Κεφάλαιο 5

Ονομασία, Ευρετηρίαση και Εντοπισμός Πόρων στα Κ.Σ.

Σύνοψη
Σε αυτό το κεφάλαιο εξετάζονται τρεις πολύ σημαντικές υπηρεσίες, οι οποίες είναι απαραίτητες για τη λειτουργία των Κατανεμημένων Συστημάτων. Αυτές είναι η Υπηρεσία Ονομάτων, η Υπηρεσία Ευρετηρίου και η Υπηρεσία Εντοπισμού Πόρων. Μια Υπηρεσία Ονομάτων απαιτεί την παροχή ενός ενιαίου χώρου ονομάτων και τη μετάφραση των ονομάτων των πόρων σε διευθύνσεις δικτύου. Ως εκ τούτου, η υπηρεσία ονομάτων παρέχει τη διαχείριση των ονομάτων των κατανεμημένων πόρων καθώς και των αναγνωριστικών τους. Επιπρόσθετα παρουσιάζονται οι χώροι ονομάτων, η συγχώνευση χώρων ονομάτων και η υλοποίηση χώρων ονομάτων, καθώς και η πολύ γνωστή υπηρεσία ονομάτων DNS (Domain Name System). Κατόπιν, παρουσιάζονται οι Υπηρεσίες Ευρετηρίου, οι οποίες απαιτούν την αναζήτηση της διεύθυνσης του κατανεμημένου πόρου, χρησιμοποιώντας ως πρόσθετα κριτήρια, τον τύπο, την γεωγραφική θέση και τον ιδιοκτήτη του αναζητούμενου πόρου. Παρουσιάζονται με αναλυτικό τρόπο τρεις δημοφιλείς υπηρεσίες ευρετηρίου, η υπηρεσία ευρετηρίου X.500 της ISO, η υπηρεσία ευρετηρίου LDAP καθώς και η υπηρεσία ευρετηρίου Active Directory της Microsoft. Τέλος, παρουσιάζονται οι Υπηρεσίες Εντοπισμού, οι οποίες απαιτούν την τρέχουσα θέση του κινούμενου πόρου, και τη δυνατότητα να συνεργάζεται με τις υπηρεσίες ονομασίας και ευρετηρίου. Τέλος, αναλύονται θέματα όπως η οικιακή τοποθεσία και οι δείκτες προώθησης.

Προαπαιτούμενη Γνώση

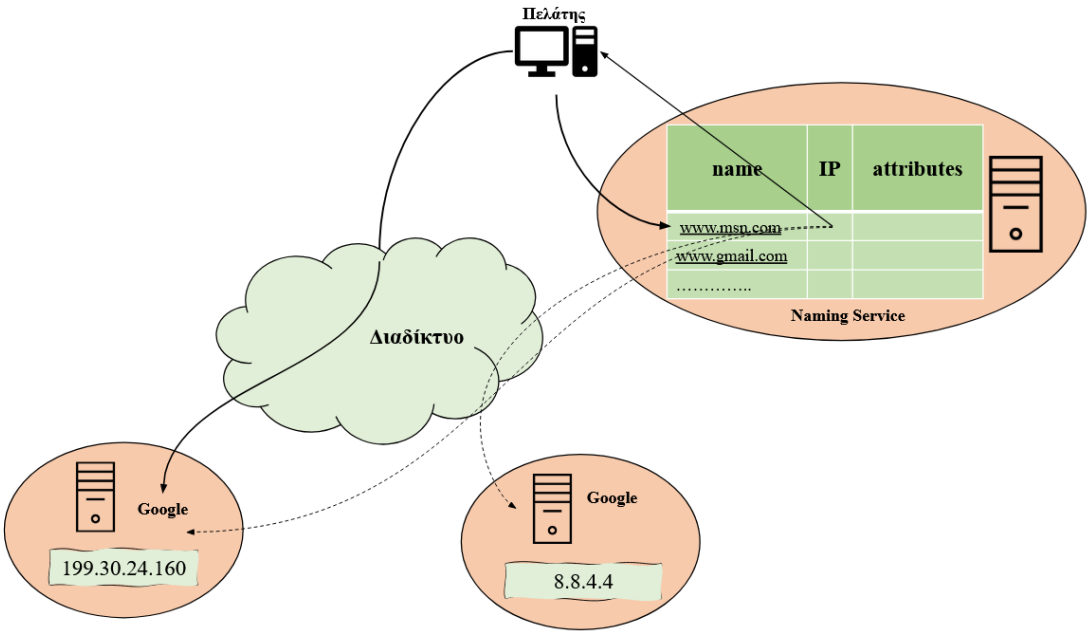
1) *Δουληγέρης, Χ., Μητρόπουλος, Σ., 2015. Πληροφοριακά συστήματα στο διαδίκτυο. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο στο: http://hdl.handle.net/11419/3969*
2) *Shari Lawrence Pfleeger (2011), Τεχνολογία Λογισμικού Θεωρία και Πράξη, Έκδοση: 2η Αμερικανική, Εκδόσεις Κλειδάριθμος ΕΠΕ.*
3) *Andrew S. Tanenbaum, Herbert Bos (2018), Σύγχρονα Λειτουργικά Συστήματα, Έκδοση: 4η Αμερικανική, Εκδόσεις Κλειδάριθμος ΕΠΕ*
4) *Κάβουρας Ι.Κ. (2009), Λειτουργικά Συστήματα (2ος τόμος), Έκδοση: 7η, Εκδόσεις Κλειδάριθμος ΕΠΕ.*

5.1 Υπηρεσία Ονομάτων

Σε ένα κατανεμημένο σύστημα, τα ονόματα χρησιμοποιούνται για να μπορέσει να γίνει δυνατή η διαχείριση ενός μεγάλου αριθμού πόρων, όπως υπολογιστών, υπηρεσιών, απομακρυσμένων αντικειμένων, αρχείων, και χρηστών. Η ονοματοθεσία αποτελεί ένα θεμελιώδες ζήτημα στον σχεδιασμό ενός κατανεμημένου συστήματος, καθώς διευκολύνει την επικοινωνία και την κοινή χρήση πόρων. Απαιτείται ένα όνομα με μια συγκεκριμένη μορφή, όπως είναι η URL για την πρόσβαση σε μια συγκεκριμένη ιστοσελίδα. Οι διεργασίες δεν μπορεί να μοιράζονται μεταξύ τους πόρους, τους οποίους διαχειρίζεται ένα σύστημα υπολογιστή εκτός εάν μπορούν να τους ονομάσουν

με συνέπεια. Οι χρήστες δεν μπορούν να επικοινωνούν μεταξύ τους μέσα στο κατανεμημένο σύστημα, εκτός εάν μπορούν να ονομάσουν ο ένας τον άλλον, π.χ. μέσω διευθύνσεων email. Εκτός των ονομάτων ένα άλλο χρήσιμο μέσο αναγνώρισης είναι τα περιγραφικά χαρακτηριστικά.

Το ερώτημα που ανακύπτει είναι το πώς οι υπηρεσίες ονομάτων διευκολύνουν την επικοινωνία και την κοινή χρήση πόρων σε ένα κατανεμημένο σύστημα. Μια διεύθυνση URL διευκολύνει τον εντοπισμό ενός πόρου που εκτίθεται στον Ιστό. Μια συνεπής και ομοιόμορφη ονομασία πόρων βοηθά τις διαδικασίες σε ένα κατανεμημένο σύστημα να διαλειτουργούν και να διαχειρίζονται πόρους, π.χ. οι εταιρείες χρησιμοποιούν το .com. ενώ οι μη κερδοσκοπικοί οργανισμοί χρησιμοποιούν το .org. Οι χρήστες αναφέρονται ο ένας στον άλλο μέσω των ονομάτων τους (δηλαδή μέσω της διεύθυνσης του ηλεκτρονικού ταχυδρομείου τους) και όχι μέσω των αναγνωριστικών του συστήματός τους. Οι υπηρεσίες ονομάτων δεν είναι χρήσιμες μόνο για τον εντοπισμό πόρων, αλλά και για τη συλλογή πρόσθετων πληροφοριών σχετικών με αυτούς, όπως χαρακτηριστικά που μπορεί να είναι μοναδικά ή όχι. Η Εικόνα 1 δείχνει την πρόσβαση ενός πελάτη υπολογιστή σε εξυπηρετητές μέσω της επίλυσης του ονόματος URL σε πραγματικές διευθύνσεις.



Εικόνα 1 Επίλυση URL

5.1.1 Ονόματα και πόροι

Με τον όρο πόρος αναφερόμαστε σε πολλές και διαφορετικές κατηγορίες αγαθών. Για αυτόν τον λόγο διαχωρίζεται:

- το όνομα του πόρου μέσα σε ένα δεδομένο σύστημα αρχείων,
- η διαδικασία αναγνώρισης της ενέργειας ή της διεργασίας στην οποία είναι υπεύθυνο κάποιο αρχείο,
- και η διεύθυνση IP ενός υπολογιστή.

Οι ομοιόμορφοι κατανεμητές πόρων (Uniform Resource Identifiers - URIs) προσφέρουν μια γενική λύση για κάθε τύπο πόρου. Τα URIs προέκυψαν από την ανάγκη αναγνώρισης πόρων στον Ιστό και άλλων πόρων στο Διαδίκτυο, όπως τα ηλεκτρονικά γραμματοκιβώτια. Ένας σημαντικός στόχος ήταν να εντοπιστούν οι πόροι με συνεκτικό τρόπο, ώστε να μπορεί όλοι

να υποβληθούν σε επεξεργασία από ένα κοινό λογισμικό, όπως μέσα από τα προγράμματα περιήγησης. Τα URIs είναι «ομοιόμορφα» καθώς η σύνταξή τους ενσωματώνει απεριόριστες επιλογές σε ένα σύνολο πολλών μεμονωμένων τύπων αναγνωριστικών πόρων (δηλαδή σχήματα URI), για αυτό το λόγο υπάρχουν διαδικασίες για τη διαχείριση του καθολικού χώρου των ονομάτων. Το πλεονέκτημα αυτής της ομοιομορφίας είναι ότι διευκολύνει τη διαδικασία εισαγωγής νέων τύπων αναγνωριστικών, καθώς και τη χρήση υπαρχόντων τύπων αναγνωριστικών σε νέα περιβάλλοντα, χωρίς να διακόπτεται η υπάρχουσα χρήση. Υπάρχουν δύο κύριες κατηγορίες URI, τα URL και τα URN.

Uniform Resource Locator (URL)

Ένας ομοιόμορφος εντοπιστής πόρων (Uniform Resource Locator URL):

- συμπληρώνεται από το πεδίο πρωτοκόλλου (http, ftp, nfs, κτλ.),
- μέρος του ονόματος του είναι συγκεκριμένο για την υπηρεσία,
- οι ονοματοδοτούμενοι πόροι δεν μπορεί να μετακινηθούν μεταξύ τομέων.

Ορισμένα URI περιέχουν τις απαραίτητες πληροφορίες προκειμένου να είναι δυνατός ο εντοπισμός του πόρου, καθώς και η πρόσβαση στον αντίστοιχο πόρο. Ο όρος Uniform Resource Locator (URL) χρησιμοποιείται συχνά για τα URI που παρέχουν πληροφορίες τοποθεσίας και τα οποία καθορίζουν τη μέθοδο πρόσβασης στον πόρο.

