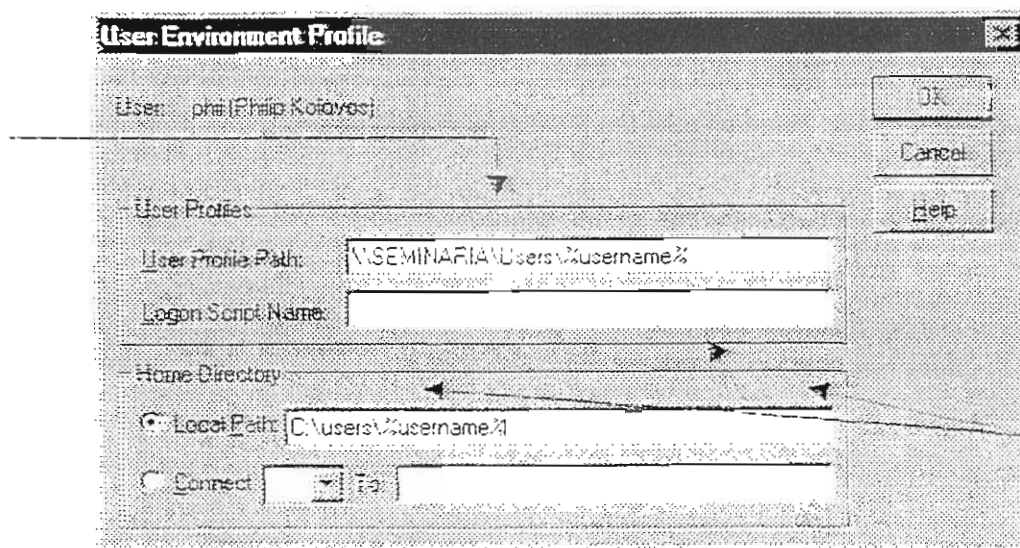
8. Εκκινείτε τον **User Manager for Domains**, κάντε διπλό κλικ στο χρήστη του οποίου το profile θέλετε να ρυθμίσετε και πατήστε το πλήκτρο **Profiles**.
9. Για το πλαίσιο διαλόγου **User Profile Path**, γράψτε το δικτυακό μονοπάτι (network path), προς το server του δικτύου π.χ.
`\\SEMINARIA\\Users\\Profiles\\user_name`

Απο εδώ και πέρα για κάθε νέο χρήστη που θα δημιουργείται, θα πηγαίνετε στον κατάλογο εκείνο που περιέχει τα profiles των χρηστών (\\SEMINARIA\\Users\\Profiles), θα δημιουργείτε ένα κατάλογο για το νέο αυτό χρήστη και θα προσθέτετε το network path, προς τον κατάλογο αυτό στις ιδιότητες **Profiles** του χρήστη.

Υπάρχει και η επιλογή να μη δημιουργήσετε καθόλου **roaming user profiles**. Στην περίπτωση αυτή δεν ακολουθείτε τα παραπάνω βήματα και δεν προσθέτετε τίποτα στα πλαίσια εκείνα που περιέχουν το path προς τον κατάλογο των profiles. Έτσι το σύστημα θα δημιουργεί αυτόματα μία καταχώρηση για το profile (στο **C:\\Windows\\Profiles**) στον τοπικό υπολογιστή για τον εκάστοτε χρήστη που κάνει login.

Κατάλογοι Εργασίας (Home folders)

Για το θέμα αυτό έχουμε ήδη μιλήσει.



Εδώ γράφουμε το drive & path στο οποίο θέλουμε να συνδέεται ο χρήστης για να βρίσκει τον κατάλογο εργασίας του κάθε φορά που κάνει login στο δίκτυο.

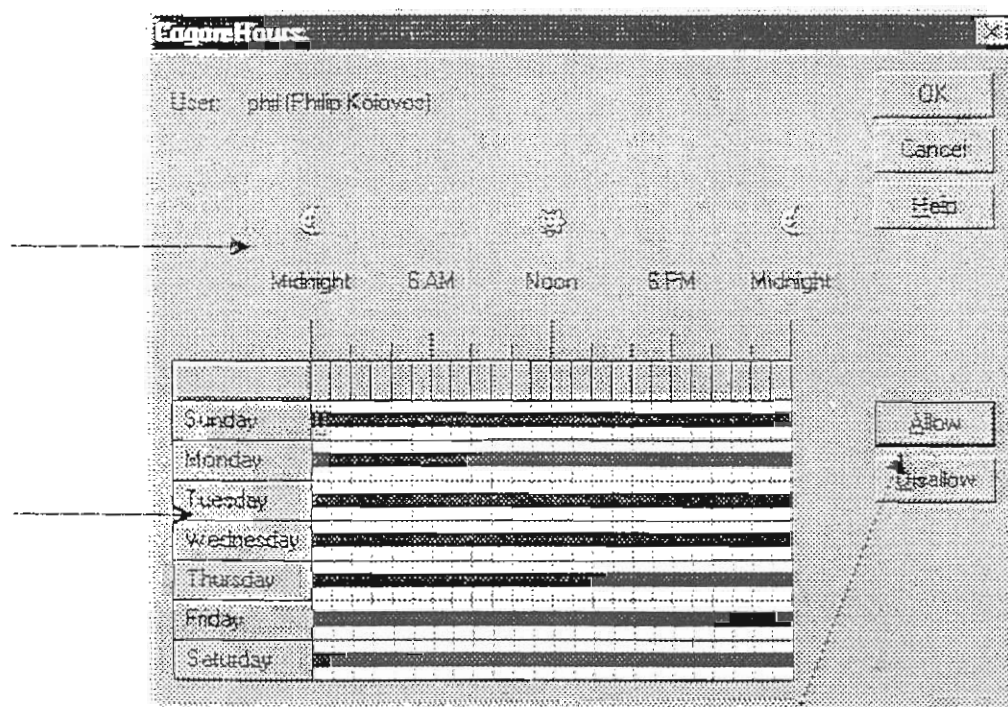
Στο πλαίσιο αυτό γράφουμε τον κατάλογο στον οποίο θα είναι αποθηκευμένο το profile του χρήστη. Στην περίπτωση που αυτό είναι roaming ή mandatory, τότε πρέπει να δώσουμε και το όνομα του server στη μορφή: \\SERVERNAME\\path. Σε άλλη περίπτωση, απλά προσδιορίζουμε τον κατάλογο του τοπικού δίσκου στον οποίο θα αποθηκεύεται το profile. Ο χρήστης phil στην περίπτωση αυτή έχει roaming profile και είναι αποθηκευμένο στον κατάλογο users του server SEMINARIA. Τέλος η μεταβλητή %username%, είναι μεταβλητή συστήματος και αντικαθίσταται αυτόματα με το όνομα του χρήστη, εδώ phil.

Στο πλαίσιο αυτό επίσης, γράφουμε τον κατάλογο ο οποίος θα αποτελέσει τον home folder του χρήστη. Και πάλι μπορεί να είναι είτε τοπικός είτε να βρίσκεται στον server του δικτύου μας. Στην τελευταία περίπτωση προσδιορίζουμε σε ποιο drive (δίσκο), θέλουμε να συνδέεται κάθε φορά ο χρήστης και μετά σε ποιο path. Στην περίπτωση του local path, αρκεί να προσδιοριστεί μόνο το path. Ο χρήστης phil, στην περιπτώσή μας, έχει local home folder.

ΣΗΜΕΙΩΣΗ: Υπάρχει και η δυνατότητα να μην γράψουμε τίποτα σε κανένα από τα παραπάνω πεδία, οπότε και μπαίνουν σε λειτουργία οι εξ' ορισμού ρυθμίσεις (default configurations) σχετικά με τα profiles & home folders.

ΕΠΙΤΡΕΠΤΕΣ ΩΡΕΣ ΧΡΗΣΗΣ ΤΟΥ ΔΙΚΤΥΟΥ (LOGON HOURS)

Όταν δημιουργούμε ένα χρήστη, μπορούμε να ρυθμίσουμε και ποιες ώρες και μέρες θα μπορεί αυτός να χρησιμοποιεί το δίκτυο. Το εξ' ορισμού είναι κάθε ημέρα 24 ώρες το 24ωρο, αλλά αν θέλουμε μπορούμε να το αλλάζουμε για κάποιον χρήστη. Παρακάτω βλέπουμε το σχετικό πλαίσιο διαλόγου στο οποίο μπορούμε να μεταβούμε πατώντας το πλήκτρο Hours.

