ΜΑΘΗΜΑ 2

ΘΕΜΑ : ΟΙ ΒΑΣΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΣΤΑ WINDOWS 2008 SERVER

ΣΚΟΠΟΣ : Να κατανοήσεις την λειτουργία των βασικών υπηρεσιών στα Windows 2008 Server.

- **Να κατανοήσεις τις υπηρεσίες:**
- **Τομέα Ενεργού Καταλόγου (AD DS)**
- **Ονομάτων Τομέα (DNS)**
- **Πρωτόκολλο Δυναμικής Διευθέτησης Υπολογιστών (DHCP)**

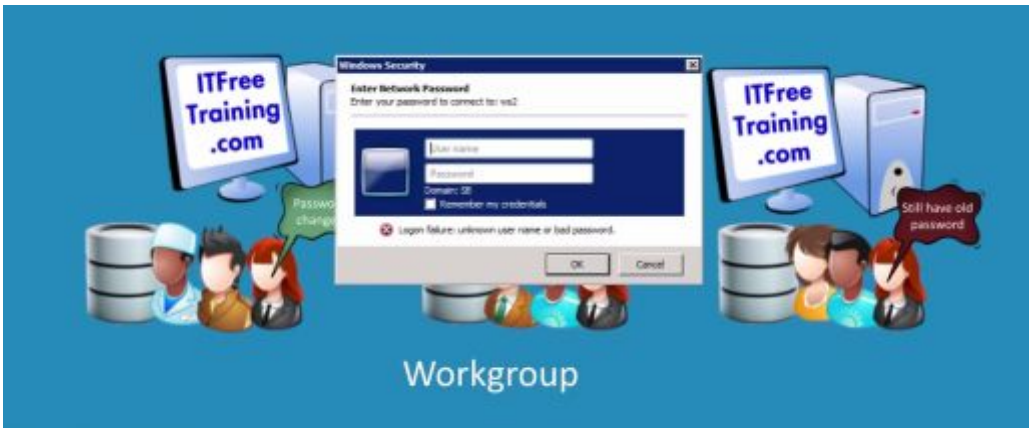
ΧΡΗΣΙΜΕΣ ΠΛΗΡΟΦΟΡΙΕΣ – ΕΛΑΧΙΣΤΕΣ ΑΠΑΙΤΟΥΜΕΝΕΣ ΓΝΩΣΕΙΣ

Ο ΕΝΕΡΓΟΣ ΚΑΤΑΛΟΓΟΣ (ACTIVE DIRECTORY)

1. **Τι είναι ο Ενεργός Κατάλογος**

Για την ιστορία ο Ενεργός Κατάλογος, εμφανίστηκε για πρώτη φορά στα Windows 2000 Server και από τότε αποτελεί την καρδιά των λειτουργικών Server της Microsoft. Με τα πιο λίγα και απλά λόγια θα μπορούσαμε να πούμε ότι ο Ενεργός κατάλογος είναι μια μεγάλη και **δυναμική βάση δεδομένων**. Οι Υπηρεσίες Ενεργού Καταλόγου Τομέα (Active Directory Domain Services) όπως είναι η πλήρη ονομασία τους, παρέχουν την λειτουργικότητα που απαιτείται για την αποθήκευση πληροφοριών σχετικά με χρήστες , υπολογιστές, εκτυπωτές και γενικά όλους τους πόρους ενός δικτύου, και διαθέτει κεντρικά αυτές τις δυνατότητες σε όλα τα αντικείμενα του δικτύου, με βάση τις δυνατότητες που έχει το καθένα από αυτά να τις προσπελάσει. Ας δούμε ένα παράδειγμα για να καταλάβουμε και την διαφορά που ο Ενεργός Κατάλογος δημιουργεί μεταξύ των δύο τύπων δικτύων : του ομότιμου δικτύου και του δικτύου διακομιστή – πελάτη. Έστω ότι έχουμε ένα ομότιμο δίκτυο (Workgroup) τριών Η/Υ.

