Οδηγός Διαχειριστή

Ubuntu 6.06

Copyright (c) Δαγκουλής Γιάννης, Κολλαλάς Σταύρος, Μελαδιανός Χρήστος.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover
Texts. A copy of the license is included in the section entitled "GNU
Free Documentation License".

Κατάλογος περιεχομένων

Οδηγός Διαχειριστή....1
Ubuntu 6.06....1
Εγκατάσταση & Διαχείριση DNS Server....5
Εισαγωγή....5
Η λειτουργία του DNS....7
Η ιεραρχική δομή του DNS....7
Οι Εγγραφές Πόρων (Resource Records)....7
Ανάθεση Διαχείρισης (Delegation)....8
Τύποι Εξυπηρετητών Ονομάτων....8
Τα Δεδομένα....8
Η διαδικασία του resolution....8
Εγκατάσταση του BIND στο UBUNTU....10
Διαχείριση της Υπηρεσίας DNS....12
SOA (Start Of Authority)....12
NS (Name Server)....14
Address και CNAME....14
PTR....14
MX....15
Η διεύθυνση loopback....15
Ρυθμίσεις DNS Server μέσω Webmin....16
Gateway-Firewall-NAT....19
Ubuntu Repositories @ home....23
Proxy Server (Squid server)....25
Εγκατάσταση και Διαχείριση του squid Proxy Server 25
Εισαγωγή....25
Εγκατάσταση του Squid στο LINUX , διανομή ubuntu....26
Βασικές λειτουργίες μέσω του script που βρίσκεται στη διαδρομή /etc/init.d/squid27
Άλλες λειτουργίες μέσω παραμέτρων του προγράμματος squid: 27
Ρύθμιση των τερματικών....28
Η Διάφανη Πληρεξουσιοδότηση (Transparent Proxy) 28
Διαχείριση του Squid....28
Λάθη λογικής....33
ΒΙΒΛΙΑ ΚΑΙ FAQ ΣΤΟ ΙΝΤΕΡΝΕΤ....33
Παράρτημα 34
ACL elements....34
Access Lists....34
DHCP SERVER....35
Εγκατάσταση και ρυθμίσεις DHCP Server στο Linux , διανομή Ubuntu....35
Ρύθμιση του Server....35
SambaPDC Server....38
Εισαγωγή....38

Postfix MTA....46
Εισαγωγή – Το Ηλεκτρονικό Ταχυδρομείο....46
Εγκατάσταση – Πρώτες Ρυθμίσεις....47
Primary Domain Controller LDAP σε λειτουργικό σύστημα Linux....52
Διανομή Ubuntu (6.06 LTS) Server (Έκδοση 1)....52
Εισαγωγή....52
Σημερινή κατάσταση....52
Τι είναι το LDAP....53
Πως λειτουργεί ο LDAP Server....53
Εγκατάσταση....53
Προγράμματα εγκατάστασης....53
Βήμα 1 Εγκατάσταση του DNS Server....53
Βήμα 2 Εγκατάσταση Apache2 Web Server....53
Βήμα 3 Εγκατάσταση του LDAP Server....54
Τι θα αλλάξουμε στο slapd.conf....58
Βήμα 4 Εγκατάσταση του εργαλείου PhpLdapadmin....59
Δομή δέντρου του καταλόγου LDAP και Schemas....61
Αρχεία ldif....62
Καταχώρηση πρώτων εγγραφών....62
Βήμα 5 Εγκατάσταση Samba 66
Βήμα 6 Client authentication (Πιστοποίηση πελάτη)....71
GNU Free Documentation License....74

Εισαγωγή

Ο παρών οδηγός απευθύνεται σε διαχειριστές δικτύων που σκοπεύουν να χρησιμοποιήσουν τις δυνατότητες που παρέχει το Ubuntu 6.06 (LTS) ώστε να προσφέρουν υπηρεσίες δικτύου. Σκοπός του είναι εύκολη και ουσιώδης κατανόηση άρα και χρήση των υπηρεσιών που παρέχονται από έναν server σε ένα σύγχρονο τοπικό δίκτυο και ιδιαίτερα στο σχολικό δίκτυο σε επίπεδο σχολικής μονάδας.

Θέμα	***Συγγραφέας***
Εγκατάσταση & Διαχείριση DNS Server	*Κολαλάς Σταύρος-Μελαδιανός Χρήστος*
Gateway-Firewall-NAT	*Κολαλάς Σταύρος*
Ubuntu Repositories @ home	*Κολαλάς Σταύρος*
Proxy Server (Squid server)	*Μελαδιανός Χρήστος*
DHCP Server	*Μελαδιανός Χρήστος*
SambaPDC Server	*Κολαλάς Σταύρος*
Postfix	*Κολαλάς Σταύρος*
LDAP Server	*Δαγκουλής Γιάννης*

Εγκατάσταση & Διαχείριση DNS Server

Εισαγωγή

Όποιος έχει χρησιμοποιήσει το Διαδίκτυο για οποιοδήποτε σκοπό (ιστός, ηλεκτρονική αλληλογραφία κλπ.) έχει αναγκαστικά χρησιμοποιήσει και μία υπηρεσία που όσο απαραίτητη είναι, άλλο τόσο παρεξηγημένη είναι: το Domain Name Service - DNS. Κι αυτό διότι οι υπολογιστές που είναι δικτυωμένοι επικοινωνούν μεταξύ τους με αριθμούς και όχι ονόματα. Αλλά είναι σαφώς ευκολότερο να θυμόμαστε το www.firiki.gr παρά το 192.168.0.11 π.χ. Τη διαδικασία αντιστοίχισης του ονόματος (address) www.firiki.gr στον αριθμό (IP address) 192.168.0.11 την αναλαμβάνει ο DNS server.

Ουσιαστικά, η συγκεκριμένη υπηρεσία είναι μια βάση δεδομένων που διατίθεται στο Διαδίκτυο. Έτσι δίνεται η δυνατότητα να λαμβάνει κάποιος πληροφορίες απο παντού.

Επίσης δίνεται η δυνατότητα να μοιράζεται ο φόρτος εργασίας σε πολλά και όχι σε ένα συγκεκριμένο μηχάνημα., ακολουθώντας μια ιεραρχική δομή. Το λογισμικό του διακομιστή έχει τη δυνατότητα να μοιράζει πληροφορίες από έναν υπολογιστή σε άλλους. Για να γίνει αυτό, το λογισμικό διαχείρισης που εξετάζουμε (BIND – Berkeley Internet Name Domain) ψάχνει σε ορισμένους υπολογιστές για να ξεκινήσει την αναζήτηση της ιεραρχίας.

Οι πιο πρόσφατη έκδοση είναι η 9.3.2 και παρέχεται δωρεάν από το ISC (Internet Systems Consortium – http://www.isc.org). Οι εκδόσεις ξεκινήσαν με τη σειρά 4, ακολούθησε η σειρά 8 και τώρα η σειρά 9. Για αυτούς που χρησιμοποιούν ακόμα τη σειρά 4 και είναι αδύνατη η αναβάθμιση σε σειρά 8 ή 9, προτείνεται η 4.9.11. Η σειρά 8 είναι ακόμα εξαιρετικά δημοφιλής, ενώ η σειρά 9 εκτός από κάποια παραπάνω χαρακτηριστικά χρησιμοποιείται επίσης στους λεγόμενους forwarders (servers που προωθούν απλά αιτήματα και δεν δίνουν πληροφορίες)

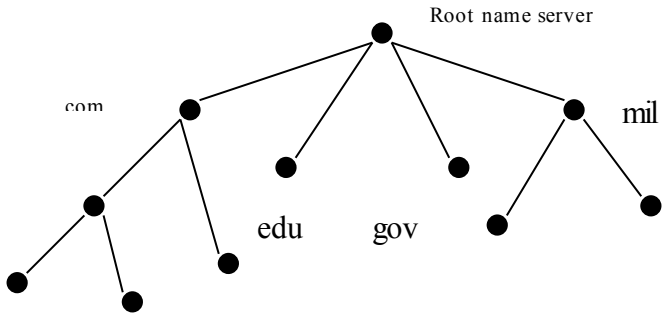
Για να καταλάβουμε την λειτουργία της υπηρεσίας, πρέπει να θυμηθούμε ορισμένα στοιχεία του ARPAnet (το DNS σχεδιάστηκε να εξυπηρετεί το ARPAnet). Το ARPAnet είναι ένα Wide Area Network – WAN που σχεδιάστηκε, για στρατιωτικούς σκοπούς αρχικά, στην Αμερική στα τέλη της δεκαετίας του 60, ώστε να είναι εφικτή η επικοινωνία, ο διαμοιρασμός πόρων και η ανάπτυξη εφαρμογών σε δικτυωμένους υπολογιστές. Αργότερα εμφανίστηκε και το πρωτόκολλο TCP/IP που κυριάρχησε σαν πρωτόκολλο επικοινωνίας μεταξύτων υπολογιστών του ARPAnet. Με τη διάθεση του BSD (δωρεάν έκδοση του UNIX για εκπαιδευτικά ιδρύματα) έγινε εφικτή η δικτύωση σημαντικά μεγάλου αριθμού υπολογιστών μέσα από το προϋπάρχον ARPAnet. Έτσι δημιουργήθηκε ένας κορμός (backbone) αρκετών χιλιάδων υπολογιστών μέσα στο ARPAnet (που μέχρι τότε αριθμούσε μερικές δεκάδες υπολογιστές) δικτυωμένων μεταξύ τους μέσω του TCP/IP. Οι ολοένα αυξανόμενοι αριθμοί ανάπτυξης έφεραν το σημερινό Διαδίκτυο: εταιρίες που ενώνουν όλα τα υπόλοιπα τοπικά δίκτυα, βασισμένα στο ARPAnet.

Στην αρχή όλες οι πληροφορίες βρίσκονταν σε ένα αρχείο στον Οργανισμό Κεντρικής Διαχείρισης της υπηρεσίας Name Service (Internic) και όποιο μηχάνημα ήθελε να ενημερωθεί έπαιρνε ένα αντίγραφο του αρχείου αυτού. Με την εμφάνιση όμως του TCP/IP, δημιουργήθηκαν

ορισμένα πολύ σοβαρά προβλήματα:

- Το κόστος σε επίπεδο δικτυακών πόρων της υπεύθυνης εταιρείας για τον διαμοιρασμό του πρωτότυπου αρχείου μεγάλωσε υπερβολικά αφού οι υπολογιστές που ζητούσαν αντίγραφο αυξάνονταν συνεχώς
- Δύο υπολογιστές μέσα στο πρωτότυπο αρχείο δεν μπορούσαν να έχουν το ίδιο όνομα. Η εταιρεία όμως δεν μπορούσε να ελέγξει την αντιστοιχία ονόματος – διεύθυνσης και ολόκληρο το σχήμα δεν προχωρούσε ομαλά.
- Ο διαμοιρασμός του πρωτότυπου αρχείου σε πολλούς υπολογιστές ήταν ασύμφορος. Μέχρι το αρχείο να φτάσει στον πιο απομακρυσμένο υπολογιστή του δικτύου κάποια αλλαγή είχε γίνει στο πρωτότυπο.

Με άλλα λόγια, η αναπάντεχη και γρήγορη ανάπτυξη του δικτύου ARPAnet οδήγησε στην απενεργοποίησή του αρχικού σχεδιασμού του. Η λύση ήρθε με την εμφάνιση της υπηρεσίας Name Service και τους Εξυπηρετητές της (Name Servers). Βασισμένα στην αρχιτεκτονική Πελάτη – Εξυπηρετητή (client – server) έχουν πλέον ένα μικρό μέρος της ευθύνης ονοματοδοσίας που κανονικά θα είχε ολόκληρη η βάση. Οι πελάτες (resolvers) στέλνουν πλέον ερωτήματα στους εξυπηρετητές. Η δομή του DNS είναι αντεστραμμένο δέντρο με κάθε κόμβο να έχει πληροφορίες για τη θέση του σε σχέση με τον γονέα του. Έχει κρατηθεί κάποιος κόμβος ως ριζικός κόμβος (root node) και από εκεί αρχίζει η ανάπτυξη του δέντρου. Κάθε κόμβος μπορεί να είναι ριζικός για μια υποϊεραρχία. Αυτό ονομάζεται domain. Κάτω από έναν τέτοιο κόμβο (domain) μπορούν να υπάρχουν άλλοι κόμβοι που να ορίζουν ιεραρχικά άλλες περιοχές οι οποίες όμως εξακολουθούν να είναι και κάτω από τον κόμβο – ρίζα του domain. Αυτό ονομάζεται υποπεριοχή (subdomain).



Κάθε domain στο δέντρο έχει μοναδικό όνομα. Δηλαδή, το όνομά του καθορίσει και τη θέση του. Όπως ένα μονοπάτι καθορίζει τη θέση ενός αρχείου μέσα στο λειτουργικό σύστημα ενός υπολογιστή. Στο DNS η διαχείριση κάθε domain γίνεται από διαφορετικό οργανισμό που είναι υπεύθυνος για τα στοιχεία της περιοχής του. Επίσης κάθε οργανισμός μπορεί να δημιουργήσει νέες ιεραρχίες και να μοιράσει την ευθύνη σε άλλους. Η σχέση τους τότε θα είναι αυτή του πρόγονου – απόγονου στην ιεραρχία. Για παράδειγμα το τμήμα διαχείρισης ονομάτων Internet του Ινστιτούτου Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας είναι υπεύθυνο για τη διαχείριση της ονοματοδοσίας του domain .gr αλλά έχει μοιράσει τη διαχείριση του domain .edu-net.gr στους υπεύθυνους του τελευταίου οργανισμού. Σε αυτή την περίπτωση το domain gr είναι ο πρόγονος του domain edu-net.

Τα domains είναι ο δείκτης της υπηρεσίας DNS: τα δεδομένα είναι μέρος ενός domain. Αυτό, μπορεί να περιέχει υπολογιστές (ή γενικότερα αντικείμενα δικτυωμένα) ή υποπεριοχές (subdomains). Τα δεδομένα κάθε περιοχής είναι κυρίως IP διευθύνσεις, πληροφορίες για το routing του domain. Μία ενδιαφέρουσα κατηγορία δεδομένων σε κάθε περιοχή είναι τα aliases : αποτελούν

δείκτες που στοχεύουν σε κάποια άλλη περιοχή. Για παράδειγμα, το όνομα www.edu-net.gr δείχνει στο όνομα olympus.noc.uoa.gr. Ο τελευταίος έχει την IP διεύθυνση 195.134.100.100.

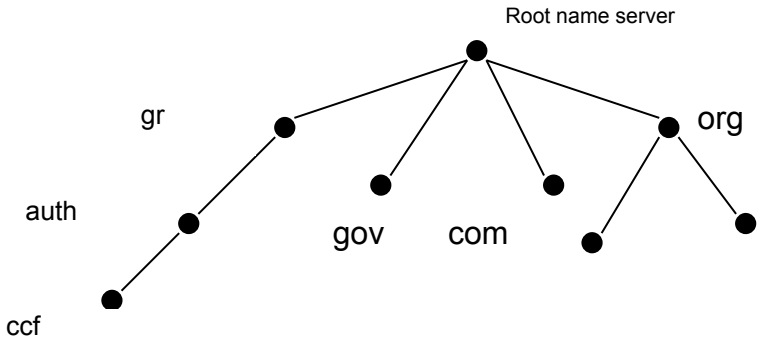
Αυτός ο περίπλοκος σχεδιασμός είναι απαραίτητος για να μην δημιουργούνται φαινόμενα σύγκρουσης ονομάτων. Για παράδειγμα, ο υπολογιστής που ονομάζεται www και βρίσκεται μέσα στο domain edu-net.gr (www.edu-net.gr) δεν είναι όμοιος με τον υπολογιστή που έχει το ίδιο όνομα αλλά είναι μέσα στο domain auth.gr (www.auth.gr). Ακριβώς το ίδιο συμβαίνει με την ιεραρχική δομή ενός λειτουργικού συστήματος: το αρχείο /usr/local/bin/run_me δεν είναι το ίδιο με το αρχείο ίδιου ονόματος αλλά διαφορετικής τοποθεσίας /usr/bin/run_me.

Η λειτουργία του DNS

Η ιεραρχική δομή του DNS

Κάθε κόμβος στο παρακάτω σχήμα έχει ένα όνομα (χωρίς τις τελείες) το οποίο μπορεί να είναι μέχρι και 63 χαρακτήρες. Το κενό όνομα είναι αφιερωμένο στη ριζική περιοχή (root domain). Το Πλήρως Πιστοποιημένο Όνομα Περιοχής κάθε κόμβου (Fully Qualified Domain Name) είναι αυτό που αρχίζει από το δικό του όνομα και καταλήγει στο root domain. Συνήθως το root domain συμβολίζεται με μια μία τελεία (.), όμως τα σύγχρονα προγράμματα που χρησιμοποιούν την υπηρεσία του DNS το προσθέτουν νοερά και έτσι ο χρήστης δεν χρειάζεται να βάζει την τελεία στο τέλος κάθε ονόματος.

Όπως έχει ειπωθεί το υποδέντρο ολόκληρης της ιεραρχίας ονομάζεται domain. Αυτό μπορεί να ανήκει σε ένα μεγαλύτερο domain ή να περιέχει μικρότερα domains. Για παράδειγμα, το domain auth βρίσκεται κάτω από το μεγαλύτερο gr και πάνω από το μικρότερο ccf.



Μέσα ,λοιπόν, σε κάθε κόμβο (domain) του δέντρου υπάρχουν πληροφορίες για όλους τους υπολογιστές που ανήκουν στη συγκεκριμένη περιοχή αλλά και δείκτες για τα μικρότερα domains. Για παράδειγμα, μέσα στην περιοχή auth.gr υπάρχουν οι υπολογιστές με ονόματα όπως www, ftp, news , mail αλλά και πληροφορίες για τις υποπεριοχές ccf.auth.gr, civil.auth.gr, math.auth.gr. Όλα αυτά αποτελούν subdomains του auth.gr και με τη σειρά τους περιέχουν ονόματα υπολογιστών όπως www.math.auth.gr, www.civil.auth.gr ή υποϊεραρχίες όπως analysis.math.auth.gr ή skyrodema.civil.auth.gr. Όπως είναι φανερό οι υπολογιστές με τις περιοχές στο ιεραρχικό σύστημα έχουν τη σχέση μιας μονάδας η οποία ανήκει σε ένα σύνολο.

Τα ονόματα των περιοχών συχνά καλούνται και ανάλογα με το επίπεδό τους. Έτσι, η ριζική περιοχή ονομάζεται περιοχή κορυφαίου επιπέδου (top level domains), η περιοχή gr (και οι ανάλογές με αυτή) πρώτου επιπέδου (first level domain) κ. ο. κ.

Οι Εγγραφές Πόρων (Resource Records)

Τα δεδομένα μέσα σε κάθε domain ,δηλαδή, οι μεμονωμένοι υπολογιστές καλούνται Εγγραφές

Πόρων (Resource Records ή πιο σύντομα RR). Αυτές οι εγγραφές χωρίζονται σε κλάσεις καθεμιά από τις οποίες έχει τους δικούς της τύπους. Με τη σειρά του ο κάθε τύπος έχει το δικό του συντακτικό. Για παράδειγμα, η πιο διαδεδομένη κλάση RRs είναι αυτή του Internet και ένας πολύ γνωστός τύπος αυτής της κλάσης είναι αυτός της διεύθυνσης (address type).

Ανάθεση Διαχείρισης (Delegation)

Ένας από τους κύριους στόχους της υπηρεσίας του DNS είναι η ανάθεση της διαχείρισης των υποϊεραρχιών. Έτσι, ο φόρτος εργασίας διανέμεται ομαλά και η υπηρεσία μπορεί να μεγαλώνει δυναμικά με πολύ γρήγορους ρυθμούς. Για παράδειγμα, οι διαχειριστές του domain gr έχούν αναθέσει τη διαχείριση του edu-net στους υπεύθυνους του έργου. Επίσης, οι υπεύθυνοι του edu-net μπορούν να διαμοιράσουν τη διαχείριση των subdomains σε άλλους. Με άλλα λόγια ο υπολογιστής που έχει μοιράσει κάποια domains περιέχει μόνο δείκτες που στοχεύουν στα μηχανήματα που είναι υπεύθυνα για αυτά τα domains και όχι τα δεδομένα τους (στην πραγματικότητα μπορεί και είναι καλό να περιέχει ένα αντίγραφο των δεδομένων) .

Τύποι Εξυπηρετητών Ονομάτων

Η υπηρεσία του DNS διακρίνει δύο είδη Name Servers : το ένα είναι master και το άλλο είναι slave. Ο master διαβάζει τα δεδομένα για τους υπολογιστές από τοπικά αρχεία ενώ ο slave μεταφέρει αντίγραφα των πρωτότυπων αρχείων μέσα από το δίκτυο. Η διάκριση ανάμεσα στα δύο είδη Name Servers είναι σχετική και όχι απόλυτη. Δηλαδή, ένας Name Server μπορεί να είναι master για κάποιες ζώνες και slave για κάποιες άλλες. Η πληροφορία για το αν ένας εξυπηρετητής είναι master ή slave για κάποια ζώνη δηλώνεται στο configuration file του. Η παλαιότερη ονομασία των εξυπηρετητών ήταν primary και secondary. Καταλαβαίνει κανείς ότι οι slaves δεν είναι εξυπηρετητές ‘δεύτερης κατηγορίας’ αλλά ίσης αξίας με τους masters. Κάθε φορά που γίνεται μια αλλαγή στα τοπικά αρχεία του master, ο τελευταίος ειδοποιεί τους slaves για τη μετατροπή και αυτοί φροντίζουν να παραλάβουν μέσα από το δίκτυο ένα αντίγραφο των νέων δεδομένων. Σε περίπτωση που ο master δεν μπορεί να εξυπηρετήσει τους resolvers (είναι οι clients στην ορολογία του Name Service) αναλαμβάνουν οι slaves name servers. Είναι ,λοιπόν, σημαντικό να διαθέτει ένας οργανισμός πάνω από έναν slave name server για μεγαλύτερη ασφάλεια.

Τα Δεδομένα

Τα αρχεία από τα οποία οι masters ‘φορτώνουν’ τις απαραίτητες πληροφορίες για τις ζώνες ονομάζονται αρχεία δεδομένων ή απλά δεδομένα. Αυτά τα αρχεία τα λαμβάνουν οι slaves μέσα από το δίκτυο. Όταν ένας slave αρχίσει να λειτουργεί επικοινωνεί με τον master και λαμβάνει αντίγραφα των δεδομένων από τον master.