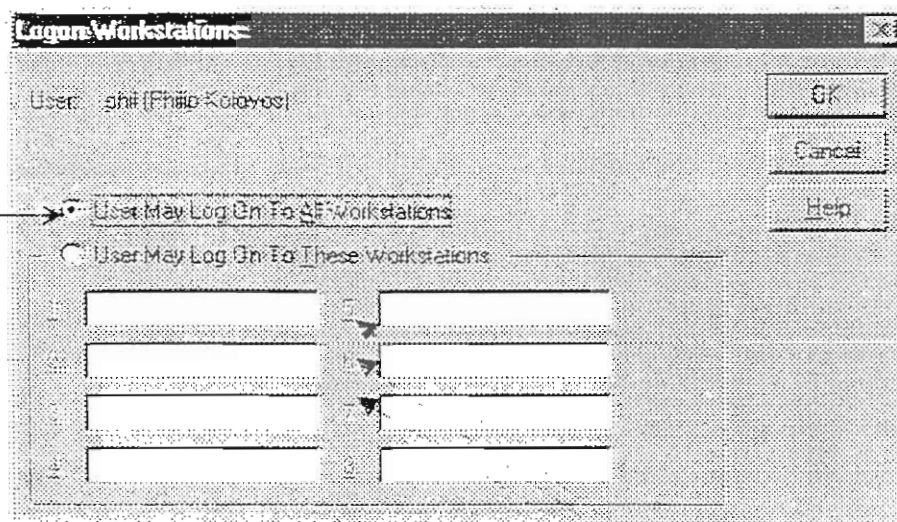


Οι ημέρες και ώρες κατά τις οποίες μπορεί να χρησιμοποιεί το δίκτυο ο εκάστοτε χρήστης

Για να αλλάξουμε τις ρυθμίσεις πρόσβασης για τον χρήστη phil. «επιλέγουμε» με το ποντίκι την περιοχή εκείνη στην οποία θέλουμε να εφαρμόσουμε τις αλλαγές μας και πατάμε Allow ή Disallow, ανάλογα με το τι θέλουμε να κάνουμε

ΠΕΡΙΟΡΙΣΜΟΙ ΣΤΑΘΜΩΝ ΕΡΓΑΣΙΑΣ (WORKSTATION PERMISSIONS)

Μπορούμε επίσης, να θέσουμε και τον περιορισμό σε κάποιον χρήστη, σχετικά με το από ποιον σταθμό εργασίας (υπολογιστή), θα μπορεί να χρησιμοποιεί το δίκτυο. Μπορούμε δηλαδή, να ορίσουμε ότι ο Χ χρήστης θα μπορεί να κάνει login, μόνο από τους σταθμούς εργασίας COMPUTER1 & COMPUTER3, ενώ ο Υ θα μπορεί να κάνει login από οποιονδήποτε σταθμό εργασίας. Αυτό γίνεται μέσω του παρακάτω πλαισίου διαλόγου:

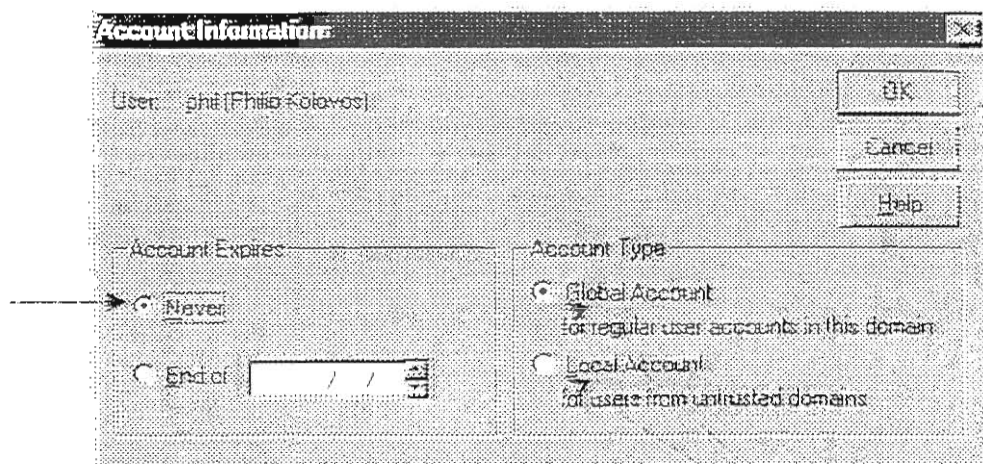


Επιλέγουμε εδώ, όταν θέλουμε ο χρήστης μας να μπορεί να χρησιμοποιεί το δίκτυο από οποιονδήποτε σταθμό εργασίας (είναι επιλεγμένο εξ' ορισμού).

Επιλέγουμε εδώ, όταν θέλουμε ο χρήστης μας να μπορεί να χρησιμοποιεί το δίκτυο από συγκεκριμένους σταθμούς εργασίας. Θα πρέπει επίσης, να προσθέσουμε και τα ονόματα των σταθμών εργασίας από τα οποία θα γίνεται το login.

ACCOUNT configurations

Με αυτό το πλαίσιο διαλόγου μπορούμε να θέσουμε μερικές παραπάνω ιδιότητες για το χρήστη μας. Πιο συγκεκριμένα:

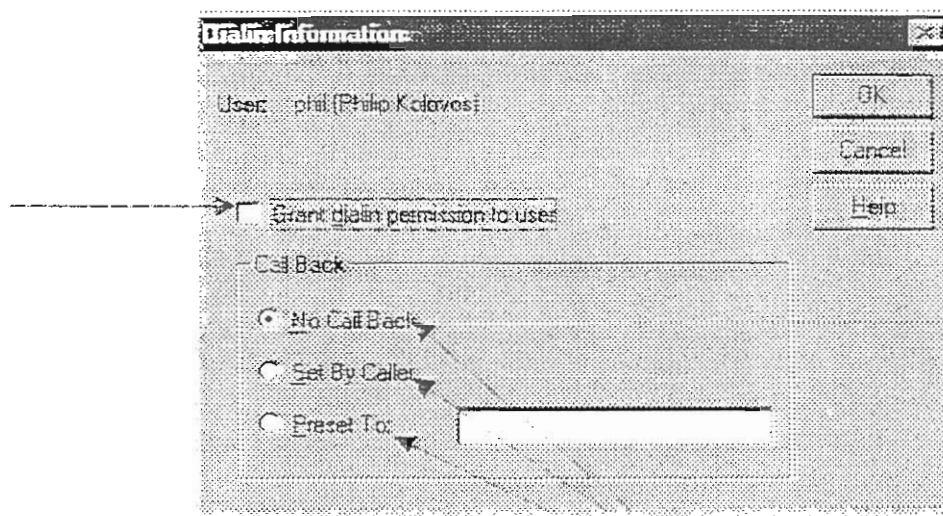


Εδώ μπορούμε να καθορίσουμε για το αν ο λογαριασμός του χρήστη μας θα είναι εποχιακός ή όχι, δηλαδή για το αν θα έχει ημερομηνία λήξεως. Αυτό είναι χρήσιμο στην περίπτωση όπου έχουμε εποχιακούς εργαζομένους στην εταιρεία, οι οποίοι είναι απαραίτητο να χρησιμοποιήσουν το δίκτυο

Εδώ καθορίζουμε για το αν ο λογαριασμός του χρήστη θα είναι global (θα «φαίνεται» σε ολόκληρο το domain), ή θα είναι local (θα «φαίνεται», μόνο στον τοπικό υπολογιστή από τον οποίο δημιουργείται το account).

DIALIN PERMISSIONS

Οι dialin permissions αφορούν μόνο τις περιπτώσεις των χρηστών εκείνων που έχουν τη δυνατότητα να κάνουν login από το σπίτι τους, μέσω τηλεφώνου. Μπορούμε είτε να επιτρέπουμε σε κάποιον χρήστη του δικτύου να χρησιμοποιεί το δίκτυο μέσω τηλεφώνου ή όχι με το παρακάτω πλαίσιο διαλόγου:



Επιλέγουμε εδώ για να επιτρέψουμε σε κάποιον χρήστη να κάνει χρήση του δικτύου μέσω τηλεφώνου.

Μπορούμε, επίσης, να ρυθμίσουμε έτσι τον server ώστε να μπορεί να καλείται ο χρήστης από το σύστημα κάθε φορά που κάνει dialup login, έτσι ώστε να χρεώνεται η εταιρεία το τηλεφώνημα. Μπορούμε να μην έχουμε ενεργοποιήσει καθόλου την υπηρεσία αυτή (No Call Back), είτε να δίδεται ένα τηλεφωνικό νούμερο από τον καλών (Set By Caller), είτε να έχουμε ορίσει ένα προκαθορισμένο τηλεφωνικό νούμερο (Preset To:).

ΠΟΛΙΤΙΚΕΣ ΛΟΓΑΡΙΑΣΜΩΝ ΧΡΗΣΤΩΝ (USER ACCOUNTS POLICIES)

Μέσω του παρακάτω πλαισίου διαλόγου, μπορούμε να ρυθμίσουμε τι πολιτική θα ακολουθηθεί για όλους τους χρήστες του δικτύου. Πιο συγκεκριμένα:

Maximum Password Age
Μέγιστος χρόνος ζωής των κωδικών ασφαλείας των χρηστών. Καθορίζει το μέγιστο χρόνο που μπορεί να περνοει το password του χρήστη.

Minimum Password Length
Καθορίζει το ελάχιστο μήκος (σε γράμματα) που θα μπορεί να έχει ο κωδικός.

Domain: STARTREK

Password Restrictions

Maximum Password Age

☐ Password Never Expires

☒ Expires in 42 Days

Minimum Password Age

☒ Allow Changes Immediately

☐ Allow Changes in Days

Minimum Password Length

☒ Permit Blank Password

☐ At least Characters

Password Uniqueness

☒ Do Not Keep Password History

☐ Remember Passwords

☒ No account lockout

☐ Account lockout

Lockout after bad login attempts

Reset count after minutes

Lockout Duration

☐ Forever (until admin unlocks)

☐ Duration minutes

☐ Enforceably disconnect remote users from server when login hours expire

☐ Users must log on in order to change password

Minimum Password Age

Ελάχιστος χρόνος ζωής των κωδικών ασφαλείας των χρηστών. Καθορίζει ένα ελάχιστο χρονικό όριο για το οποίο ο χρήστης δε θα μπορεί να αλλάξει τον κωδικό του.