Uniform Resource Names (URN)

Τα ομοιόμορφα ονόματα πόρων (Uniform Resource Names - URN) είναι URI που χρησιμοποιούνται ως καθαρά ονόματα πόρων και όχι ως εντοπιστές:

- απαιτούν μια καθολική υπηρεσία αναζήτησης ονόματος πόρων - ένα σύστημα παρόμοιο με το DNS για όλους τους πόρους,
- η μορφή τους είναι: urn:<nameSpace>:<name-within-namespace>

Παρακάτω δίνουμε μερικά παραδείγματα URN:[1]

urn:isbn:0451450523 - αναφέρεται σε ένα βιβλίο του 1968 "*The Last Unicorn*", σε αυτήν την περίπτωση η αναγνώριση δεν γίνεται με βάση τον τίτλο του βιβλίου, αλλά με βάση τον μοναδικό αριθμό του isbn.

urn:mpeg:mpeg7:schema:2001 - αναφέρεται στους προεπιλεγμένους κανόνες χώρου ονομάτων (namespaces) για τα μετα-δεδομένα των βίντεο μορφής MPEG-7.

urn:uuid:6e8bc430-9c3a-11d9-9669-0800200c9a66 - αναφέρεται σε ένα τυχαίο καθολικά μοναδικό αναγνωριστικό (universally unique identifier - UUID) έκδοσης 1.

5.1.2 Τι είναι οι υπηρεσίες ονομασίας

Σε ένα κατανεμημένο σύστημα, μια υπηρεσία ονομασίας ορίζεται ως μια συγκεκριμένη υπηρεσία η οποία έχει ως στόχο να παρέχει μια συνεπή και ομοιόμορφη ονομασία στους πόρους και στα αγαθά ενός κατανεμημένου συστήματος επιτρέποντας έτσι την τοπική προσαρμογή σε άλλα προγράμματα ή υπηρεσίες. Με αυτόν τον τρόπο, μεταδίδονται τα κατάλληλα μεταδεδομένα με σκοπό την αλληλεπίδρασή τους στο κατανεμημένο σύστημα. Γενικά, η κύρια λειτουργία είναι η θέσπιση ενός σχήματος ονοματοδοσίας με βάση κάποια προκαθορισμένα χαρακτηριστικά.

Βασικά οφέλη της δυνατότητας αυτής είναι ο ευκολότερος εντοπισμός πόρων και αγαθών του συστήματος, η ομοιόμορφη και εύκολα αντιληπτή ονομασία και η ανεξάρτητη διευθυνσιοδότηση συσκευών με αποτέλεσμα να γίνεται δυνατή η μετακίνηση ενός ονόματος,

[1] Uniform Resource Name - Wikipedia (πρόσβαση: 08-10-2022)

ενός τομέα ή μιας τοποθεσίας από έναν διακομιστή σε άλλο διακομιστή χωρίς προβλήματα. (ένας τομέας είναι μια ομάδα αντικειμένων, όπως χρήστες ή συσκευές, που μοιράζονται την ίδια βάση δεδομένων μιας υπηρεσίας ευρετηρίου.)

Μια υπηρεσία ονομάτων αποθηκεύει μια συλλογή από ένα ή περισσότερα περιβάλλοντα ονομασίας, καθώς και σύνολα που συνδέουν τα ονόματα μεταξύ τους με τη μορφή κειμένου και χαρακτηριστικών για αντικείμενα όπως χρήστες, υπολογιστές, υπηρεσίες και απομακρυσμένα αντικείμενα.

5.1.3 Τί είναι η υπηρεσία ευρετηρίου

Η υπηρεσία ευρετηρίου αποτελεί μια γενίκευση της υπηρεσίας ονομασίας που περιγράφηκε παραπάνω. Η υπηρεσία ευρετηρίου ή υπηρεσία καταλόγου είναι μια κοινή πληροφοριακή υποδομή που είναι υπεύθυνη για την αναζήτηση διαφόρων οντοτήτων που συνδέονται με το δίκτυο. Η αναζήτηση γίνεται με βάση διάφορες ιδιότητες που μπορεί να έχει η οντότητα - αντικείμενο που ψάχνουμε, όπως ο τύπος, η γεωγραφική θέση και σε ποιον ανήκει. Μια υπηρεσία καταλόγου είναι ένα κρίσιμο στοιχείο για την λειτουργία ενός δικτύου. Ένας διακομιστής καταλόγου ή ένας διακομιστής ονομάτων είναι ένας διακομιστής που παρέχει μια τέτοια υπηρεσία, απλά ο κάθε ένας το κάνει με τον τρόπο του. Κάθε πόρος στο δίκτυο θεωρείται οντότητα - αντικείμενο από τον διακομιστή καταλόγου. Οι πληροφορίες σχετικά με έναν συγκεκριμένο πόρο αποθηκεύονται ως μια συλλογή χαρακτηριστικών που σχετίζονται με αυτόν τον πόρο ή αντικείμενο.

5.1.4 Τί είναι ο Χώρος ονομάτων

Ο χώρος ονομάτων είναι αυτό που χρησιμοποιείται για να δώσει σε καθένα από τα αντικείμενα ένα όνομα, το οποίο είναι ουσιαστικά ένα μοναδικό αναγνωριστικό. Ένας χώρος ονομάτων σε ένα δίκτυο ορίζεται συχνά από μια υπηρεσία ευρετηρίου. Η ονομασία και η αναγνώριση των πόρων δικτύου συχνά διέπεται από ένα σύνολο κανόνων που περιλαμβάνονται στα ευρετήρια. Αυτοί οι κανόνες περιλαμβάνουν σχεδόν πάντα την απαίτηση τα αναγνωριστικά να είναι τόσο διακριτά όσο και σαφή. Όταν χρησιμοποιείται μια υπηρεσία ευρετηρίου, ένας χρήστης απαλλάσσεται από την ανάγκη να θυμάται τη φυσική θέση ενός πόρου δικτύου, καθώς ο πόρος μπορεί απλώς να εντοπιστεί παρέχοντας το όνομά του. Ορισμένες υπηρεσίες ευρετηρίου διαθέτουν μηχανισμούς ελέγχου πρόσβασης, οι οποίοι περιορίζουν τη διαθεσιμότητα των πληροφοριών ευρετηρίου μόνο σε εκείνους τους χρήστες που τους έχει επιτραπεί να τις δουν.

Η ονομασία τομέων είναι ένας χώρος ονομάτων για τον οποίο υπάρχει ένα ενιαίο σύνολο αρχών και κανόνων για την ανάθεση ονομάτων (βλέπε επόμενο κεφάλαιο) εντός αυτού του χώρου. Οι τομείς στο DNS είναι συλλογές ονομάτων τομέα. Συντακτικά, το όνομα ενός τομέα είναι η κοινή κατάληξη των ονομάτων τομέα μέσα στον χώρο ονομάτων. Η διαχείριση τομέων μπορεί να ανατεθεί και σε υποτομείς. Για παράδειγμα https://www.**cs**.unipi.gr/acis/ και https://www.**ds**.unipi.gr/en/home-en/. Εδώ έχουμε δύο περιπτώσεις όπου ο κεντρικός τομέας [gr] μας αποκαλύπτει την χώρα (είναι ίδιος) και ο πρώτος υποτομέας [unipi] το πανεπιστήμιο (είναι ίδιος). Ο δεύτερος υποτομέας είναι διαφορετικός [cs],[ds] και αποκαλύπτει τα διαφορετικά τμήματα του πανεπιστημίου, με σκοπό την καλύτερη διαχείριση των τομέων.

Όσον αφορά στον χώρο ονομάτων θα πρέπει να καλύπτονται κάποιες απαιτήσεις όπως να:

- επιτρέπεται η χρήση απλών αλλά ουσιαστικών ονομάτων,
- επιτρέπεται δυνητικά άπειρος αριθμός ονομάτων,
- είναι δομημένος,
- επιτρέπονται παρόμοια υπο-ονόματα χωρίς συγκρούσεις,

- επιτρέπεται ομαδοποίηση σχετικών ονομάτων,
- επιτρέπεται η αναδιάρθρωση των δέντρων ονομάτων, δηλαδή για ορισμένους τύπους, αλλαγών, τα παλιά προγράμματα θα πρέπει να συνεχίσουν να λειτουργούν,
- υπάρχει διαχείριση εμπιστοσύνης.

5.2 DNS - Το σύστημα ονομάτων τομέα Διαδικτύου

Το DNS είναι μια υπηρεσία σχεδίασης ονομάτων της οποίας η κύρια βάση δεδομένων ονομάτων χρησιμοποιείται στο Διαδίκτυο. Προτάθηκεε το 1987 για να αντικαταστήσει το αρχικό σχήμα ονοματοδοσίας στο Διαδίκτυο, στο οποίο όλα τα ονόματα και οι διευθύνσεις κεντρικών υπολογιστών διατηρούνταν σε ένα ενιαίο κεντρικό κύριο αρχείο είτε γινόταν λήψη τους με χρήση FTP στους υπολογιστές που το απαιτούσαν. Το παλαιό σύστημα είχε σημαντικές ελλείψεις για αυτό και αντικαταστάθηκε. Επισης ήταν δύσκολη η κλιμάκωσή του. Οι οργανισμοί επιθυμούσαν να διαχειρίζονται οι ίδιοι τοπικά τα δικά τους συστήματα ονοματοδοσίας. Οι ανάγκες έδειχναν την ανάδειξη μιας λύσης με βάση την λογική της γενικής υπηρεσίας ονομάτων, όχι μια υπηρεσία που εξυπηρετεί μόνο την αναζήτηση διευθύνσεων υπολογιστή. Για αυτόν τον λόγο προτάθηκε το DNS κάποια σημερινά χαρακτηριστικά του παρουσιάζονται παρακάτω.

Το DNS έχει τις εξής δυνατότητες:

- Μετάφραση ονομάτων σε διευθύνσεις IP.
- Εντοπισμό εξυπηρετητών email .
- Επιτρέπει ανεξαρτησία κατα την χρήση των ονομάτων τομέα σε σχέση με οποιαδήποτε εκχώρηση διεύθυνσης IP.
- Χρήση ψευδώνυμων.

Με τον όρο Ψευδώνυμα ορίζουμε ένα όνομα τομέα, ο οποίος αντιπροσωπεύει ένα όνομα χρησιμοποιώντας κάποιο άλλο διαφορετικό όνομα για τον ίδιο σκοπό. Για παράδειγμα http://unipi.go.com/ και http://www.unipi.com. Η χρήση ψευδωνύμων κατά τη διαχείριση του DNS, σε περίπτωση που η διαχείριση περάσει σε άλλο μηχάνημα διακομιστή, προσφέρει τη δυνατότητα να μην αλλάξουν τα ονόματα και οι διευθύνσεις από τα δύο μηχανήματα που έγινε η αλλαγή. Επίσης δίνεται η δυνατότητα σύνδεσης πολλών ψευδώνυμων σε ένα μηχάνημα διακομιστή, όπως συμβαίνει στο παραπάνω παράδειγμα.