Η διαδικασία του resolution

Οι Name Servers όχι μόνο μπορούν να απαντήσουν σε ερωτήματα απομακρυσμένων υπολογιστών για τα δεδομένα που οι ίδιοι κρατάνε, αλλά έχουν την ικανότητα να ψάξουν το Internet για να βρούνε κάποια πληροφορία την οποία δεν την γνωρίζουν – δεν είναι ,δηλαδή, μέσα στις ζώνες που εξυπηρετούν. Οι εξυπηρετητές χρειάζονται μόνο μία σημαντική πληροφορία για να αρχίσουν την έρευνα για κάποιο στοιχείο το οποίο δεν έχουν : τους ριζικούς εξυπηρετητές ονομάτων (Root Name Servers). Οι τελευταίοι διαθέτουν πληροφορίες για κάθε top level domain αλλά μόνο αυτές – δεν έχουν ποτέ πληροφορίες για το πού βρίσκεται κάποιο συγκεκριμένο δεδομένο. Κάθε εξυπηρετητής ονομάτων ,λοιπόν, πρέπει να έχει ένα αρχείο με όλους τους Root Name Servers (είναι δεκατρείς σε όλο τον κόσμο). Τι ακριβώς συμβαίνει κάθε φορά που ζητάτε να δείτε μια σελίδα, για παράδειγμα την www.nasa.gov στον Παγκόσμιο Ιστό;

Ο πλοηγός (browser) στον οποίο έχετε δώσει την παραπάνω διεύθυνση δεν μπορεί να βρει τον συγκεκριμένο υπολογιστή αφού δεν γνωρίζει την IP address του (θυμηθείτε ότι οι υπολογιστές επικοινωνούν στο δίκτυο με τους αριθμούς των IP addresses!). Στον υπολογιστή σας έχετε δηλώσει κάποια τετράδα αριθμών ως DNS server. Ο browser , λοιπόν, παίρνει την πρωτοβουλία και ρωτάει τον συγκεκριμένο server για την IP address του υπολογιστή με το όνομα www.nasa.gov. Ο DNS server όμως γνωρίζει στοιχεία μόνο για τη ζώνη edu-net.gr. Αυτό που κάνει είναι να ρωτήσει έναν από τους ριζικούς εξυπηρετητές ονομάτων για το που βρίσκονται στοιχεία για το top level domain gov. (προσέξτε ότι δεν ρωτάει την IP address του ονόματος www.nasa.gov). Ο ριζικός εξυπηρετητής του απαντάει ότι το μηχάνημα υπεύθυνο για το domain gov είναι το A.ROOT-SERVERS.NET . Αμέσως μετά ο server που προσπαθεί να βρει την IP address ρωτάει τον τελευταίο για το που μπορεί να βρει το domain nasa. Ο υπολογιστής A.ROOT-SERVERS.NET ο οποίος γνωρίζει ποια μηχανήματα είναι υπεύθυνα για τα subdomains του απαντάει ότι είναι ο υπολογιστής NS1.JPL.nasa.gov . Το τελευταίο βήμα είναι να ρωτήσει τον προηγούμενο υπολογιστή για την IP address που αντιστοιχεί στο όνομα www.nasa.gov. Εφόσον πάρει απάντηση ο πλοηγός θα αποκαλύψει τα περιεχόμενα της τοποθεσίας www.nasa.gov.

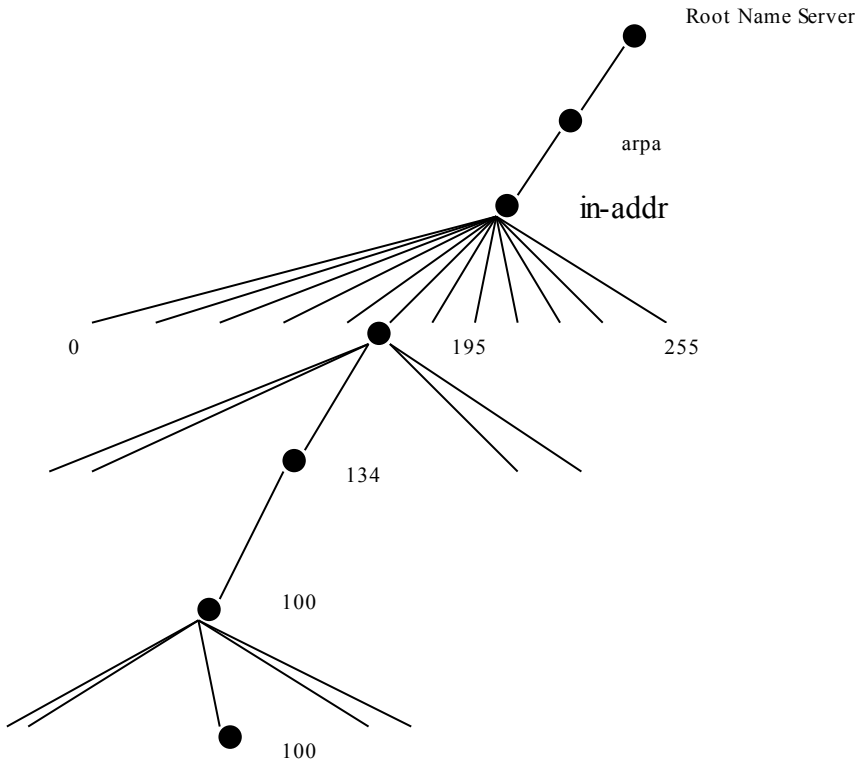
Προσέξτε ότι υπάρχουν που δύο είδη ερωτημάτων: Το ένα είναι ‘βρες μου την IP address που αντιστοιχεί στο τάδε όνομα’ και το κάνουν πάντα οι πελάτες (ονομάζονται resolvers στην ορολογία του DNS) των εξυπηρετητών ονομάτων. Αυτού του είδους οι ερωτήσεις ονομάζονται recursive. Το δεύτερο είναι ‘ξέρεις που μπορώ να βρω περισσότερες πληροφορίες για αυτό που ψάχνω;’ και είναι τα ερωτήματα που ανταλλάσσουν μεταξύ τους οι Name Servers κάθε φορά που χρειάζεται να αντιστοιχίσουν ένα όνομα σε μία IP address.

Κάθε φορά ,λοιπόν, που δίνεται μια διεύθυνση στον browser σας ή προσπαθείτε να στείλετε e-mail ο Name Server που σας εξυπηρετεί πρέπει να κάνει ‘τον γύρο του κόσμου για να βρει την απάντηση;’. Τα πράγματα ευτυχώς δεν είναι ακριβώς έτσι.

Ο κάθε εξυπηρετητής ονομάτων διαθέτει μνήμη (cache) που καταγράφει τα στοιχεία που έχει ήδη μάθει. Έτσι δεν χρειάζεται να καταφεύγει κάθε φορά στους root Name servers για να βρει μια πληροφορία – αν και αυτό συμβαίνει πολλές φορές!

Οι εξυπηρετητές ονομάτων όμως δεν αντιστοιχίζουν μόνο ονόματα υπολογιστών σε IP διευθύνσεις. Μπορούν να βρουν και που ακριβώς βρίσκεται ένας υπολογιστής με μια δεδομένη IP address. Κι αυτό γιατί πολλά προγράμματα που λειτουργούν μέσα από το δίκτυο χρειάζονται πληροφορίες βασισμένες σε IP διευθύνσεις και όχι σε ονόματα υπολογιστών. Για αυτήν τη διαδικασία ,δηλαδή, την εύρεση του δρόμου που πρέπει να ακολουθηθεί για να βρεθεί ένας υπολογιστής στο δίκτυο, υπάρχει μια ξεχωριστή ιεραρχική δομή παρόμοια με αυτήν των domains και zones : είναι η ιεραρχία του in-addr.arpa domain.

Το δίκτυο ARPAnet δεν είναι πλέον σε λειτουργία. Η ιεραρχία του in-addr.arpa όμως έχει δημιουργηθεί από αυτό το δίκτυο. Κάθε κόμβος αυτής αντί για όνομα έχει έναν δεκαδικό αριθμό από το 1 ως το 255 και ακολουθούνται οι ίδιοι κανόνες με την ιεραρχία των ονομάτων για να εξασφαλιστεί η μοναδικότητα και η κατανομή του υπολογιστικού φόρτου.



Μια εμφανής διαφορά μεταξύ της IP διεύθυνσης και του ονόματος ενός υπολογιστή είναι το ότι η πρώτη 'κινείται' από το γενικότερο στο ειδικότερο, ενώ συμβαίνει το αντίθετο με το όνομα του υπολογιστή.

olympus.noc.uoa.gr

100.100.134.195

Εγκατάσταση του BIND στο UBUNTU

```
apt-get install bind9
```

Εάν όμως θέλουμε για λόγους ασφαλείας να τρέχει το BIND όχι με τις εξ' ορισμού ρυθμίσεις αλλά σε chrooted environment (κλειδωμένος χρήστης bind στο περιβάλλον του με τα απολύτως απαραίτητα χωρίς να έχει πρόσβαση στο υπόλοιπο σύστημα) πρέπει να κάνουμε και κάποιες άλλες κινήσεις. Μετά από αυτό όμως πρέπει η να εκκινούμε το bind χειροκίνητα (σαν root) ή να αλλάξουμε το script.

```
/etc/init.d/bind9 stop
```

Αλλάζουμε το αρχείο */etc/default/bind9* ώστε ο daemon να τρέχει από τον unprivileged user 'bind', chrooted στο */var/lib/named*. Αλλάζουμε λοιπόν τη γραμμή: *OPTIONS="-u bind"* έτσι ώστε να γίνει *OPTIONS="-u bind -t /var/lib/named"*
Δημιουργούμε τα απαραίτητα directories στο */var/lib/*

```
mkdir -p /var/lib/named/etc
mkdir /var/lib/named/dev
mkdir -p /var/lib/named/var/cache/bind
mkdir -p /var/lib/named/var/run/bind/run
```

και μετακινούμε το directory με τις ρυθμίσεις

```
mv /etc/bind /var/lib/named/etc
```

Δημιουργούμε ένα συμβολικό δεσμό (symlink) από την παλιά τοποθεσία στην καινούρια ώστε να αποφύγουμε προβλήματα σε τυχόν αναβαθμίσεις του bind.

```
ln -s /var/lib/named/etc/bind /etc/bind
```

Δημιουργούμε τις null και random devices που χρειάζονται και αλλάζουμε τα permissions.

```
mknod /var/lib/named/dev/null c 1 3
mknod /var/lib/named/dev/random c 1 8
chmod 666 /var/lib/named/dev/null /var/lib/named/dev/random
chown -R bind:bind /var/lib/named/var/*
chown -R bind:bind /var/lib/named/etc/bind
```

Αλλάζουμε το script εκκίνησης /etc/init.d/sysklogd του sysklogd ώστε να παίρνουμε τα απαραίτητα logs. Η γραμμή που λέει SYSLOGD="-u syslog" αλλάζει σε SYSLOGD="-u syslog -a /var/lib/named/dev/log"

Ξαναξεκινάμε το sysklogd daemon

```
/etc/init.d/sysklogd restart
```

και ξεκινάμε το bind

```
/etc/init.d/bind9 start
```

και τσεκάρουμε το /var/log/syslog για τυχόν λάθη.

Διαχείριση της Υπηρεσίας DNS

Το σημαντικότερο στοιχείο στη διαχείριση του DNS είναι η εσωτερική οργάνωση των δεδομένων. Τα κυριότερα δεδομένα που θα βρει κανείς σε έναν name server είναι τα εξής:

- SOA (Start Of Authority)

Δείχνει ότι ο name server είναι υπεύθυνος για τη συγκεκριμένη ζώνη

- NS (Name Server)

Καθορίζει τον Name Server για μια ζώνη

- A (Address)

Αντιστοιχία ονόματος με IP διεύθυνση

- PTR (Pointer)

Αντίστροφη αντιστοιχία (IP διεύθυνση σε όνομα)

- CNAME (Canonical Name)

Δείκτης σε Canonical Name

- MX

Δείκτης σε Mail Server

SOA (Start Of Authority)

Στην αρχή κάθε αρχείου δεδομένων του εξυπηρετητή ονομάτων θα πρέπει να εμφανίζεται το SOA που θα υποδεικνύει ότι ο συγκεκριμένος υπολογιστής είναι η καλύτερη πηγή πληροφοριών για τα δεδομένα που ακολουθούν (authoritative name server). Ας πάρουμε για παράδειγμα τη ζώνη auth.gr. Στην αρχή του αρχείου που καθορίζει τα δεδομένα της παραπάνω ζώνης πρέπει να μπει το εξής :

```
;
;       AUTHORITATIVE DATA FOR DOMAIN AUTH.GR
;
;
;name    ttl     addr-cl SOA     Origin          Person in charge
;
```

```
 auth.gr.        IN      SOA     evia.ccf.auth.gr. noc.evia.ccf.auth.gr.
(
                                2000011201      ; Serial number
                                86400                ; Refresh 24 hours
                                43200                ; Retry   12 hours
                                3600000            ; Expire  1000 hours
                                345600 )           ; Minimum 96 hours
```

Το όνομα auth.gr. πρέπει να μπει στην πρώτη στήλη του κειμένου και να τελειώνει με μια τελεία (.). Το IN προέρχεται από τη λέξη Internet. Είναι μια κλάση δεδομένων – ίσως η πιο διαδεδομένη. Το επόμενο πεδίο μετά το SOA είναι το όνομα του master name server για τη συγκεκριμένη ζώνη. Προσέξτε την τελεία μετά το όνομα του υπολογιστή. Αυτός είναι ένας κανόνας που πρέπει να ακολουθείται σε όλα τα ονόματα των υπολογιστών που φιλοξενεί η βάση δεδομένων του BIND. Αν παραληφθεί η τελεία τότε το όνομα θα είναι σχετικό ως προς το όνομα του domain. Για παράδειγμα, ο υπολογιστής evia.ccf.auth.gr θα σήμαινε πως ονομάζονταν evia.ccf.auth.gr.auth.gr. Αμέσως μετά έρχεται η ηλεκτρονική διεύθυνση του υπεύθυνου της υπηρεσίας. Η πρώτη τελεία (.) είναι στην ουσία το σύμβολο @. Στη συνέχεια συναντάει κανείς μερικές μεταβλητές που καθορίζουν τη συμπεριφορά του εξυπηρετητή – ανεξάρτητα αν αυτός είναι master ή slave:

Serial : Είναι ο αύξων αριθμός που αντιστοιχεί στην τελευταία αλλαγή που έγινε στα δεδομένα της συγκεκριμένης ζώνης. Κάθε φορά που ένας slave επικοινωνεί με έναν master 'ρωτάει' για το serial number κάθε ζώνης. Αν αυτό που έχει ο slave είναι μικρότερο από αυτό του master ζητάει ένα αντίγραφο της ζώνης. Ο αριθμός αυτός μπορεί να αυξάνεται σειριακά ή να έχει τη μορφή ημερομηνίας.

Refresh : Είναι το διάστημα που πρέπει να περάσει μέχρι ο slave επικοινωνήσει με τον master για να διαπιστώσει αν υπάρχουν νέα δεδομένα. Αυτό , όμως, το διάστημα μπορεί να είναι πολύ μικρότερο αν ο master ειδοποιήσει τον slave ότι τα δεδομένα έχουν αλλάξει.

Retry : Αν ο slave αποτύχει για κάποιο λόγο να παραλάβει ένα αντίγραφο των δεδομένων θα πρέπει να ξαναπροσπαθήσει μετά από retry δευτερόλεπτα.

Expire : Αν ο slave δεν έχει καταφέρει να πάρει αντίγραφο μετά από expire δευτερόλεπτα από τον master, τότε αυτόματα σταματάει να απαντάει σε ερωτήματα που αφορούν τη συγκεκριμένη ζώνη. Αυτό βασίζεται στο σκεπτικό ότι είναι καλύτερα να μην έχει καθόλου δεδομένα παρά να έχει παλιά δεδομένα.

TTL (Time To Live) : Όταν κάποιος name server επικοινωνήσει με αυτόν θα κρατήσει τα δεδομένα στη μνήμη του για TTL δευτερόλεπτα. Αν τα δεδομένα της ζώνης δεν αλλάζουν πολύ συχνά η τιμή του TTL πρέπει να είναι υψηλή.

Το όνομα του domain μπορεί να παραληφθεί σε περίπτωση που είναι ίδιο με το origin. Τότε πρέπει να το αντικαταστήσετε με το σύμβολο @ :

```
@       IN      SOA     evia.ccf.auth.gr. noc.evia.ccf.auth.gr.
```

Γενικά, οι τιμές των SOA μεταβλητών θα πρέπει να είναι η 'χρυσή τομή' ανάμεσα στην καλή ανταπόκριση των νέων δεδομένων και στον ικανοποιητικό χρόνο κράτησης των δεδομένων στη μνήμη.

NS (Name Server)

Σε κάθε ζώνη πρέπει να υπάρχει ένας τουλάχιστον εξυπηρετητής ονομάτων.

```
                        IN      NS      evia.ccf.auth.gr.
                        IN      NS      philippos.ccf.auth.gr.
                        IN      NS      thalia.ccf.auth.gr.
```

Address και CNAME

Στη συνέχεια πρέπει να γίνει η αντιστοίχηση από τα ονόματα στα IP addresses. Το γράμμα A σημαίνει Address.

```
laplace         IN      A       155.207.114.55
```

Ένας υπολογιστής (όνομα υπολογιστή) μπορεί να έχει πάνω από μία IP διεύθυνση. Αυτό συμβαίνει σε μηχανήματα που συνδέουν δύο τοπικά δίκτυα ή γενικότερα σε routers. Το CNAME προέρχεται από το Canonical Name. Είναι ένα 'ψευδώνυμο' κάποιου υπολογιστή. Για παράδειγμα, το πραγματικό όνομα (canonical) του υπολογιστή www.edu-net.gr είναι olympus.noc.uoa.gr . Οι εγγραφές CNAME χρησιμεύουν συνήθως σε servers για διάφορες υπηρεσίες όπως αυτή του ηλεκτρονικού ταχυδρομείου, του παγκόσμιου ιστού ή των Usenet News στις οποίες δηλώνεται ένα συμβολικό όνομα που είναι πιο εύκολο να το θυμάται κανείς:

```
www                     IN      CNAME   philippos10.ccf.auth.gr.
```

PTR

Η συνέχεια ανήκει στην αντίστροφη διαδικασία: στην αντιστοίχηση των IP διευθύνσεων σε ονόματα.

```
6       IN      PTR     ep5.irep.ad.auth.gr.
```

MX

Η εγγραφή MX σημαίνει Mail Exchange. Ο υπολογιστής που έχει μια τέτοια εγγραφή στην υπηρεσία του DNS είναι υπεύθυνος για την αποστολή ηλεκτρονικού ταχυδρομείου. Κάθε ζώνη πρέπει να έχει τουλάχιστον ένα υπολογιστή με εγγραφή MX. Και αυτό γιατί είναι πολύ πιθανό να υπάρχει ένας back-up mail server που θα λειτουργήσει σε περίπτωση που ο πρώτος έχει πρόβλημα. Πώς καταλαβαίνει ο εξυπηρετητής ονομάτων ποιος είναι ο πρώτος mail server και ποιος ο back-up ;

Κάθε εγγραφή MX συνοδεύεται και από έναν αριθμό. Όσο πιο μικρός είναι ο αριθμός αυτός τόσο ψηλά είναι ο συγκεκριμένος υπολογιστής σε σειρά προτεραιότητας ως mail server. Αν για κάποιο λόγο αυτός με τον μικρότερο αριθμό MX δεν λειτουργεί αυτόματα το BIND θα επιλέξει το μηχάνημα με τον αμέσως μεγαλύτερο αριθμό MX.

```
                        IN      MX      100 mml0.ccf.auth.gr.
                        IN      MX      200 philippos.ccf.auth.gr.
```

Η διεύθυνση loopback

Μια σημαντική υποϊεραρχία του domain in-addr.arpa είναι η διεύθυνση loopback και είναι πάντα η 127.0.0.1. Γιατί χρειάζεται η διεύθυνση αυτή;

Κανείς εξυπηρετητής ονομάτων δεν είναι υπεύθυνος για το 127.0.0. domain. Γι αυτό ο κάθε name server πρέπει να εξυπηρετεί τον εαυτό του για τα πακέτα που παραμένουν μέσα στο μηχάνημα (πακέτα που περνάνε από το ένα πρόγραμμα στο άλλο χωρίς να επικοινωνούν με κάποιο άλλο μηχάνημα).

```
                    localhost       IN      A       127.0.0.1
```

Ας δούμε και μερικά παραδείγματα: Έχουμε ένα εσωτερικό δίκτυο 192.168.0.0/24, το domain middleearth, με τρεις υπολογιστές, τους gandalf, frodo και aragorn και τις αντίστοιχες διευθύνσεις τους. Άρα θα πρέπει να έχουμε ένα αρχείο ζώνης για το domain (το middleearth.hosts) και ένα αντίστροφο 192.168.0.rev
Ας δούμε πρώτα το 192.168.0.rev

```
  $ttl 38400
  0.168.192.in-addr.arpa.  IN          SOA         gandalf.middleearth.
admin.middleearth. (
                        1130653244
                        10800
                        3600
```

```
                        604800
                        38400 )
 0.168.192.in-addr.arpa. IN      NS      gandalf.middleearth.
 1.0.168.192.in-addr.arpa.       IN      PTR     gandalf.middleearth.
 5.0.168.192.in-addr.arpa.       IN      PTR     aragorn.middleearth.
 6.0.168.192.in-addr.arpa.       IN      PTR     frodo.middleearth.
```

Το αντίστοιχο hosts αρχείο

```
 $ttl 38400
 middleearth.    IN      SOA     gandalf.middleearth. admin.middleearth.
(
                        1130743673
                        10800
                        3600
                        604800
                        38400 )
 middleearth.    IN      NS      gandalf.middleearth.
 gandalf.middleearth.    IN      A       192.168.0.1
 aragorn.middleearth.    IN      A       192.168.0.5
 frodo.middleearth.      IN      A       192.168.0.6
 middleearth.      IN      TXT     "v=spf1 mx ~all"
 gandalf.middleearth.  IN      TXT     "v=spf1 a -all"
 middleearth.      IN      MX      10 gandalf.middleearth.
```

Οι TXT RRs αφορούν το sender policy framework όπως αυτό ορίστηκε το 2004 και εξασφαλίζει πως ο MTA (mail transfer agent) δέχεται για αποστολή mail που έρχονται από το domain middleearth και στέλνονται μέσω του server gandalf.middleearth.

Ρυθμίσεις DNS Server μέσω Webmin

Σκοπός : η εγκατάσταση DNS Server σε τοπικό δίκτυο έτσι ώστε να μπορούμε να

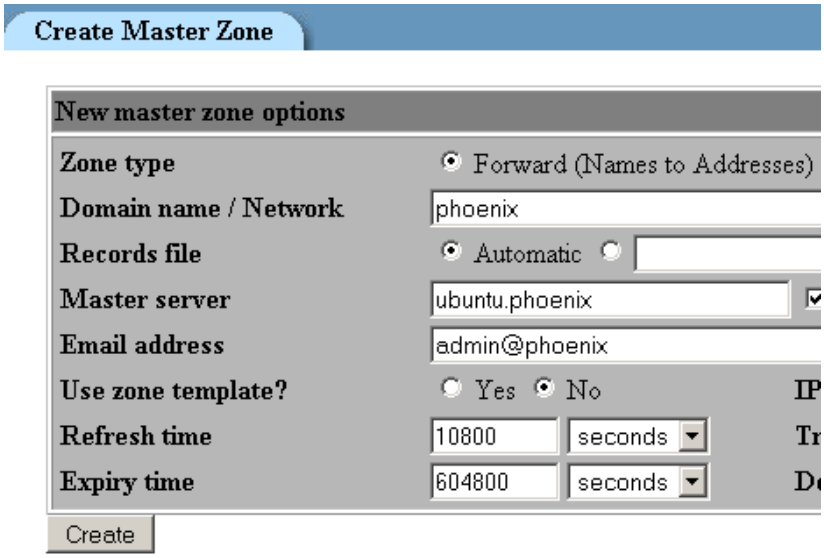
χρησιμοποιούμε σε διάφορες υπηρεσίες π.χ. ping ονόματα Η/Υ αντί για τις διευθύνσεις τους.