Password Uniqueness

Καθορίζει το κατά πόσο η επόμενη password του χρήστη θα μπορεί να είναι ίδια με κάποια παλιά του.

Lockout Duration

Καθορίζουμε για πόσο καιρό θα παραμένει κλειδωμένο το account.

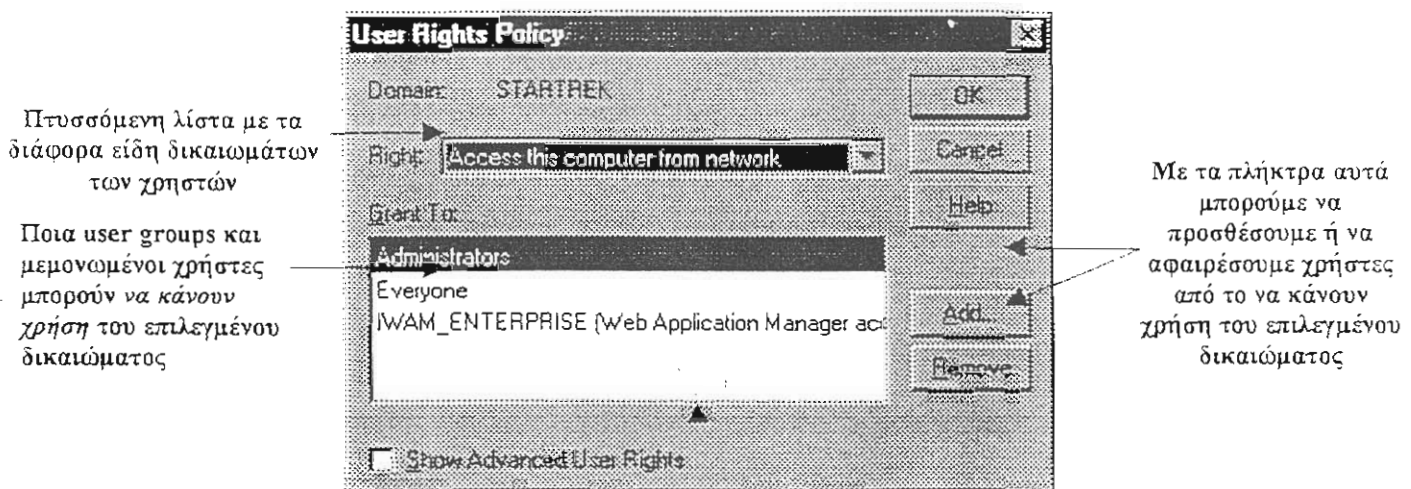
Account LockOut

Καθορίζουμε εάν ή όχι θα κλειδώνεται ο λογαριασμός του χρήστη. Ορίζουμε για παράδειγμα, ότι αν ένας χρήστης δώσει τρεις φορές λάθος τον κωδικό του, τότε ο λογαριασμός του θα κλειδώνεται, που σημαίνει ότι ακόμη και με το σωστό password δε θα μπορεί να κάνει login.

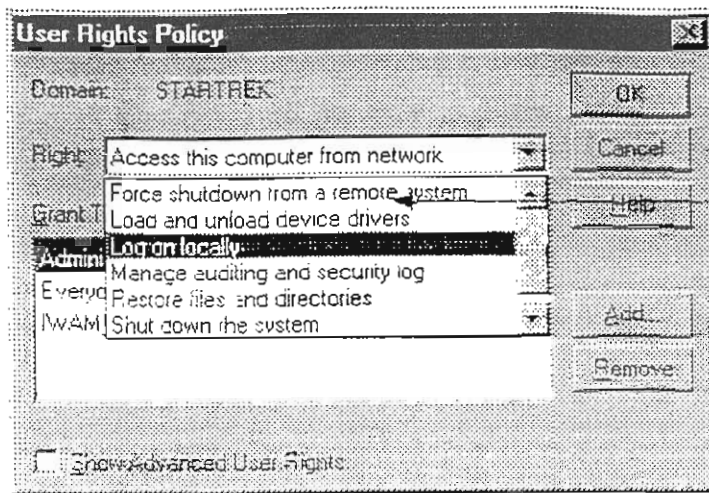
Στην περίπτωση αυτή θα πρέπει να επικοινωνήσει με το διαχειριστή του δικτύου.

ΠΟΛΙΤΙΚΕΣ ΔΙΚΑΙΩΜΑΤΩΝ ΤΩΝ ΧΡΗΣΤΩΝ (USER RIGHTS)

Όπως μπορούμε να καθορίσουμε πολιτικές σχετικά με τους λογαριασμούς των χρηστών, έτσι μπορούμε να καθορίσουμε και πολιτικές σχετικά με τα δικαιώματα που θα έχει ο κάθε χρήστης στο δίκτυο. Τέτοια δικαιώματα μπορεί να είναι π.χ. το αν θα μπορεί να κάνει Shut Down στο σύστημα, για το αν θα μπορεί να κάνει restore σε αρχεία και καταλόγους, για το αν θα μπορεί να κάνει *log on locally* και πολλά άλλα. Ειδικά η τελευταία περίπτωση είναι απαραίτητο να ισχύει για όλους τους χρήστες ενός Domain. Για να μπορέσει να κάνει ένας χρήστης log in στο Domain, θα πρέπει να μπορεί να έχει αλληλεπίδραση με τον κεντρικό server του domain. Θα πρέπει δηλαδή, να μπορεί να κάνει *interactive logon*, έτσι ώστε να μπορεί να αναγνωριστεί το password του, το username του, και τα διάφορα άλλα δικαιώματα που μπορεί να έχει σε αρχεία και καταλόγους. Πιο συγκεκριμένα:



Με αυτό το πλαίσιο διαλόγου μπορούμε να ρυθμίσουμε τα δικαιώματα έχει ο κάθε χρήστης (ή η ομάδα εργασίας καποιων χρηστών-user group).



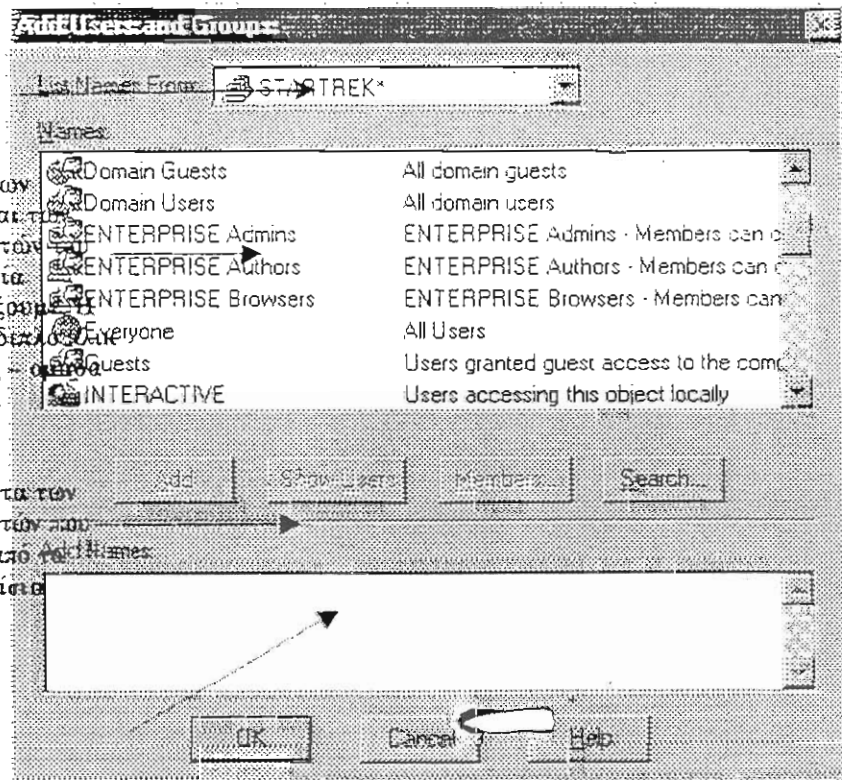
Θα πρέπει να προσθέτουμε κάθε χρήστη μεμονωμένα να μπορεί να κάνει χρήση του δικαιώματος αυτού, έτσι ώστε να μπορεί να κάνει logon *interactively* με τον server του Domain.

Παρακάτω βλέπουμε και το πλαίσιο διαλόγου εκείνο με το οποίο μπορούμε να προσθέσουμε έναν μεμονωμένο χρήστη(ες) ή ομάδες(ες) στη λίστα χρήσης ενός επιλεγμένου δικαιώματος.