Ο χώρος ονομάτων DNS έχει τα εξής χαρακτηριστικά

- Είναι ένα κατευθυνόμενο δέντρο με ρίζα.
- Υποστηρίζει μέχρι 63/255 χαρακτήρες ανά ακμή/διαδρομή.
- Χρησιμοποιεί τον χαρακτήρα της τελείας για διαχωρισμό.

Η δομή του ονόματος αντικατοπτρίζει τη διοικητική δομή του Διαδικτύου. Αναθέτει γρήγορα τα ονόματα τομέα σε διευθύνσεις IP και εκμεταλλεύεται σε μεγάλο βαθμό την προσωρινή αποθήκευση. Επιπλέον, ο τυπικός χρόνος ερωτήματος είναι πολύ μικρός (~100 χιλιοστά του δευτερολέπτου). Υπάρχει δυνατότητα τεράστιας κλιμάκωσης σε εκατομμύρια υπολογιστές. Υπάρχει δυνατότητα προσωρινής αποθήκευσης, καθώς και ανθεκτικότητα σε αποτυχία κάποιου διακομιστή.

5.2.1 Ονόματα τομέα

Ο χώρος ονομάτων DNS Διαδικτύου είναι διαμερισμένος τόσο οργανωτικά όσο και γεωγραφικά. Τα ονόματα γράφονται με τον τομέα υψηλότερου επιπέδου στα δεξιά. Παρακάτω παρουσιάζονται οι αρχικοί οργανωτικοί τομείς ανώτατου επιπέδου (ονομάζονται επίσης γενικοί τομείς):

– com: εμπορικοί οργανισμοί

– edu: πανεπιστήμια και άλλα εκπαιδευτικά ιδρύματα

– gov: κυβερνητικές υπηρεσίες

– mil: Στρατιωτικοί οργανισμοί

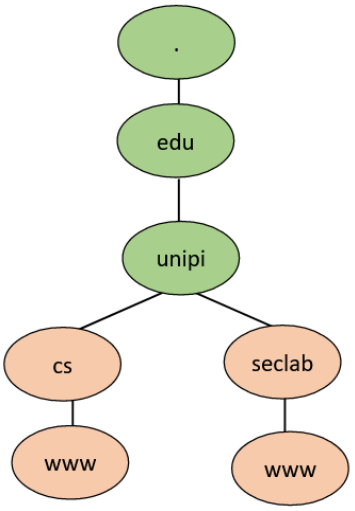
– net: μεγάλα κέντρα υποστήριξης δικτύου

– org: οργανισμοί που δεν αναφέρονται παραπάνω

– int: διεθνείς οργανισμοί

– us, uk, fr, ca, cn

Η Εικόνα 2 δείχνει το επίπεδο που βρίσκεται κάθε κομμάτι ενός url ενός εκπαιδευτικού ιδρύματος.



Εικόνα 2 Ονόματα τομέα

Ζητήματα DNS αποτελούν τα παρακάτω:

- Οι πίνακες ονομάτων αλλάζουν σπάνια, αλλά όταν αλλάζουν χρησιμοποιείται ένα είδος προσωρινής αποθήκευσης, που μπορεί να οδηγήσει στη διανομή των παλαιών δεδομένων, δηλαδή των δεδομένων πριν την αλλαγή.Οι πελάτες είναι υπεύθυνοι για τον εντοπισμό αυτού του ζητήματος και την ανάκτηση των δεδομένων μετά την αλλαγή.
- Ο σχεδιασμός του DNS κάνει τις αλλαγές στη δομή του χώρου ονομάτων αρκετά δύσκολες. Για παράδειγμα, η συγχώνευση προηγούμενων ξεχωριστών δέντρων τομέα κάτω από μια νέα ρίζα είναι μία διαδικασία που μπορεί να δημιουργήσει θέματα, όπως αυτό που αναφέρθηκε προηγουμένως με την προσωρινή αποθήκευση της προηγούμενης δομής.
- Η μετακίνηση υποδέντρων σε διαφορετικό μέρος της δομής (π.χ. εάν η Ουαλία έγινε ξεχωριστή χώρα, οι τομείς της θα πρέπει να μετακινηθούν όλοι σε ένα νέο επίπεδο χώρας).

5.2.2 Ο ρόλος των υπηρεσιών ονομάτων

Όπως προαναφέρθηκε, η πρόσβαση στους υπολογιστικούς πόρους γίνεται με χρήση κάποιου αναγνωριστικού ή μέσω κάποιας αναφοράς. Αυτό σημαίνει ότι ένα αναγνωριστικό μπορεί να αποθηκευτεί σε μεταβλητές και να ανακτηθεί γρήγορα από αντίστοιχους πίνακες στους

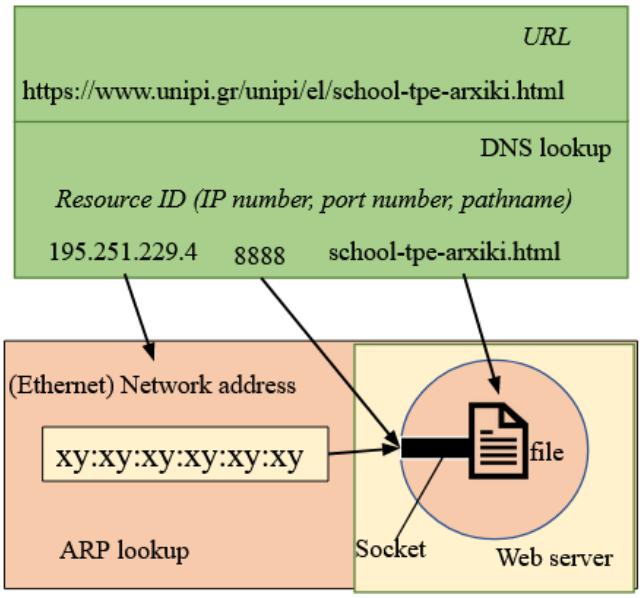
οποίους είναι καταγεγραμμένο. Το αναγνωριστικό επιπλέον περιλαμβάνει ή μπορεί να μετατραπεί σε μια διεύθυνση για ένα αντικείμενο. Αυτό συμβαίνει στην περίπτωση που γίνεται λήψη κάποιου αρχείου NFS, ή και κάποια αναφορά απομακρυσμένου αντικειμένου Java RMI ή CORBA μέσα στο κατανεμημένο σύστημα

Επίσης, ένα όνομα μιας διεύθυνσης ή ενός πόρου μπορεί να είναι αναγνωρίσιμο από τον άνθρωπο δηλαδή να έχει καθοριστεί ένα όνομα – μια συμβολοσειρά,. Αυτό συμβαίνει κυρίως στις περιπτώσεις που θέλουμε να ονοματίσουμε έναν τομέα Διαδικτύου, κάποια διαδρομή αρχείου ή και κάποιον αριθμό μιας διαδικασίας π.χ./etc/passwd, http://www.cs.ionio.gr/.

Για πολλούς σκοπούς, τα ονόματα είναι προτιμότερα από τα αναγνωριστικά επειδή η σύνδεση του κατονομαζόμενου πόρου σε μια φυσική τοποθεσία μπορεί να αλλάξει. Επιπλέον, επειδή τα ονόματα που χρησιμοποιούν φυσική γλώσσα ή κάτι παρεμφερές έχουν μεγαλύτερη σημασιολογική αξία για τους χρήστες, χρησιμοποιούνται και για την ονομασία των πόρων του συστήματος δίνοντας αναγνωριστικά ή και άλλα χρήσιμα χαρακτηριστικά. Αυτό πρακτικά σημαίνει ότι ένα όνομα μεταφράζεται σε δεδομένα σχετικά με τον ονομαζόμενο πόρο ή αντικείμενο, ή συχνά καλείται μια ενέργεια που είναι χαρακτηριστική του πόρου αυτού.

Η συσχέτιση μεταξύ ονόματος και αντικειμένου λέγεται δέσιμο (binding). Τα ονόματα συνδέονται με τα χαρακτηριστικά των ονομαζόμενων αντικειμένων. Ένα χαρακτηριστικό είναι η τιμή μιας ιδιότητας που σχετίζεται με ένα αντικείμενο. Για παράδειγμα, το DNS αντιστοιχίζει τα ονόματα τομέα με τα χαρακτηριστικά ενός κεντρικού υπολογιστή, δηλαδή τη διεύθυνση IP.

Στην Εικόνα 3 παρουσιάζεται ένα παράδειγμα λειτουργίας του μηχανισμού DNS με σκοπό την πρόσβαση σε ένα πόρο μέσω διεύθυνσης URL, χρησιμοποιώντας υπηρεσίες ονομασίας. Αρχικά εξετάζεται ένα πραγματικό url. Έπειτα βλέπουμε τη διαδικασία επίλυσης (resolve). Το τμήμα ονόματος τομέα της διεύθυνσης UR επιλύθηκε πρώτα μέσω του DNS. Το τελευταίο τμήμα της διεύθυνσης URL επιλύεται από το σύστημα αρχείων στον διακομιστή ιστού για τον εντοπισμό του σχετικού αρχείου



Εικόνα 3 Χρήση υπηρεσιών ονομασίας για την πρόσβαση σε ένα πόρο μέσω μιας διεύθυνσης URL

5.2.3 Ανάθεση Ονόματος

Όπως είναι λογικό, κανένας διακομιστής δεν έχει τη δυνατότητα να εξυπηρετεί όλα τα αιτήματα που αφορούν την ανάθεση ονομάτων. Άλλωστε το διαδίκτυο δουλεύει ως ένα μεγάλο κατανεμημένο σύστημα, κάτι που σημαίνει ότι είναι στη φύση του ιδίου, αλλά και οι τεχνολογίες μέσα σε αυτό να έχουν "κατανεμημένο χαρακτήρα". Για αυτούς τους λόγους, οι διακομιστές που είναι υπεύθυνοι για την εξυπηρέτηση των αιτημάτων που αφορούν στην ανάθεση ονομάτων στις περιπτώσεις που δεν μπορούν να εξυπηρετήσουν συνεργάζονται με άλλους εξυπηρετητές που έχουν την σχετική απάντηση στο αίτημα του πελάτη.

Ο τοπικός διακομιστής ονομάτων δεν μπορεί να απαντήσει σε όλα τα ερωτήματα χωρίς τη συνεργασία άλλων διακομιστών ονομάτων. Η διαδικασία εντοπισμού δεδομένων ονομασίας ανάμεσα σε περισσότερα από ένα ονόματα χρησιμοποιώντας τον διακομιστή για την επίλυση ενός ονόματος ονομάζεται πλοήγηση (navigation).