Για να προσπελάσει ένας χρήστης ενός Η/Υ, έναν άλλον Η/Υ , θα πρέπει να δημιουργήσουμε τον λογαριασμό του και στον δεύτερο Η/Υ. Αν πάλι θελήσει ο ίδιος χρήστης να προσπελάσει και τον τρίτο Η/Υ , θα πρέπει και εκεί να δημιουργήσουμε τον λογαριασμό του, γιατί οι λογαριασμοί χρηστών του κάθε Η/Υ διατηρούνται στην τοπική του βάση δεδομένων. Αν τώρα ο χρήστης αυτός για κάποιο λόγο αλλάξει τον κωδικό του, δεν θα έχει πρόσβαση στους άλλους δύο Η/Υ μέχρι να πάμε στις τοπικές τους βάσεις δεδομένων και να τις ενημερώσουμε για την αλλαγή.



Αν τώρα οι Η/Υ του Workgroup γίνουν περισσότεροι τότε η κατάσταση είναι ανεξέλεγκτη.

Σε αντίθεση με αυτή την κατάσταση, που μπορεί να είναι αποδεκτή σε πολύ μικρά δίκτυα, η χρήση του Ενεργού Καταλόγου είναι μονόδρομος για μεσαία και μεγάλα, ειδικά εταιρικά δίκτυα, γιατί ο Ενεργός Κατάλογος:

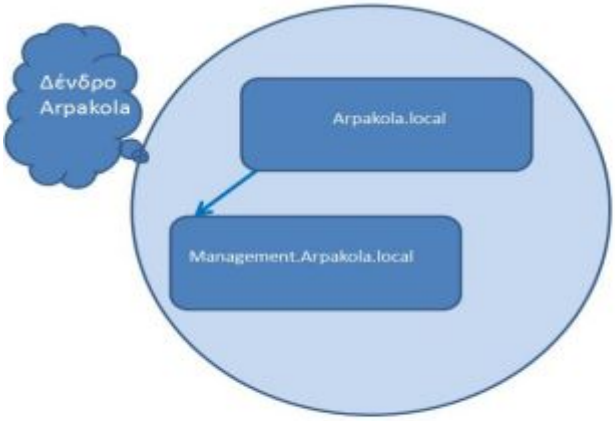
- Είναι μια κεντρικά ελεγχόμενη δυναμική βάση δεδομένων.
- Ενημερώνεται και ενημερώνει για κάθε αλλαγή που αφορά κάθε αντικείμενο (object) του δικτύου.
- Διανέμει τους πόρους του δικτύου σε κάθε αντικείμενο σύμφωνα με τις δυνατότητες προσπέλασης που έχουν οριστεί για αυτό.
- Διαμορφώνεται σε αυτόν και εφαρμόζεται κεντρικά η όποια πολιτική του δικτύου.
- Στηρίζει την λειτουργία πλήθους υπηρεσιών του δικτύου (π.χ. email).

ΤΟΜΕΑΣ (DOMAIN)