Από ποιο Domain θέλουμε να προσθέσουμε νέους χρήστες/groups

Περιέχει ονόματα των ομάδων χρηστών και των μεμονωμένων χρηστών του Domain από τα οποία μπορούμε να διαλέξουμε. Η επιλογή γίνεται με διπλό κλικ επάνω στον χρήστη που μας ενδιαφέρει

Περιέχει τα ονόματα των ομάδων και/ή χρηστών που έχουμε επιλέξει από τα παραπάνω πλαίσια



Πατάμε OK για να προστεθούν οι χρήστες/ομάδες στη λίστα χρήσης του δικαιώματος

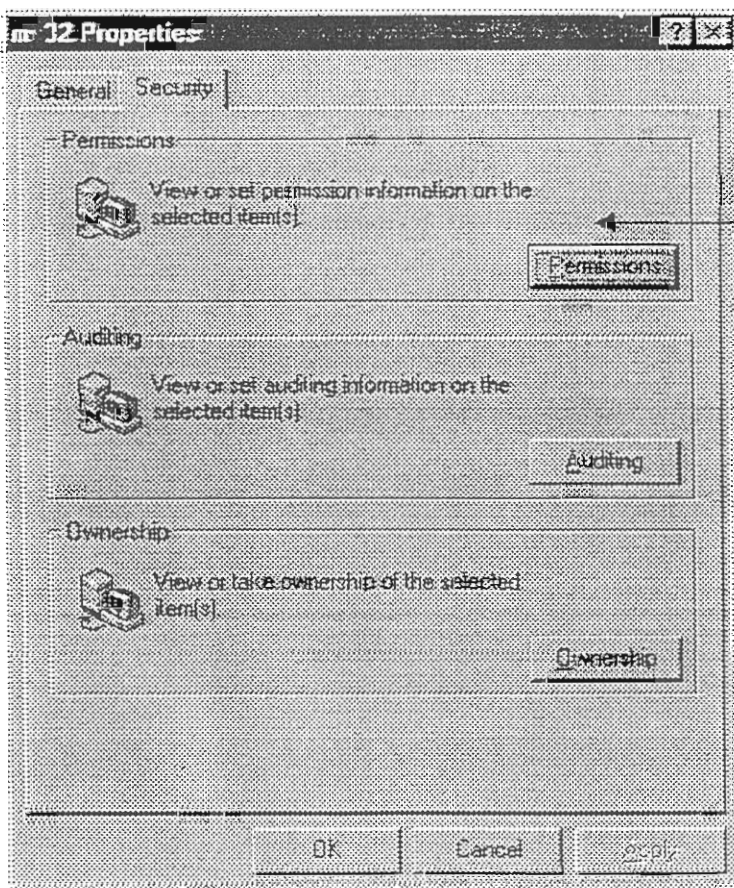
ΑΔΕΙΕΣ ΚΑΤΑΛΟΓΩΝ ΚΑΙ ΑΡΧΕΙΩΝ (FILE & DIRECTORY ACCESS PERMISSIONS)

Στο τμήμα αυτό, θα μιλήσουμε για τις άδειες των καταλόγων και αρχείων και για το πως μπορούμε να τις χειριστούμε. Επίσης, θα μιλήσουμε και για μερικά θέματα σχετικά με το **Sharing** των καταλόγων, το οποίο με λίγα λόγια αφορά το διαμοιρασμό των καταλόγων ενός υπολογιστή από τους υπόλοιπους υπολογιστές του δικτύου.

Καταρχήν, είναι απαραίτητο να σημειώσουμε ότι για να μπορούμε να θέτουμε άδειες σε καταλόγους και αρχεία θα πρέπει το *σύστημα αρχείων* να είναι NTFS και όχι FATxx (xx=16 ή 32). Μόνο τα NTFS volumes μπορούν να παρέχουν άδειες αρχείων και καταλόγων.

Συνεχίζοντας, παρακάτω βλέπετε το πλαίσιο διαλόγου με το οποίο μπορούμε να χειριστούμε τις άδειες των καταλόγων και των αρχείων μας. Για να εμφανιστεί το πλαίσιο αυτό, κάνουμε δεξί κλικ σε ένα αρχείο ή κατάλογο στο δίσκο μας και επιλέγουμε **Properties**. Στη συνέχεια, στο πλαίσιο διαλόγου των ιδιοτήτων του αρχείου/καταλόγου επιλέγουμε την καρτέλα **Security**.

Έχουμε κάνει δεξί κλικ
στο αρχείο mv32.log

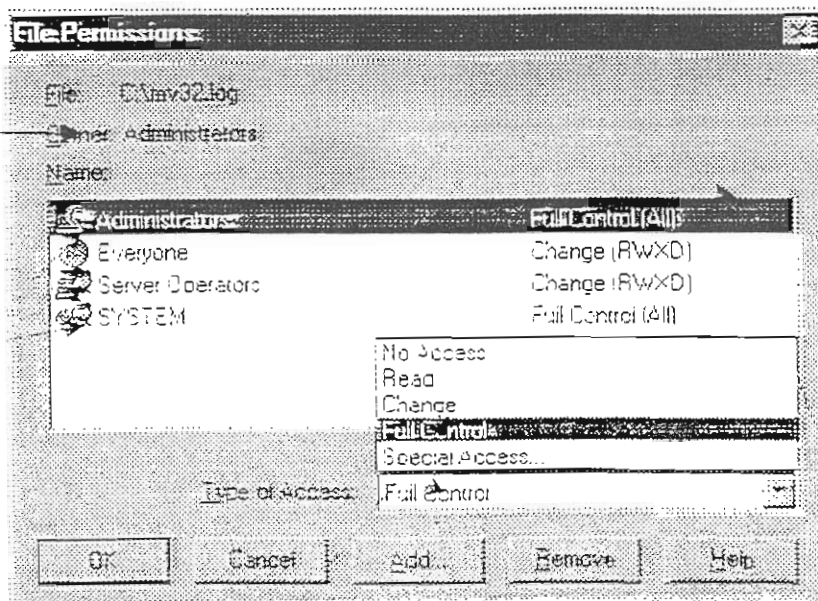


Με το πλήκτρο αυτό,
ρυθμίζουμε τις άδειες
χρήσης του
καταλόγου/αρχείου

Πατώντας το πλήκτρο **Permissions**, μεταβαίνουμε στο παρακάτω πλαίσιο διαλόγου με το οποίο μπορούμε να δούμε τις ιδιότητες που κατέχει το αρχείο C:\mv32.log

Μερικά στοιχεία σχετικά με το υπο-μελέτη αρχείο

Ποιες ομάδες χρηστών και ποιοι μεμονωμένοι χρήστες έχουν δικαίωμα να χειριστούν το αρχείο

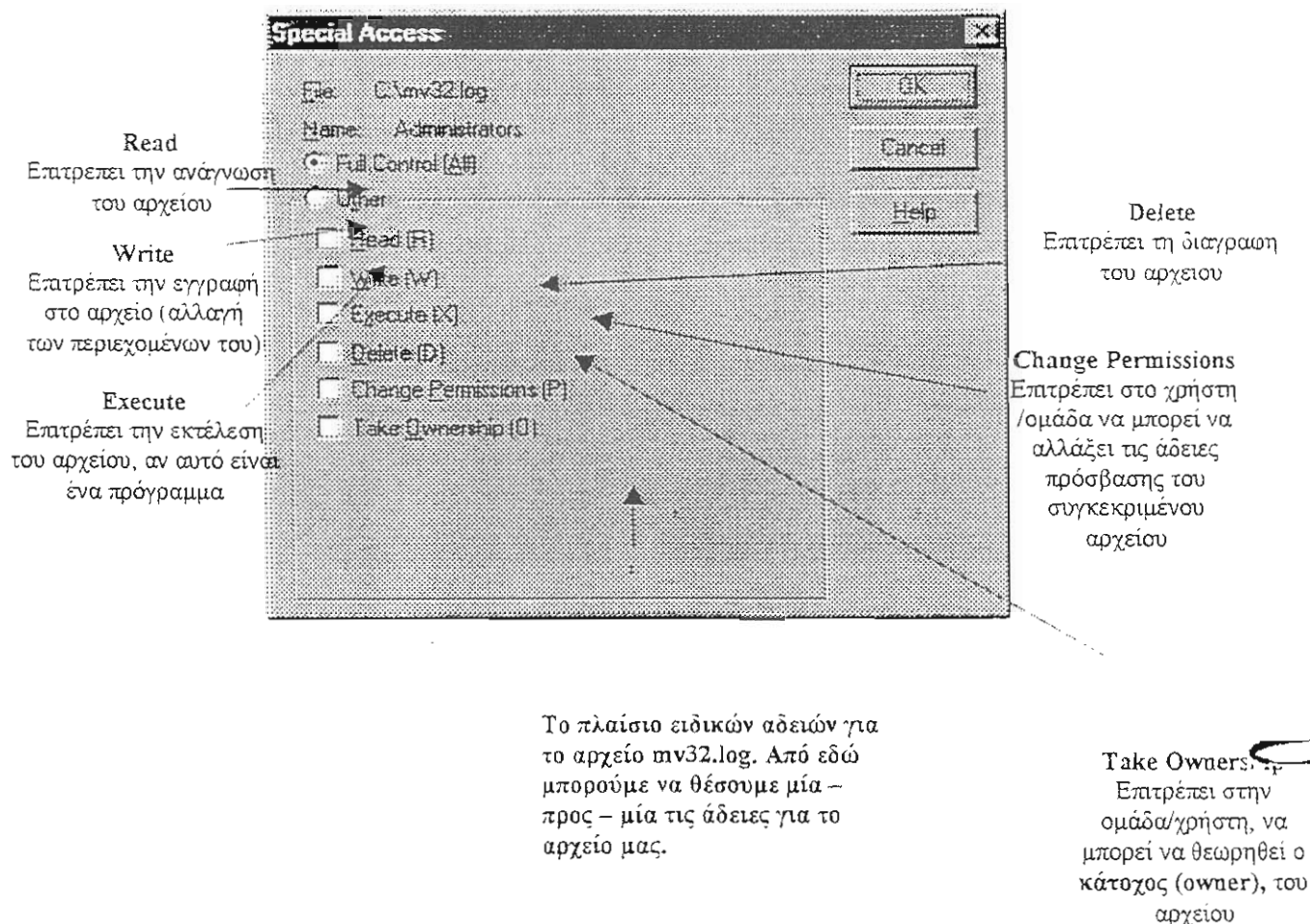


Μια πτυσσόμενη λίστα, μέσω της οποίας μπορούμε να αναθέσουμε προκαθορισμένες άδειες στον κατάλογο/αρχείο για μια ομάδα ή χρήστη. Για παράδειγμα ο τύπος αδειών Change θέτει ότι το συγκεκριμένο group ή χρήστης μπορεί να διαβάσει (R), να αλλάξει (επανεγγράφει - W), να εκτελεί (σε περίπτωση που είναι πρόγραμμα - X) και να διαγράψει (D) το αρχείο αυτό. Δηλαδή (RWXD).