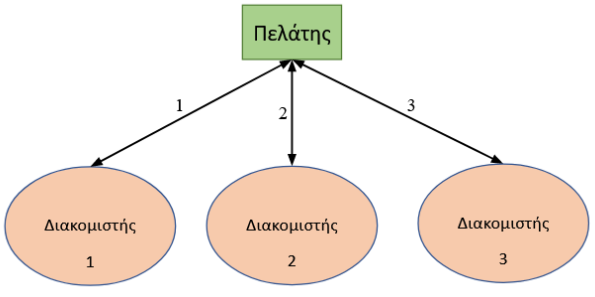
Όσον αφορά στην πλοήγηση θα πρέπει :

- να επιτρέπουν οι δομημένοι χώροι ονομάτων επαναληπτική πλοήγηση.
- οι διευθύνσεις URL να παρέχουν μια προεπιλεγμένη δομή που να μπορεί να αποσυντεθεί.
  - Η αποσύνθεση έχει σκοπό να αποκαλύπτει τη θέση ενός πόρου σε:
    - κάποιο πρωτόκολλο που χρησιμοποιείται για ανάκτηση.
    - τελικό διαδικτυακό σημείο της υπηρεσίας που αποκαλύπτει τον πόρο.
    - συγκεκριμένη διαδρομή υπηρεσίας.
  - Η αποσύνθεση διευκολύνει την επίλυση του ονόματος στον αντίστοιχο πόρο.

Υπάρχουν δύο μεγάλες κατηγορίες πλοηγήσεων σε περίπτωση μη δυνατότητας εξυπηρέτησης του διακομιστή ανάθεσης ονομάτων, η επαναληπτική πλοήγηση και η μη αναδρομική - αναδρομική πλοήγηση ελεγχόμενη από διακομιστή.

Επαναληπτική πλοήγηση

Όπως φαίνεται στην Εικόνα 4, ο πελάτης επικοινωνεί επαναληπτικά με διακομιστές ονομάτων 1, 2, 3 για να αναθέσει ένα όνομα.



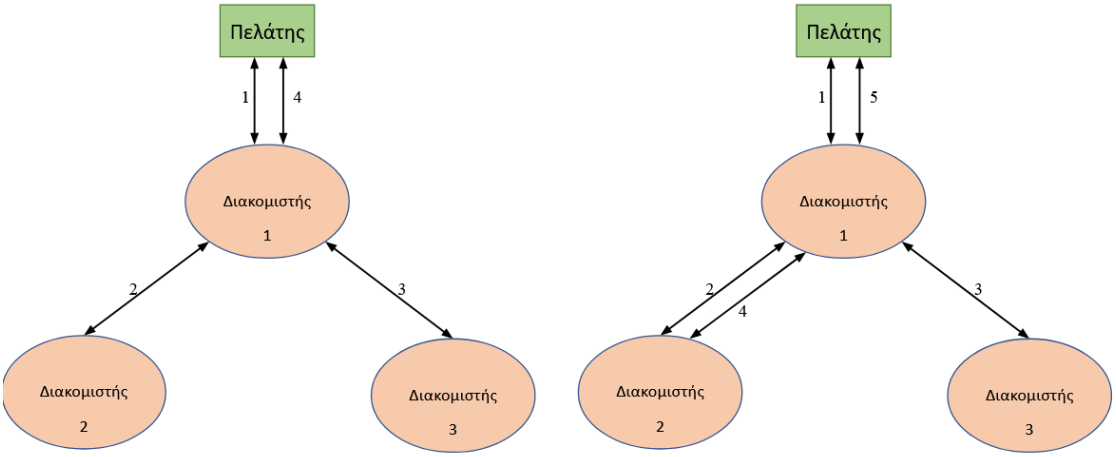
Εικόνα 4 Επικοινωνία πελάτη με διακομιστές ονομάτων

Το DNS υποστηρίζει το μοντέλο που είναι γνωστό ως επαναληπτική πλοήγηση. Αυτό σημαίνει ότι για την ανάθεση ενός ονόματος, ένας πελάτης παρουσιάζει ολόκληρο το όνομα στους διακομιστές, ξεκινώντας από έναν τοπικό διακομιστή, NS1. Εάν το NS1 έχει το ζητούμενο όνομα τότε απαντάει κατευθείαν στον πελάτη, διαφορετικά το NS1

προτείνει επικοινωνία με το NS2 (διακομιστής για έναν τομέα που περιλαμβάνει το ζητούμενο όνομα) και ούτω καθεξής.

Μη αναδρομική και αναδρομική πλοήγηση ελεγχόμενη από διακομιστή

Όπως φαίνεται στην Εικόνα 5, ένας διακομιστής ονομάτων επικοινωνεί με άλλους διακομιστές ονομάτων για λογαριασμό ενός πελάτη.



Εικόνα 5 Μη αναδρομικός(σχήμα αριστερά) και αναδρομικός(σχήμα δεξιά) έλεγχος διακομιστή

Ένα εναλλακτικό μοντέλο που υποστηρίζει το DNS είναι όταν ένας διακομιστής ονομάτων συντονίζει την ανάλυση του ονόματος και επιστρέφει το αποτέλεσμα στον χρήστη-πελάτη.

Μη αναδρομικός ελεγχόμενος από διακομιστή: οποιοσδήποτε διακομιστής ονομάτων μπορεί να επιλεγεί από τον πελάτη.

Αναδρομικός ελεγχόμενος από διακομιστή: ο πελάτης έρχεται σε επαφή με έναν μόνο διακομιστή. Η αναδρομική πλοήγηση πρέπει να χρησιμοποιείται σε τομείς που περιορίζουν την πρόσβαση πελάτη στις πληροφορίες DNS τους για λόγους ασφαλείας.

5.3 Υπηρεσίες ευρετηρίου (καταλόγου)

Μερικές φορές οι χρήστες επιθυμούν να βρουν ένα συγκεκριμένο άτομο ή έναν συγκεκριμένο πόρο, αλλά δεν γνωρίζουν το όνομά του, παρά μόνο μερικά από τα χαρακτηριστικά του. Για παράδειγμα το πού εργάζεται ή κάποιο άλλο χαρακτηριστικό του. Τις περισσότερες φορές οι χρήστες δεν δείχνουν ιδιαίτερο ενδιαφέρον στον τρόπο ή στο ποιος παρέχει την οποιαδήποτε υπηρεσία, προτεραιότητά τους είναι να απλά να βρίσκουν αυτό που ζητούν, δηλαδή το αποτέλεσμα. Αυτόν λοιπόν τον σκοπό έρχεται να εξυπηρετήσει η υπηρεσία καταλόγου.

Οι υπηρεσίες καταλόγων κατά κύριο λόγο αποθηκεύουν συλλογές καταχωρήσεων που περιέχουν πολλές καταχωρήσεις μαζί με διάφορα χαρακτηριστικά για κάθε μία από αυτές. Έτσι δίνεται η δυνατότητα για αναζήτηση των καταχωρήσεων με γνώμονα τα χαρακτηριστικά, δηλαδή κάποιος μπορεί να αναζητά καταχωρήσεις που ταιριάζουν με προδιαγραφές που βασίζονται σε χαρακτηριστικά.

Εδώ να υπογραμμίσουμε ότι η τεχνολογία του DNS περιέχει ορισμένα περιγραφικά δεδομένα, αλλά τα δεδομένα είναι πολύ ελλιπή που σημαίνει ότι το DNS δεν είναι οργανωμένο για αναζήτηση.

Η Υπηρεσία εντοπισμού είναι μια υπηρεσία καταλόγου που έχει τα εξής χαρακτηριστικά:

- Ενημερώνεται αυτόματα καθώς αλλάζει η διαμόρφωση του δικτύου.
- Ανταποκρίνεται στις ανάγκες των πελατών σε αυθόρμητα δίκτυα.
- Ανακαλύπτει υπηρεσίες που απαιτούνται από έναν πελάτη εντός του τρέχοντος πεδίου. Για παράδειγμα, να βρει την καταλληλότερη υπηρεσία εκτύπωσης για αρχεία εικόνας μετά την άφιξη του χρήστη σε έναν π.χ. συνεδριακό χώρο, έχοντας πρόσβαση σε στοιχεία τα οποία δείχνουν ότι βρισκόμαστε στον συγκεκριμένο συνεδριακό χώρο.

5.3.1 Υπηρεσία ευρετηρίου X.500 της ISO

Το πρωτόκολλο X.500 εγκρίθηκε για πρώτη φορά το 1988 και στη συνέχεια ενισχύθηκε το 1993 από την Διεθνή Ένωση Τηλεπικοινωνιών (ITU). Σκοπός του ήταν να παρέχει ένα διεθνές πρότυπο για συστήματα καταλόγων [4].

Μοντέλο

Η αρχιτεκτονική του πρωτοκόλλου X.500 αποτελείται από ένα σύστημα πελάτη-διακομιστή που επικοινωνεί μέσω του μοντέλου δικτύωσης Open Systems Interconnection (OSI). Ο πελάτης ονομάζεται Directory Service Agent (DUA) και ο διακομιστής ονομάζεται the Directory System Agent (DSA).

Υπάρχουν δύο υπο-πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία μεταξύ συστημάτων. Το πρωτόκολλο επικοινωνίας μεταξύ ενός DUA (Πελάτης) και ενός DSA (Διακομιστής) είναι αυτό που ονομάζεται Πρωτόκολλο Πρόσβασης Καταλόγου (DAP). Το πρωτόκολλο επικοινωνίας μεταξύ ενός DSA (Διακομιστής) και ενός άλλου DSA ονομάζεται Κατάλογος Πρωτόκολλου Συστήματος (DSP). Το X.500 χρησιμοποιεί το υπο-πρωτόκολλο DSP για να δώσει μια «κατανεμημένη» και «σφαιρική άποψη» των δεδομένων. Δηλαδή δεν είναι όλα τα δεδομένα αποθηκευμένα σε έναν διακομιστή αλλά διανέμονται σε πολλούς διακομιστές. Ωστόσο, όταν ένας πελάτης έχει πρόσβαση σε ένα σύστημα X.500 μέσω DAP, τα δεδομένα συλλέγονται από έναν ή περισσότερους διακομιστές που χρησιμοποιούν DSP και παρουσιάζονται ως μία καθολική προβολή των δεδομένων.[5]

Δεδομένα

Τα δεδομένα εντός της αρχιτεκτονικής X.500 αποθηκεύονται σε αντικείμενα και χαρακτηριστικά. Αυτό είναι ανάλογο με τους Πίνακες και τις Στήλες στη γλώσσα των βάσεων δεδομένων ή τις Εγγραφές και τα Πεδία στη γλώσσα της αποθήκευσης αρχείων. Τα αντικείμενα αναγνωρίζονται με μοναδικούς αριθμούς που ονομάζονται Αναγνωριστικά Αντικειμένων ή OID. Τα χαρακτηριστικά περιέχονται μέσα σε αντικείμενα και αντιπροσωπεύουν συγκεκριμένα στοιχεία δεδομένων, όπως όνομα, και διεύθυνση.

Η πρόσβαση στα δεδομένα γίνεται μέσω ενός δέντρου πληροφοριών καταλόγου (DIT). Ένα DIT είναι μία ιεραρχική δομή που αποτελείται από μια ρίζα με πολλούς κόμβους ή κλάδους (παρόμοια με μια δομή καταλόγου αρχείων). Για παράδειγμα, ένα τηλεφωνικό DIT θα αποτελείται από μια ρίζα με κόμβους. Η κάθε χώρα θα είναι η ρίζα που περιέχει κόμβους. Οι κόμβοι θα είναι οι κωδικοί περιοχής. Η κάθε περιοχή θα περιέχει κόμβους που θα αντιστοιχούν σε κάθε αριθμό τηλεφώνου.