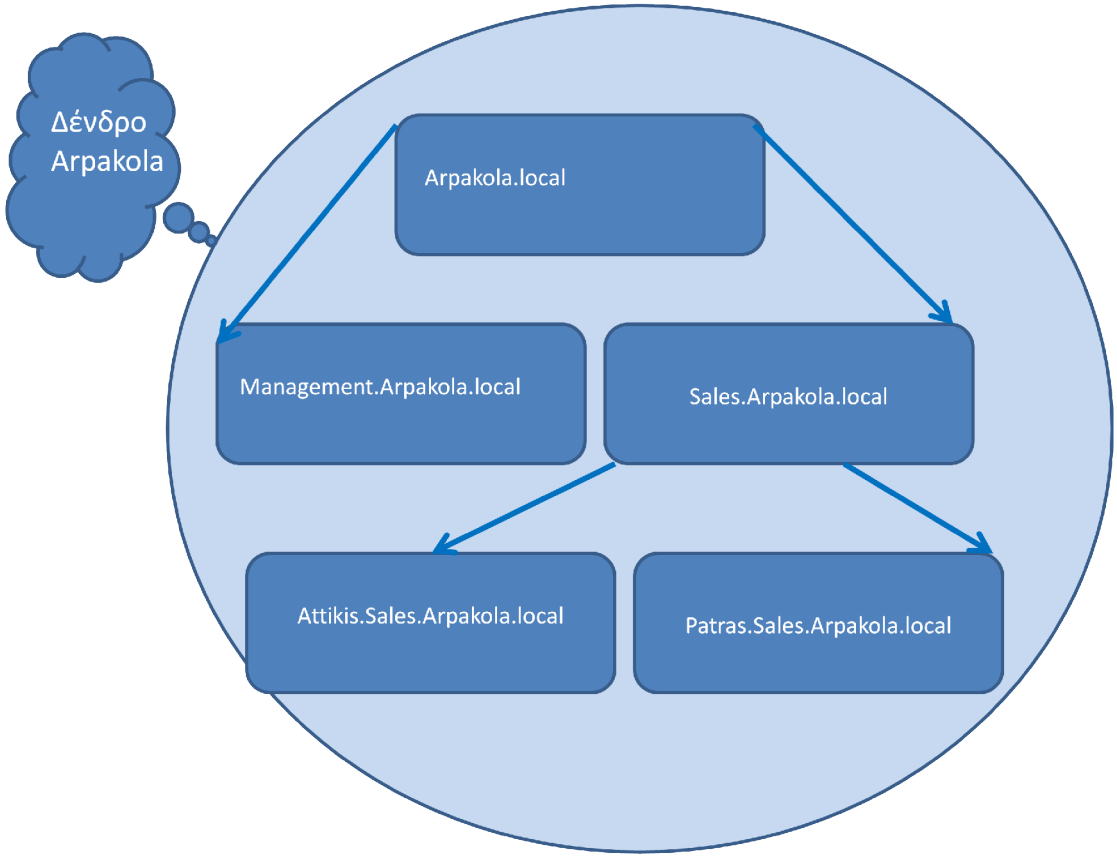
Με τον όρο Τομέας (Domain), σε ένα δίκτυο ονομάζουμε ένα λογικό σύνολο Η/Υ που μοιράζονται την ίδια βάση δεδομένων (το ίδιο Active Directory) και έχουν κοινό «χώρο» ονόματος (namespace). Έστω στο δίκτυο που θα δημιουργήσετε και θα ονομάσετε τον Τομέα: Arpakola.local, θα υπάρχουν άλλοι δύο Η/Υ που θα ανήκουν σε αυτό το δίκτυο με Computer Name : Mitsos και Kitsos. Τότε οι Η/Υ Mitsos και Kitsos, θα μοιράζονται το Active Directory του Domain Arpakola και τα πλήρες όνοματά τους (Full Computer Name) θα είναι : Mitsos.Arpakola.local και αντίστοιχα Kitsos.Arpakola.local. Το ίδιο θα συμβαίνει και για όποιον άλλο Η/Υ θα ανήκει στο δίκτυο αυτό.