Το είδος της πρόσβασης το οποίο έχει η συγκεκριμένη ομάδα/χρήστης. Πρώτα είναι το όνομα του είδους της άδειας (Change κλπ) και μέσα στην παρένθεση περιέχονται οι συγκεκριμένες άδειες για το αρχείο (RWXD - ReadWriteExecuteDelete)

Με το πλήκτρο αυτό μπορούμε να προσθέσουμε νέους χρήστες - ομάδες στις άδειες χρήσης του αρχείου/καταλόγου. Ο τρόπος προσθήκης νέων χρηστών - ομάδων γίνεται με τον τρόπο που περιγράφηκε παραπάνω

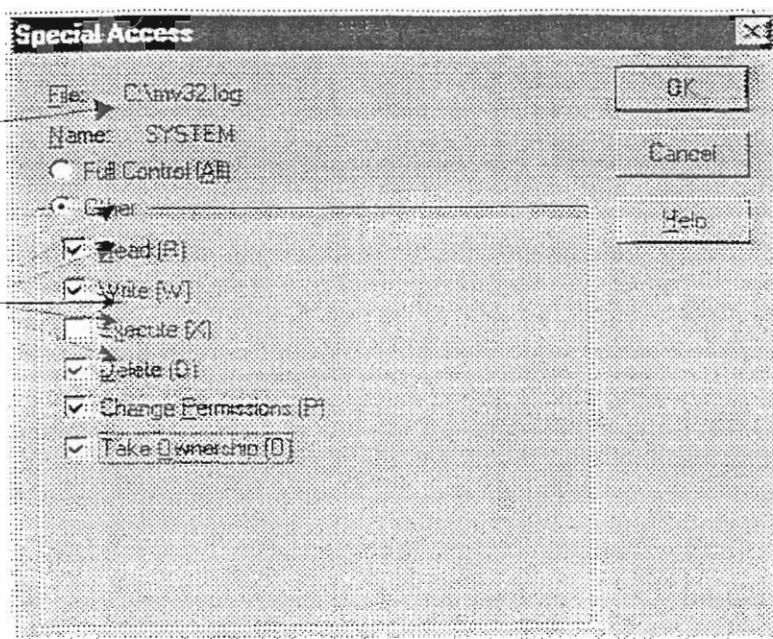
Πέρα από τα προκαθορισμένα είδη αδειών που μπορούμε να θέσουμε στα αρχεία μας μέσω της πτυσσόμενης λίστας, μπορούμε να προσδιορίσουμε και ένα δικό μας τύπο πρόσβασης, ο οποίος θα είναι διαφορετικός από όλες τις επιλογές της λίστας. Για παράδειγμα μπορεί να θέλαμε να προσδιορίσουμε ότι για το συγκεκριμένο αρχείο (mv32.log), η ομάδα χρηστών SYSTEM θα μπορεί να έχει μόνο τις άδειες: (RWDPO – Read, Write, Delete, Change Permissions και Take Ownership). Για να το καταφέρουμε αυτό, θα πρέπει να επιλέξουμε στο παραπάνω πλαίσιο διαλόγου με το ποντίκι την ομάδα χρηστών SYSTEM, και να κάνουμε διπλό κλικ επάνω της. Τότε, θα εμφανιστεί το παρακάτω πλαίσιο διαλόγου, το οποίο αφορά τις άδειες χρήσης, μία-προς-μία του αρχείου mv32.log. Αυτό το πλαίσιο διαλόγου ονομάζεται *πλαίσιο διαλόγου ειδικών αδειών – special access dialog box*. Από εδώ και πέρα μπορούμε να θέσουμε τις όποιες άδειες θέλουμε για το επιλεγμένο group ή χρήστη.



Οπότε, αν θέλαμε να δώσουμε στην ομάδα χρηστών SYSTEM τις άδειες RWDPO για το συγκεκριμένο αρχείο, θα έπρεπε το προηγούμενο πλαίσιο διαλόγου να είχε την παρακάτω μορφή:

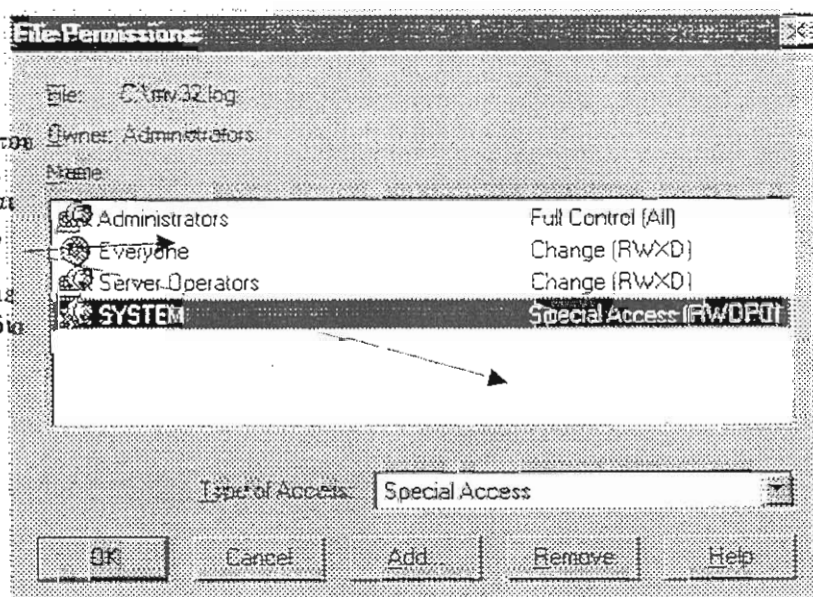
Η ομάδα της οποίας τις
άδειες θέλουμε να
αλλάζουμε

Οι άδειες πρόσβασης
για το συγκεκριμένο
αρχείο



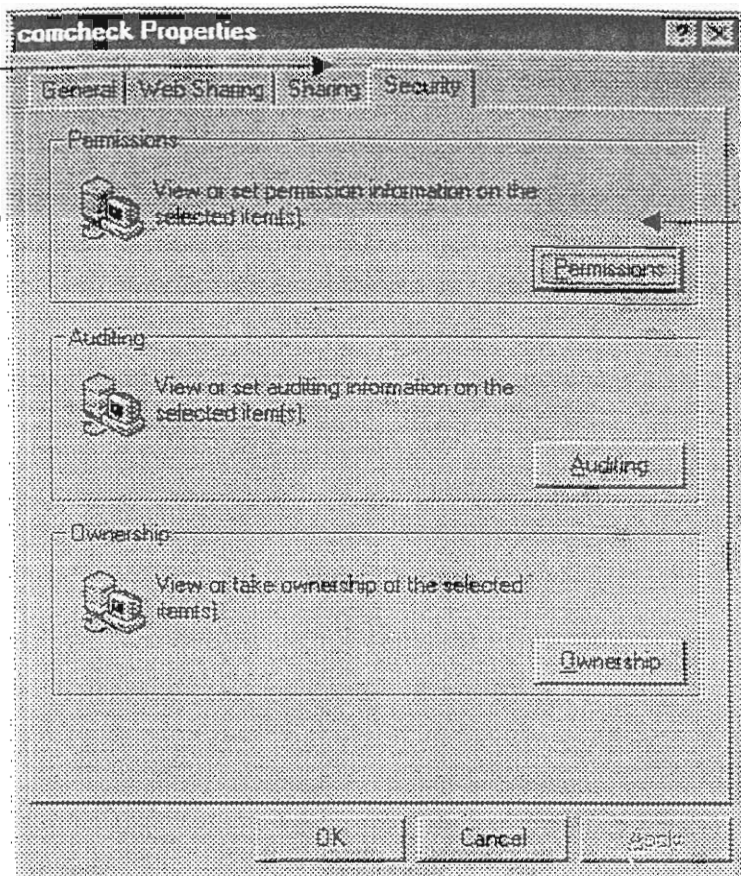
Πατώντας OK γυρίζουμε στο προηγούμενο πλαίσιο διαλόγου, το οποίο θα πρέπει να έχει την παρακάτω μορφή:

Παρατηρήστε πως οι άδειες χρήσης του
αρχείου έχουν αλλάξει για την ομάδα
SYSTEM. Τώρα πια, δε συνοδεύονται
από μια προκαθορισμένη περιγραφή,
αλλά από τη λέξη *Special Access*.
Πατώντας και πάλι OK, εφαρμόζουμε
τις άδειες στο αρχείο win32.log. Το ίδιο
κάνουμε και για οποιοδήποτε άλλο
αρχείο του δίσκου.