Τα δεδομένα κωδικοποιούνται εντός του X.500 σε Abstract Syntax Notation (ASN.1), και σε Βασική Μορφή Κανόνων Κωδικοποίησης (BER). Τα δεδομένα ενημερώνονται (προστίθενται, αλλάζουν ή διαγράφονται) από συναλλαγές που περιγράφονται από το πρωτόκολλο.

Ασφάλεια

Το πρωτόκολλο X.500 χρησιμοποιεί την υποδομή δημόσιου κλειδιού X.509 (PKI) η οποία χρησιμοποιεί ψηφιακά πιστοποιητικά για τον έλεγχο ταυτότητας.

Αντιγραφή

Το πρωτόκολλο X.500 προβλέπει την αναπαραγωγή της βάσης δεδομένων. Αυτό σημαίνει ότι τα δεδομένα καταλόγου μπορεί να αναπαραχθούν ή να διανεμηθούν σε αντίγραφα σε πολλούς διακομιστές για σκοπούς κατανομής του φορτίου σε περίπτωση που βρεθεί σε έκτακτη ανάγκη το σύστημα.

Συνεδρία

Μια τυπική συνεδρία X.500 μπορεί να προχωρήσει ως εξής:

• Πελάτης: Συνδέεται και ζητά πρόσβαση στον διακομιστή. Η λειτουργία αυτή ονομάζεται λειτουργία δέσμευσης (Binding).

• Διακομιστής: Ο διακομιστής ελέγχει την ταυτότητα του πελάτη και ολοκληρώνει τη δέσμευση.

Λειτουργία

• Πελάτης: Ζητάει μια υπηρεσία από τον διακομιστή. Η υπηρεσία αυτή είναι η αναζήτηση μιας καταχώρησης στον κατάλογο. Έτσι ο πελάτης παρουσιάζει παραμέτρους και δεδομένα που ταιριάζουν στην καταχώρηση που αναζητεί.

• Διακομιστής: Εκτελεί το αίτημα υπηρεσίας του πελάτη. Για να υλοποιηθεί το αίτημα μπορεί να συνδεθεί με άλλο X.500. Μόλις υλοποιηθεί το αίτημα ο διακομιστής επικοινωνεί στέλνοντας μια απάντηση.

• Πελάτης: Λαμβάνει την απάντηση και αποδεσμεύει ή τερματίζει την σύνδεση.

Προσδιορισμός

Το πρωτόκολλο X.500 περιγράφεται σε μια σειρά προδιαγραφών:

• X.501: Έννοιες και μοντέλα.

• X.509: Έλεγχος ταυτότητας πελατών και διακομιστές.

• X.511: Λειτουργικές υπηρεσίες του X.500 (π.χ. αναζήτηση, τροποποίηση κ.λπ.)

• X.518: Λειτουργίες που εκτείνονται σε πολλαπλούς διακομιστές.

• X.519: Περιγράφει το συνολικό X.500 πρωτόκολλο και τα υποπρωτόκολλα: Πρωτόκολλο πρόσβασης καταλόγου (DAP), Directory Operational Binding Πρωτόκολλο (DOP), Directory System Protocol (DSP), και Πρωτόκολλο σκίασης πληροφοριών καταλόγου (DISP).

• X.520: Καλύπτει τους επιλεγμένους τύπους χαρακτηριστικών που υπάρχουν στον κατάλογο

• X.521: Ορισμός κλάσης αντικειμένου.

• X.525: Λειτουργία αναπαραγωγής μεταξύ πολλών διακομιστών.

5.3.2 Lightweight Directory Access Protocol (LDAP)

Η ανάγκη μείωσης του φορτίου με σκοπό την καλύτερη υποστήριξη από την πλευρά των πελατών όσον αφορά στο πρωτόκολλο Πρόσβασης Καταλόγου (DAP), οδήγησε στη δημιουργία του πρωτοκόλλου LDAP (Lightweight Directory Access Protocol). Αρχικά, σχεδιάστηκε το LDAP, ώστε να είναι μία πιο ελαφριά εναλλακτική από την πλευρά του πελάτη στο αρχικό πρωτόκολλο του X.500 (DAP)[6][7].

Μοντέλο

Η αρχιτεκτονική του πρωτοκόλλου LDAP αποτελείται από το σύστημα πελάτη-διακομιστή που επικοινωνεί μέσω του μοντέλου δικτύωσης TCP/IP. Συνήθως οι διακομιστές LDAP είναι ανεξάρτητοι και επικοινωνούν μόνο με πελάτες LDAP. Αντί όμως να παρουσιάζει την υπηρεσία καταλόγου με μία διαδικασία που στοχεύει στην καθολική προβολή όπως το X.500, το LDAP χρησιμοποιεί έναν μηχανισμό παραπομπής. Όταν ένας πελάτης ζητά δεδομένα από έναν διακομιστή LDAP που δεν περιέχει αυτά τα ζητούμενα δεδομένα, ο διακομιστής απαντά με μια άλλη διεύθυνση URL ενός διακομιστή που περιέχει τις ζητούμενες αυτές πληροφορίες, κάτι παρόμοιο με αυτό που συμβαίνει στον Παγκόσμιο Ιστό.

Δεδομένα

Η αρχιτεκτονική LDAP, όπως και η αρχιτεκτονική X.500, αποθηκεύει δεδομένα σε αντικείμενα και Ιδιότητες. Ωστόσο, το LDAP προσδιορίζει τα αντικείμενα με ένα μοναδικό όνομα αντί για έναν αριθμό. Το LDAP χρησιμοποιεί επίσης πληροφορίες καταλόγου δέντρου για πρόσβαση στις πληροφορίες και το ASN.1/BER για κωδικοποίηση. Ωστόσο υπάρχει μια τρέχουσα προσπάθεια να χρησιμοποιηθεί κωδικοποίηση XML αντί για BER.

Επιπλέον, το LDAP προσθέτει μια άλλη δυνατότητα που ονομάζεται Μορφή Ανταλλαγής Δεδομένων LDAP (LDIF).Η LDIF είναι μια μέθοδος επικοινωνίας πελατών και διακομιστών LDAP με σχήματα και ενημερώσεις μέσω μορφής κειμένου. Αυτό επιτρέπει στους χρήστες LDAP να ανακαλύπτουν εύκολα τις διατάξεις δεδομένων άγνωστων σχημάτων με σκοπό να γίνεται ενημέρωση του εκάστοτε καταλόγου.

Ασφάλεια

Το πρωτόκολλο LDAP χρησιμοποιεί το επίπεδο απλού ελέγχου ταυτότητας και ασφάλειας προδιαγραφής (SASL) για την αναγνώριση και τον έλεγχο ταυτότητας. Το επίπεδο SASL είναι ευέλικτο στο ότι ενεργοποιεί άλλους μηχανισμούς ασφαλείας (όπως το Kerberos ή το GSSAPI) για το κομμάτι των υλοποιήσεων και των συνδέσεων. Εφόσον το LDAP χρησιμοποιεί το TCP/IP μπορεί να μεταφερθεί μέσω συνδέσεων χρησιμοποιώντας το Secure Socket Layer (SSL).

Αντιγραφή

Το πρωτόκολλο LDAP, όπως και το X.500, παρέχει επίσης αναπαραγωγή βάσεων δεδομένων. Δηλαδή, οι ενημερώσεις αναπαράγονται μέσω του πρωτοκόλλου για να μπορέσουν να αντικατοπτρίσουν τις τοποθεσίες LDAP.

Συνεδρία

Μια τυπική συνεδρία LDAP μπορεί να προχωρήσει ως εξής:

- Πελάτης: Συνδέεται (Binding) και ζητά πρόσβαση στο διακομιστή.

- Διακομιστής: Ο διακομιστής ελέγχει την ταυτότητα του πελάτη και ολοκληρώνει τη λειτουργία Binding.
- Πελάτης: Ζητάει μια υπηρεσία από τον διακομιστή, όπως αναζήτηση για μια καταχώρηση στον κατάλογο και παρουσιάζει οποιαδήποτε παράμετρο - δεδομένα.
- Διακομιστής: Εκτελεί την υπηρεσία και στέλνει μια απάντηση ή παραπέμπει τον πελάτη σε άλλο διακομιστή LDAP.
- Πελάτης: Λαμβάνει την απάντηση και αποδεσμεύει ή τερματίζει τη σύνδεση, όπως και μπορεί να συνδεθεί σε κάποιον άλλο διακομιστή. (Ο συγκεκριμένος διακομιστής που συνδέεται ο πελάτης είναι ο ίδιος με αυτόν που τον παραπέμπει στο προηγούμενο βήμα ο διακομιστής).

Προσδιορισμός

Το πρωτόκολλο LDAP περιγράφεται σε μια σειρά προδιαγραφών:

- RFC 2251: Πρωτόκολλο LDAPv3 – Ορισμός πρωτοκόλλου LDAP.
- RFC 2252: Ορισμοί σύνταξης χαρακτηριστικών LDAPv3 - Τύπος χαρακτηριστικού ή
- ορισμός στοιχείου δεδομένων.
- RFC 2253: LDAPv3 UTF-8 – Κωδικοποίηση χαρακτήρων UTF-8 των κλειδιών εισαγωγής καταλόγου.
- RFC 2254: Η αναπαράσταση συμβολοσειράς των φίλτρων αναζήτησης LDAP – Μηχανισμοί ερωτημάτων για χρήση σε URL και API.
- RFC 2255: Μορφή URL LDAP – Κατασκευή ενιαίου εντοπιστή πόρων.
- RFC 2222: Απλό επίπεδο ελέγχου ταυτότητας και ασφάλειας (SASL) – Μηχανισμοί ασφαλείας επιπέδου μεταφοράς σε plug-in

5.3.3 Active Directory

Το Active Directory (AD) είναι η πλατφόρμα για υπηρεσίες καταλόγου, την οποία έχει αναπτύξει η Microsoft. Προσφέρεται μαζί με τον Windows Server και επιτρέπει στους διαχειριστές να διαχειρίζονται τα δικαιώματα και την πρόσβαση στους πόρους ενός εταιρικού δικτύου.

Το Active Directory αποθηκεύει και συντηρεί τα δεδομένα που σχετίζονται με τους πόρους ως κατανεμημένα αντικείμενα. Τα αντικείμενα αυτά αποτελούν μεμονωμένα στοιχεία και μπορεί να είναι λογαριασμοί χρηστών, ομάδες χρηστών, εφαρμογές, εκτυπωτές, σαρωτές, κ.ά.. Τα αντικείμενα αυτά ουσιαστικά αναπαριστούν τους λεγόμενους πόρους του εταιρικού δικτύου, είτε είναι υλισμικό είτε άυλες οντότητες, όπως χρήστες ή ομάδες.

Το Active Directory διαχειρίζεται τα υπό διαχείριση αντικείμενα του καταλόγου με βάση τα χαρακτηριστικά/ιδιώματά του. Χαρακτηριστικό παράδειγμα αποτελεί ο λογαριασμός ενός χρήστη, ο οποίος πέρα από το όνομα του χρήστη, περιέχει πρόσθετες πληροφορίες, όπως ο κωδικός πρόσβασης, τα κλειδιά κρυπτογράφησης/αποκρυπτογράφησης, δικαιώματα πρόσβασης, κτλ..