Υπόθεση : Έστω ότι το όνομα domain είναι το phoenix, ο DNS Server ο ubuntu στην IP 192.168.1.202

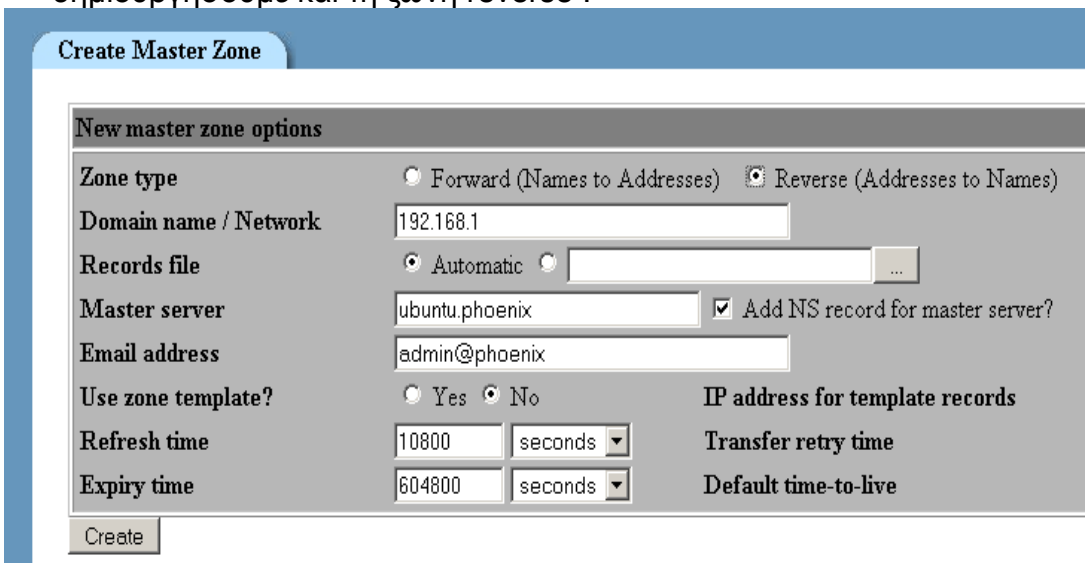
1. Εγκατάσταση

```
Δίνουμε ως Root : apt-get install bind9
```

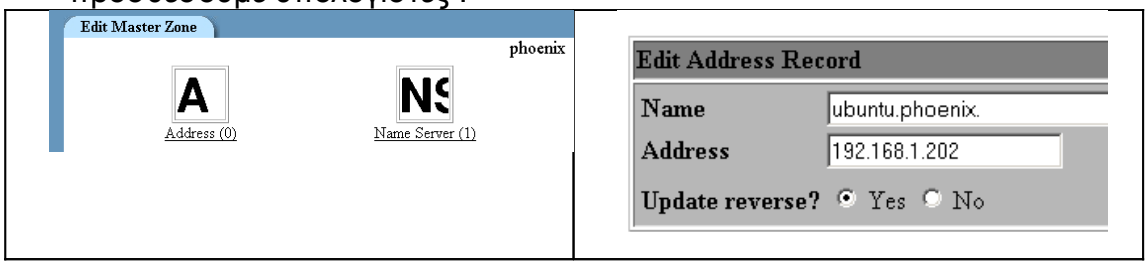
2. Μπαίνουμε στο webmin (http://localhost:10000) και επιλέγουμε Servers, Bind DNS Server.
   a. Επιλέγουμε : Create master zone και γράφουμε το όνομα του Domain και του server :



3. Επιλέγουμε Return to zone list και μετά πάλι Create master zone για να δημιουργήσουμε και τη ζώνη reverse :



Επιλέγουμε Return to zone list και μετά στη ζώνη του δικτύου μας, Address για να προσθέσουμε υπολογιστές :



Προσθέτουμε τους Η/Υ. Η προσθήκη στη ζώνη reverse γίνεται αυτόματα .

4. Ο έλεγχος του DND server γίνεται από τις λειτουργίες του script :

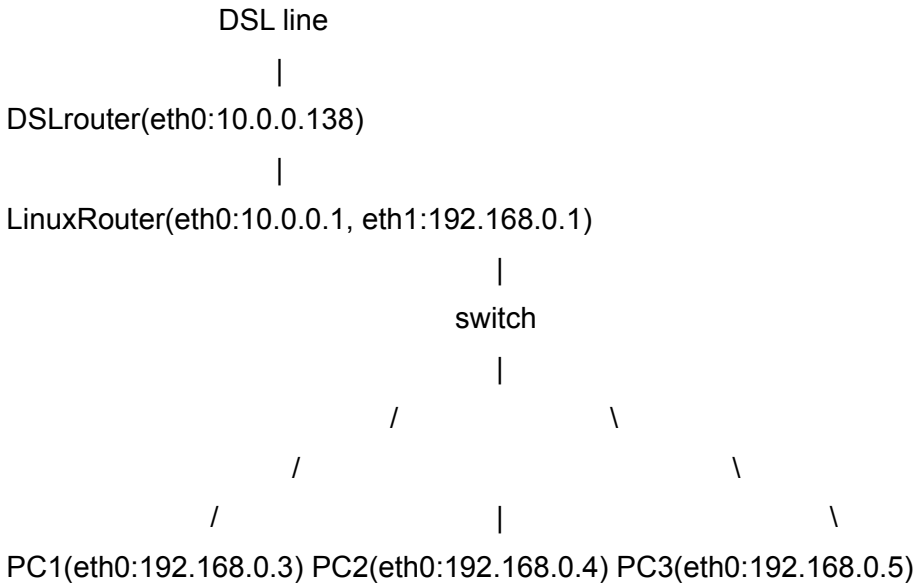
```
/etc/init.d/bind9

Και είναι start, stop, restart, reload, force-reload
```

Gateway-Firewall-NAT

Με την ευρεία διάδοση που γνωρίζει το DSL ακόμα και στη χώρα μας, όλο και περισσότεροι έχουν φανταστεί ένα τοπικό δίκτυο στο σπίτι, το γραφείο και αλλού το οποίο να μπορεί να επικοινωνεί με το Διαδίκτυο μέσω ενός τοπικού διακομιστή ο οποίος να αναλαμβάνει να διακινεί πακέτα προς και από το τοπικό δίκτυο, μεταφράζοντας τις τοπικές διευθύνσεις, ελέγχοντας τους προορισμούς, αποκόβοντας και δρομολογώντας πακέτα. Με λίγα λόγια να λειτουργεί σαν router. Το linux και ιδιαίτερα η διανομή ubuntu είναι μια ιδιαίτερα φθηνή και φιλική λύση γιαυτό το σκοπό, παρόλο που οι σημερινοί hardware DSL routers μπορούν να κάνουν αυτή τη δουλειά. Εμείς ας φανταστούμε το εξής σενάριο: Έχουμε μια γραμμή DSL που φτάνει στο σπίτι μας στο οποίο έχουμε έναν υπολογιστή με linux και δύο κάρτες δικτύου, η μία πηγαίνει κατευθείαν στο DSL Router και απο εκεί στο Διαδίκτυο και η άλλη σε ένα switch πάνω στο οποίο καταλήγουν και οι κάρτες δικτύου των υπολοίπων υπολογιστών. Χρησιμοποιώντας λοιπόν linux και *iptables* θα φτιάξουμε μία πύλη η οποία θα επιτρέπει τα μηχανήματα στο τοπικό δίκτυο να έχουν πρόσβαση στο Διαδίκτυο μέσω της εξωτερικής IP, χρησιμοποιώντας μια τεχνική που ονομάζεται NAT (Network Address Translation) ή masquerading. Επίσης θα κάνουμε το βασικό σετάρισμα ώστε το iptables να προστατεύει σαν firewall το εσωτερικό δίκτυο. Ας δούμε τώρα σε γενικές γραμμές τη δομή του αρχείου που θα χρησιμοποιεί το iptables.

Το αρχείο αυτό χωρίζεται σε πίνακες (tables). Οι πίνακες αφορούν το αν θα γίνεται φιλτράρισμα (filter) των πακέτων, αλλαγή (mangle), ή θα γίνεται μεταβολή διεύθυνσης (NAT). Οι πίνακες τώρα με τη σειρά τους αποτελούνται από αλυσίδες κανόνων (chains) οι οποίες με τη σειρά τους αποτελούνται από κανόνες οι οποίοι ενεργοποιούνται βάσει κάποιας συνθήκης που ορίζει η αλυσίδα και ο κανόνας και εκτελούν κάποια ενέργεια στα πακέτα. Π.χ. Ο πίνακας FILTER αποτελείται από τις αλυσίδες INPUT (εισερχόμενα πακέτα), OUTPUT (εξερχόμενα) και FORWARD (προωθούμενα) ενώ ο πίνακας NAT από τις αλυσίδες PREROUTING (πακέτα πριν τη δρομολόγηση), OUTPUT (εξερχόμενα) και POSTROUTING (πακέτα μετά τη δρομολόγηση). Δε θα ασχοληθούμε με τον πίνακα MANGLE γιατί ξεφεύγει από το σκοπό μας και με την αλυσίδα OUTPUT του πίνακα NAT γιατί δεν θέλουμε να κάνουμε τίποτα στα εξερχόμενα του NAT.



Κατ' αρχάς πρέπει να εξασφαλίσουμε πως τα πακέτα μας προωθούνται από τη μία κάρτα στην άλλη σε επίπεδο πυρήνα (kernel level):

```
echo 1 > /proc/sys/net/ipv4/ip_forward # Enables packet forwarding by kernel
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

Εάν θέλουμε να μονιμοποιήσουμε αυτήν την κατάσταση γράφουμε την παραπάνω γραμμή στο script που ενεργοποιεί το firewall κατά την εκκίνηση (πιθανώς κάποιο /etc/init.d/firewall στο τμήμα που αφορά την εκκίνηση).

Χρησιμοποιώντας τώρα το iptables θα φτιάξουμε το αρχείο μας.

Διαγραφές. Ο εξ'ορισμού πίνακας είναι ο filter. Άλλοι όπως ο nat πρέπει να αναφέρονται ξεχωριστά.

```
iptables --flush # Διαγραφή όλων των κανόνων στους πίνακες filter και nat
iptables --table nat --flush
iptables --delete-chain # Διαγραφή όλων των αλυσίδων που δεν είναι στους πίνακες filter και nat
iptables --table nat -delete-chain
```

```
# IP FORWARDing και MASQUERADING
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface eth1 -j ACCEPT
```

Η πρώτη γραμμή έκανε το εξής: Στον πίνακα NAT πρόσθεσε στην αλυσίδα POSTROUTING τον κανόνα να κάνει MASQUERADE στα πακέτα που εξέρχονται από την eth0. Δηλαδή ένα πακέτο που φαινόταν να έχει πηγή (source address) κάποια ip του εσωτερικού δικτύου, βγαίνει τώρα προς τα έξω σαν να έχει source την eth0.

Ο κανόνας της δεύτερης γραμμής προσθέτει στην αλυσίδα FORWARD (του πίνακα filter – δε χρειάζεται να το δηλώνουμε αυτό μιας και είναι ο εξ' ορισμού πίνακας) να δέχεται για προώθηση τα πακέτα που εισέρχονται από την eth1 (η εσωτερική κάρτα του μηχανήματος)

Θα προσθέσουμε τώρα και μερικούς άλλους κανόνες απαραίτητους για τη σωστή λειτουργία του firewall. Πλέον δε θα χρησιμοποιούμε ολοκληρωμένα τα ορίσματα (π.χ. --append κλπ) αλλά συντομογραφίες (π.χ -a).

Θα αρχίσουμε με τον πίνακα FILTER και πρώτα με την αλυσίδα INPUT

#Δεχόμαστε όλα τα πακέτα που προέρχονται στην eth0 και έχουν κατάσταση ESTABLISHED, RELATED

```
iptables -A INPUT -m state -i eth0 --state ESTABLISHED,RELATED -j ACCEPT
```

#Δεχόμαστε τα πακέτα που έρχονται στις eth1 και localhost

```
iptables -A INPUT -i eth1 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
```

#Δεν δεχόμαστε αυτά που έρχονται στην eth0 αλλά φαίνονται να προέρχονται από το εσωτερικό δίκτυο ή από το localhost

```
iptables -A INPUT -s 192.168.0.0/24 -i eth0 -j DROP
iptables -A INPUT -s 127.0.0.0/8 -i eth0 -j DROP
```

#Δεχόμαστε πακέτα tcp που έρχονται στην eth0 και έρχονται από τη θύρα 22 (ssh)

```
iptables -A INPUT -p tcp -m tcp -i eth0 --sport 22 -j ACCEPT
```

#Ανοίγουμε τις πόρτες 21 (ftp) και 22 (ssh) στα πακέτα tcp

```
iptables -A INPUT -p tcp -i eth0 --dport 21 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT
```

Συνεχίζουμε με την αλυσίδα FORWARD

#Μια πιο σωστή έκφραση του κανόνα που είδαμε παραπάνω δέχεται για προώθηση από την eth1 στην eth0

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

#Για να γίνει όμως η αντίστροφη προώθηση από έξω προς τα μέσα (από την eth0 στην eth1) απαιτούμε επιπλέον η κατάσταση των πακέτων να είναι ήδη established, related έτσι ώστε να μην μπορεί να εισέλθει πακέτο από έξω

```
iptables -A FORWARD -m state -i eth0 -o eth1 --state ESTABLISHED,RELATED -j ACCEPT
```

Ας δούμε και κάτι χρήσιμο. Έστω ότι το μηχάνημα 192.168.0.3 χρησιμοποιείται ως κατεβαστήρι torrent. Αυτό σημαίνει πως πρέπει κι αυτό να επικοινωνεί απ' ευθείας με τον έξω κόσμο διότι ναι μεν τα πακέτα του θα φαίνονται σαν να προέρχονται από την εξωτερική μας ip αλλά όταν κάποιο άλλο μηχάνημα θα ζητήσει να επικοινωνήσει μ' αυτό στη συγκεκριμένη ip θα συναντήσει ένα τείχος αφού η συγκεκριμένη ip ανήκει στο linux router μας. Άρα πρέπει με κάποιο τρόπο για συγκεκριμένες θύρες να πούμε στα πακέτα μας (εισερχόμενα και εξερχόμενα) πως το αντίστοιχο στην εξωτερική ip μηχάνημα δεν είναι το linux router αλλά κάποιο άλλο και μάλιστα με συγκεκριμένη εσωτερική ip την 192.168.0.3 και έστω πως οι πόρτες αυτές είναι η δεκάδα 40401-40410.

#Πρέπει να δεχόμαστε για προώθηση τα πακέτα tcp που έχουν πηγή και προορισμό (source και destination) τις θύρες 40401-40410

```
iptables -A FORWARD -p tcp -m tcp --sport 40401:40410 -j ACCEPT
iptables -A FORWARD -p tcp -m tcp --dport 40401:40410 -j ACCEPT
```

#Πρέπει επίσης να δηλώσουμε πως τα πακέτα που έρχονται στην eth0 και έχουν προορισμό αυτές τις πόρτες πρέπει να πάν στο ip 192.168.0.3

```
iptables -A PREROUTING -p tcp -m tcp -i eth0 --dport 40401:40410 -j
```

```
DNAT --to-destination 192.168.0.3:40401-40410
```

#Απορρίπτουμε όλα τα υπόλοιπα

```
iptables -P INPUT DROP
```

Αποθηκεύουμε το σετ κανόνων:

```
/sbin/iptables-save > /etc/sysconfig/iptables.rules
```

Ενώ για την εκτέλεση (π.χ. κατά την εκκίνηση) θέλουμε πρώτα επαναφορά των κανόνων:

```
/sbin/iptables-restore < /etc/sysconfig/iptables.rules
```

Ubuntu Repositories @ home

Εγκαθιστούμε το dpkg-dev αν δεν το έχουμε ήδη κάνει:

```
apt-get install dpkg-dev
```

Δημιουργούμε σαν root ένα directory το οποίο θα χρησιμοποιηθεί σαν repository:

```
mkdir -p /firiki
chmod a+r,a+w,a+x /firiki
```

Μέσα σ' αυτό το directory δημιουργούμε το εξής directory tree:

```
repository/
repository/dists/
repository/dists/breezy/
repository/dists/breezy/local/
repository/dists/breezy/local/binary-i386/
repository/pool-i386/local/
repository/updaterepo
```

Προσθέτουμε τις παρακάτω γραμμές στο /etc/apt/sources.list:

```
## Local Breezy Repository
deb file:///firiki/repository/ breezy local
```

Το παραπάνω φυσικά είναι για το τοπικό μηχάνημα. Σε remote μηχάνημα οι γραμμές θα γίνουν:

```
deb http://<hostname ή ip>/firiki/repository breezy local
```

και αναγκαστικά το directory tree του firiki θα το φτιάξουμε στο /var/www/

Το updaterepo script περιέχει τις γραμμές:

```
#!/bin/bash
dpkg-scanpackages pool-i386/local /dev/null | gzip -9c > dists/breezy/local/binary-i386/Packages.gz
chmod a+r,a+w,a-x dists/breezy/local/binary-i386/Packages.gz
Το κάνουμε εκτελέσιμο chmod a+x updaterepo
```

Έτσι από τώρα και στο εξής όποτε βρίσκουμε ένα πακέτο deb το βάζουμε στο αντίστοιχο directory (ανάλογα με την αρχιτεκτονική του συστήματος φυσικά, τα ίδια θα φτιάχναμε και για amd-64). Δηλαδή ένα πακέτο για i386 θα το βάλουμε στο /firiki/repository/pool-i386/local και μετά θα τρέξουμε το script για ανανέωση:

```
cd /firiki/repository
sudo updaterepo
```

Τα ίδια με τις ανάλογες αλλαγές θα κάναμε και για sources πακέτα με τις ανάλογες αλλαγές στο directory tree, στο sources.list (deb-src) και στο script (dpkg-scansources κλπ.)

Αν τώρα ψάξουμε με το synaptic θα βρούμε **μόνο με search όμως** τα πακέτα που μεταφέραμε.

Καλή διασκέδαση.

Πηγές: http://www.ubuntuforums.org/showthread.php?t=42862#top

Proxy Server (Squid server)
Εγκατάσταση και Διαχείριση του squid Proxy Server
Εισαγωγή

Το πρόγραμμα Squid αποθηκεύει (caches) δεδομένα. Κάτι τέτοιο γίνεται με τον εξής τρόπο: δέχεται αιτήσεις από τους πελάτες (clients) για διάφορα αρχεία που βρίσκονται στο Internet και αυτός αναλαμβάνει να τους τα διαβιβάσει. Με άλλα λόγια, όταν κάποιος θέλει να 'κατεβάσει' στον υπολογιστή του μια σελίδα της υπηρεσίας παγκόσμιου ιστού (www) τότε θα την ζητήσει από το πρόγραμμα Squid . Αυτός με τη σειρά του θα συνδεθεί με τον εξυπηρετητή που βρίσκεται αποθηκευμένη η σελίδα και θα τη ζητήσει. Αμέσως μετά και χωρίς να γίνεται ορατό στον πελάτη του μοιράζει τη σελίδα που ζήτησε αλλά κρατάει και ένα αντίγραφο αυτής. Την επόμενη φορά που κάποιος πελάτης ζητάει την ίδια σελίδα το πρόγραμμα Squid το μόνο που έχει να κάνει είναι να διαβάσει τη σελίδα από τον τοπικό του δίσκο και να τη στείλει στο χρήστη αμέσως χωρίς να χρειάζεται να συνδεθεί με τον απομακρυσμένο εξυπηρετητή.

Με τον τρόπο αυτό μειώνεται ο χρόνος πρόσβασης στα δεδομένα και στην κατανάλωση του εύρους ζώνης (bandwidth). Αυτό βέβαια εξαρτάται και από τη χρήση, δηλαδή αν οι χρήστες επισκέπτονται διαφορετικές σελίδες ή κατεβάζουν διαφορετικά αρχεία το κέρδος δεν είναι μεγάλο. Στα πλαίσια όμως των μαθημάτων ενός σχολικού εργαστηρίου συνήθως οι αιτήσεις στο internet είναι σχετικά κοινές. Μπορεί μάλιστα ο καθηγητής να επισκευθεί τις σελίδες από πριν έτσι ώστε όταν θα μπουν οι μαθητές να φορτώνουν αμέσως.

Το όνομα Squid προέρχεται από τον αρχική κωδική ονομασία του προγράμματος η οποία παρέμεινε και μετά το στάδιο της παραγωγής του. Στο σχεδιασμό του προγράμματος έχουν συμβάλει αρκετά άτομα. Είναι ,δηλαδή, το αποτέλεσμα μιας συλλογικής προσπάθειας.

Την τελευταία έκδοση του προγράμματος μπορείτε να τη βρείτε στη διεύθυνση ftp://ftp.squid-cache.org/pub ή σε mirrors sites σε όλο τον κόσμο στη διεύθυνση http://www.squid-cache.org/mirrors.html .

Το πρόγραμμα Squid έχει σχεδιαστεί για να λειτουργεί σε όλα σχεδόν τα Unix λειτουργικά συστήματα. Μερικά από αυτά είναι : Linux, FreeBSD, NetBSD, BSDI, OSF και Digital Unix, IRIX, SunOS/Solaris, NeXTStep, SCO Unix, AIX, HP-UX, OS/2. Οι πρόσφατες εκδόσεις του Squid μπορούν να λειτουργήσουν σε πλατφόρμες Windows/NT αρκεί ο υπολογιστής να έχει το πακέτο GNU-Win32. Όμως, έχουν παρατηρηθεί προβλήματα απόδοσης του προγράμματος στις παραπάνω πλατφόρμες.

Υπάρχουν κάποια θέματα που δημιουργούν ερωτήματα για τη λειτουργία του caching όπως ποια είναι η χρησιμότητα της διαδικασίας αυτής και ποια αντικείμενα πρέπει ή δεν πρέπει να αποθηκεύονται. Δεν είναι σωστό ή δεν είναι χρήσιμο για παράδειγμα να αποθηκεύονται 'ευαίσθητες' πληροφορίες όπως οι αριθμοί πιστωτικών καρτών, τα αποτελέσματα προγραμμάτων που εκτελούνται σε απομακρυσμένους εξυπηρετητές, sites που αλλάζουν συχνά τα περιεχόμενά τους ή sites που απλά δεν επιθυμούν τα περιεχόμενά τους να αποθηκεύονται σε καμία περίπτωση.

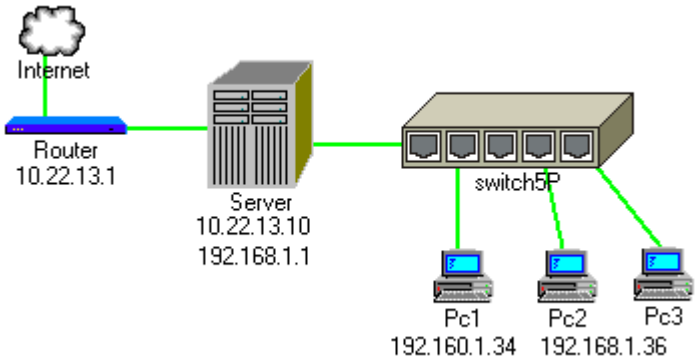
Το Squid μπορεί να διαχειριστεί αυτές τις περιπτώσεις αρκετά καλά. Ο διαχειριστής μπορεί να ρυθμίσει το πρόγραμμα ως προς την ποσότητα και την ποιότητα των δεδομένων που αποθηκεύονται καθώς και το χρόνο που θα διαρκέσει η φύλαξη.

Τώρα το κατά πόσο η αποθήκευση των δεδομένων είναι όντως χρήσιμη (ή καλύτερα κάτω από ποιες συνθήκες μπορεί να γίνει χρήσιμη) είναι ένα διαφορετικό θέμα. Για παράδειγμα, ένας πληρεξούσιος εξυπηρετητής (proxy server) που διαθέτει έναν μικρής χωρητικότητας σκληρό δίσκο θα έχει πολύ μεγάλη πρόσβαση από τους χρήστες για τα δεδομένα που έχει φυλάξει. Και αυτό γιατί θα έχει αντικείμενα που έχουν μεγάλη ζήτηση. Αν διπλασιαστεί η χωρητικότητα του δίσκου δεν θα διπλασιαστεί απαραίτητα η πρόσβαση στον δίσκο του εξυπηρετητή. Διότι, ο δίσκος τότε θα περιέχει δεδομένα από διευθύνσεις στο Internet που δεν είναι και τόσο δημοφιλή. Ο διαχειριστής του

προγράμματος θα πρέπει να βρει τη χρυσή τομή ανάμεσα στη χρήση και στο κόστος του εξυπηρετητή.

Εγκατάσταση του Squid στο LINUX , διανομή ubuntu.

Από τα προηγούμενα είναι κατανοητό ότι για να λειτουργήσει ο Proxy θα πρέπει να υπάρχει μια διάταξη όπως η παρακάτω :



Ο Server έχει δυο κάρτες δικτύου μια που συνδέεται στο Router και μια στο εσωτερικό δίκτυο μέσω του switch. Επίσης η πρώτη κάρτα δικτύου μπορεί να αντικατασταθεί στη εικόνα από ένα modem.

Στη γραμμή εντολών ως root δίνουμε :