ΔΑΣΗ (FOREST) **ΚΑΙ ΔΕΝΔΡΑ** (TREES)

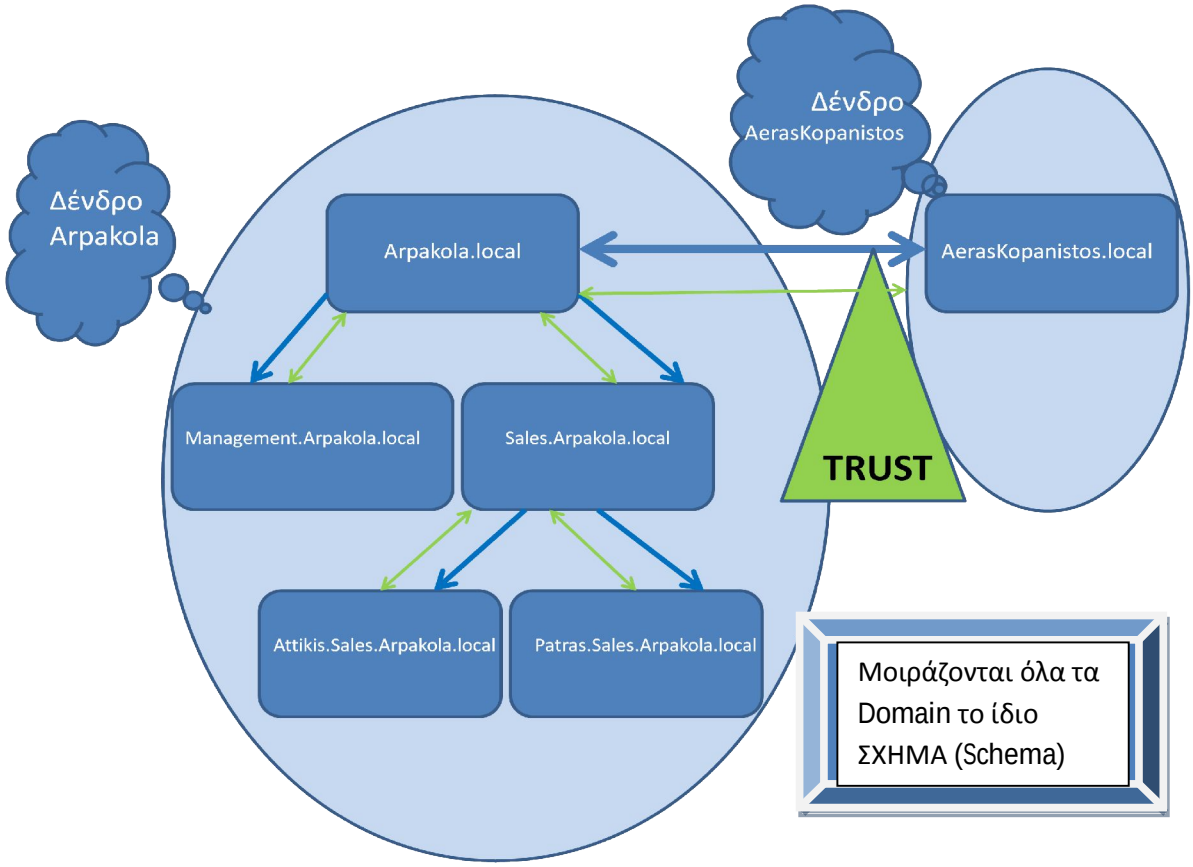
Ιδανική και απλοποιημένη κατάσταση και στην εγκατάσταση αλλά και στην διαχείριση είναι σε ένα εταιρικό τοπικό δίκτυο, να υπάρχει ένας Τομέας (αυτό συνήθως συμβαίνει). Σε κάποιες περιπτώσεις όμως μεγάλων τοπικών δικτύων ή ακόμα περισσότερο διαδικτυακών δικτύων δεν συμβαίνει κάτι τέτοιο. Έστω λοιπόν ότι στο παράδειγμά μας η εταιρεία Aprakola απαιτεί ένα διαφορετικό Τομέα για τους ανθρώπους της Διοίκησης. Θα ονομάσουμε το νέο Domain: Management και θα το δημιουργήσουμε κάτω από την εταιρεία Arpakola. Αυτό το σχήμα (Schema) που δημιουργήθηκε ονομάζεται δένδρο Τομέα.