Κύρια υπηρεσία στο Active Directory είναι η Υπηρεσία Τομέα (Active Directory Domain Service - AD DS), η οποία χειρίζεται τις πληροφορίες ενός καταλόγου, καθώς και την αλληλεπίδραση του χρήστη με τον τομέα στον οποίο ανήκει. Για να συνδεθεί ένας χρήστης μέσω δικτύου σε έναν τομέα απαιτείται να επαληθευθεί ως έγκυρος χρήστης από το AD DS. Για την πρόσβαση του χρήστη το AD DS διατηρεί ένα σύνολο πολιτικών ασφαλείας ανά ομάδα χρηστών.

Το AD DS χρησιμοποιείται από άλλα συστήματα της Microsoft και διαλειτουργεί με αυτά. Τέτοια συστήματα είναι ο Exchange Server και ο SharePoint Server, τα οποία απαιτούν προφανώς έλεγχο πρόσβασης.

5.3.3.1 Λειτουργίες Active Directory

Πολλές διαφορετικές υπηρεσίες περιλαμβάνουν το Active Directory, το οποίο συνιστά μια υπηρεσία καταλόγου. Η κύρια υπηρεσία είναι η Υπηρεσία Τομέα (Domain Service), αλλά περιλαμβάνονται επίσης κι άλλες υπηρεσίες, όπως ελαφρού καταλόγου (AD LDS), ελαφρύ πρωτόκολλο πρόσβασης καταλόγου (LDAP), πιστοποιητικών (AD CS), ομοσπονδίας (AD FS) και διαχείρισης δικαιωμάτων (AD RMS). Κάθε μία από αυτές τις άλλες υπηρεσίες επεκτείνει τις δυνατότητες διαχείρισης του καταλόγου του προϊόντος[8].

Το Lightweight Directory Services έχει την ίδια βάση κώδικα με το AD DS, και παρέχει παρόμοιες λειτουργίες, όπως η διεπαφή προγράμματος εφαρμογής. Το AD LDS, ωστόσο, μπορεί να εκτελεστεί σε πολλές περιπτώσεις σε έναν διακομιστή και διατηρεί δεδομένα καταλόγου σε ένα χώρο αποθήκευσης δεδομένων χρησιμοποιώντας το Lightweight Directory Access Protocol, το οποίο είναι ένα πρωτόκολλο εφαρμογής που χρησιμοποιείται για την πρόσβαση και τη διατήρηση υπηρεσιών καταλόγου μέσω δικτύου. Το LDAP αποθηκεύει αντικείμενα, όπως ονόματα χρήστη και κωδικούς πρόσβασης, σε υπηρεσίες καταλόγου, όπως η υπηρεσία καταλόγου Active Directory και μοιράζεται αυτά τα δεδομένα αντικειμένων στο δίκτυο.

Οι Υπηρεσίες Πιστοποιητικών στο Active Directory δημιουργούν, διαχειρίζονται και μοιράζονται πιστοποιητικά. Ένα τέτοιο πιστοποιητικό, πχ, χρησιμοποιεί κρυπτογράφηση για να επιτρέπει σε έναν χρήστη να ανταλλάσσει πληροφορίες μέσω του Διαδικτύου με ασφάλεια με ένα δημόσιο κλειδί.

Οι υπηρεσίες Active Directory Federation Services επαληθεύουν την πρόσβαση των χρηστών σε πολλαπλές εφαρμογές (ακόμη και σε διαφορετικά δίκτυα) χρησιμοποιώντας μία σύνδεση Single Sign On (SSO). Όπως υποδηλώνει το όνομα, το SSO απαιτεί από τον χρήστη να συνδεθεί μόνο μία φορά, αντί να χρησιμοποιεί πολλαπλά αποκλειστικά κλειδιά ελέγχου ταυτότητας για κάθε υπηρεσία.

Οι Υπηρεσίες Διαχείρισης Δικαιωμάτων ελέγχουν τα δικαιώματα και τη διαχείριση πληροφοριών. Το AD RMS κρυπτογραφεί περιεχόμενο, όπως έγγραφα email ή Microsoft Word, σε έναν διακομιστή για να περιορίσει την πρόσβαση.

5.3.3.2 Κύρια χαρακτηριστικά στις υπηρεσίες τομέα Active Directory

Το Active Directory Domain Services χρησιμοποιεί μια κλιμακωτή δομή διάταξης που αποτελείται από τομείς, δέντρα και δάση για τον συντονισμό των δικτυωμένων στοιχείων. Τα πεδία είναι τα μικρότερα από τα κύρια επίπεδα, ενώ τα δάση είναι τα μεγαλύτερα. Διαφορετικά αντικείμενα, όπως χρήστες και συσκευές, που μοιράζονται την ίδια βάση δεδομένων βρίσκονται στον ίδιο τομέα. Ένα δέντρο είναι ένας ή περισσότεροι τομείς ομαδοποιημένοι με ιεραρχικές σχέσεις εμπιστοσύνης. Ένα δάσος είναι μια ομάδα από πολλά δέντρα. Τα δάση παρέχουν όρια ασφαλείας, ενώ οι τομείς

(που μοιράζονται μια κοινή βάση δεδομένων) μπορούν να διαχειρίζονται για ρυθμίσεις, όπως ο έλεγχος ταυτότητας και η κρυπτογράφηση.

Ένας τομέας είναι μια ομάδα αντικειμένων, όπως χρήστες ή συσκευές, που μοιράζονται την ίδια βάση δεδομένων AD. Οι τομείς έχουν σύστημα ονομάτων τομέα.

Ένα δέντρο είναι ένας ή περισσότεροι τομείς ομαδοποιημένοι. Η δενδρική δομή χρησιμοποιεί έναν συνεχόμενο χώρο ονομάτων για να συγκεντρώσει τη συλλογή των τομέων σε μια λογική ιεραρχία. Τα δέντρα μπορεί να θεωρηθούν ως σχέσεις εμπιστοσύνης, όπου μια ασφαλής σύνδεση ή εμπιστοσύνη είναι κοινή μεταξύ δύο τομέων. Μπορεί να είναι αξιόπιστοι πολλοί τομείς - όπου ένας τομέας μπορεί να εμπιστευτεί έναν δεύτερο και ο δεύτερος τομέας μπορεί να εμπιστευτεί έναν τρίτο. Λόγω της ιεραρχικής φύσης αυτής της ρύθμισης, ο πρώτος τομέας μπορεί σιωπηρά να εμπιστευτεί τον τρίτο τομέα χωρίς να χρειάζεται ρητή εμπιστοσύνη.

Ένα δάσος είναι μια ομάδα πολλών δέντρων. Ένα δάσος αποτελείται από κοινόχρηστους καταλόγους, σχήματα καταλόγου, πληροφορίες εφαρμογών και διαμορφώσεις τομέα. Το σχήμα ορίζει την κλάση και τις ιδιότητες ενός αντικειμένου σε ένα δάσος. Επιπλέον, οι διακομιστές καθολικού καταλόγου παρέχουν μια λίστα με όλα τα αντικείμενα σε ένα δάσος.

Οι Οργανωτικές Μονάδες (OU) οργανώνουν χρήστες, ομάδες και συσκευές. Κάθε τομέας μπορεί να περιέχει το δικό του OU. Ωστόσο, τα OU δεν μπορούν να έχουν ξεχωριστούς χώρους ονομάτων, καθώς κάθε χρήστης ή αντικείμενο σε έναν τομέα πρέπει να είναι μοναδικός. Για παράδειγμα, δεν μπορεί να δημιουργηθεί ένας λογαριασμός χρήστη με το ίδιο όνομα χρήστη.

Τα κοντέινερ είναι παρόμοια με τα OU, αλλά τα αντικείμενα πολιτικής ομάδας δεν μπορεί να εφαρμοστούν ή να συνδεθούν με αντικείμενα κοντέινερ.

5.3.3.3 Εμπιστοσύνη στο Active Directory

Η υπηρεσία καταλόγου Active Directory βασίζεται σε καταπιστεύματα για τον έλεγχο των δικαιωμάτων πρόσβασης πόρων μεταξύ τομέων. Υπάρχουν διάφοροι τύποι καταπιστεύσεων:

- Σε μια μονόδρομη εμπιστοσύνη ένας πρώτος τομέας επιτρέπει δικαιώματα πρόσβασης σε χρήστες σε έναν δεύτερο τομέα. Ωστόσο, ο δεύτερος τομέας δεν επιτρέπει την πρόσβαση σε χρήστες στον πρώτο τομέα.
- Σε μια αμφίδρομη εμπιστοσύνη υπάρχουν δύο τομείς και κάθε τομέας επιτρέπει την πρόσβαση στους χρήστες του άλλου τομέα.
- Ένας αξιόπιστος τομέας είναι ένας μεμονωμένος τομέας που επιτρέπει την πρόσβαση του χρήστη σε έναν άλλο τομέα, ο οποίος ονομάζεται αξιόπιστος τομέας.
- Ένα μεταβατικό καταπίστευμα μπορεί να επεκταθεί πέρα από δύο τομείς και να επιτρέπει την πρόσβαση σε άλλους αξιόπιστους τομείς μέσα σε ένα δάσος.
- Μια αμετάβατη εμπιστοσύνη είναι μια μονόδρομη εμπιστοσύνη που περιορίζεται σε δύο τομείς.
- Μια ρητή εμπιστοσύνη είναι μια μονόδρομη, μη μεταβατική εμπιστοσύνη που δημιουργείται από έναν διαχειριστή δικτύου.

- Μια αξιοπιστία διασύνδεσης είναι ένας τύπος ρητής εμπιστοσύνης. Οι αξιοπιστίες διασύνδεσης λαμβάνουν χώρα μεταξύ τομέων εντός του ίδιου δέντρου, χωρίς σχέση παιδιού-γονέα μεταξύ των δύο τομέων ή εντός διαφορετικών δέντρων.
- Ένα δασικό καταπίστευμα ισχύει για τομείς σε ολόκληρο το δάσος και μπορεί να είναι μονόδρομος, αμφίδρομος ή μεταβατικός.
- Μια συντόμευση ενώνει δύο τομείς που ανήκουν σε ξεχωριστά δέντρα. Οι συντομεύσεις μπορεί να είναι μονόδρομες, αμφίδρομες ή μεταβατικές.
- Ένα βασίλειο είναι ένα καταπίστευμα που είναι μεταβατικό, αμετάβατο, μονόδρομο ή αμφίδρομο.
- Ένα εξωτερικό καταπίστευμα δημιουργείται με έναν εξωτερικό τομέα έξω από το σύμπλεγμα δομών αυτού του αξιόπιστου τομέα. Επιπλέον συνδέει τομείς σε ξεχωριστά δάση ή τομείς που δεν είναι AD. Τα εξωτερικά καταπιστεύματα μπορεί να είναι μη μεταβατικά, μονόδρομα ή αμφίδρομα.
- Ένα καταπίστευμα διαχείρισης ιδιωτικής πρόσβασης (PAM) είναι ένα μονόδρομο καταπίστευμα που δημιουργείται από το Microsoft Identity Manager μεταξύ ενός δάσους παραγωγής και ενός δάσους προμαχώνων.