```
apt-get install squid
```

και απαντάμε yes σε σχετικό μήνυμα.

Μετά από λίγο έχει γίνει η εγκατάσταση, έχει δημιουργηθεί το **squid spool directory** , τα **Swap didectories** και ο **squid τρέχει αυτόματα**. Αυτά φαίνονται κατά την εγκατάσταση και στην οθόνη.

Αν γράψουμε squid στη γραμμή εντολών θα πάρουμε το μήνυμα :

```
Squid is already running ! Process ID 11156
```

Το πιο σημαντικό αρχείο του προγράμματος είναι το **squid.conf**. Είναι το configuration file του Squid και αυτό που καθορίζει τη συμπεριφορά του προγράμματος. Μέσα στο πακέτο της εγκατάστασης υπάρχει και ένα δείγμα του παραπάνω αρχείου που μπορείτε να το χρησιμοποιήσετε ως οδηγό.

Σε κάποιες άλλες διανομές Linux :

1. για να ξεκινήσει το πρόγραμμα να εκτελείται θα πρέπει πρώτα να έχει δημιουργηθεί χειροκίνητα ο κατάλληλος αποθηκευτικός χώρος στο δίσκο :

```
#squid -z
```

2. για να ξεκινήσει το κύριο πρόγραμμα είτε καταλαμβάνοντας το τερματικό
#/usr/local/squid/bin/squid -NCd1
είτε αφήνοντας αδέσμευτο το τερματικό (daemon):
#/usr/local/squid/bin/squid .

Για να διαπιστώσετε αν το πρόγραμμα έχει εκτελεστεί σωστά μπορείτε να χρησιμοποιήσετε την

εντολή :

```
squid status
```

Βασικές λειτουργίες μέσω του script που βρίσκεται στη διαδρομή /etc/init.d/squid

ΕΝΤΟΛΗ	ΛΕΙΤΟΥΡΓΙΑ
`/etc/init.d/squid start`	Ξεκινάει ο squid daemon
`/etc/init.d/squid stop`	Σταματάει
`/etc/init.d/squid reload`	Ξαναφορτώνει το **squid.conf**
`/etc/init.d/squid force-reload`	
`/etc/init.d/squid restart`	Σταματάει και ξεκινάει πάλι.

Άλλες λειτουργίες μέσω παραμέτρων του προγράμματος squid:

Στην σειρά 2.x του προγράμματος μπορεί κανείς να επιλέξει τη λειτουργία του Squid από εντολές μέσα από το τερματικό:

-a Καθορίζει μια πόρτα για κλήσεις μέσα από το πρωτόκολλο HTTP

-d Καθορίζει το επίπεδο αποσφαλμάτωσης (debugging)

-f Καθορίζει κάποιο διαφορετικό αρχείο squid.conf

-h Τυπώνει το μήνυμα ‘βοήθειας’

-k reconfigure Επανεκκινεί το πρόγραμμα

-k shutdown Κλείνει όποιες συνδέσεις υπάρχουν ενεργές και σταματά την εκτέλεση του προγράμματος

-k interrupt Σταματάει το πρόγραμμα αμέσως

-k kill Όμοια με την παραπάνω. Να χρησιμοποιείται με προσοχή

-k debug Παράγει πλήρη στοιχεία αποσφαλμάτωσης

-k check Ελέγχει αν το πρόγραμμα είναι σε λειτουργία

-v Τυπώνει την έκδοση του προγράμματος

-z Δημιουργεί τον αποθηκευτικό χώρο στο σκληρό δίσκο του συστήματος

-N Καταλαμβάνει το τερματικό (όχι δαίμονας)

Ρύθμιση των τερματικών

Εξ ορισμού η TCP θύρα του squid είναι η **3128**. Θα πρέπει επομένως να ρυθμίσουμε τα clients έτσι ώστε να έχουν Internet. Επομένως για το προηγούμενο παράδειγμα οι ρυθμίσεις του Firefox θα είναι Proxy 192.168.1.1 και θύρα 3128.

Η Διάφανη Πληρεξουσιοδότηση (Transparent Proxy)

Είναι δυνατό να γίνεται χρήση του proxy server ακόμα και αν οι πελάτες δεν έχουν δώσει την εντολή αυτή στους πλοηγούς (browsers) τους. Σε αυτή την περίπτωση οι πελάτες επικοινωνούν πάντα με τον proxy server ακόμα και αν δεν το γνωρίζουν. Για να γίνει κάτι τέτοιο πρέπει να ακολουθηθούν τέσσερα βήματα:

1. **Τα πακέτα πρέπει να περνάνε από τον proxy server**. Αυτό μπορεί να γίνει με διάφορους τρόπους. Για παράδειγμα, αν ο proxy server πραγματοποιεί δρομολόγηση ανάμεσα στους χρήστες και το υπόλοιπο Internet τότε αναγκαστικά όλα τα πακέτα θα περνάνε από τον εξυπηρετητή. Από την άλλη μεριά, αν ο proxy δεν είναι στο φυσικό μονοπάτι των πακέτων πρέπει με κάποιο τρόπο να πραγματοποιηθεί εκτροπή των πακέτων έτσι ώστε να περνάνε αναγκαστικά από τον proxy. Αυτό μπορεί να γίνει με έναν δρομολογητή (router) ή με έναν μεταγωγέα (switch).

2. **Ο proxy server πρέπει να δέχεται τα πακέτα**. Αντίστοιχα, ο εξυπηρετητής πρέπει να ρυθμιστεί έτσι ώστε να δέχεται όλα τα πακέτα και να τα στέλνει στον αποθηκευτικό του χώρο.
3. **Πρέπει να εγκατασταθεί proxy server με την παραπάνω επιλογή**. Αν υπάρχει εγκατεστημένος εξυπηρετητής χωρίς την παραπάνω επιλογή θα πρέπει να διαγραφτεί από το σύστημα και να εγκατασταθεί ξανά έχοντας επιλέξει τη συγκεκριμένη λειτουργία.
4. **Θα πρέπει να γίνουν οι κατάλληλες αλλαγές στο αρχείο squid.conf**. Ένα παράδειγμα εγγραφής στο συγκεκριμένο αρχείο είναι το εξής:

```
http_port 3128
   httpd_accel_host virtual
   httpd_accel_port 80
   httpd_accel_with_proxy  on
   httpd_accel_uses_host_header on
```

Η εγγραφή της πρώτης γραμμής δίνει εντολή να εκτρέπονται όλα τα πακέτα που έρχονται στην πόρτα 80 στην πόρτα 3128 (η πόρτα του Squid). Στη δεύτερη και στην τρίτη γραμμή βρίσκεται η εντολή που πραγματοποιεί τη ‘διάφανη’ αποθήκευση. Στην τέταρτη, υπάρχει η εντολή που οδηγεί το Squid να δέχεται αιτήσεις στην πόρτα 80 και παράλληλα να αποθηκεύει τις πληροφορίες. Στην τελευταία, ο proxy server αποθηκεύει τα δεδομένα ‘κάτω’ από το όνομα του υπολογιστή και όχι την IP διεύθυνσή του. Αυτό μπορεί να φανεί χρήσιμο σε περιπτώσεις που υλοποιείται η αρχιτεκτονική του πρόγονου – απόγονου.

Διαχείριση του Squid

Όλες οι ρυθμίσεις γίνονται στο **/etc/squid/squid.conf**

Το ανοίγουμε με τον αγαπημένο μας κειμενογράφο π.χ. **pico /etc/squid/squid.conf**

Για να δουλέψει άμεσα το Squid ψάχνουμε τη γραμμή :

```
#Default :
# http_access deny all
```

Και την αλλάζουμε (βγάζουμε και το σχόλιο #)

```
http_access allow all
```

Κάνουμε αποθήκευση του squid.conf και επανεκκίνηση (/etc/init.d/squid restart)

Ο Έλεγχος Πρόσβασης (Access Control)

Ο έλεγχος πρόσβασης μπορεί να υλοποιηθεί με διάφορους τρόπους στο Squid.

Χρησιμοποιούμε μια ACL (access list) για να ορίσουμε κάτι. Το όνομα κάθε ACL στοιχείου πρέπει να είναι **μοναδικό.**

Ακολουθούν κάποια παραδείγματα για κάποιες χρήσιμες περιπτώσεις.

Παράδειγμα 1.

Απαγορεύοντας το κατέβασμα exe αρχείων :

```
acl            EXE            urlpath_regex            \.exe
http_access deny EXE
http_access allow all
```

Η εγγραφή *urlpath_regex* οδηγεί το πρόγραμμα να ερευνήσει όλο το path του URL μέχρι να βρει τη λέξη που έχει οριστεί. Παρατηρούμε ότι η τελευταία γραμμή είναι **http_access allow all** δηλαδή επιτρέπεται η πρόσβαση σε όλα τα υπόλοιπα. Να πούμε εδώ ότι εξ' ορισμού η λέξη all ορίζεται μέσα στο squid.conf οπότε στα παραδείγματα θα τη θεωρούμε δεδομένη :

```
acl all src 0.0.0.0/0.0.0.0
```

Για να το κάνουμε την αναζήτηση 'αναίσθητη' σε κεφαλαία – πεζά μπορούμε να χρησιμοποιήσουμε σύνολα και αλλάζουμε την πρώτη γραμμή σε :

```
acl EXE urlpath_regex \.[eE][xX][eE]
```

Επίσης μπορούμε να ορίσουμε και περισσότερα είδη αρχείων στη πρόταση ACL :

```
acl Downloads urlpath_regex  \.zip \.ZIP \.exe \.EXE \.mp3 \.MP3 \.avi
\.AVI \.mpg \.mpeg
http_access deny Downloads
http_access allow all
```

Παρατηρούμε ότι όλα τα στοιχεία που ακολουθούν την acl συνδέονται ουσιαστικά με ένα τελεστή OR , δηλαδή είτε ζητηθεί αρχείο zip είτε mp3 η συμπεριφορά θα είναι η ίδια.

Παράδειγμα 2.

Αν θέλει κάποιος να απαγορεύσει την αποθήκευση όλων των αντικειμένων που έχουν να κάνουν με μαγειρική θα προσθέσει στο αρχείο squid.conf:

```
acl Cooking1 url_regex cooking
acl Recipe1 url_regex recipe
http_access deny Cooking1
http_access deny Recipe1
http_access allow all
```

Δηλαδή, θα απαγορεύσει την πρόσβαση σε κάθε αντικείμενο που περιέχει τις λέξεις cooking και recipe.

Ένας άλλος τρόπος για να υλοποιηθεί αυτός ο περιορισμός είναι να απαγορευτεί η είσοδος σε γνωστά sites μαγειρικής:

```
acl Cooking2 dstdomain gourmet-chef.com
http_access deny Cooking2
http_access allow all
```

Η εγγραφή *dstdomain* οδηγεί το πρόγραμμα να ερευνήσει όλο το URL μέχρι να βρει το domain *gourmet-chef.com*.

Παράδειγμα 3.

Πώς μπορώ να ‘κόψω’ κάποιες TCP πόρτες ;

```
acl Safe_ports port 80 21 443 563 70 210 1025-65535
 http_access deny !Safe_ports
```

Στο παράδειγμα αυτό το πρόγραμμα δεν δέχεται συνδέσεις στις πόρτες εκτός της παραπάνω λίστας. **Ο τελεστής ! είναι ο λογικός τελεστής NOT** (από τη C). Ένας άλλος τρόπος είναι ο εξής :

```
acl Dangerous_ports 7 9 19 22 23 25 53 109 110 119
http_access deny Dangerous_ports
```

Έτσι το πρόγραμμα δεν δέχεται συνδέσεις στην παραπάνω λίστα.

Παράδειγμα 4.

Παράκαμψη του Squid για κάποια site. Χρησιμοποιούμε την **always_direct** .

```
acl hotmail dstdomain .hotmail.com
always_direct allow hotmail
```

Παράδειγμα 5.

Αποτρέπω τους χρήστες από τη μεταφόρτωση (download) μεγάλων αρχείων με την παράμετρο reply_body_max_size που είναι εξ' ορισμού απενεργοποιημένη.

```
# reply_body_max_size 0 allow all

acl           html           rep_mime_type           text/html
reply_body_max_size           0           allow           html
reply_body_max_size 4096 allow all
```

Το παραπάνω επιτρέπει οποιοδήποτε μέγεθος για σελίδα html ενώ για όλα τα υπόλοιπα αρχεία το μέγεθος περιορίζεται στα 4Kb.

Παράδειγμα 6.

Πώς μπορώ να επιτρέψω σε ένα client να επισκέπτεται μια ιστοσελίδα ενώ τα υπόλοιπα clients να μη μπορούν ;

```
acl special_client src 10.1.2.3

acl special_url url_regex ^http://www.squid-cache.org/Doc/FAQ/$

http_access allow special_client special_url

http_access deny special_url
```

Παράδειγμα 7.

Επιτρέπω τη χρήση του Squid proxy σε ορισμένα PCs μόνο, αυτά που είναι στο δίκτυο τάξης C 192.168.0.1.

```
acl           localnet           src           192.168.1.0/255.255.255.0
http_access                        allow                        localnet
http_access                           deny                           all
```

Άλλος τρόπος

```
acl localnet src 192.168.1.0/255.255.255.0

http_access deny all !localnet

If the IP is in myNet, the result is 1 AND (NOT 1) = 1 AND 0 = 0, thus
access will be granted. If the request is coming from the outside world
(the IP is not defined in myNet), the result will be 1 AND (NOT 0) = 1 AND
1 = 1, so access will be denied.
```

Παράδειγμα 8.

Πρόσβαση ανάλογα με την ώρα και ημέρα. Χρησιμοποιούμε τα παρακάτω format :

```
acl        aclname        time        [day-abbrevs]        [h1:m1-h2:m2]
day-abbrevs:
S                                -                                  Sunday
M                                -                                  Monday
T                               -                                 Tuesday
W                              -                                Wednesday
```

```
H                                -                                Thursday
F                                 -                                 Friday
A                                -                                Saturday
```

Το παρακάτω επιτρέπει την πρόσβαση τις εργάσιμες ημέρες και ώρες :

```
acl      workdays      time      M      T      W      H      F      9:00-17:00
http_access allow workdays
```

Λάθη λογικής

Όπως είδαμε στο παράδειγμα 1 όλα τα στοιχεία που ακολουθούν μια acl συνδέονται με ένα τελεστή OR . Αντίθετα όλα τα στοιχεία που ακολουθούν μια access_list συνδέονται με ένα τελεστή AND. Ας προσέξουμε το παρακάτω παράδειγμα :

```
acl ME src 192.168.1.1
acl YOU src 192.168.1.2
http_access allow ME YOU
```

Περιμένουμε να επιτρέπεται η πρόσβαση στο ΜΕ και στο YOU αλλά αυτό δε θα γίνει επειδή δεν είναι δυνατό να έχει κάποιο PC τη διεύθυνση ΜΕ και τη διεύθυνση YOU. Το παράδειγμα εργασίας μπορεί να γραφτεί όπως αυτό :

```
acl ME src 192.168.1.1
acl YOU src 192.168.1.2
http_access allow ME
http_access allow YOU
```

Δηλαδή όταν ζητήσει πρόσβαση ο ΜΕ ικανοποιείται γιατί υπάρχει ταίριασμα στη γραμμή 3 , το ίδιο συμβαίνει και με το pc YOU.

Επίσης σωστό είναι και το :

```
acl US 192.168.1.1 192.168.1.2
http_access allow US
```

ΒΙΒΛΙΑ ΚΑΙ FAQ ΣΤΟ INTEPNET

- http://www.squid-cache.org/Doc/FAQ/
- http://squid-docs.sourceforge.net/latest/html/book1.html
- **http://wiki.squid-cache.org**
- **http://www.brennan.id.au/index.html**

Παράρτημα

Ακολουθεί η αναφορά στα ACL elements και Access Lists από το FAQ της http://www.squid-cache.org/Doc/FAQ/

ACL elements

- **src**: source (client) IP addresses
- **dst**: destination (server) IP addresses
- **myip**: the local IP address of a client's connection
- **srcdomain**: source (client) domain name
- **dstdomain**: destination (server) domain name
- **srcdom_regex**: source (client) regular expression pattern matching
- **dstdom_regex**: destination (server) regular expression pattern matching
- **time**: time of day, and day of week
- **url_regex**: URL regular expression pattern matching
- **urlpath_regex**: URL-path regular expression pattern matching, leaves out the protocol and hostname
- **port**: destination (server) port number
- **myport**: local port number that client connected to
- **proto**: transfer protocol (http, ftp, etc)
- **method**: HTTP request method (get, post, etc)
- **browser**: regular expression pattern matching on the request's user-agent header
- **ident**: string matching on the user's name
- **ident_regex**: regular expression pattern matching on the user's name
- **src_as**: source (client) Autonomous System number
- **dst_as**: destination (server) Autonomous System number
- **proxy_auth**: user authentication via external processes
- **proxy_auth_regex**: user authentication via external processes
- **snmp_community**: SNMP community string matching
- **maxconn**: a limit on the maximum number of connections from a single client IP address
- **req_mime_type**: regular expression pattern matching on the request content-type header
- **arp**: Ethernet (MAC) address matching
- **rep_mime_type**: regular expression pattern matching on the reply (downloaded content) content-type header. This is only usable in the http_reply_access directive, not http_access.
- **external**: lookup via external acl helper defined by external_acl_type

Access Lists

- **http_access**: Allows HTTP clients (browsers) to access the HTTP port. This is the primary access control list.
- **http_reply_access**: Allows HTTP clients (browsers) to receive the reply to their request. This further restricts permissions given by http_access, and is primarily intended to be used together with the rep_mime_type acl type for blocking different content types.
- **icp_access**: Allows neighbor caches to query your cache with ICP.
- **miss_access**: Allows certain clients to forward cache misses through your cache. This further restricts permissions given by http_access, and is primarily intended to be used for enforcing sibling relations by denying siblings from forwarding cache misses through your cache.
- **no_cache**: Defines responses that should not be cached.
- **redirector_access**: Controls which requests are sent through the redirector pool.
- **ident_lookup_access**: Controls which requests need an Ident lookup.
- **always_direct**: Controls which requests should always be forwarded directly to origin servers.
- **never_direct**: Controls which requests should never be forwarded directly to origin servers.
- **snmp_access**: Controls SNMP client access to the cache.
- **broken_posts**: Defines requests for which squid appends an extra CRLF after POST message bodies as required by some broken origin servers.
- **cache_peer_access**: Controls which requests can be forwarded to a given neighbor (peer).

DHCP SERVER

Εγκατάσταση και ρυθμίσεις DHCP Server στο Linux , διανομή Ubuntu

Ο σκοπός ενός διακομιστή DHCP είναι να παρέχει αυτόματα διευθύνσεις IP, και ρυθμίσεις DNS και Gateway σε ένα δίκτυο Η/Υ έτσι ώστε να μη χρειάζεται να ρυθμίζουμε εμείς κάθε client ξεχωριστά. Διευκολύνει πάρα πολύ σε δίκτυα με πολλά clients.

Η εγκατάσταση του DHCP Server γίνεται με την εντολή :

```
#apt-get install dhcp3-server
```

Ρύθμιση του Server.

Παράδειγμα. Έστω ότι η eth1 είναι η κάρτα δικτύου με η οποία συνδέεται με το τοπικό δίκτυο.

IP κάρτας eth0 :192.168.0.1

Περιοχή IP διευθύνσεων που μοιράζει ο server : 192.168.0.100 έως 192.168.0.200

Subnet Mask: 255.255.255.0

Θέλουμε το client να παίρνει αυτόματα τις παρακάτω ρυθμίσεις :

DNS Servers: 202.188.0.133, 202.188.1.5

Domains: tm.net.my

Gateway Address: 192.168.0.1

Αρχικά δηλώνουμε τη κάρτα δοκτύου στο αρχείο **/etc/default/dhcp3-server** και καλό είναι πριν κάνουμε οποιαδήποτε αλλαγή να κρατήσουμε ένα αντίγραφο του αρχικού.

```
#cp /etc/default/dhcp3-server /etc/default/dhcp3-server_backup
```

Στη συνέχεια ανοίγουμε το αρχείο για διόρθωση.

```
#pico /etc/default/dhcp3-server
```

Ψάχνουμε την γραμμή :

```
INTERFACES=""
```

Και την αλλάζουμε :

```
INTERFACES="eth1"
```

Αποθηκεύουμε το αρχείο.

Μετά ανοίγουμε το βασικό αρχείο ρυθμίσεων,το **/etc/default/dhcp3-server** και καλό είναι πριν κάνουμε οποιαδήποτε αλλαγή να κρατήσουμε ένα

αντίγραφο του αρχικού.