Ο Τομέας Arpakola.local σε συτή τη περίπτωση είναι ο γονικός τομέας (parent domain) ενώ ο Τομέας Management.Arpakola.local είναι ο θυγατρικός (child domain). Μεταξύ τους αυτόματα υπάρχει σχέση εμπιστοσύνης και οι δύο domain controller συνεργάζονται. Αυτή η κατάσταση μπορεί να επεκταθεί κατά το δοκούν και να καταλήξει και με άλλους Τομείς σε δενδροειδή σχέση όπως περίπου στο παρακάτω σχήμα, στο οποίο προστέθηκε ακόμα ένας θυγατρικός Τομέας της Arpakola, αυτός των Πωλήσεων (Sales), ο οποίος με την σειρά του δημιούργησε δύο δικούς του θυγατρικούς αυτόν των Πωλήσεων στην Αττική (Attikis.Sales.Arpakola.local) και αυτόν στην Πάτρα (Patras.Sales.Arpakola.local). Αν ο Η/Υ Mitsos είναι στις πωλήσεις της Αττικής τότε το πλήρες όνομά του θα είναι: Mitsos.Attikis.Sales.Arpakola.local. Σε αυτή τη περίπτωση εννοείται ότι το κάθε Domain έχει το δικό του Active Directory με τον δικό του Domain Controller (DC).



Και εκεί που νομίζουμε ότι όλα είναι στη θέση τους με ένα δέντρο και πέντε τομείς, ανακοινώνεται ότι εξαγοράστηκε η εταιρεία του κάτω ορόφου: η AerasKopanistos που ήδη διαθέτει το δικό της ομώνυμο Domain και θα πρέπει να ενσωματωθεί στο δένδρο της Arpakola. Σε αυτή την περίπτωση δημιουργείται η σχέση εμπιστοσύνης μεταξύ των δύο δένδρων και έχουμε την δημιουργία του δάσους (forest). Συνολικά λοιπόν το σχήμα έχει 1 Forest, 2 Trees και 6 Domains.



Με τις σχέσεις εμπιστοσύνης σε αυτές τις πολύπλοκες καταστάσεις οι χρήστες του κάθε domain μπορούν να έχουν πρόσβαση σε πόρους οποιουδήποτε άλλου domain στο ίδιο σχήμα (Schema). Απαραίτητη προϋπόθεση σε αυτή την περίπτωση οι Domains Controllers να είναι Καθολικού Καταλόγου (Global Catalog). Οι διακομιστές Καθολικού Καταλόγου διαθέτουν εξ ορισμού ευρετήριο (Index) όλων των αντικειμένων του Δάσους (για παράδειγμα για το σύνολο των εκτυπωτών των Domain).

ΥΠΗΡΕΣΙΑ ΟΝΟΜΑΤΩΝ ΤΟΜΕΑ (Domain Name Services)

Το DNS με απλά λόγια μπορούμε να πούμε ότι είναι μια υπηρεσία ανάλυσης ονομάτων, η οποία αντιστοιχίζει ονόματα Η/Υ σε διευθύνσεις IP. Με το DNS, ένα πλήρως προσδιορισμένο όνομα Η/Υ, όπως για παράδειγμα το Mitsos.Arpakola.local, μπορεί να αναλυθεί σε μια διεύθυνση IP που δίνει στους Η/Υ την δυνατότητα να εντοπίζουν ο ένας τον άλλο. Το DNS σχεδιάστηκε έτσι ώστε να λειτουργεί μέσα από το πρωτόκολλο TCP/IP, και στις εκδόσεις των Windows Server (μετά τα 2000 Server) να μπορεί να ενοποιηθεί και να συνεργαστεί με κρίσιμες υπηρεσίες, όπως τις AD DS και την DHCP.