5.3.3.4 Ιστορικό και ανάπτυξη του Active Directory

Η Microsoft προσέφερε μια προεπισκόπηση του Active Directory το 1999 και το κυκλοφόρησε ένα χρόνο αργότερα με τον Windows 2000 Server. Η Microsoft συνέχισε να αναπτύσσει νέες δυνατότητες με κάθε διαδοχική έκδοση του Windows Server. Ο Windows Server 2003 περιελάμβανε μια αξιοσημείωτη ενημέρωση για την προσθήκη δασών και τη δυνατότητα επεξεργασίας και αλλαγής της θέσης των τομέων εντός των δασών. Οι τομείς στον Windows Server 2000 δεν μπορούσαν να υποστηρίξουν νεότερες ενημερώσεις AD που εκτελούνται στον Server 2003. Ο Windows Server 2008 παρουσίασε το AD FS. Επιπλέον, η Microsoft μετονομάστηκε στον κατάλογο για τη διαχείριση τομέα ως AD DS και ο όρος AD έγινε γενικός όρος για τις υπηρεσίες που βασίζονται σε κατάλογο που υποστήριζε.

Ο Windows Server 2016 ενημέρωσε το AD DS για να βελτιώσει την ασφάλεια του AD και να μετεγκαταστήσει περιβάλλοντα AD σε περιβάλλοντα cloud ή υβριδικά cloud. Οι ενημερώσεις ασφαλείας περιελάμβαναν την προσθήκη του PAM (Privileged Access Manager - Προνομιούχος Διαχειριστής Πρόσβασης). Το PAM παρακολουθούσε την πρόσβαση σε ένα αντικείμενο, τον τύπο πρόσβασης που χορηγήθηκε και τις ενέργειες που έκανε ο χρήστης. Το PAM πρόσθεσε παραπάνω δάση στο AD, για να μπορεί να παρέχει το AD ένα επιπλέον ασφαλές και απομονωμένο δασικό περιβάλλον. Ο Windows Server 2016 τελείωσε την υποστήριξη για συσκευές στον Windows Server 2003.

Τον Δεκέμβριο του 2016, η Microsoft κυκλοφόρησε το Azure AD Connect για να συμμετάσχει σε ένα εσωτερικό σύστημα Active Directory με το Azure Active Directory (Azure AD) για να ενεργοποιήσει το SSO για τις υπηρεσίες cloud της Microsoft, όπως το Office 365. Το Azure AD Connect λειτουργεί με συστήματα που εκτελούν Windows Server 2008, Windows Server 2012, Windows Server 2016, καθώς και Windows Server 2019.

5.3.3.5 Τομείς έναντι ομάδων εργασίας.

Η **ομάδα εργασίας** είναι ο όρος της Microsoft για μηχανήματα Windows που συνδέονται μέσω δικτύου peer-to-peer. Οι ομάδες εργασίας είναι μια άλλη μονάδα οργάνωσης των υπολογιστών με Windows σε δίκτυα. Οι ομάδες εργασίας επιτρέπουν σε αυτά τα μηχανήματα να μοιράζονται αρχεία, πρόσβαση στο Διαδίκτυο, εκτυπωτές

και άλλους πόρους μέσω του δικτύου. Η ομότιμη δικτύωση (peer-to-peer) καταργεί την ανάγκη για έναν διακομιστή για τον έλεγχο ταυτότητας. Υπάρχουν πολλές διαφορές μεταξύ τομέων και ομάδων εργασίας:

- Οι τομείς, σε αντίθεση με τις ομάδες εργασίας, μπορούν να φιλοξενήσουν υπολογιστές από διαφορετικά τοπικά δίκτυα.
- Οι τομείς μπορεί να χρησιμοποιηθούν για να φιλοξενήσουν πολύ περισσότερους υπολογιστές σε σχέση με τις ομάδες εργασίας. Οι τομείς μπορεί να περιλαμβάνουν χιλιάδες υπολογιστές, σε αντίθεση με τις ομάδες εργασίας, οι οποίες συνήθως έχουν ένα ανώτερο όριο κοντά στο 20.
- Στους τομείς υπάρχει τουλάχιστον ένας διακομιστής που είναι ένας υπολογιστής, ο οποίος χρησιμοποιείται για τον έλεγχο των δικαιωμάτων και των δυνατοτήτων ασφαλείας για κάθε υπολογιστή εντός του τομέα. Στις ομάδες εργασίας, δεν υπάρχει διακομιστής και οι υπολογιστές είναι όλοι ομότιμοι.
- Οι χρήστες τομέα απαιτούν συνήθως αναγνωριστικά ασφαλείας, όπως στοιχεία σύνδεσης και κωδικούς πρόσβασης, σε αντίθεση με τις ομάδες εργασίας.

5.3.3.6 Κύριοι ανταγωνιστές της Active Directory

Άλλες υπηρεσίες καταλόγου στην αγορά που παρέχουν παρόμοια λειτουργικότητα με το AD είναι το Red Hat Directory Server, το Apache Directory και το OpenLDAP.

Ο διακομιστής καταλόγου Red Hat διαχειρίζεται την πρόσβαση των χρηστών σε πολλαπλά συστήματα σε περιβάλλοντα Unix. Παρόμοια με το AD, ο διακομιστής καταλόγου Red Hat περιλαμβάνει αναγνωριστικό χρήστη και έλεγχο ταυτότητας που βασίζεται σε πιστοποιητικό για τον περιορισμό της πρόσβασης στα δεδομένα στον κατάλογο.

Ο Κατάλογος Apache είναι ένα έργο ανοιχτού κώδικα που εκτελείται σε Java και λειτουργεί σε οποιονδήποτε διακομιστή LDAP, συμπεριλαμβανομένων συστημάτων σε Windows, macOS και Linux. Ο Κατάλογος Apache περιλαμβάνει ένα πρόγραμμα περιήγησης σχήματος και έναν επεξεργαστή και πρόγραμμα περιήγησης LDAP. Ο Κατάλογος Apache υποστηρίζει πρόσθετα Eclipse.

Το OpenLDAP είναι ένας κατάλογος LDAP ανοιχτού κώδικα που βασίζεται σε Windows. Το OpenLDAP επιτρέπει στους χρήστες να περιηγούνται, να αναζητούν και να επεξεργάζονται αντικείμενα σε έναν διακομιστή LDAP. Οι δυνατότητες του OpenLDAP περιλαμβάνουν την αντιγραφή, τη μετακίνηση και τη διαγραφή δέντρων στον κατάλογο, καθώς και την ενεργοποίηση της περιήγησης σε σχήματα, της διαχείρισης κωδικού πρόσβασης και της υποστήριξης LDAP SSL (Secure Sockets Layer).

5.4 Υπηρεσίες Εντοπισμού

Παραπάνω, εξηγήσαμε ότι τα αναγνωριστικά είναι βολικά για να αναπαριστούν μοναδικές οντότητες. Είδαμε διαφόρους μηχανισμούς εύρεσης και ονοματοθεσίας να εκτελούνται με κατανεμημένο τρόπο και να βασίζονται κυρίως στα στοιχεία του ίδιου του ονόματος ή του αναγνωριστικού. Υπάρχουν όμως πολλές περιπτώσεις, όπου τα αναγνωριστικά είναι απλώς τυχαίες συμβολοσειρές, τις οποίες βολικά αναφέρουμε ως μη δομημένα ή επίπεδα ονόματα. Μια σημαντική ιδιότητα ενός τέτοιου ονόματος είναι ότι δεν περιέχει καμία απολύτως πληροφορία σχετικά με τον τρόπο εντοπισμού του σημείου πρόσβασης της συσχετισμένης οντότητας. Σε αυτήν την ενότητα, θα ρίξουμε

μια ματιά στον τρόπο επίλυσης των επίπεδων ονομάτων ή, ακόμα πώς μπορούμε να εντοπίσουμε μια οντότητα όταν δίνεται μόνο το αναγνωριστικό της.

5.5.1 Απλές λύσεις

Αρχικά εξετάζουμε δύο απλές λύσεις για τον εντοπισμό μιας οντότητας. Και οι δύο λύσεις ισχύουν μόνο για τοπικά δίκτυα. Ωστόσο, σε αυτό το περιβάλλον, συχνά κάνουν τη δουλειά τους καλά, κάνοντας την απλότητά τους ιδιαίτερα ελκυστική.

Εκπομπή και Πολυεκπομπή

Ο εντοπισμός μιας οντότητας σε ένα τέτοιο περιβάλλον είναι απλός. Αρχικά ένα μήνυμα που περιέχει το αναγνωριστικό της οντότητας μεταδίδεται σε κάθε μηχάνημα και κάθε μηχάνημα καλείται να ελέγξει εάν περιέχει αυτήν την οντότητα. Τα μηχανήματα που περιέχουν - συνδέονται με την οντότητα σε κάποιο σημείο πρόσβασης στέλνουν ένα μήνυμα απάντησης που περιέχει τη διεύθυνση (απομακρυσμένη αναφορά) αυτού του σημείου πρόσβασης.

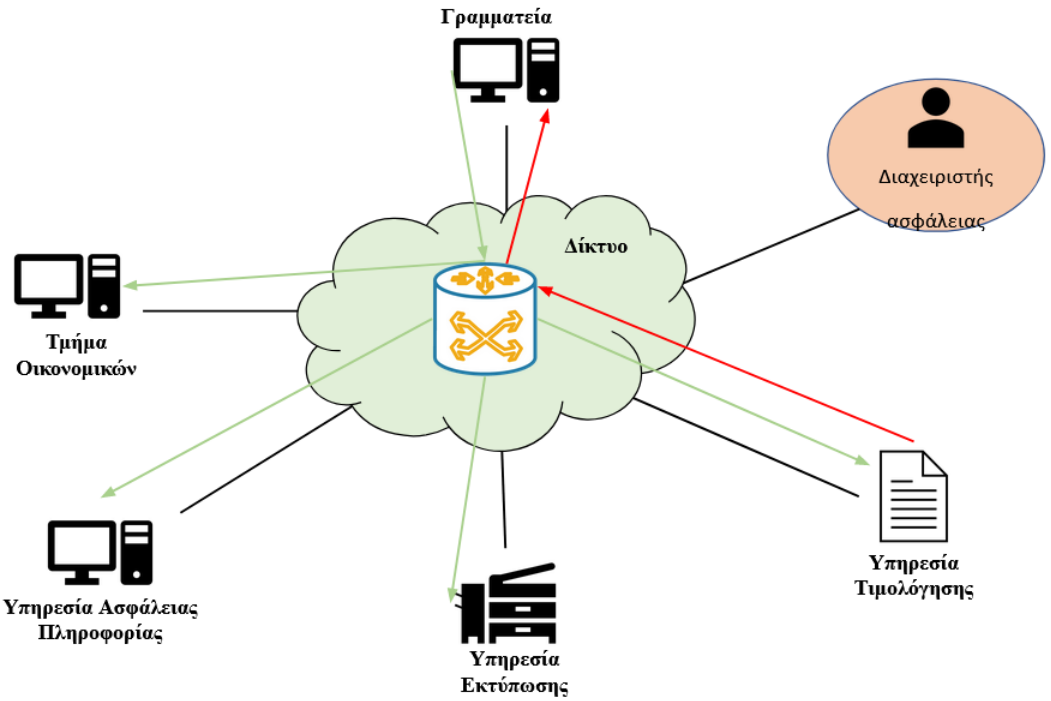
Αυτή η αρχή χρησιμοποιείται στο Πρωτόκολλο Ανάλυσης Διεύθυνσης Διαδικτύου (ARP) για την εύρεση της διεύθυνσης σύνδεσης δεδομένων ενός μηχανήματος. Στην ουσία, ένα μηχάνημα εκπέμπει (broadcast) ένα πακέτο στο τοπικό δίκτυο ρωτώντας ποιος είναι ο κάτοχος μιας δεδομένης διεύθυνσης IP. Όταν το μήνυμα φτάνει σε κάποιο μηχάνημα, αυτό με τη σειρά του ελέγχει εάν πρέπει να ακούσει την ζητούμενη διεύθυνση IP. Εάν ναι, στέλνει ένα πακέτο απάντησης που περιέχει, για παράδειγμα, τη διεύθυνση τοπικού δικτύου (π.χ. Ethernet) του.