```
#cp /etc/dhcp3/dhcpd.conf /etc/dhcp3/dhcpd.conf_backup
#pico /etc/dhcp3/dhcpd.conf
```

Ψάχνουμε το τμήμα :

```
 # option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;
```

...

Και το αλλάζουμε (βάζουμε σχόλια) :

```
#option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;

#default-lease-time 600;
#max-lease-time 7200;
Ψάχνουμε το τμήμα  :
...
# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#  range 10.5.5.26 10.5.5.30;
#  option domain-name-servers ns1.internal.example.org;
#  option domain-name "internal.example.org";
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}
```

...

Και το αλλάζουμε :

```
# A slightly different configuration for an internal subnet.
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.100 192.168.0.200;
```

```
    option domain-name-servers 202.188.0.133, 202.188.1.5;
    option domain-name "tm.net.my";
    option routers 192.168.0.1;
    option broadcast-address 192.168.0.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Αποθηκεύουμε το αρχείο και κάνουμε restart τον server :

```
# /etc/init.d/dhcp3-server restart
```

ΠΡΟΣΟΧΗ. Αν χρησιμοποιούμε τοπικό DNS server στον οποίο θέλουμε να είναι δηλωμένα ονόματα και διευθύνσεις Η/Υ ή θέλουμε κάποια μηχανήματα να έχουν τις ίδιες διευθύνσεις IP πάντα τότε θα στείλουμε IP ανάλογα με τη MAC address

Στο παράδειγμα που ακολουθεί στέλνεται στο PC με MAC address 00:A0:78:8E:9E:AA πάντα η IP address 192.168.0.4.

```
host apex {
   option host-name "apex.example.com";
   hardware ethernet 00:A0:78:8E:9E:AA;
   fixed-address 192.168.0.4;
}
```

SambaPDC Server

Εισαγωγή

Τα παρακάτω δεν είναι μια προσπάθεια να υποκατασταθεί ένας Microsoft server με όλα όσα προσφέρει όπως active directory (ότι κι αν αυτό σημαίνει) κλπ. Ένα μηχάνημα όμως με linux μπορεί να προσφέρει βασικές ευκολίες σε ένα τοπικό δίκτυο όπως κοινόχρηστους πόρους ελεγχόμενους σε επίπεδο χρηστών κ.ά.

Εγκατάσταση

Η εγκατάσταση θα γίνει με μία γραμμή:

```
apt-get install samba samba-common samba-doc libcupsys2-gnutls10 libkrb53 winbind smbclient
```

Παραμετροποίηση

Η βασική παραμετροποίηση γίνεται στο αρχείο /etc/samba/smb.conf οπότε κρατάμε ένα αντίγραφο του και προχωράμε.

Παρακάτω δίνεται ένα παράδειγμα από τρέχουσα εγκατάσταση samba:

```
[global]
        log file = /var/log/samba/log.%m
                passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n .
        obey pam restrictions = yes
        socket options = TCP_NODELAY
#       interfaces = eth1/255.255.255.0
        encrypt passwords = true
        passwd program = /usr/bin/passwd %u
        passdb backend = tdbsam guest
        dns proxy = no
        netbios name = gandalf
        server string = %h server (Samba, Ubuntu)
        invalid users = root
        message command = /bin/sh -c '/usr/bin/linpopup
        workgroup = middleearth
```

```
          os level = 65
  #       socket address = 192.168.0.1
          syslog = 0
          panic action = /usr/share/samba/panic-action %d
          max log size = 1000
          preserve case = yes
          hosts allow = 127.0.0.1 192.168.0.
          short preserve case = yes
          case sensitive = no
          preferred master = yes
          domain master = yes
          local master = yes
  #        logon path = \\%L\profiles\%u
  #        logon home = \\%L\%U
  #        logon drive = z:
  #        logon script = logon.bat
          admin users = @admins
          domain logons = yes
          guest ok = yes
          add user script = /usr/sbin/useradd -m %u
          delete user script = /usr/sbin/userdel -r -%u
          add group script = /usr/sbin/groupadd %g
          delete group script = /usr/sbin/groupdel %g
          add user to group script = /usr/sbin/groupmod -A %u %g
          delete user from group script = /usr/sbin/groupmod -R %u %g
              add machine script = /usr/sbin/useradd -s /bin/false -d
/var/lib/nobody %u
  [homes]
     comment = Home Directories
     browseable = no

  # By default, the home directories are exported read-only. Change next
  # parameter to 'yes' if you want to be able to write to them.
     writable = yes

  # File creation mask is set to 0700 for security reasons. If you want
to
```

```
  # create files with group=rw permissions, set next parameter to 0775.
     create mask = 0775

  # Directory creation mask is set to 0700 for security reasons. If you
want to
  # create dirs. with group=rw permissions, set next parameter to 0775.
     directory mask = 0775

  # Un-comment the following and create the netlogon directory for Domain
Logons
  # (you need to configure Samba to act as a domain controller too.)
  [netlogon]
     comment = Network Logon Service
     path = /usr/local/samba/netlogon
     guest ok = yes
  #   writable = no
     share modes = no
     read only = no
     write list = @admins
     read list = @admins, @users, @guests

  [profiles]
     comment = Profile Share
     path = /usr/local/samba/profiles
     read only = no
     profile acls = yes

  #[printers]
  #   comment = All Printers
  #   browseable = no
  #   path = /tmp
  #   printable = yes
  #   public = no
  #   writable = no
  #   create mode = 0700

  [admins]
```

```
   comment = Shared for Admins
   path = /home/samba/admins
   valid users = @admins
   read list = @admins
   write list = @admins
   force group = @admins
   read only = no
   create mask = 0774
   directory mask = 0775

[software]
   comment = Shared Software
   path = /home/samba/software
   valid users = @admins, @users
   admin users = @admins
   read list = @admins, @users
   write list = @admins
   force group = admins
   read only = no
   create mask = 0774
   directory mask = 0775

[domainstuff]
   comment = Domain Stuff
   path = /home/domuser/domainstuff
   browseable = yes
   guest ok = no
   writable = yes

[publicstuff]
   comment = Public Stuff
   path = /home/domuser/public
   browseable = yes
   write list = @admins, @users
   create mask = 0774
   directory mask = 0775
```

Σημειώσεις:

1. Το netbios name πρέπει να είναι ίδιο με το hostname του μηχανήματος.
2. Workgroup=middleearth είναι το domain για το οποίο φτιάχνουμε τον controller
3. logon drive =z: είναι το drive σαν το οποίο οι κοινόχρηστοι πόροι θα φαίνονται στα windows
4. Με το logon script = logon.bat μπορείτε να ορίσετε ενέργειες που θα εκτελούνται μόλις γίνει η σύνδεση όπως π.χ. κάποια net use.

Ας φτιάξουμε τώρα τα directories που χρειαζόμαστε:

```
mkdir /home/samba
mkdir /home/samba/admins
mkdir /home/samba/software
mkdir /home/domuser
mkdir /home/domuser/public
mkdir /home/domuser/domainstuff
mkdir /usr/local/samba
mkdir /usr/local/samba/profiles
mkdir /usr/local/samba/netlogon
chown -R root:users /home/samba/
chmod -R 771 /home/samba/
```

Πρέπει τώρα να φτιάξουμε το χρήστη root του Samba (alias:Administrator) που χρειάζεται για να προσθέσουμε μηχανήματα στο domain, να δημιουργήσουμε το αρχείο smbusers και να προσθέσουμε το χρήστη root με ψευδώνυμο Administrator. Έτσι θα μπορούμε να χρησιμοποιούμε το κοινό όνομα Administrator των Windows σαν ψευδώνυμο του χρήστη root του Samba.

```
root@gandalf:/home/samba# smbpasswd -a root
New SMB password:
Retype new SMB password:
root@gandalf:/etc/samba#     echo     "root     =     Administrator"     >
/etc/samba/smbusers
```

Ξεκινάμε το Samba:

```
root@gandalf:/etc/samba# /etc/init.d/samba restart
 * Stopping Samba daemons...
   ...done.
      *      Starting      Samba      daemons..file:///usr/share/ubuntu-
artwork/home/locales/index-el.html
```

```
    ...done.
```

Ας δοκιμάσουμε τι κάναμε μέχρι τώρα:

```
root@gandalf:/etc/samba# smbclient -L localhost -U%
Domain=[MIDDLEEARTH] OS=[Unix] Server=[Samba 3.0.14a-Ubuntu]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk      Network Logon Service
        profiles        Disk      Profile Share
        admins          Disk      Shared for Admins
        software        Disk      Shared Software
        domainstuff     Disk      Domain Stuff
        publicstuff     Disk      Public Stuff
         IPC$            IPC       IPC Service (gandalf server (Samba,
Ubuntu))
         ADMIN$          IPC       IPC Service (gandalf server (Samba,
Ubuntu))
Domain=[MIDDLEEARTH] OS=[Unix] Server=[Samba 3.0.14a-Ubuntu]

        Server               Comment
        ---------            -------
        ARAGORN              aragorn
        FRODO                lap
        GANDALF              gandalf server (Samba, Ubuntu)

        Workgroup            Master
        ---------            -------
        MIDDLEEARTH          GANDALF
```

(Υπενθυμίζουμε πως βλέπετε πραγματικά στοιχεία γιαυτό και εμφανίζονται και άλλα δυο μηχανήματα στο domain)

Ας δημιουργήσουμε τώρα τρία linux groups στα οποία θα αντιστοιχήσουμε τρία domain groups. Όπως είδαμε στο config χρειαζόμαστε τα groups admins, users και guests

```
groupadd admins
groupadd users
```

```
groupadd guests
```

Και αφού δημιουργήσουμε χρήστες linux και τους βάλουμε σε groups όπως τα παραπάνω, θα αναθέσουμε τα groups αυτά σε ομάδες domain.

```
net groupmap modify ntgroup="Domain Admins" unixgroup=admins
net groupmap modify ntgroup="Domain Users"  unixgroup=users
net groupmap modify ntgroup="Domain Guests" unixgroup=groups
```

Έτσι μπορούμε να βάλουμε χρήστες στο σύστημα και μετά να τους βάλουμε στο domain

```
root@gandalf:/etc/samba# useradd luthien -m -G users
root@gandalf:/etc/samba# smbpasswd -a luthien
New SMB password:
Retype new SMB password:
Added user luthien.
```

Θα μπούμε πρώτα σαν luthien στο home directory:

```
root@gandalf:/etc/samba# smbclient //gandalf/luthien -Uluthien
Password:
Domain=[MIDDLEEARTH] OS=[Unix] Server=[Samba 3.0.14a-Ubuntu]
smb: \> dir
  .                                   D        0  Tue May  9 18:24:20
2006
  ..                                  D        0  Tue May  9 18:24:20
2006
  .bashrc                             H     2227  Tue May  9 18:24:20
2006
  .bash_profile                       H      414  Tue May  9 18:24:20
2006

                57004 blocks of size 1048576. 42478 blocks available
smb: \> q
Και τώρα θα δοκιμάσουμε να μπούμε στον πόρο publicstuff:
root@gandalf:/etc/samba# smbclient //gandalf/publicstuff -Uluthien
Password:
Domain=[MIDDLEEARTH] OS=[Unix] Server=[Samba 3.0.14a-Ubuntu]
smb: \> dir
  .                                   D        0  Tue Nov 15 09:23:49
2005
  ..                                  D        0  Sun Oct 30 10:30:03
2005
```

```
    mp3                                 D        0  Tue Nov 15 09:27:02
2005
    movies                              D        0  Tue Nov 15 07:01:34
2005
    ebooks                              D        0  Tue Nov 15 09:25:50
2005

                57004 blocks of size 1048576. 42478 blocks available
  smb: \> q
  root@gandalf:/etc/samba#
  Μπορούμε άραγε να μπούμε και στον πόρο admins;
  root@gandalf:/etc/samba# smbclient //gandalf/admins -Uluthien
  Password:
  Domain=[MIDDLEEARTH] OS=[Unix] Server=[Samba 3.0.14a-Ubuntu]
  tree connect failed: NT_STATUS_ACCESS_DENIED
```

Με πειράματα θα φτάσετε στο επιθυμητό αποτέλεσμα.

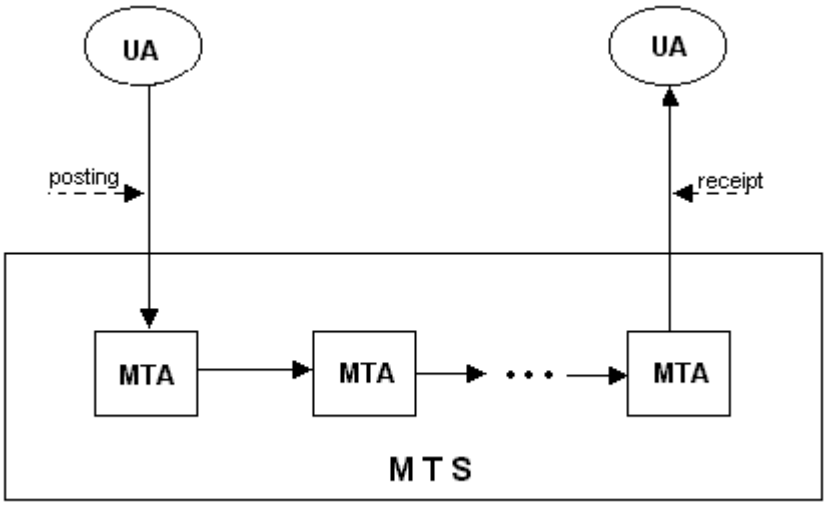
Postfix MTA

Εισαγωγή – Το Ηλεκτρονικό Ταχυδρομείο

Το ηλεκτρονικό ταχυδρομείο επιτρέπει την αποστολή μηνυμάτων μεταξύ των χρηστών του Διαδικτύου. Οι διευθύνσεις του ηλεκτρονικού ταχυδρομείου βασίζονται στις διευθύνσεις του Internet και έχουν την μορφή *"user@domain"*, όπου *user* το όνομα του χρήστη και *domain* το όνομα του υπολογιστή.

Παρακάτω φαίνεται πως μεταφέρονται τα ηλεκτρονικά μηνύματα. *Ο User Agent (UA)* είναι το πρόγραμμα client στον υπολογιστή του χρήστη που αναλαμβάνει την διαχείριση και ανάκτηση του ταχυδρομείου. Με την βοήθεια αυτού του προγράμματος ο χρήστης γράφει τα μηνύματα του, τα στέλνει, παραλαμβάνει άλλα μηνύματα και τα διαβάζει. Ο *Mail Transfer Agent (MTA)* παραλαμβάνει τα μηνύματα από τον UA και τα προωθεί στον επόμενο MTA μέχρι να βρεθεί ο MTA που έχει άμεση σύνδεση με τον υπολογιστή του χρήστη. Ο τελευταίος MTA επικοινωνεί με τον UA του παραλήπτη για την παράδοση των μηνυμάτων. Το σύνολο των MTA καλείται *Message Transfer System (MTS)*.

Η επικοινωνία από MTA σε MTA γίνεται με χρήση του



πρωτοκόλλου *SMTP (Simple Mail Transfer Protocol*, ενώ η επικοινωνία του UA με τον MTA γίνεται με χρήση των πρωτοκόλλων *POP (Post Office Protocol)* και IMAP *(Internet Message Access Protocol)*. Τα ίδια τα μηνύματα συντάσσονται με βάσει το πρωτόκολλο *MIME (Multipurpose Internet Mail Extensions)* ή με το RFC822.

Το παραπάνω σύστημα παράδοσης του ηλεκτρονικού ταχυδρομείου επιτρέπει το ηλεκτρονικό ταχυδρομικό του χρήστη να βρίσκεται σε κάποιον server και έτσι δεν είναι απαραίτητο να είναι εν λειτουργία ο υπολογιστή του αποδέκτη κατά την αποστολή του μηνύματος. Ο αποδέκτης θα παραλάβει τα μηνύματα του όταν ανοίξει τον υπολογιστή του και συνδεθεί με τον server (MTA).

Εμείς θα ασχοληθούμε με το POSTFIX που είναι ο εξ' ορισμού MTA του UBUNTU, την εγκατάσταση, τις ρυθμίσεις και τις κυριότερες λειτουργίες του και τον COURIER-POP3 για τη λήψη – αποστολή των μηνυμάτων τοπικά.

Εγκατάσταση – Πρώτες Ρυθμίσεις

Κατ' αρχάς πρέπει να εγκαταστήσουμε το Postfix με SMTP-AUTH (smtp authentication module) και TLS (ένα ασφαλές πλαίσιο επικοινωνίας):

apt-get install postfix postfix-tls libsasl2 sasl2-bin libsasl2-modules libdb3-util procmail

dpkg-reconfigure postfix

και απαντάμε στις ερωτήσεις ως εξής:

- Internet Site
- NONE
- srv.firiki.gr
- firiki.gr, middleearth, localhost, localhost.localdomain
- No
- 127.0.0.0/8
- Yes
- 0
- +
- all

Έπειτα εκτελούμε με τη σειρά τις ακόλουθες εντολές:

```
### Configure Postfix to do SMTP AUTH using SASL (saslauthd)
postconf -e 'smtpd_sasl_local_domain ='
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'smtpd_sasl_security_options = noanonymous'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
postconf -e 'inet_interfaces = all'
echo 'pwcheck_method: saslauthd' >> /etc/postfix/sasl/smtpd.conf
echo 'mech_list: plain login' >> /etc/postfix/sasl/smtpd.conf

### Generate certificates to be used for TLS encryption and/or certificate Authentication
mkdir /etc/postfix/ssl
cd /etc/postfix/ssl/
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
chmod 600 smtpd.key
openssl req -new -key smtpd.key -out smtpd.csr
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
```

```
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
mv -f smtpd.key.unencrypted smtpd.key
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650

### Configure Postfix to do TLS encryption for both incoming and outgoing mail
postconf -e 'smtpd_tls_auth_only = no'
postconf -e 'smtp_use_tls = yes'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtp_tls_note_starttls_offer = yes'
postconf -e 'smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key'
postconf -e 'smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt'
postconf -e 'smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem'
postconf -e 'smtpd_tls_loglevel = 1'
postconf -e 'smtpd_tls_received_header = yes'
postconf -e 'smtpd_tls_session_cache_timeout = 3600s'
postconf -e 'tls_random_source = dev:/dev/urandom'
postconf -e 'myhostname = srv.firiki.gr'
Το αρχείο /etc/postfix/main.cf πρέπει να δείχνει κάπως έτσι:
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
myhostname = srv.firiki.gr
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = firiki.gr, middleearth, localhost.localdomain, localhost
mynetworks = 127.0.0.0/8
mailbox_command =
mailbox_size_limit = 0
```

```
recipient_delimiter = +
relayhost =
inet_interfaces = all
smtpd_sasl_local_domain =
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
smtpd_tls_auth_only = no
smtpd_use_tls = yes
smtp_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_sesiion_cache_timeout = 3600
tls_random_source = dev:/dev/urandom
```

Ας κλείσουμε και ξαναεκινήσουμε το Postfix:

```
/etc/init.d/postfix restart
```

Ο έλεγχος ταυτότητας (authentication) θα γίνεται μέσα από το saslauthd. Επειδή τρέχει chrooted (περιορισμένος χρήστης σε συγκεκριμένο τμήμα του λειτουργικού) στο */var/spool/postfix* , πρέπει να κάνουμε τα παρκάτω:

```
mkdir -p /var/spool/postfix/var/run/saslauthd
rm -fr /var/run/saslauthd
```

Τώρα πρέπει στο αρχείο */etc/default/saslauthd* να κάνουμε κάποιες αλλαγές. Πρέπει να αφαιρέσουμε το σχόλιο από τη γραμμή # START = yes και να προσθέσουμε τη γραμμή *PARAMS="-m /var/spool/postfix/var/run/saslauthd"*

Τέλος πρέπει να προσθέσουμε σχόλιο στο */etc/init.d/saslauthd* στη γραμμή *dir=`dpkg-statoverride --list $PWDIR` που θα γίνει:*

```
#dir=`dpkg-statoverride --list $PWDIR`
```

και να αλλάξουμε τις μεταβλητές PWDIR και PIDFILE και να προσθέσουμε τη μεταβλητή dir στην αρχή του αρχείου:

```
PWDIR="/var/spool/postfix/var/run/${NAME}"
PIDFILE="${PWDIR}/saslauthd.pid"
```

dir="root sasl 755 ${PWDIR}"

και ας ξεκινήσουμε το saslauthd

/etc/init.d/saslauthd

Για να δούμε αν το SMTP-AUTH και το TLS δουλεύουν εκτελούμε:

telnet localhost 25

Όταν συνδεθούμε με το Postfix γράφουμε

ehlo localhost

Αν στα αποτελέσματα δούμε 250-AUTH κάτι και 250-STARTTLS όλα πήγαν καλά.

root@gandalf:/etc/init.d# telnet localhost 25

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

220 srv.comtek.gr ESMTP Postfix (Ubuntu)

ehlo localhost

250-srv.comtek.gr

250-PIPELINING

250-SIZE 10240000

250-VRFY

250-ETRN

250-STARTTLS

250-AUTH LOGIN PLAIN

250-AUTH=LOGIN PLAIN

250 8BITMIME

quit

221 Bye

Connection closed by foreign host.

root@gandalf:/etc/init.d#

(Παράδειγμα από πραγματική χρήση)

Τέλος θα εγκαταστήσουμε το Courier-POP3 και μάλιστα με SSL (Secure Socket Layer) encryption και επικοινωνία στην θύρα 995

apt-get install courier-authdaemon courier-base courier-pop courier-pop-ssl courier-ssl gamin libgamin0 libglib2.0-0

και απαντάμε No και OK στις δύο ερωτήσεις που μας γίνονται και επίσης

postconf -e 'home_mailbox = Maildir/'

postconf -e 'mailbox_command ='

για να χρησιμοποιούνται οι φάκελοι Maildir των χρηστών για τα μηνύματά

```
τους.

  Μπορούμε τώρα να φτιάξουμε το αρχείο /etc/aliases στο οποίο να έχουμε
ψευδώνυμα χρηστών που να αντιστοιχούν σε πραγματικούς χρήστες του
συστήματος όσο αφορά τα e-mail. Π.χ. Εγγραφές της μορφής:

  root:  stavros #Μηνύματα που πανε στο χρήστη root απευθύνονται και στο
χρήστη stavros

  clamav: root

  admin: admin

  info: info@firiki.gr #μηύματα που πάνε στο χρήστη info πάνε στη
διεύθυνση info@firiki.gr

  webmaster: webmaster@firiki.gr
```

Primary Domain Controller LDAP σε λειτουργικό σύστημα Linux Διανομή Ubuntu (6.06 LTS) Server (Έκδοση 1)

Εισαγωγή

Σημερινή κατάσταση

Η ανάγκη για μία κεντρική διαχείριση χρηστών και πόρων ενός δικτύου Η/Υ έχει οδηγήσει στην δημιουργία της έννοιας του Primary Domain Controller (PDC Server) ή ελληνικά του Κεντρικού Διαχειριστή Τομέα. Σκοπός του PDC Server είναι η διευκόλυνση του διαχειριστή/ων ενός δικτύου Η/Υ στην προσπάθεια να εγκαταστήσει και να συντηρήσει το δίκτυο των Η/Υ καθώς και τους χρήστες του. Για να επιτευχθεί αυτό πρέπει να ικανοποιηθούν κάποιες προδιαγραφές:

- Κεντρική διαχείριση όλου του δικτύου από ένα μηχάνημα.
- Κεντρική διαχείριση λογαριασμών χρηστών που συνδέονται σε ένα δίκτυο Η/Υ.
- Υπηρεσίες υποστήριξης για την λειτουργία των παραπάνω.