Αν από την άλλη, κάνουμε δεξί κλικ με το ποντίκι σε έναν κατάλογο αντί σε αρχείο τότε
θα εμφανιστεί το παρακάτω πλαίσιο διαλόγου:

Διαφέρει από το αντίστοιχο πλαίσιο διαλόγου για τα αρχεία, στο ότι περιέχει και την καρτέλα *Sharing*, η οποία αναφέρεται στο διαμοιρασμό του καταλόγου στο δίκτυο



Κάνουμε πάλι κλικ εδώ για να εμφανιστεί το πλαίσιο διαλόγου με τις άδειες των καταλόγων.

Όπως βλέπετε είναι λίγο διαφορετικό από το πλαίσιο διαλόγου για τα αρχεία, στο ότι περιέχει και μια καρτέλα για το διαμοιρασμό (*sharing*) του καταλόγου στο δίκτυο. Παρακάτω θα αναφερθούμε αναλυτικότερα σε θέματα σχετικά με το διαμοιρασμό των καταλόγων.

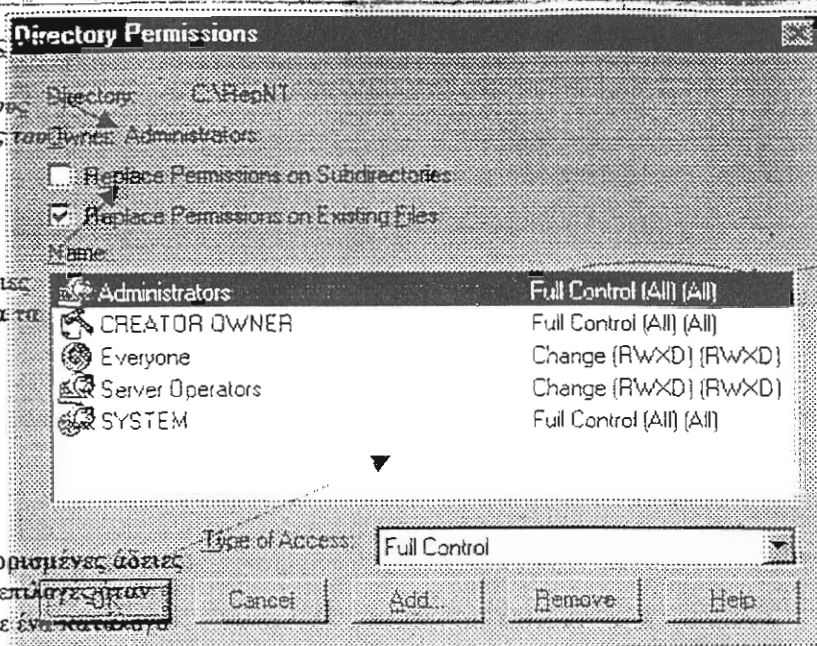
Αν πατήσουμε το πλήκτρο **Permissions**, οδηγούμαστε σε ένα άλλο dialog box, το οποίο διαφέρει επίσης από το αντίστοιχο πλαίσιο διαλόγου για τα αρχεία, στα εξής τρία σημεία:

1. Περιέχει δύο ακόμη checkboxes
2. Διαθέτει περισσότερες προκαθορισμένες άδειες
3. Οι διαθέσιμες άδειες για το κάθε group / user αποτελούνται από δύο τμήματα

Αν επιλέξουμε αυτό το checkbox, τότε οι αλλαγές στις άδειες χρηστών θα εφαρμοστούν σε όλους τους υποκαταλόγους του καταλόγου αυτού

Με το checkbox αυτό ενεργοποιημένο, οι άδειες θα εφαρμοστούν σε όλα τα αρχεία του καταλόγου αυτού

Η λίστα με τις προκαθορισμένες άδειες περιέχει περισσότερες επιλογές, αλλάζουμε τις άδειες σε ένα κατάλογο



Εδώ βλέπουμε να υπάρχουν δύο τμήματα αδειών. Π.χ. Change(RWXD)(RWXD). Το πρώτο αναφέρεται στις άδειες που θα ισχύουν στους υποκαταλόγους και το δεύτερο στα αρχεία του καταλόγου αυτού.

Πιο αναλυτικά, τα δύο τμήματα των αδειών (οι δύο παρενθέσεις με απλά λόγια) αναφέρονται στις άδειες που θα ισχύουν για τους υποκαταλόγους και τα αρχεία αντίστοιχα του καταλόγου του οποίου τις άδειες αλλάζουμε (στην περίπτωση μας τον C:\RepNT). Δηλαδή, έστω ότι η ομάδα χρηστών SYSTEM, είχε τις εξής ειδικές άδειες πρόσβασης: Special Access (RX)(R). Αυτό σημαίνει τα εξής:

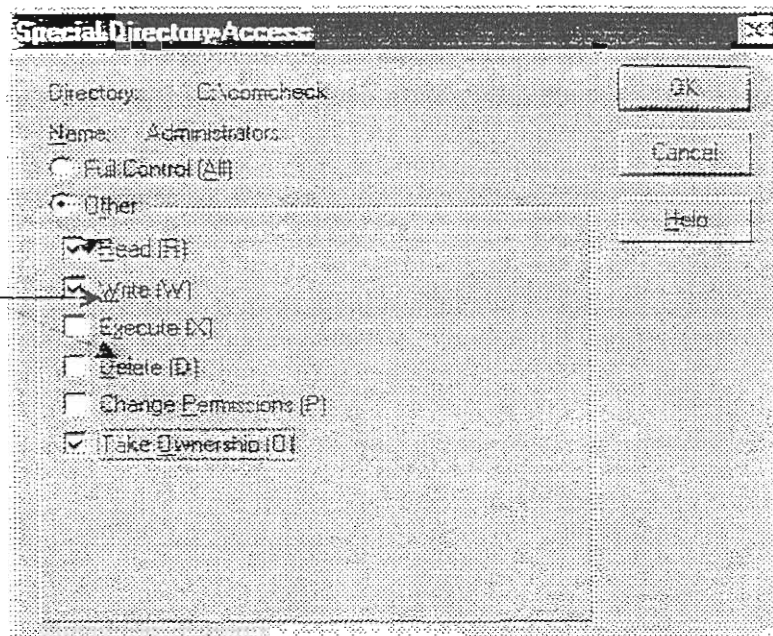
1. Ότι οι χρήστες της ομάδας SYSTEM μπορούν μόνο να διαβάσουν (R), και να εκτελέσουν (X) τα περιεχόμενα του καταλόγου αυτού.
2. Έχουν δικαίωμα να διαβάσουν μόνο τα αρχεία του (R).

Συνεχίζοντας, εάν κάνουμε διπλό κλικ επάνω σε μια ομάδα χρηστών (ή μεμονωμένο χρήστη), τότε θα οδηγηθούμε στο πλαίσιο διαλόγου εκείνο με το οποίο μπορούμε να ρυθμίσουμε ειδικά τις άδειες για τους υποκαταλόγους του συγκεκριμένου καταλόγου. Μέσα από το πλαίσιο αυτό μπορούμε να αναθέσουμε οποιονδήποτε συνδυασμό αδειών επιθυμούμε, όπως και στην προηγούμενη περίπτωση.

Αν από την άλλη θέλουμε να εμφανίσουμε το πλαίσιο ειδικών αδειών για τα αρχεία του συγκεκριμένου καταλόγου, θα πρέπει να επιλέξουμε *Special File Access...*, από την πτυσσόμενη λίστα με τις προκαθορισμένες άδειες. Ας δούμε, όμως πιο παραστατικά πως μπορούμε να επιτελέσουμε τις παραπάνω λειτουργίες:

Κάνοντας διπλό κλικ επάνω σε μια ομάδα χρηστών (ή μεμονωμένο χρήστη), τότε θα εμφανιστεί το παρακάτω πλαίσιο διαλόγου με το οποίο μπορούμε να θέσουμε τις άδειες για τους υποκαταλόγους του καταλόγου αυτού:

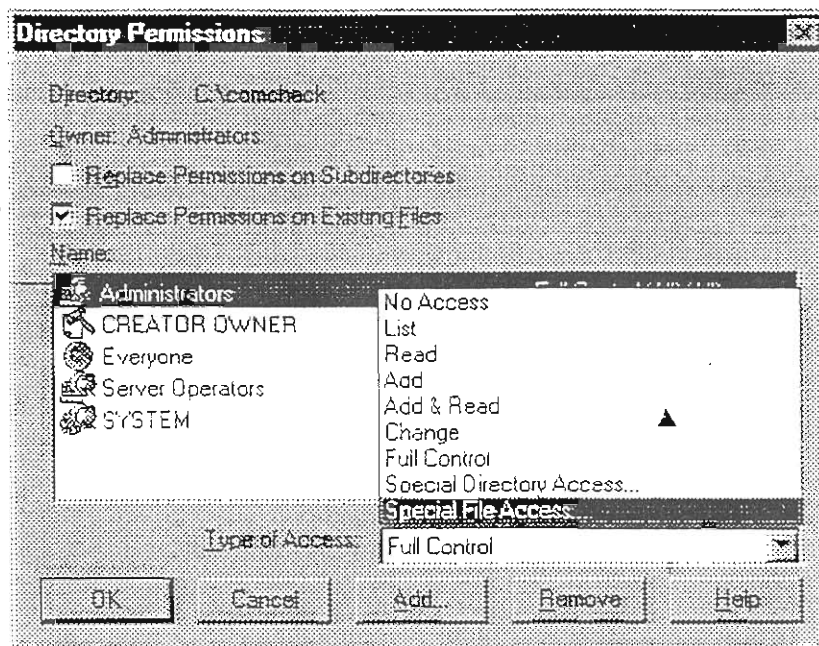
Η συγκεκριμένη ομάδα χρηστών έχει άδεια να γραφεί να διαβάσει και να αποκτά την κυριότητα τους (RWO)