Το DNS οργανώνει ομάδες Η/Υ σε τομείς (domains) σε ιεραρχική δομή σε εταιρικό επίπεδο (για τα LAN) είτε σε επίπεδο διαδικτύου (για τα WAN). Τα διάφορα επίπεδα αυτής της ιεραρχίας προσδιορίζουν:

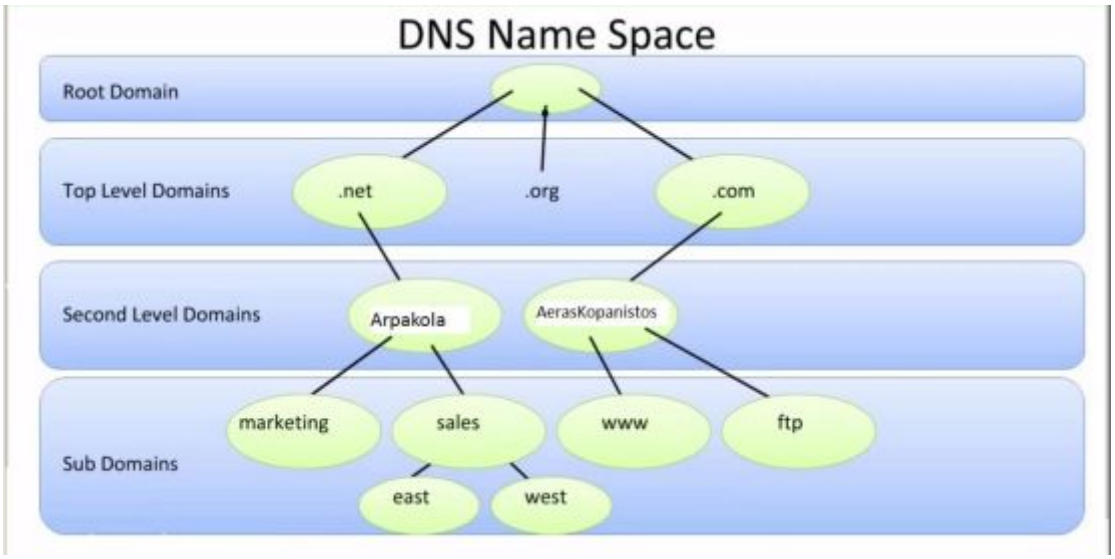
- μεμονωμένους Η/Υ
- Οργανωτικούς Τομείς
- Τομείς ανωτάτου επιπέδου

Έτσι σε ένα τοπικό δίκτυο για τον Η/Υ: Mitsos.Arpakola.local, το Mitsos είναι το όνομα Η/Υ, το Arpakola είναι ο Οργανωτικός Τομέας και το local ο Τομέας Ανώτατου επιπέδου. Αντίστοιχα αν ο Mitsos ανήκε σε ένα διαδικτυακό δίκτυο και το πλήρες όνομά του ήταν Mitsos.Arpakola.com , τότε το com θα ήταν ο τομέας Ανωτάτου επιπέδου και πάλι το Arpakola ο Οργανωτικός Τομέας ενώ το όνομα Η/Υ θα ήταν Mitsos. Στο διαδίκτυο, σε ακόμα υψηλότερο επίπεδο, βρίσκονται οι DNS Servers Υποδείξεων Ρίζας (Root Hints), που είναι παγκοσμίως συνολικά 13, όπως φαίνονται στον πίνακα που ακολουθεί και είναι υπεύθυνοι για την παγκόσμια διαχείριση των ζωνών DNS και της απόδοσης των διεθνών καταλήξεων είτε μορφών είτε χωρών (πχ : .com - .org - .gr - .us κλπ).

Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC

Hostname	IP Addresses	Manager
l.root-servers.net	199.7.83.42, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Κάτω βέβαια από τον δικό σας Οργανωτικό Τομέα (parent domain, πχ Arpakola), μπορείτε να δημιουργήσετε όσους τομείς εσείς κρίνετε απαραίτητους (child domain πχ Sales.Arpakola).