Για την κάλυψη λοιπόν των παραπάνω προδιαγραφών επινοήθηκε η έννοια των υπηρεσιών καταλόγου. Η υπηρεσία καταλόγου είναι ουσιαστικά η συγκέντρωση πληροφοριών που αφορούν ένα δίκτυο Η/Υ και η εύκολη διαχείριση αυτών. Για την υλοποίηση της υπηρεσίας καταλόγου προτάθηκε από την υπηρεσία Network Working Group το πρωτόκολλο X.500(OSI Standard). Βάση αυτού του πρωτοκόλλου αναπτύχθηκε το πρωτόκολλο LDAP το οποίο αποτελεί μία “ελαφριά” έκδοση του X500 καθώς δεν απαιτεί μεγάλο υπολογιστικό φόρτο εργασίας λόγω του ότι εκτελεί λιγότερες διαδικασίες από ότι το OSI X.500. Παράλληλα έχουν αναπτυχθεί και άλλες λύσεις όπως το NDS της Novell, το Active Directory System της Microsoft κ.α. Στο Λ.Σ Unix παραδοσιακά οι υπηρεσίες καταλόγου παρεχόταν μέσω του NIS το οποίο όμως φαίνεται να παραγκωνίζεται τα τελευταία χρόνια από το LDAP.

Σήμερα στα περισσότερα σχολεία η διαχείριση των πόρων ενός δικτύου Η/Υ καθώς και των χρηστών γίνεται κατά συντριπτική πλειοψηφία μέσω Windows Servers (Windows 2003 Server) και την χρήση του Active Directory. Εδώ θα παρουσιαστεί πως μπορούμε να φθάσουμε στο ίδιο αποτέλεσμα με προϊόντα ανοικτού λογισμικού (Ubuntu Linux) παρέχοντας τις αντίστοιχες υπηρεσίες.

Τι είναι το LDAP

Το LDAP (Lightweight Directory Access Protocol) είναι ένα ελαφρύ πρωτόκολλο επικοινωνίας πελάτη εξυπηρετητή με στόχο στην πρόσβαση υπηρεσιών καταλόγου, βασισμένο ειδικά στο X.500 πρωτόκολλο υπηρεσιών καταλόγου. Το πρωτόκολλο LDAP εκτελείται στο ανώτερο επίπεδο του προτύπου TCP/IP που αποτελεί και στόχο της παρούσας μελέτης.

Πως λειτουργεί ο LDAP Server

Για την παροχή υπηρεσιών καταλόγου ένας ή παραπάνω LDAP servers συνεργάζονται για να δημιουργήσουν το LDAP δέντρο καταλόγου ή την βάση δεδομένων LDAP. Ένας πελάτης LDAP συνδέεται με τον LDAP server και θέτει μία ερώτηση. Ο server απαντά στην ερώτηση είτε δίνοντας την απάντηση που θέλει ο πελάτης είτε δείχνοντας του ποιος server μπορεί να απαντήσει στην ερώτηση του πελάτη (Συνήθως ένας άλλος server). Ανεξάρτητα από τον LDAP server στον οποίο θα συνδεθεί, ο πελάτης πάντα λαμβάνει την ίδια όψη του καταλόγου: Ένα όνομα καταλόγου στο οποίο αναφέρεται ένας LDAP server είναι το ίδιο και σε κάποιον άλλο LDAP server του δικτύου. Με αυτό τον τρόπο έχουμε μία ενιαία υπηρεσία καταλόγου μέσω του πρωτοκόλλου LDAP.

Εγκατάσταση

Προγράμματα εγκατάστασης

Τα προγράμματα που θα εγκαταστήσουμε αναφέρονται παρακάτω.

- LDAPv3 (έκδοση 2.2.26 ημερ. 28-04-2005)
- Samba(έκδοση 3.0.14a Ubuntu)
- DNS Server
- Webmin (προαιρετικά)
- Apache2 Web Server
- Phpldapadmin

Βήμα 1 Εγκατάσταση του DNS Server

Επειδή η υπηρεσία καταλόγου χρειάζεται έναν τομέα πάνω στον οποίο θα λειτουργήσει πρέπει αρχικά να εγκατασταθεί και να λειτουργήσει ένας DNS Server. Το πώς γίνεται αυτή η διαδικασία μπορείτε να διαβάσετε σε άλλο κεφάλαιο των σημειώσεων.

Βήμα 2 Εγκατάσταση Apache2 Web Server

Ο web server χρειάζεται για την λειτουργία του εργαλείου Phpldapadmin το οποίο αποτελεί ένα γραφικό περιβάλλον για την διαχείριση του LDAP Server. Το πως γίνεται αυτή η διαδικασία μπορείτε να το διαβάσετε στο κεφάλαιο εγκατάστασης του Apache Web Server. Πρέπει να προσέξετε ώστε να εγκαταστήσετε οπωσδήποτε το module php4-ldap.

```
sudo apt-get install --force-yes -y apache2 php4 php4-ldap libapache2-mod-
php4
```

Βήμα 3 Εγκατάσταση του LDAP Server

Για την εγκατάσταση του LDAP Server:

slapd: είναι το πακέτο προγραμμάτων που υποστηρίζουν τον Open Ldap Server.

smbldap-tools: Είναι ένα πακέτο προγραμμάτων που περιλαμβάνει μία σειρά απο scripts που σκοπό έχουν την διαχείριση χρηστών και ομάδων που αποθηκεύονται σε έναν ldap Server.

ldap-utils: Είναι ένα πακέτο προγραμμάτων που περιλαμβάνει βοηθήματα (utilities) για την διαχείριση του Ldap Server.

openssl: Είναι ένα πακέτο προγραμμάτων που περιλαμβάνει την βιβλιοθήκη δημιουργίας openssl κρυπτογράφησης.

libldap2: Είναι ένα πακέτο βιβλιοθηκών που χρησιμοποιούνται απο κοινού απο τον Ldap Server και Ldap Client.

Οπότε δίνουμε την εντολή

```
sudo apt-get install --force-yes -y slapd smbldap-tools ldap-utils openssl libldap2
```

Κάποια στιγμή θα μας ζητηθεί να δώσουμε έναν κωδικό για τον LDAP Server. Σημειώστε τον κάπου γιατί θα είναι ο κωδικός διαχείρισης του LDAP Server. Αφού εγκαταστήσουμε επιτυχημένα τον LDAP server στην συνέχεια πρέπει να ορίσουμε σωστά την παραμετροποίηση του μέσω του αρχείου ***slapd.conf***. Για αυτό τον λόγο βρίσκουμε αυτό το αρχείο το οποίο στο Ubuntu πρέπει να βρίσκεται στην παρακάτω τοποθεσία:

```
/etc/ldpap/slapd.conf
```

Για να δοκιμάσουμε αν το αρχείο slapd.conf δεν έχει κάποιο συντακτικό λάθος δίνουμε την εντολή **slapdtest**. Στο αρχείο αυτό ορίζουμε τις γενικές οδηγίες για την λειτουργία του LDAP server καθώς και τον τρόπο με τον οποίο συνδέεται στην βάση του LDAP Server. Στην περίπτωση του ubuntu η βάση αυτή είναι η BDB (Berkley DataBase).

Δομή του αρχείου slpad.conf

Το αρχείο slapd.conf είναι το αρχείο παραμετροποίησης του LDAP Server. Το αρχείο χωρίζεται σε 3 τομείς.

1. Γενικός τομέας (Global)
2. τομέας παραμετροποίησης backend (Backend Specific)
3. τομέας παραμετροποίησης βάσης δεδομένων (Database specific)

Γενικός τομέας

Οι οδηγίες παραμετροποίησης που αναφέρονται στον γενικό τομέα αποτελούν τις γενικές οδηγίες και εφαρμόζονται στους άλλους δύο τομείς παραμετροποίησης εκτός εάν ορισθούν διαφορετικά στον τομέα παραμετροποίησης βάσεων δεδομένων είτε σε συγκεκριμένο backend του τομέα παραμετροποίησης backend. Οι οδηγίες παραμετροποίησης του γενικού τομέα είναι προκαθορισμένες και δεν θα τις αναλύσουμε εδώ. Για περισσότερες πληροφορίες μπορείτε να δείτε τον οδηγό slapdconfig στην διεύθυνση www.openldap.org.

Τομέας παραμετροποίησης backend

Ο τομέας παραμετροποίησης backend καθορίζει τον τύπο backend που θα χρησιμοποιηθεί για την αποθήκευση των δεδομένων των υπηρεσιών του καταλόγου και έχει την παρακάτω

παράμετρο:

backend <type> όπου type τον τύπο της backend βάσης.

Τομέας παραμετροποίησης βάσεων δεδομένων

Ο τομέας παραμετροποίησης βάσεων δεδομένων περιλαμβάνει οδηγίες για την παραμετροποίηση της βάσης που έχει ορισθεί μέσω της παραμέτρου backend στον προαναφερόμενο τομέα backend. Εδώ ορίζονται χαρακτηριστικά όπως το όνομα της βάσης δεδομένων, το όνομα του domain κ.α. Μπορούμε να έχουμε απο πριν ορισμένες τις οδηγίες για περισσότερες από μία βάσεις δεδομένων αλλά θα πρέπει να κάνουμε ορίσουμε ως ενεργή μία βάση δεδομένων με την χρήση της παραμέτρου backend <type> όπως έχουμε προαναφέρει. Στην περίπτωση μας θα χρησιμοποιήσουμε ως βάση την βάση BDB (Berkeley DB Transactional Backend). Οι ελάχιστες οδηγίες-παράμετροι που πρέπει να ορισθούν είναι οι παρακάτω:

- **database:** bdb Εδώ ορίζουμε την βάση που θα χρησιμοποιήσουμε
- **suffix (κατάληξη):** Πρέπει να ορίσουμε κατάληξη του τομέα (domain) τον οποίο υποστηρίζει η βάση μας. Μπορούμε να ορίσουμε παραπάνω από μία καταλήξεις αλλά πρέπει οπωσδήποτε να ορίσουμε τουλάχιστον μία. π.χ (testschool.gr)
- **rootdn (root Distinguished Name= Το μονοπάτι στην δομή του LDAP δέντρου για τον μοναδικό προσδιορισμό του root):** Η παράμετρος αυτή καθορίζει το DN που δεν υπόκειται σε κανενός είδους έλεγχο ή περιορισμό από την βάση. (ουσιαστικά εννοείται ο λογαριασμός διαχειριστή του συστήματος). Το DN μπορεί να αναφέρεται σε μία ταυτότητα κρυπτογράφησης SASL. Ο χρήστης που ορίζεται εδώ δεν είναι απαραίτητο να έχει εγγραφεί στον κατάλογο LDAP. Π.χ rootdn "cn="**admin_ldap,dc=kvwn"**
- **rootpw:** Η παράμετρος αυτή ορίζει τον κωδικό για τον λογαριασμό rootdn. Η τιμή του κωδικού μπορεί να εμφανίζεται όπως είναι ορισμένη με κίνδυνο φυσικά για την ασφάλεια, είτε με κωδικοποίηση hash, π.χ για τον κωδικό secret μπορούμε να τον ορίσουμε με τους παρακάτω δύο τρόπους:
  - rootpw secret
  - rootpw {SSHA}ZKKuqbEKJfKSXhUbHG3fG8MDn9j1v4QN όπου το SSHA αναφέρεται στην μέθοδο hash που χρησιμοποιήθηκε και ακολουθεί ο παραγόμενος κωδικός της λέξης secret με την μέθοδο SSHA

Για να παράγουμε τον κωδικό, με την μέθοδο hash, που θέλουμε να χρησιμοποιήσουμε στο αρχείο slapd.conf μπορούμε να κάνουμε χρήση της εντολής **slappasswd**.

- directory <path> Εδώ ορίζουμε που βρίσκονται τα αρχεία της βάσης μας, είναι συνήθως σωστά ορισμένο απο πρίν και δεν χρειάζεται αλλαγή.
- **index** Εδώ ορίζουμε τους δείκτες της βάσης. Συνήθως ορίζουμε μόνο έναν δείκτη τον :
  - index objectClass eq ο οποίος λειτουργεί σαν δείκτης σε όλες τις κλάσεις τύπου object.

Φυσικά υπάρχουν και άλλες παράμετροι για την βάση άλλα θα τις προσπεράσουμε καθώς ξεφεύγουν από τα όρια του παρόντος οδηγού και θα επικεντρωθούμε στον έλεγχο της πρόσβασης και πως αυτός επιτυγχάνεται.

Έλεγχος πρόσβασης

Ο έλεγχος της πρόσβασης επιτυγχάνεται με οδηγίες που μπορούν να ορισθούν οπουδήποτε στο αρχείο slapd.conf και ανάλογα να έχουν διαφορετική ισχύ. Καταρχήν η δομή των εντολών πρόσβασης ελέγχου είναι η παρακάτω:

```
        <access directive> ::= access to <what>
                [by <who> <access> <control>]+
        <what> ::= * |
                [dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]
                [filter=<ldapfilter>] [attrs=<attrlist>]
        <basic-style> ::= regex | exact
        <scope-style> ::= base | one | subtree | children
         <attrlist> ::= <attr> [val[.<basic-style>]=<regex>] | <attr> ,
<attrlist>
        <attr> ::= <attrname> | entry | children
        <who> ::= * | [anonymous | users | self
                                | dn[.<basic-style>]=<regex> | dn.<scope-
style>=<DN>]
                [dnattr=<attrname>]
                                [group[/<objectclass>[/<attrname>][.<basic-
style>]]=<regex>]
                [peername[.<basic-style>]=<regex>]
                [sockname[.<basic-style>]=<regex>]
                [domain[.<basic-style>]=<regex>]
                [sockurl[.<basic-style>]=<regex>]
                [set=<setspec>]
                [aci=<attrname>]
        <access> ::= [self]{<level>|<priv>}
        <level> ::= none | auth | compare | search | read | write
        <priv> ::= {=|+|-}{w|r|s|c|x|0}+
        <control> ::= [stop | continue | break]
```

Η πρώτη σημαντική παράμετρος είναι η **access to <what>** η οποία προσδιορίζει που εφαρμόζεται η εντολή ελέγχου. Η εφαρμογή της μπορεί να είναι σε ένα αντικείμενο (object) κλάσης ή χαρακτηριστικό (attribute). Για περισσότερες πληροφορίες σχετικά με την π αράμετρο μπορείτε να δείτε στην διεύθυνση http://www.openldap.org/doc/admin23/slapdconfig.html

Στην συνέχεια πρέπει να ορίσουμε την παράμετρο **by <who>** η οποία προσδιορίζει το ποιός θα έχει πρόσβαση στα αντικείμενα και χαρακτηριστικά που έχουν δηλωθεί με την παράμετρο what. Ακολουθεί ο πίνακας με τις παραμέτρους που μπορεί να λάβει η εντολή who.

Specifier	Entities
*	Οποιοσδήποτε, συμπεριλαμβανόμενων ανώνυμων ή πιστοποιημένων χρηστών . (All, including anonymous and

	authenticated users)
anonymous	Ανώνυμοι μη πιστοποιημένοι χρήστες (Anonymous (non-authenticated) users)
users	Πιστοποιημένοι χρήστες Authenticated users
self	User associated with target entry
dn[.<basic-style>]=<regex>	Users matching a regular expression
dn.<scope-style>=<DN>	Users within scope of a DN

Τέλος έχουμε την παράμετρο **<access>** που χαρακτηρίζει τον τύπο της πρόσβασης και μπορεί να πάρει τις παρακάτω τιμές:

Level	Privileges	Description
none	=0	Μη πρόσβασιμο no access
auth	=x	needed to bind
compare	=cx	needed to compare
search	=scx	needed to apply search filters
read	=rscx	needed to read search results
write	=wrscx	needed to modify/rename

Όταν γίνεται αίτηση από έναν LDAP πελάτη εξετάζεται αν στην ενέργεια στην οποία θέλει να προβεί ο πελάτης π.χ. γράψιμο ενός αρχείου, έχει ο πελάτης ίσα ή παραπάνω δικαιώματα σε σχέση με τα δικαιώματα που απορρέουν από τον έλεγχο πρόσβασης στο slapd.conf. Αν δεν έχει τότε απορρίπτεται η αίτηση του.

Σειρά εκτέλεσης των εντολών ελέγχου

Όταν γίνεται μία αίτηση από έναν LDAP πελάτη πραγματοποιείται η ακόλουθη σειρά εκτέλεσης των εντολών ελέγχου πρόσβασης:

1. Ελέγχονται οι εντολές ελέγχου πρόσβασης στον τομέα παραμετροποίησης της βάσης δεδομένων και συγκεκριμένα ελέγχεται η βάση στην οποία είναι αποθηκευμένη η εγγραφή για την οποία ζητήθηκε η πρόσβαση.
2. Στην συνέχεια ο τομέας παραμετροποίησης της βάσης δεδομένων μπορεί να έχει παραπάνω από μία εντολές ελέγχου πρόσβασης. Σε αυτή την περίπτωση ο έλεγχος γίνεται σειριακά εντολή προς εντολή και η σάρωση των εντολών ελέγχου σταματά όταν η εγγραφή ταιριάξει με μία από τις δομές ελέγχου πρόσβασης (δηλαδή ελέγχεται η παράμετρος what). Η εντολή ελέγχου που ταίριασε θα χρησιμοποιηθεί για τον έλεγχο του who, δηλαδή του ποιος έχει δικαιώματα για αυτή την εγγραφή. Στην συνέχεια θα ελεγχθεί και το access, δηλαδή ο τύπος πρόσβασης από την ίδια εντολή ελέγχου.

3. Εφόσον τελειώσουν οι δομές ελέγχου χωρίς επιτυχές ταίριασμα στον τομέα παραμετροποίησης της βάσης δεδομένων, ξεκινά ο έλεγχος του Γενικού Τομέα όπου πάλι ακολουθείται η σειριακή αναζήτηση στις εντολές ελέγχου του Γενικού Τομέα.

Βάση των παραπάνω βγαίνει το συμπέρασμα ότι οι εντολές ελέγχου που προσδιορίζουν συγκεκριμένα αντικείμενα ή χαρακτηριστικά, καθώς και οι παράμετροι who και access εφόσον αφορούν ένα εξειδικευμένο υποσύνολο του δικτύου θα πρέπει να καταγράφονται πρώτες, ειδάλλως πάντα θα επικαλύπτονται από πιο γενικές εντολές ελέγχου. Παρακάτω ακολουθεί ένα γενικό παράδειγμα κατανόησης που δεν μπορεί φυσικά να χρησιμοποιηθεί απευθείας σε ένα αρχείο slapd.conf άλλα είναι απλοποιημένο για λόγους ευκολίας κατανόησης.

Έστω ότι έχουμε την ριζική περιοχή Ελλάδα dn=”Ellada” και το αντικείμενο Kavala.

Εστω ότι έχουμε δύο εντολές ελέγχου και ότι ισχύει ότι το αντικείμενο kavala ανήκει στο υποσύνολο του αντικειμένου Ellada..

1. access to Ellada by * write
2. access to kavala by Γιάννης read

Έστω ότι τις βάλαμε στον τομέα της παραμετροποίησης βάσεων δεδομένων με την παραπάνω σειρά. Έστω λοιπόν ότι έρχεται κάποια στιγμή ο χρήστης ο οποίος είναι καταχωρημένος στο σύστημα μας ως Γιάννης και κάνει αίτηση να γράψει στο αντικείμενο kavala. Σύμφωνα με την παραπάνω δομή πρώτα θα εκτελεστεί η εντολή ελέγχου 1. Από την δομή της εντολής δίνεται το δικαίωμα σε όλους τους χρήστες να γράψουν στο αντικείμενο Ellada το οποίο περιέχει το αντικείμενο kavala. Άρα η δομή ελέγχου 1 δίνει το δικαίωμα σε οποιονδήποτε χρήστη (*) να γράψει στο αντικείμενο Ellada άρα και στο αντικείμενο kavala. Εδώ τελειώνει και η ανάγνωση των εντολών ελέγχου αφού ταίριασε μία εντολή ελέγχου με την αίτηση του πελάτη. Με αυτό όμως τον τρόπο υπερκαλύπτεται η επόμενη εντολή ελέγχου 2 με αποτέλεσμα να δημιουργείται ρήγμα στην πολιτική ελέγχου πρόσβασης αφού σκοπός του διαχειριστή ήταν ο χρήστης Γιάννης να έχει δικαίωμα μόνο ανάγνωσης στο αντικείμενο kavala. Για να λειτουργήσει σωστά η πολιτική ελέγχου πρόσβασης θα έπρεπε να προηγείται η εντολή 2 της εντολής 1.

Για περισσότερα παραδείγματα με πραγματική δομή και δείτε στην διεύθυνση http://www.openldap.org/doc/admin23/slapdconfig.html

Τι θα αλλάξουμε στο slapd.conf

- suffix “dc=xxxx” όπου xxxx είναι το όνομα του τομέα μας.
- rootdn “cn=admin_ldap,dc=xxxx”
- #include /etc/ldap/schema/samba.schema σε σχόλιο γιατί θα το χρησιμοποιήσουμε αργότερα

Τέλος πρέπει να αλλάξουμε τα δικαιώματα εκτέλεσης του αρχείου slapd.conf ώστε να μπορεί να το διαβάσει και ο slapd deamon.

sudo chmod 644 /etc/ldap/slapd.conf.