Το πλαίσιο διαλόγου για τους υποκαταλόγους είναι όμοιο με εκείνο για τα αρχεία

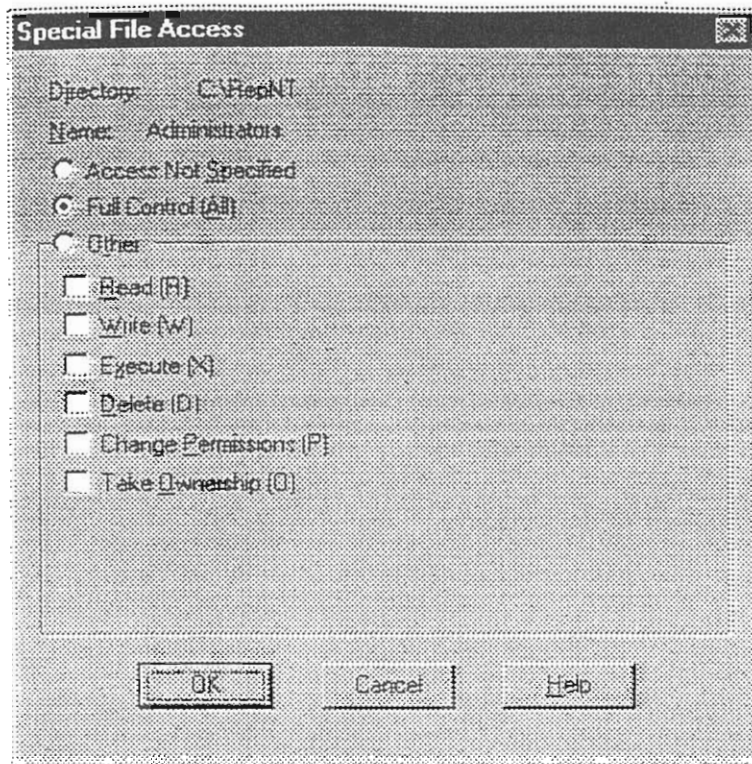
Για να θέσουμε Special Access για τα αρχεία, θα πρέπει να επιλέξουμε *Special File Access...* από την πτυσσόμενη λίστα των προκαθορισμένων αδειών. Δηλαδή:

Κάνουμε μόνο κλικ στην ομάδα χρηστών της οποίας θέλουμε να αλλάξουμε τις άδειες πρόσβασης, ώστε να την επιλέξουμε



Επιλέγουμε *Special File Access...* για να αλλάξουμε τις άδειες μία – προς – μία για τα αρχεία του υποκαταλόγου

Μόλις επιλέξουμε από την πτυσσόμενη λίστα *Special file Access...* τότε θα οδηγηθούμε στο πλαίσιο διαλόγου εκείνο με το οποίο μπορούμε να αλλάξουμε τις άδειες για τα αρχεία του καταλόγου αυτού. Δηλαδή:



Το πλαίσιο διαλόγου είναι όμοιο με
το αντίστοιχο πλαίσιο διαλόγου για
τα αρχεία.

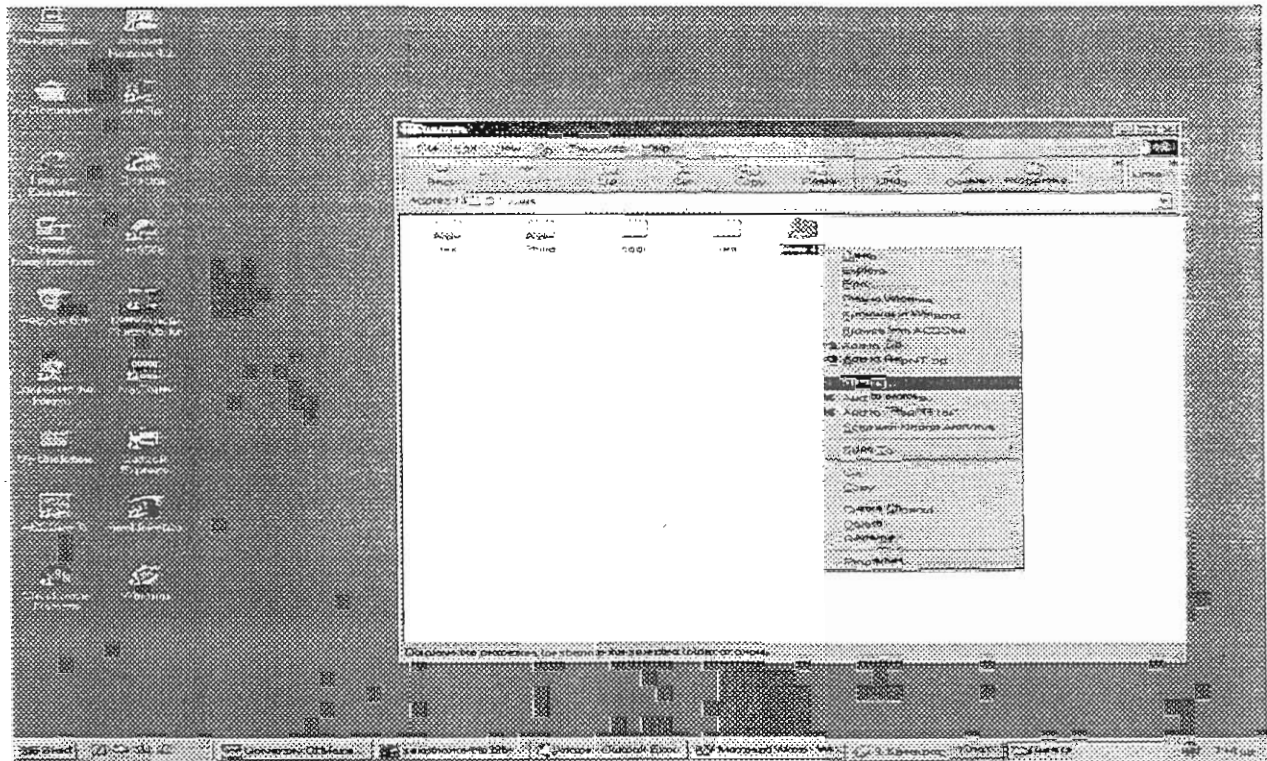
Με το πλαίσιο αυτό ο χρήστης μπορεί να αλλάζει τις άδειες των αρχείων που εμπεριέχονται στον υποκατάλογο αυτόν. Αν, επιπρόσθετα, είχε επιλέξει στο προηγούμενο πλαίσιο διαλόγου και το checkbox *Replace Permissions on SubDirectories*, τότε οι αλλαγές θα επηρεάσουν και τα αρχεία των υποκαταλόγων του καταλόγου αυτού.

ΔΙΑΜΟΙΡΑΣΜΟΣ ΚΑΤΑΛΟΓΩΝ (FOLDER SHARING)

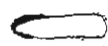
Θα κλείσουμε τη συζήτησή μας αναφερόμενοι στον τρόπο με τον οποίο μπορούμε να διαμοιραζόμαστε τους καταλόγους των υπολογιστών του δικτύου. Από τη στιγμή που δύο υπολογιστές είναι συνδεδεμένοι, είτε απευθείας είτε μέσω δικτύου, είναι δυνατό οι

κατάλογοι ενός υπολογιστή να είναι ορατοί από κάποιον άλλο και αντιστρόφως. Η υπηρεσία αυτή λέγεται File sharing και υλοποιείται ως εξής:

1. Καταρχήν, κάνουμε διπλό κλικ στο My Computer, που βρίσκεται στην επιφάνεια εργασίας μας.
2. Στη συνέχεια επιλέγουμε τον κατάλογο εκείνο τον οποίο θέλουμε να μοιραστούμε με τους υπόλοιπους υπολογιστές του δικτύου.
3. Κανούμε δεξί κλικ στον επιλεγμένο κατάλογο μας ώστε να εμφανιστεί το υπομενού και επιλέγουμε *Sharing...*

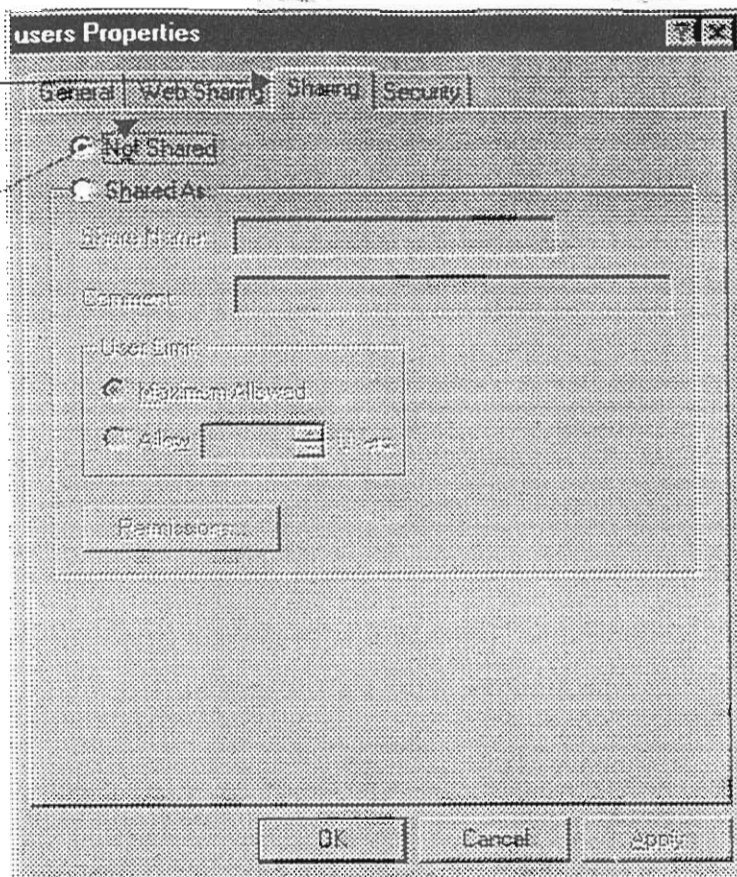


4. Θα πρέπει να εμφανιστεί το παρακάτω πλαίσιο διαλόγου:



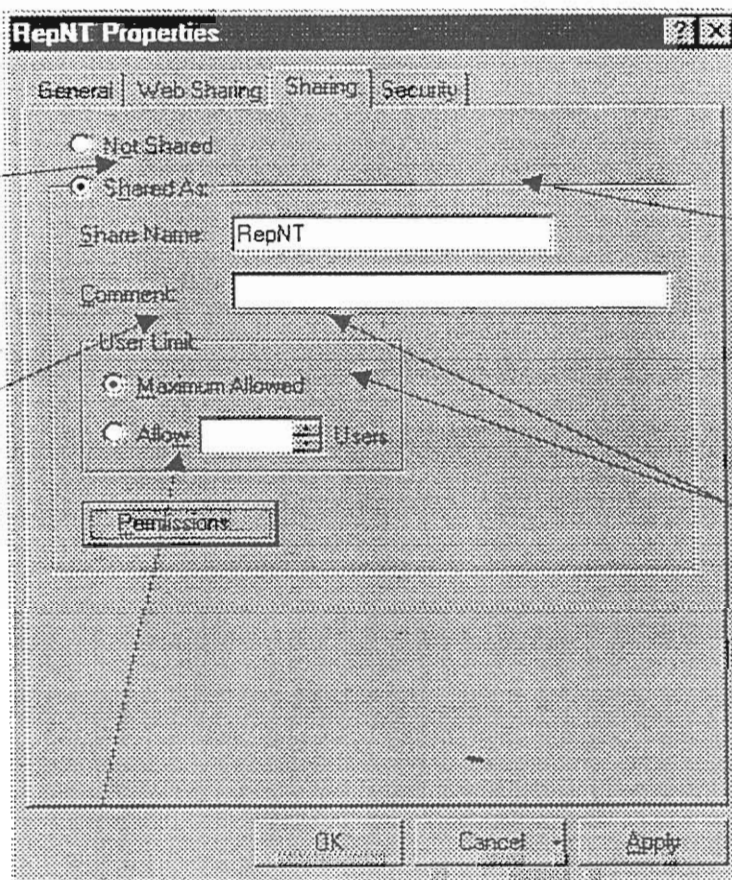
Η καρτέλα με την οποία διαχειριζόμαστε το *sharing* του καταλόγου

Ο κατάλογος αυτός δε «φαίνεται» για την ώρα στο υπόλοιπο δίκτυο



Επιλέγουμε εδώ όταν θέλουμε να διαμοιραστούμε τον κατάλόγό μας με το υπόλοιπο δίκτυο (στην περίπτωση μας είναι ο RepNT)

Όριο χρηστών που θα μπορούν να προσπελάσουν ταυτόχρονα τον κατάλογο αυτό

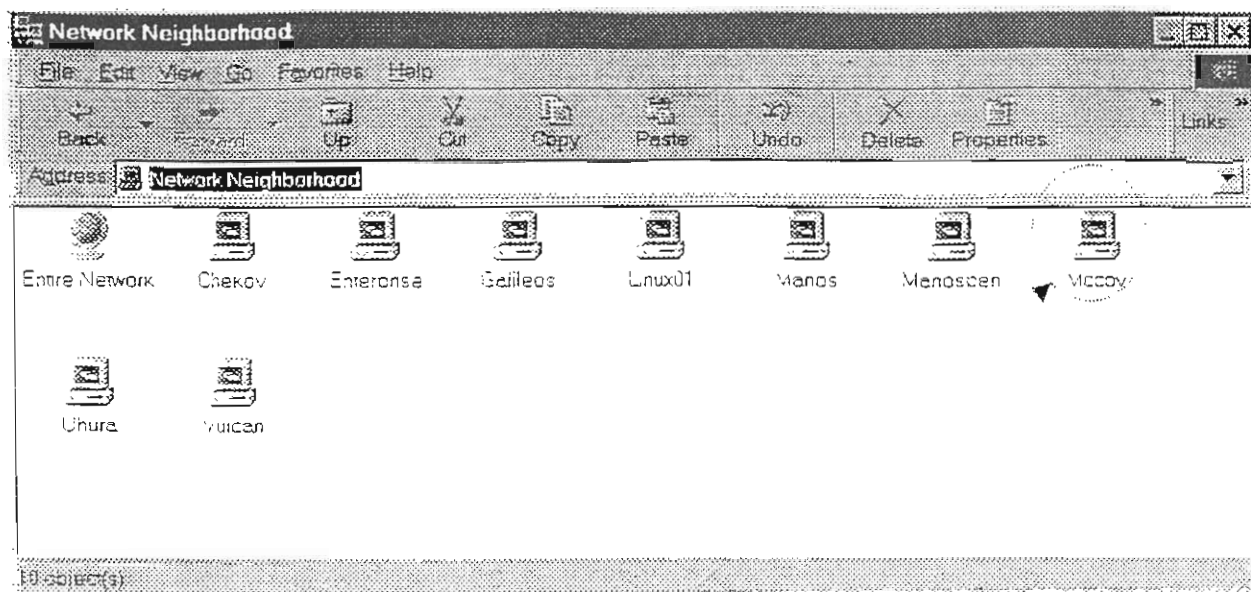


Το όνομα με το οποίο οι υπόλοιποι υπολογιστές θα μπορούν να βλέπουν τον κατάλογο αυτό (μπορούμε να προσδιορίσουμε ένα οποιοδήποτε όνομα).

Μπορούμε να προσδιορίσουμε είτε ένα μέγιστο αριθμό ταυτόχρονων προσπελάσεων είτε όσο είναι δυνατό

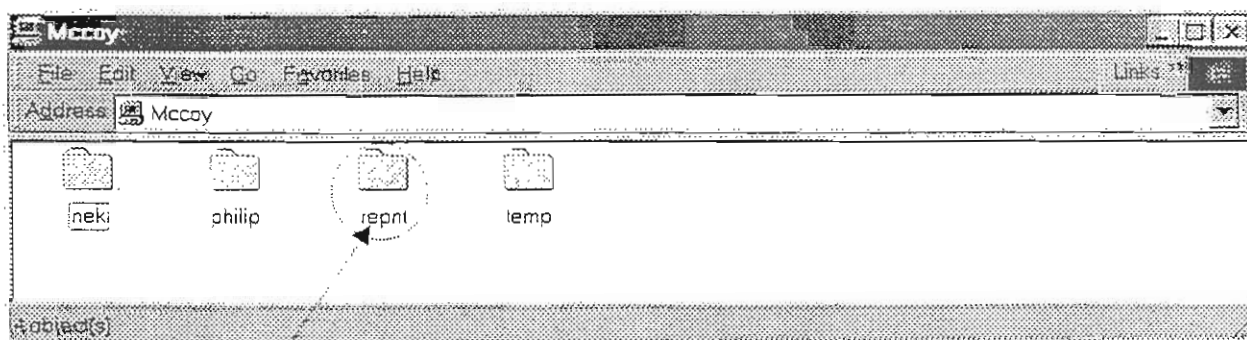
Με το πλήκτρο αυτό μπορούμε να θέσουμε τις άδειες πρόσβασης για τον κατάλογο αυτό. Η διαδικασία είναι η ίδια με την περιγραφείσα

Μόλις πατήσουμε ΟΚ, οι υπόλοιποι χρήστες του δικτύου, θα μπορούν να «βλέπουν» τον κατάλογο αυτό από τον υπολογιστή τους ως εξής:



Κάνουμε διπλό κλικ στον υπολογιστή που περιέχει
το διαμοιραζόμενο κατάλογο

Μέσα από το Network Neighborhood, από έναν οποιονδήποτε υπολογιστή, επιλέγουμε
τον υπολογιστή στον οποίο βρίσκεται ο shared κατάλογος (στην περίπτωση μας έστω ο
Mccoy) και μετά μπορούμε να προσπελάσουμε τον κατάλογο στον άλλο υπολογιστή.



Ο Shared κατάλογος RepNt

ΠΕΡΙΩΣΗ: Για να μπορεί ένας χρήστης να έχει πλήρη πρόσβαση σε ένα διαμοιραζόμενο κατάλογο (εννοώντας να μπορεί να γράψει, να διαβάσει, να διαγράψει, κλπ δεδομένα από αυτόν), θα πρέπει και να έχει δοθεί η απαραίτητη άδεια από τον κάτοχο του καταλόγου. Δεν αρκεί δηλαδή μόνο η υπηρεσία Sharing να είναι ενεργοποιημένη, αλλά να ισχύουν και οι κατάλληλες άδειες πρόσβασης στον κατάλογο αυτόν.