Το AD DS και το DNS είναι αλληλένδετα σε βαθμό που πρέπει πρώτα να εγκατασταθεί το DNS για να είναι εφικτή η εγκατάσταση του AD DS.

Τα Windows 2008 Server, δίνουν την δυνατότητα Πλήρους και Μερικής ενοποίησης των AD DS και DNS. Στην περίπτωση Μερικής ενοποίησης, οι πληροφορίες DNS αποθηκεύονται σε αρχεία κειμένου με κατάληξη .dns στον φάκελο %SystemRoot%\System32\Dns και οι ενημερώσεις τους γίνονται μόνο από τον Πρωτεύοντα Διακομιστή DNS (Primary DNS Server) και θα πρέπει οι Η/Υ που τον χρησιμοποιούν και παίρνουν δυναμικές IP μέσω DHCP υπηρεσίας, να έχουν διευθετηθεί ώστε να χρησιμοποιούν αυτόν τον Primary DNS Server. Αν ο Primary DNS Server δεν ανταποκρίνεται, τότε σταματά και η απόδοση διευθύνσεων από την DHCP υπηρεσία.

Αντίθετα με την Πλήρη ενοποίηση AD DS και DNS οι πληροφορίες και τα αρχεία DNS αποθηκεύονται μέσα στον Ενεργό Κατάλογο και είναι τμήμα αυτού. Το γεγονός αυτό δημιουργεί μια σειρά πλεονεκτημάτων και καθιστά την Πλήρη ενοποίηση των υπηρεσιών AD DS και DNS ενδεδειγμένη μέθοδο.

ΠΡΩΤΟΚΟΛΛΟ ΔΥΝΑΜΙΚΗΣ ΔΙΕΥΘΕΤΗΣΗΣ ΥΠΟΛΟΓΙΣΤΩΝ (Dynamic Host Configuration Protocol)

Το πρωτόκολλο DHCP είναι ένα κεντρικό σημείο απόδοσης και ελέγχου της διευθυνσιοδότησης IP και όχι μόνο. Εκτός από την IP διεύθυνση παρέχει και άλλες πληροφορίες στους πελάτες του δικτύου, όπως η μάσκα υποδικτύου (Subnet Mask) και η προεπιλεγμένη πύλη (Default Gateway). Σκεφτείτε την υπηρεσία DHCP σαν ένα καλάθι, μια δεξαμενή (pool) που περιέχει ένα πλήθος διευθύνσεων IP. Όταν ξεκινά ένας Η/Υ του δικτύου, αναζητά μια IP διεύθυνση, την οποία του την παρέχει ο διακομιστής DHCP, ο οπίος σε δίκτυα φυσιολογικού μεγέθους είναι συνήθως ο Ελεγκτής Τομέα (Domain Controller), αλλιώς κάποιος ανεξάρτητος διακομιστής εκτελεί την DHCP υπηρεσία (DHCP Server). Η IP «βγαίνει» από την δεξαμενή και αποδίδεται στον Η/Υ που την ζήτησε με μίσθωση συγκεκριμένου χρόνου (lease). Όταν ο χρόνος αυτός καταναλωθεί στο 50%, ο πελάτης Η/Υ κάνει αίτημα ανανέωσης και αν αυτό δεν συμβεί, επαναλαμβάνει την προσπάθεια πριν την λήξη του χρόνου. Οι διευθύνσεις IP που για οποιοδήποτε λόγο δεν ανανεώνονται, επιστρέφουν στην δεξαμενή. Αν ο Η/Υ πελάτης δεν βρει διαθέσιμο DHCP Server να ανανεώσει την διεύθυνση IP του, ή δεν πάρει νέα IP, τότε γίνεται αυτόματη διευθέτηση της IP, μέσα από την περιοχή 169.254.0.0 σε κλάση Β (μάσκα υποδικτύου : 255.255.0.0) που είναι δεσμευμένη από την Microsoft για τέτοιες περιπτώσεις.