Λειτουργίες διαχείρισης του LDAP Server

Για να εκκινήσουμε τον LDAP server δίνουμε την εντολή:

```
./etc/init.d/slapd start
```

Για να κάνουμε επανεκκίνηση δίνουμε την εντολή

```
./etc/init.d/slapd restart
```

Για να τον σταματήσουμε δίνουμε την εντολή

```
./etc/init.d/slapd stop
```

Βήμα 4 Εγκατάσταση του εργαλείου PhpLdapadmin

Μπορείτε να κατεβάσετε την τελευταία έκδοση του PhpLDAPadmin από την διεύθυνση http://phpldapadmin.sourceforge.net/download.php

Στην συνέχεια εγκαθιστάτε εφόσον δεν το έχετε ήδη κάνει μέσω της παρακάτω εντολής τον apache2 WebServer καθώς και την βιβλιοθήκη `php4-ldap`.

```
sudo apt-get install --force-yes -y apache2 php4 php4-ldap libapache2-mod-php4
```

Αφού το κατεβάσετε το εγκαθιστάτε στον φάκελο /var/www για να είναι προσβάσιμο μέσω του webserver. Αρχικά δίνετε την εντολή

```
sudo chmod -R 655 /var/www/xxxxxxx
```

(όπου xxxxxxxx το όνομα του φακέλου του εργαλείου PhpLdapAdmin)

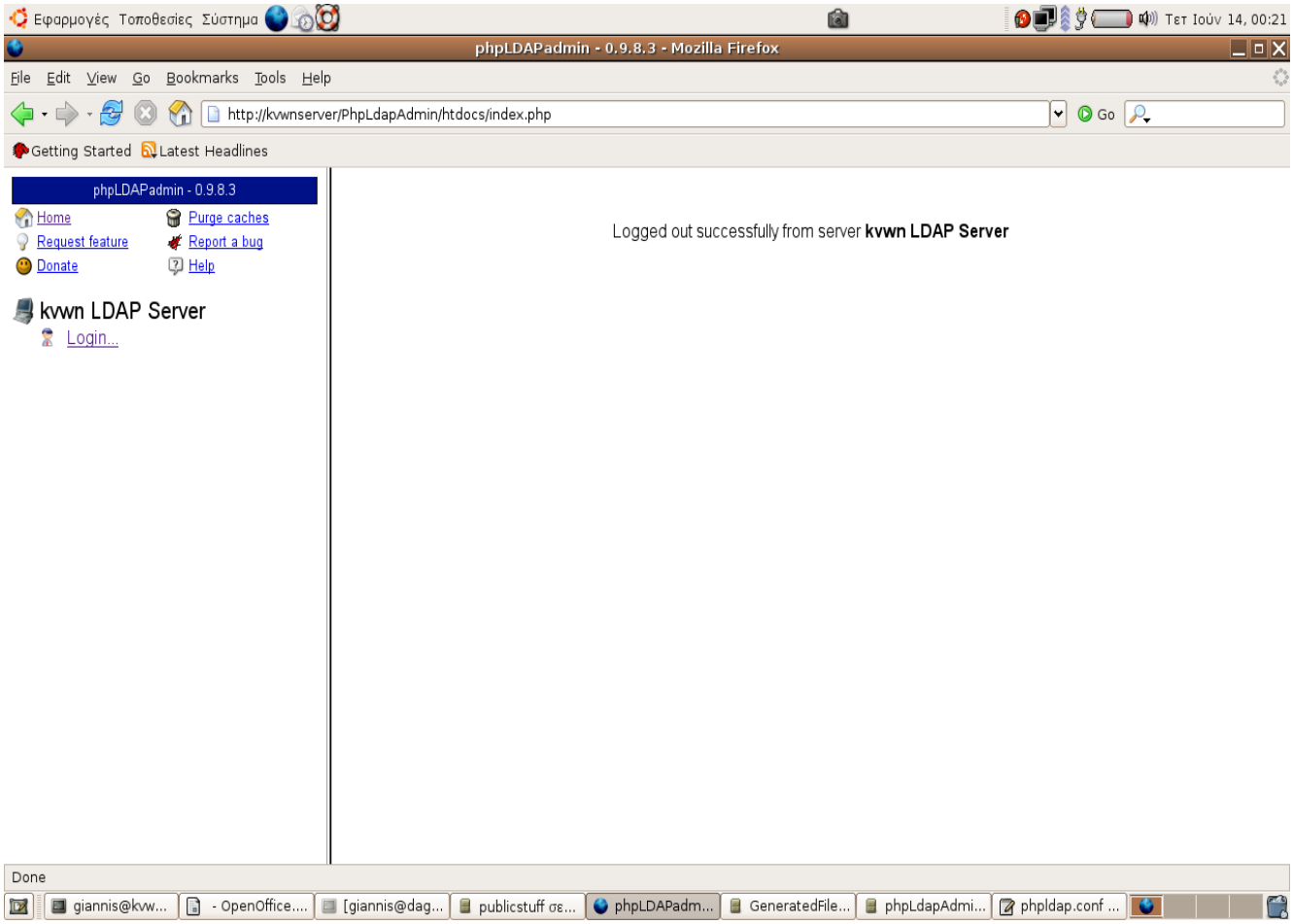
ώστε σε όλο τον φάκελο να υπάρχουν δικαιώματα ανάγνωσης και εκτέλεσης από όλους τις ομάδες αλλά και από όλους τους άλλους γενικά.

Στην συνέχεια δημιουργούμε το αρχείο config.php του οποία τις παραμέτρους ορίζουμε βάση των χαρακτηριστικών του domain μας. Το αρχείο αυτό βρίσκεται στον φάκελο config όπου μέσα εκεί υπάρχει και ένα αρχείο config.php.example το οποίο περιέχει και οδηγίες που αφορούν την παραμετροποίηση του. Αφού το φτιάξετε δίνετε την εντολή

```
sudo chmod 644 config.php
```

ώστε το αρχείο config.php να είναι αναγνώσιμο από όλους. .

Εφόσον κάνατε σωστά την παραπάνω διαδικασία στην συνέχεια μπορείτε μέσω ενός φυλλομετρητή ιστοσελίδων να χρησιμοποιήσετε το εργαλείο για να διαχειριστείτε τον LDAP Server. Αρχικά θα λάβετε την παρακάτω εικόνα.



Επιλέγοντας Login θα σας δοθεί ένα παράθυρο διαλόγου όπου θα σας προτρέπει να δώσετε τον κωδικό του διαχειριστή όπως φαίνεται στην επόμενη εικόνα.

Ο κωδικός που θα δώσετε είναι ο κωδικός του διαχειριστή που καταχωρήσατε για πρώτη φορά όταν εγκαθιστούσατε το Ldap. Εφόσον πιστοποιηθείτε με επιτυχία από το σύστημα στην συνέχεια μπορείτε να διαχειριστείτε τις εγγραφές Ldap.

Διαχείριση Εγγραφών στο Ldap

Για την διαχείριση εγγραφών στο Ldap πρέπει καταρχάς να κατανοήσουμε τις βασικές έννοιες της δόμησης των εγγραφών στο Ldap.

Δομή δέντρου του καταλόγου LDAP και Schemas

Ο κατάλογος LDAP έχει δενδρική δομή. Όλες οι εγγραφές του του καταλόγου (αντικείμενα) έχουν μία προκαθορισμένη θέση μέση στην δενδρική δομή του δέντρου και προσδιορίζονται μονοσήμαντα. Η δενδρική αυτή ιεραρχία ονομάζεται πληροφοριακός κατάλογος δέντρου (directory information tree) σε συντομογραφία DIT. Το μονοπάτι σε μία εγγραφή, το οποίο και την χαρακτηρίζει μονοσήμαντα ονομάζεται distinguished name ή DN. Οι κόμβοι που συναντούμε κατα την διαδρομή του μονοπατιού ονομάζονται relative distinguished name ή RDN.

Ο ορισμός της δομής των αντικειμένων που χρησιμοποιούνται δίδεται στα schemas. Τα schemas είναι ειδικά αρχεία με κατάληξη schema. Υπάρχουν προκαθορισμένα schemas για προκαθορισμένες δομές αντικειμένων που είναι απαραίτητο να χρησιμοποιηθούν καθώς και δομές που είναι χρήσιμο να χρησιμοποιηθούν. Επίσης μπορούμε να γράψουμε το δικό μας schema. Μπορούν να συνυπάρχουν παραπάνω από ένα schemas και ορίζονται στο αρχείο slapd.conf. Εμείς θα χρησιμοποιήσουμε τα παρακάτω schemas:

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/samba.schema
```

Κάθε schema υποστηρίζει και διαφορετικές κλάσεις αντικειμένων. Με την εντολή

```
schemacheck     on
```

στο slapd.conf αναγκάζουμε τον LDAP server να ελέγχει σε κάθε εγγραφή αντικειμένου που γίνεται, αν το υποψήφιο αντικείμενο έχει δομή που υπάρχει και ανταποκρίνεται σε ένα από τα παραπάνω schemas. Τα αρχεία των schemas βρίσκονται όπως φαίνεται στον φάκελο

```
/etc/ldap/schema/
```

Κάθε κλάση αντικειμένων περιγράφει το αντικείμενο που θα προέλθει από αυτήν με την χρήση των χαρακτηριστικών (attributes). Κάποια από αυτά τα χαρακτηριστικά είναι υποχρεωτικό να δοθούν για τον σωστό προσδιορισμό του αντικειμένου και κάποια όχι. Σαν παράδειγμα φανταστείτε ότι καταχωρούμε έναν χρήστη. Το όνομα του (username) είναι απαραίτητο να δοθεί ως χαρακτηριστικό του αντικειμένου που περιγράφει τον λογαριασμό χρήστη, ενώ δεν είναι απαραίτητο να δοθεί η διεύθυνση του σπιτιού του. Τα αντικείμενα ή καλύτερα κλάσεις αντικειμένων που περιγράφονται στα παραπάνω schemas μπορούν να κατηγοριοποιηθούν με διάφορους

τρόπους.

Καταρχάς κάποια χαρακτηρίζονται δομικά και κάποια χαρακτηρίζονται βοηθητικά. Όταν δημιουργούμε ένα αντικείμενο, το αντικείμενο αυτό μπορεί να βασίζεται μόνο σε μία δομική κλάση αντικειμένων και σε κανένα ή παραπάνω βοηθητικά. Οι ίδιες οι κλάσεις αντικειμένων έχουν ιεραρχικές σχέσεις μεταξύ τους. Όσοι γνωρίζουν την φιλοσοφία του αντικειμενοστραφούς προγραμματισμού θα κατανοήσουν πιο εύκολα τις δομές.

Τα αντικείμενα μπορούν να κατηγοριοποιηθούν και με τον παρακάτω τρόπο:

container : Τα αντικείμενα αυτού του τύπου μπορούν να περιέχουν άλλα αντικείμενα. Παραδείγματα τέτοιων αντικειμένων είναι το αντικείμενο root (το αρχικό αντικείμενο του δενδρικού καταλόγου το οποίο δεν υπάρχει στην πραγματικότητα), c (χώρα-country), ou (organization unit-μονάδα οργάνωσης) και dc (domain component -δομικό στοιχειο του τομέα). Αυτά τα αντικείμενα μπορούμε να τα παρομοιάσουμε με τους καταλόγους ενός συστήματος αρχείων.

Leaf (φύλλο): Αυτά τα αντικείμενα βρίσκονται στις άκρες του δέντρου (φύλλα) και δεν έχουν άλλα αντικείμενα πιο κάτω. Τέτοια αντικείμενα είναι τα person, InetOrgPerson, ή groupofNames. Κάθε αντικείμενο έχει μία σειρά από χαρακτηριστικά. Σε κάποια από αυτά τα χαρακτηριστικά πρέπει να δίνουμε υποχρεωτικά τιμές και σε άλλα χαρακτηριστικά η τιμή είναι προαιρετική.

Τέλος τα αντικείμενα κατηγοριοποιούνται και ανάλογα με τον σκοπό για τον οποίο είναι προορισμένα:

- Ομάδες καταλόγου, όπου περιλαμβάνονται ομάδες ομοειδών αντικειμένων ή γενικότερα ομάδες αντικειμένων.
- Τοποθεσίες, όπως το όνομα μίας χώρας και η περιγραφή της.
- Οργανισμοί.
- Άτομα.

Αρχεία ldif

Για την εισαγωγή εγγραφών στον LDAP server μπορούμε να κάνουμε χρήση των αρχείων ldif είτε να χρησιμοποιήσουμε ένα εργαλείο διαχείρισης LDAP Server όπως ο Phpldapadmin. Ο Phpldapadmin δίνει την δυνατότητα είτε να κάνουμε εισαγωγή έτοιμων εγγραφών σε ldif αρχεία είτε να τα δημιουργήσουμε από μόνοι μας μέσω του γραφικού περιβάλλοντος. Επίσης για την εισαγωγή εγγραφών μέσω αρχείων ldif, μπορούμε να χρησιμοποιήσουμε τις εντολές ldapadd, ldapdelete και ldapmodify (Για να λειτουργήσουν οι εντολές πρέπει να έχουμε κάνει εγκατάσταση μέσω apt-get την βιβλιοθήκη **ldap-utils**). Το αρχείο ldif έχει εγγραφές αντικειμένων για αντικείμενα που φυσικά θα πρέπει να είναι σωστά ορισμένα στα αντίστοιχα αρχεία schemas. Με αυτό τον τρόπο μπορούμε να βάλουμε μαζικά πολλές εγγραφές είτε μέσω της εντολής ldapadd είτε με την χρήση εργαλείων διαχείρισης LDAP.

Καταχώρηση πρώτων εγγραφών

Την πρώτη φορά λοιπόν θα πρέπει πρώτα από όλα να καταχωρήσουμε σαν εγγραφή το domain μας που θα αποτελεί και την ριζική εγγραφή του καταλόγου. Στην περίπτωση μας η ριζική εγγραφή είναι η kvwn. Για να την δημιουργήσουμε θα πρέπει να κάνουμε ένα αρχείο τύπου ldif με το παρακάτω περιεχόμενο.

```
# Organization for Example Corporation

dn: dc=kvwn

objectClass: dcObject
```

```
objectClass: organization
objectclass: simpleSecurityObject
dc: kvwn
o: kvwn test
description: Δοκιμαστική εγγραφή
userPassword: {SSHA}O6ByDXmF7U5IMaKL8n6C0wyhIt7h+SV2
```

Στην ουσία δημιουργούμε ένα νέο αντικείμενο που περιέχει τα χαρακτηριστικά από 3 άλλα αντικείμενα:

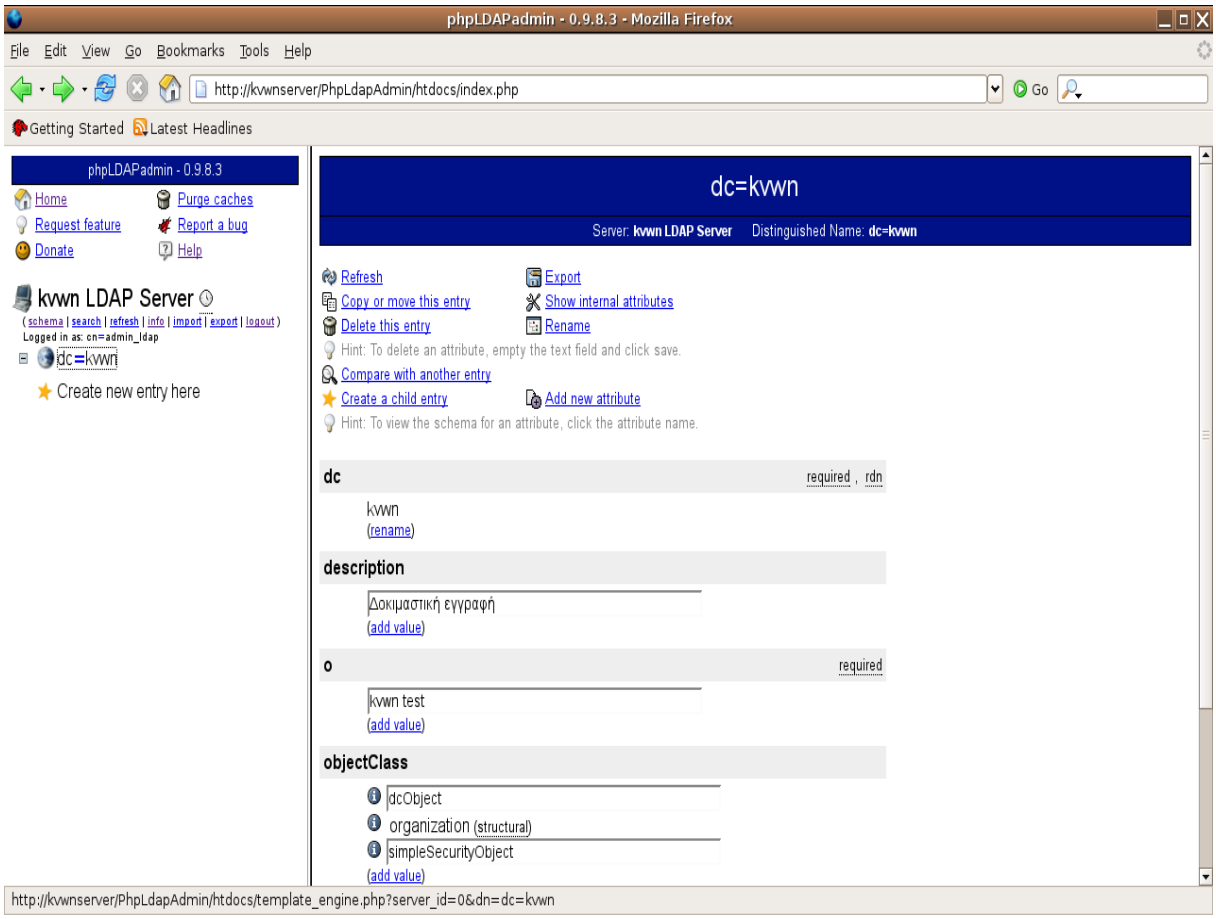
- dcObject
- organization
- simplySecurityObject

Το organization είναι το βασικό μας αντικείμενο το οποίο θα χρησιμοποιηθεί ως κύριο δομικό στοιχείο για να δημιουργηθεί το ριζικό μας αντικείμενο. Επειδή το αντικείμενο organization έχει ως απαιτούμενο χαρακτηριστικό το όνομα του (αναφερόμαστε στο χαρακτηριστικό o) για αυτό τον λόγο πρέπει να του δώσουμε μία τιμή. Επίσης πρέπει οπωσδήποτε να ορίσουμε και το userPassword που αποτελεί επίσης απαιτούμενο χαρακτηριστικό. Εδώ θα δώσετε σε μορφή hash το password που ορίσατε στην αρχή της εγκατάστασης. Επίσης υπάρχει και μία σειρά από προαιρετικά χαρακτηριστικά τα οποία δεν είμαστε υποχρεωμένοι να ορίσουμε όπως το description. Με λίγα λόγια το να μην δώσουμε τιμή στο description δεν θα επηρεάσει την εισαγωγή της εγγραφής μας. Στην συνέχεια δίνουμε την παρακάτω εντολή από το τερματικό:

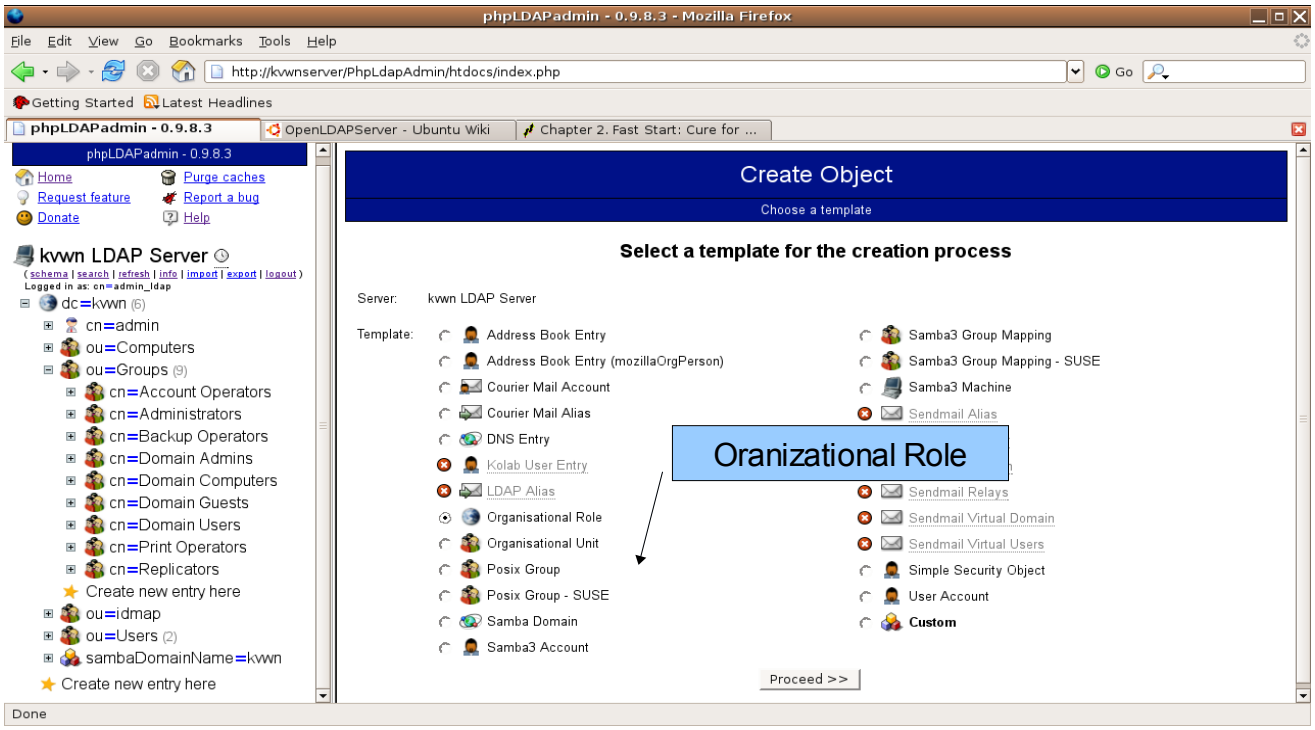
```
ldapadd -x -D "cn=admin_ldap,dc=kvwn" -w 123456 -f test.ldif
```

Με αυτή την εντολή εισάγουμε την εγγραφή που υπάρχει στο αρχείο test.ldif. Η παράμετρος -w μας δίνει την δυνατότητα να δώσουμε τον κωδικό χρήστη που στην περίπτωση μας είναι 123456. Προσοχή για να βρει το αρχείο test.ldif εφόσον δεν βρισκόμαστε στον ίδιο κατάλογο πρέπει να δώσουμε το αντίστοιχο σχετικό ή απόλυτο μονοπάτι.

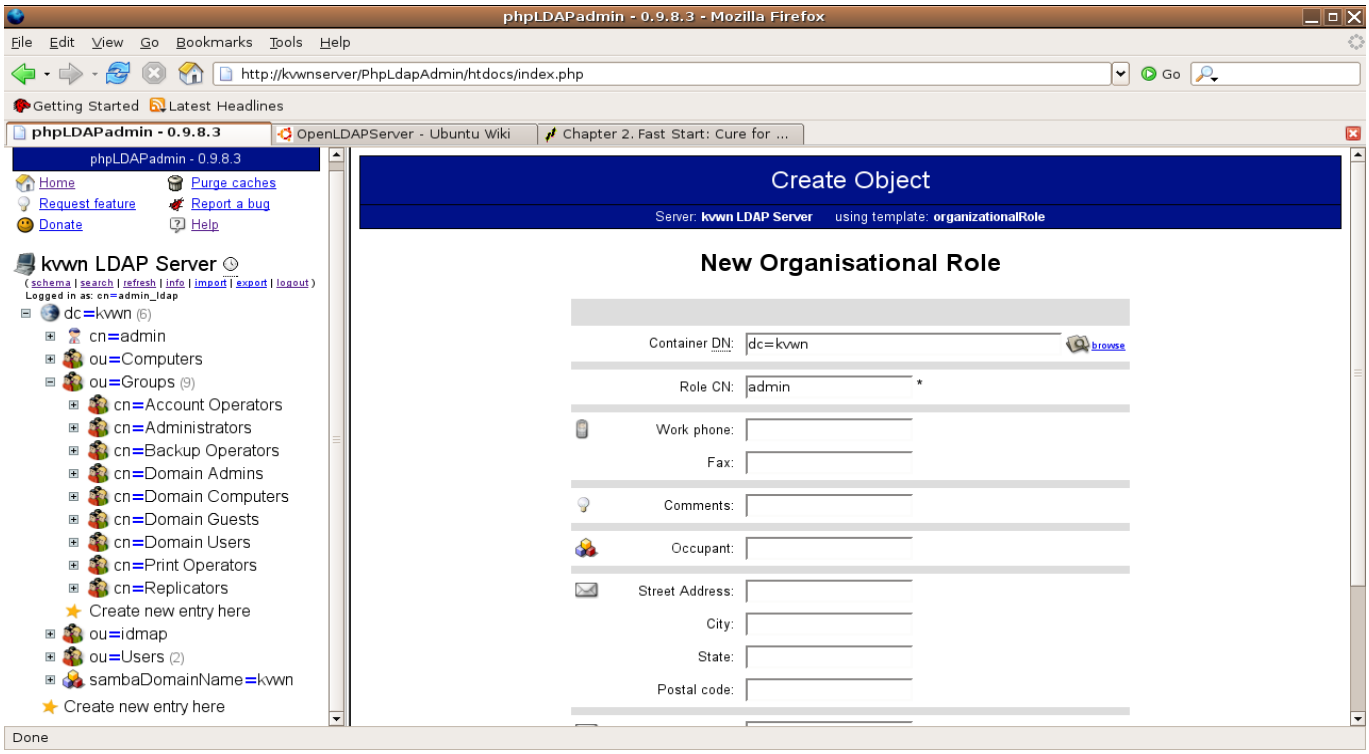
Στην συνέχεια αν πάμε από το γραφικό περιβάλλον διαχείρισης του Ldap θα δούμε ότι έχει καταχωρηθεί η εγγραφή. Αν πατήσουμε στο dc=kvwn στα αριστερά μας θα λάβουμε την παρακάτω εικόνα.



Φυσικά όπως έχουμε πει μπορούμε να καταχωρήσουμε ένα αντικείμενο και μέσα από γραφικό περιβάλλον που προσφέρουν διάφορα εργαλεία όπως το PhpLdapAdmin. Επειδή πρέπει να καταχωρήσουμε και έναν διαχειριστή που να προέρχεται από την δομική κλάση αντικειμένων organizationalRole επιλέγουμε απο το μενού στα αριστερά “Create new entry here” και στην συνέχεια όπως φαίνεται στην παρακάτω εικόνα επιλέγουμε OrganizationRole.



Αμέσως μετά θα λάβουμε την παρακάτω εικόνα.



Εδώ θα δώσουμε το υποχρεωτικό χαρακτηριστικό Role DN(σημειώνεται με *) και στην συνέχεια εφόσον θέλουμε δίνουμε και τα υπόλοιπα χαρακτηριστικά. Έπειτα καταχωρούμε την εγγραφή μας και είμαστε έτοιμοι.

Πριν προχωρήσουμε στο επόμενο βήμα, την εγκατάσταση του Samba θα πρέπει πρώτα να

αντιγράψουμε το αρχείο samba.schema στον φάκελο /etc/ldap/schema καθώς επίσης και να το προσθέσουμε στο αρχείο slapd.conf με τα συμπεριμβαλανόμενα schemas.

```
include         /etc/ldap/schema/samba.schema
```

Βήμα 5 Εγκατάσταση Samba

Το Samba είναι μία συλλογή προγραμμάτων που έχει ως σκοπό την υλοποίηση του πρωτοκόλλου SMB/CIFS. Μέσω αυτού του πρωτοκόλλου μπορούν Unix Λ.Σ να λειτουργούν ως εξυπηρετητές αρχείων ή εκτυπωτών προς διαφορετικής υλοποίησης Λ.Σ. όπως Windows, NT, OS/2, και DOS. Το Samba στην εγκατάσταση του στην διανομή Ubuntu αποτελείται από τα εξής προγράμματα:

samba: Το πακέτο προγραμμάτων που υποστηρίζει τον samba server.

samba-common: Το πακέτο αυτό αφορά προγράμματα που είναι κοινά στην λειτουργία τόσο του samba server όσο και του samba-client.

samba-doc: Το πακέτο προγραμμάτων που αφορά το επίσημο εγχειρίδιο υποστήριξης του Samba.

libcupsys2-gnutls10: Το πακέτο υποστήριξης του CUPS (Common UNIX Printing System) που αφορά την διαχείριση εκτυπωτών από το λειτουργικό σύστημα Unix.

libkrb53: Το πακέτο υποστήριξης της υπηρεσίας αυθεντικοποίησης χρηστών και υπηρεσιών στο δίκτυο με όνομα Kerberos5**.**

winbind: Το πακέτο των προγραμμάτων που υλοποιούν την υπηρεσία ανάγνωσης χρηστών και ομάδων από NT servers.

smbclient: Το πακέτο προγραμμάτων για επικοινωνία Η/Υ μέσω πρωτοκόλλου SMB/CIFS από την πλευρά του πελάτη.

smbfs: Το πακέτο προγραμμάτων που υλοποιούν την σύστημα αρχείων smbfs που υλοποιεί το πρωτόκολλο SMB/CIFS.

Για την εγκατάσταση του Samba δίνουμε την παρακάτω εντολή:

```
sudo apt-get install samba samba-common samba-doc libcupsys2-gnutls10
libkrb53 winbind smbclient smbfs
```

Αρχικά λαμβάνετε ένα αντίγραφο ασφαλείας του αρχείου smb.conf το οποίο βρίσκεται στην θέση /etc/samba.

Στην συνέχεια για να ρυθμίσουμε το Samba ώστε να λειτουργεί σωστά σύμφωνα με τις ρυθμίσεις του δικτύου μας πρέπει να επεξεργαστούμε το αρχείο smb.conf. Το αρχείο smb.conf χωρίζεται σε τομείς που ο καθένας έχει τις δικές του παραμέτρους. Αυτοί οι τομείς είναι:

1. **global Γενικός τομέας**
   - Ο γενικός τομέας αφορά τις γενικές παραμέτρους που πρέπει να ορίσουμε όπως το όνομα του domain κ.α. Εδώ αλλάζουμε τις παρακάτω παραμέτρους.
     - workgroup = xxxx, όπου xxxx είναι το domain που βρίσκεται ο Η/Υ. Π.χ. στην περίπτωση μας το kvwn
     - netbios name = xxxxx, όπου xxxxx είναι το όνομα του υπολογιστή που λειτουργεί σαν domain controller, στην περίπτωση μας ο kvwnserver
2. **Networking δίκτυο**

- Μέσα από αυτό τον τομέα μπορούμε να προσδιορίσουμε σε συγκεκριμένες συσκευές δικτύου στις οποίες θα λειτουργεί η υπηρεσία Samba αυξάνοντας έτσι την ασφάλεια του συστήματος.

3. **Debugging/Accounting**
   - Εδώ ορίζουμε που και πως θα κρατούνται τα logs.
4. **Authentication (Αυθεντικοποίηση)**
   - Εδώ ορίζουμε πως θα γίνεται η αυθεντικοποίηση των χρηστών
     - Η παράμετρος security = user
     - passdb backend = ldapsam:ldap://127.0.0.1
     - passwd program = /usr/sbin/smbldap-passwd -u "%u"
5. **Domains**
   - Σε αυτό τον τομέα ορίζουμε τα χαρακτηριστικά των domains.
   - domain logons =yes (Επιτρέπει την αυθεντικοποίηση των χρηστών του domain)
   - domain master = yes(ορίζει το Η/Υ ως τον Primary Domain Controller)
6. **Printing (Ρυθμίσεις για την πρόσβαση σε εκτυπωτές)**
   - printcap name = CUPS
   - printing = cups
7. **Misc (Οποιαδήποτε παραμετροποίηση δεν ανήκει στις παραπάνω κατηγορίες)**
8. **Share definitions (Παραμετροποίηση των μοιρασμένων καταλόγων και αρχείων)**

Πέραν των παραπάνω θα πρέπει να προσθέσουμε νέες παραμέτρους που αφορούν την συνεργασία Ldap και Samba.

```
ldap suffix = dc=kvwn
ldap admin dn = cn=admin_ldap, dc = kvwn
ldap idmap suffix = ou=idmap
ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap passwd sync = Yes
ldap ssl = no
```

Για την σωστή κωδικοποίηση των χαρακτήρων στην επικοινωνία με windows λειτουργικά πρέπει να προσθέσουμε τις παρακάτω παραμέτρους:

```
Dos charset = 850
unix charset = LOCALE
preserve case = yes
short preserve case = yes
case sensitive = no
```

Επίσης πρέπει να ορίσουμε τα scripts που θα εκτελούνται σε διάφορες διαδικασίες

```
#scripts section
```

```
        add machine script = /usr/sbin/smbldap-useradd -w "%u"
        add user script = /usr/sbin/smbldap-useradd -m "%u"
        delete user script = /usr/sbin/smbldap-userdel "%u"
        add group script = /usr/sbin/smbldap-groupadd -p "%g"
        delete group script = /usr/sbin/smbldap-groupdel "%g"
          add user to group script = /usr/sbin/smbldap-groupmod -m "%u"
"%g"
          delete user from group script = /usr/sbin/smbldap-groupmod -x
"%u" "%g"
           set primary group script = /usr/sbin/smbldap-usermod -g "%g"
"%u"
```

Τέλος πρέπει να παραμετροποιήσουμε τον διαμοιρασμό των αρχείων και των καταλόγων.

```
[netlogon]
        comment = Network Logon Service
        path = /home/samba/netlogon
        guest ok = yes
        browsable = no
        writable = no

[profiles]
   comment = Users profiles
   path = home/samba/profiles
   read only = no
   profile acls = yes
   guest ok = yes
   browseable = no
   create mask = 0600
   directory mask = 0700
   #next line is a great way to secure profiles
   force user = %U
   #next line allows administrator to access all policies
   valid users = %U @"Domain Admins"
```

Στην συνέχεια δημιουργούμε τους καταλόγους που χρειαζόμαστε όπως αναφέρονται στο smb.conf στον φάκελο /home/samba

```
sudo mkdir -p /home/samba/netlogon/Default User
```

```
sudo mkdir -p /home/samba/profiles/
sudo chmod 655 -R /home/samba/
```

Έπειτα δίνετε την εντολή **sudo smbpasswd -w κωδικός** όπου ο κωδικός θα πρέπει να είναι ίδιος με τον κωδικό του διαχειριστή LDAP.

Θα πρέπει να σας επιστρέψει ένα αντίστοιχο μήνυμα με το παρακάτω όπου θα αναφέρεται το δικό σας όνομα διαχειριστή και τομέα.

```
Setting stored password for "cn=admin_ldap, dc = kvwn" in secrets.tdb
```

Έπειτα κάνουμε επαννεκίνηση του Samba.

```
sudo /etc/init.d/samba restart
```

Παραμετροποίηση των εργαλείων smbldap-tools

Το πακέτο smbldap-tools περιέχει μία σειρά από εργαλεία που μας διευκολύνουν στην διαχείριση του Ldap Server. Για να παραμετροποιήσουμε το πακέτο πρέπει να κάνουμε τα εξής:

Αρχικά δημιουργούμε τους παρακάτω καταλόγους. (IDEALX είναι η εταιρία που έχει δημιουργήσει και συντηρεί τα εργαλεία smbldap-tools).

```
sudo mkdir -p -v /etc/opt/IDEALX/smbldap-tools/
```

Στην συνέχεια εγκαθιστούμε εδώ 2 αρχεία τα smbldap.conf και smbldap_bind.conf τα οποία τα λαμβάνουμε από την διαδρομή:

```
/usr/share/doc/smbldap-tools/examples
```

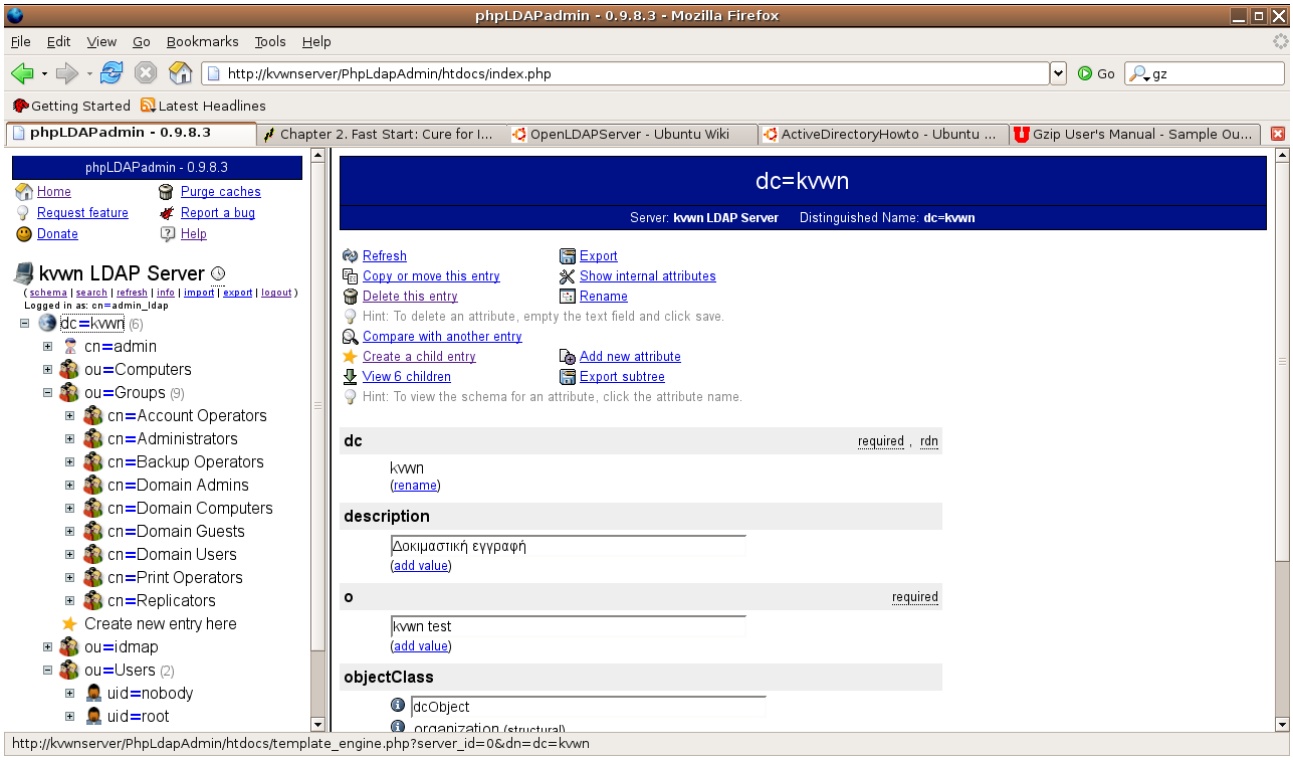
Στην συνέχεια αφού κάνουμε εκτελέσιμο το αρχείο configure.pl που βρίσκεται στην διεύθυνση

/usr/share/doc/smbldap-tools/ με την εντολή chmod 744 configure.pl το εκτελούμε. Αυτό το αρχείο χρησιμοποιείται για να ρυθμίσει εύκολα τα αρχεία smbldap.conf και smbldap_bind.conf.

Τέλος δίνουμε την εντολή

```
sudo smbldap-populate
```

Δίνοντας αυτή την εντολή ο Ldap server συμπληρώνεται με τις βασικές εγγραφές που χρειάζεται για να λειτουργήσει. Αφού καταχωρηθούν αυτές οι εγγραφές μας ζητείται και ο κωδικός του διαχειριστή. Τέλος αν πάμε στο phpldapadmin θα λάβουμε την παρακάτω εικόνα:



Όπως φαίνεται ο Ldap Server έχει τις βασικές εγγραφές ώστε να μπορέσουμε να διαχειριστούμε αποτελεσματικά το domain μας.

Στην συνέχεια πρέπει να δημιουργήσουμε ένα ακόμη organizational unit το DSA(Domain Security Accounts) το οποίο θα περιέχει τρεις λογαριασμούς για την διαχείριση του Samba, Linux και smbldap. Τους λογαριασμούς αυτούς μπορούμε να τους κάνουμε είτε μέσω του γραφικού περιβάλλοντος είτε μέσω αρχείων ldif με την χρήση της εντολής ldapadd. Εδώ θα δείξουμε μέσω της εντολής επειδή οι εικόνες καταλαμβάνουν μεγάλο χώρο στην σελίδα. Οι εγγραφές μας λοιπόν στο αρχείο ldif είναι οι παρακάτω:

```
dn: ou=DSA,dc=IDEALX,dc=ORG
objectClass: top
objectClass: organizationalUnit
ou: DSA
description: security accounts for LDAP clients

dn: cn=samba,ou=DSA,dc=IDEALX,dc=ORG
objectclass: organizationalRole
objectClass: top
objectClass: simpleSecurityObject
userPassword: sambasecretpwd
cn: samba
```

```
dn: cn=nssldap,ou=DSA,dc=IDEALX,dc=ORG
objectclass: organizationalRole
objectClass: top
objectClass: simpleSecurityObject
userPassword: nssldapsecretpwd
cn: nssldap

dn: cn=smbldap-tools,ou=DSA,dc=IDEALX,dc=ORG
objectclass: organizationalRole
objectClass: top
objectClass: simpleSecurityObject
userPassword: smbldapsecretpwd
cn: smbldap-tools
```

Αφού λοιπόν δημιουργήσουμε το αρχείο smbldap-dsa.dif το εισάγουμε στην βάση του Ldap Server με την εντολή

```
ldapadd -x -h localhost -D "cn=admin,dc=kvwn" -f smbldap-dsa.ldif -W
```

Βήμα 6 Client authentication (Πιστοποίηση πελάτη)

Για να μπορέσουμε να πιστοποιούμε χρήστες μέσω του LDAP server πρέπει να εγκαταστήσουμε τα ανάλογα πακέτα επικοινωνίας πελάτη-εξυπηρετητή.

Για αυτό τον σκοπό λοιπόν πρέπει να πάμε από τον Η/Υ πελάτη και να εγκαταστήσουμε τα πακέτα libpam-ldap libnss-ldap.

- **libpam-ldap**
  - Το πακέτο αυτό υποστηρίζει την αυθεντικοποίηση χρήστών μέσω PAM
- **libnss-ldap**
  - Το πακέτο αυτό επιτρέπει στον LDAP server να λειτουργεί σαν υπηρεσία ονομάτων.

Κατά την διάρκεια της εγκατάστασης του πακέτου libpam-ldap θα λάβουμε τις παρακάτω ερωτήσεις:

1. Την ip διεύθυνση του ldap server.
2. Την ριζική διεύθυνση του ldap. π.χ. kvwn
3. Την έκδοση του ldap. Επιλέγουμε 3
4. Στην ερώτηση να κάνουμε αν θέλουμε ο διαχειριστής της βάσης μας να είναι root απαντάμε yes
5. Στην ερώτηση ποιος είναι ο root login account απαντάμε δίνοντας αυτόν που έχουμε δημιουργήσει. π.χ. cn=admin, dc=kvwn

6. Στην συνέχεια μας ζητάει έναν κωδικό αλλά εφόσον το αφήσουμε κενό κρατά τον παλιό κωδικό του διαχειριστή

Έπειτα πάμε στο αρχείο nsswitch.conf και μέσω ενός απλού κειμενογράφου όπως ο vim αλλάζουμε τα εξής:

```
passwd:         compat
group:          compat
shadow:         compat


passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

Το αρχείο nsswitch.conf κατευθύνει το λειτουργικό σύστημα που θα αναζητήσει τα αντίστοιχα αρχεία όπως το passwd ή το group. Αλλάζοντας λοιπόν τα παραπάνω όταν δίνουμε τα στοιχεία ενός χρήστη προς αυθεντικοποίηση αρχικά αναζητείται το όνομα στα τοπικά αρχεία “files”, και στην συνέχεια αναζητείται στον κατάλογο ldap. Έτσι όταν θα δίνουμε έναν τοπικό χρήστη του συστήματος θα γίνεται αυθεντικοποίηση από το τοπικό μηχάνημα, ενώ εφόσον δεν βρεθεί στο τοπικό θα γίνεται προσπάθεια αυθεντικοποίησης από το κεντρικό σύστημα. Σε περίπτωση που δεν υπάρχει ούτε εκεί ο συγκεκριμένος χρήστης τότε θεωρείται άγνωστος χρήστης και ζητείται η επαναπληκτρολόγηση του ονόματος του και του κωδικού του.

Για να διαπιστώσουμε αν λειτουργεί σωστά δίνουμε την παρακάτω εντολή:

```
getent passwd <someldapuser>
```

όπου someldapuser θα είναι κάποιος χρήστης που έχουμε δημιουργήσει μέσω Ldap. (Ένας πολύ εύκολος τρόπος είναι με την εντολή smbldap-useradd -m someldapuser).

Τέλος πρέπει να παραμετροποιήσουμε σωστά και το PAM (Pluggable Authentication Module). Πρέπει να αλλάξουμε τα παρακάτω 4 αρχεία:

```
/etc/pam.d/common-account
/etc/pam.d/common-auth
/etc/pam.d/common-password
/etc/pam.d/common-session
```

common-account

```
$ sudo vi /etc/pam.d/common-account
Προσθέτουμε τα παρακάτω:
account sufficient      pam_ldap.so
account required        pam_unix.so
```

common-auth

```
$ sudo vi /etc/pam.d/common-auth
```

Προσθέτουμε τα παρακάτω:

```
auth    sufficient      pam_ldap.so
auth    required        pam_unix.so nullok_secure use_first_pass
```

common-password

```
$ sudo vi /etc/pam.d/common-password
```

Προσθέτουμε τα παρακάτω:

```
password        sufficient      pam_ldap.so
password        required        pam_unix.so nullok obscure min=4 max=8
md5
```

common-session

```
$ sudo vi /etc/pam.d/common-session
```

Προσθέτουμε τα παρακάτω:

```
session sufficient      pam_ldap.so
session required        pam_unix.so
```

Επίσης εφόσον θέλουμε στην πρώτη είσοδο του χρήστη στο σύστημα να δημιουργείται ο φάκελος του χρήστη στον κατάλογο /home θα πρέπει να δώσουμε τις παρακάτω οδηγίες στο αρχείο common-session αντι των προαναφερόμενων:

```
session required      pam_unix.so
session required        pam_mkhomedir.so skel=/etc/skel/
session optional        pam_ldap.so
```

Στην συνέχεια μπορείτε να αποσυνδεθείτε από τον πελάτη και στην επόμενη είσοδο σας στο σύστημα να συνδεθείτε με τον τομέα που εξυπηρετεί ο Ldap Server.

Πηγές:

1. Suse Linux Professional Administration Guide
2. The Linux Samba-OpenLDAP Howto. Jerome Tournier, Olivier Lemaire
3. https://help.ubuntu.com/community/LDAPClientAuthentication
4. https://help.ubuntu.com/community/OpenLDAPServer

GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical

connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this

License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material

copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions
of the GNU Free Documentation License from time to time. Such new
versions will be similar in spirit to the present version, but may
differ in detail to address new problems or concerns. See
http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number.
If the Document specifies that a particular numbered version of this
License "or any later version" applies to it, you have the option of
following the terms and conditions either of that specified version or
of any later version that has been published (not as a draft) by the
Free Software Foundation. If the Document does not specify a version
number of this License, you may choose any version ever published (not
as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of
the License in the document and put the following copyright and
license notices just after the title page:

> Copyright (c) YEAR YOUR NAME.
> Permission is granted to copy, distribute and/or modify this document
> under the terms of the GNU Free Documentation License, Version 1.2
> or any later version published by the Free Software Foundation;
> with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
> A copy of the license is included in the section entitled "GNU
> Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts,
replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the
> Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other
combination of the three, merge those two alternatives to suit the
situation.

If your document contains nontrivial examples of program code, we
recommend releasing these examples in parallel under your choice of
free software license, such as the GNU General Public License,
to permit their use in free software.