Η εκπομπή (broadcast) γίνεται αναποτελεσματική σε μεγάλα δίκτυα. Όχι μόνο καταναλώνεται το εύρος ζώνης του δικτύου από τα αιτήματα, αλλά και στη χειρότερη περίπτωση, πολλοί κεντρικοί υπολογιστές μπορεί να παύσουν να λειτουργούν λόγω των αιτημάτων που δεν μπορούν να απαντήσουν. Μια πιθανή λύση είναι η μετάβαση σε \πολυεκπομπή (multicasting), με την οποία μόνο μια περιορισμένη ομάδα κεντρικών υπολογιστών λαμβάνει το αίτημα.

Η πολυεκπομπή μπορεί επίσης να χρησιμοποιηθεί για τον εντοπισμό οντοτήτων σε δίκτυα από σημείο σε σημείο (point-to-point). Για παράδειγμα, το Διαδίκτυο υποστηρίζει την πολυεκπομπή σε επίπεδο δικτύου επιτρέποντας στους κεντρικούς υπολογιστές να συμμετέχουν σε μια συγκεκριμένη ομάδα πολλαπλής εκπομπής. Όταν ένας κεντρικός υπολογιστής στέλνει ένα μήνυμα σε μια διεύθυνση πολλαπλής διανομής, το επίπεδο δικτύου παρέχει μια υπηρεσία βέλτιστης προσπάθειας (best effort) για την παράδοση αυτού του μηνύματος σε όλα τα μέλη της ομάδας.

Μια διεύθυνση πολλαπλής μετάδοσης μπορεί να χρησιμοποιηθεί ως γενική υπηρεσία τοποθεσίας για πολλές οντότητες. Για παράδειγμα, κάθε εργαζόμενος σε μία εταιρεία έχει τον δικό του φορητό υπολογιστή. Όταν αυτός συνδέεται στο τοπικά διαθέσιμο δίκτυο, του εκχωρείται δυναμικά μια διεύθυνση IP. Επιπλέον, εντάσσεται σε μια συγκεκριμένη ομάδα πολυεκπομπής. Όταν μια διεργασία θέλει να εντοπίσει τον υπολογιστή Α, στέλνει ένα αίτημα του τύπου "πού είναι το Α;" στην ομάδα πολλαπλών εκπομπών. Εάν το Α είναι συνδεδεμένο, αποκρίνεται με την τρέχουσα διεύθυνση IP του.

Στην εικονα 6 υπάρχει ένα παράδειγμα στο οποίο η γραμματεία βρίσκει ένα αρχείο που βρίσκεται στην υπηρεσία τιμολόγησης στέλνοντας μηνύματα σε μία συγκεκριμένη ομάδα πολυεκπομπής.



ΕΙΚΟΝΑ 6 Παράδειγμα πολυεκπομπής (multicast)

5.5.2 Δείκτες προώθησης.

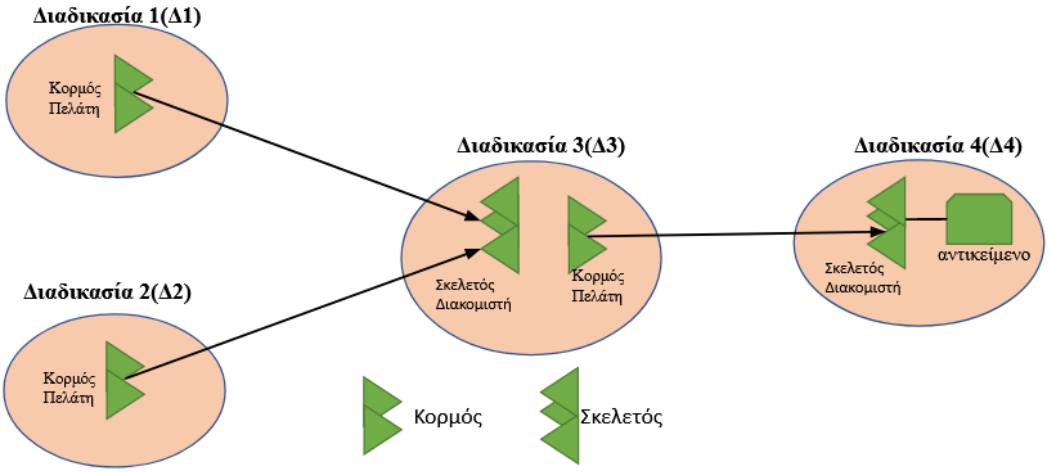
Μια άλλη δημοφιλής προσέγγιση για τον εντοπισμό οντοτήτων είναι η χρήση δεικτών προώθησης. Η αρχή είναι απλή: όταν μια οντότητα μετακινείται από το Α στο Β, αφήνει πίσω στο Α μια αναφορά για τη νέα θέση της στο Β. Η προσέγγιση αυτή χαρακτηρίζεται για την απλότητά της. Πιο συγκεκριμένα, μόλις εντοπιστεί μια οντότητα, ένας πελάτης μπορεί να αναζητήσει την τρέχουσα διεύθυνση ακολουθώντας την αλυσίδα των δεικτών προώθησης.

Υπάρχουν, όμως, ορισμένα σημαντικά μειονεκτήματα.

- Πρώτον, εάν δεν ληφθούν ειδικά μέτρα, μια αλυσίδα για μια οντότητα υψηλής κινητικότητας μπορεί να γίνει τόσο μεγάλη που ο εντοπισμός αυτής της οντότητας να είναι απαγορευτικά δαπανηρός.
- Δεύτερον, όλες οι ενδιάμεσες θέσεις σε μια αλυσίδα θα πρέπει να διατηρούν το μέρος της αλυσίδας των δεικτών προώθησης όσο χρειάζεται.
- Ένα τρίτο μειονέκτημα είναι η ευπάθεια σε κατεστραμμένους συνδέσμους. Μόλις χαθεί οποιοσδήποτε δείκτης προώθησης (για οποιονδήποτε λόγο) δεν είναι πλέον δυνατή η πρόσβαση στην οντότητα.

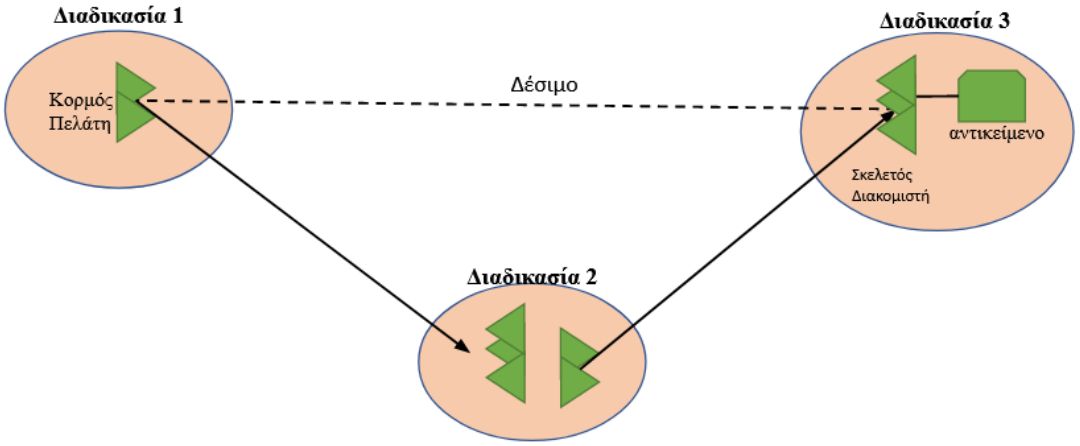
Κατά συνέπεια, ένα σημαντικό ζήτημα είναι να διατηρηθούν οι αλυσίδες σχετικά σύντομες και να διασφαλιστεί ότι οι δείκτες προώθησης είναι ισχυροί.

Στην Εικόνα 7 φαίνεται η αρχή της προώθησης δεικτών με χρήση ζευγών (κορμός πελάτη, σκελετός διακομιστή).



ΕΙΚΟΝΑ 7 Παράδειγμα δεικτών προώθησης.

Κάθε φορά που ένα αντικείμενο μετακινείται από τον χώρο διευθύνσεων του Δ3 στον χώρο του Δ4, αφήνει πίσω του ένα κορμό πελάτη στη θέση του στο Δ3 και εγκαθιστά ένα σκελετό διακομιστή στο Δ4. Στην εικόνα 7 οι Δ1 και Δ2 αναζητουν το Δ4, και το βρίσκουν μέσω του Δ3. Επιπλέον, αυτή η χρήση των δεικτών προώθησης δεν είναι σαν την διαδικασία αναζήτησης διεύθυνσης. Αντίθετα, το αίτημα ενός πελάτη προωθείται κατά μήκος της αλυσίδας μέχρι να βρει το αντικείμενο.
Για την γρηγορότερη προσπέλαση μιας αλυσίδας ζευγών (κορμός πελάτη, σκελετός διακομιστή), μια κλήση αντικειμένου “κουβαλάει” τον κορμό του πελάτη από το σημείο εκκίνησης αυτής της κλήσης. Η πληροφορία του κορμού του πελάτη αποτελείται από τη διεύθυνση επιπέδου μεταφοράς του πελάτη, σε συνδυασμό με έναν τοπικά δημιουργημένο αριθμό για την αναγνώριση αυτού του κορμού. Όταν η κλήση φτάσει στην τρέχουσα θέση του αντικειμένου, μια απάντηση αποστέλλεται πίσω στον κορμό πελάτη, όπου ξεκίνησε η κλήση (συχνά χωρίς να επιστρέψουν όλα τα μέρη της αλυσίδας). Μετά τη λήψη του μηνύματος επιστροφής ο κορμός πελάτη δένεται (binding) στο σκελετό που βρίσκεται στον τελικό διακομιστή, στην τρέχουσα θέση του αντικειμένου. Αυτή η αρχή φαίνεται στην εικόνα 8.



ΕΙΚΟΝΑ 8 Δέσιμο (binding) κορμού πελάτη στον σκελετό διακομιστή.

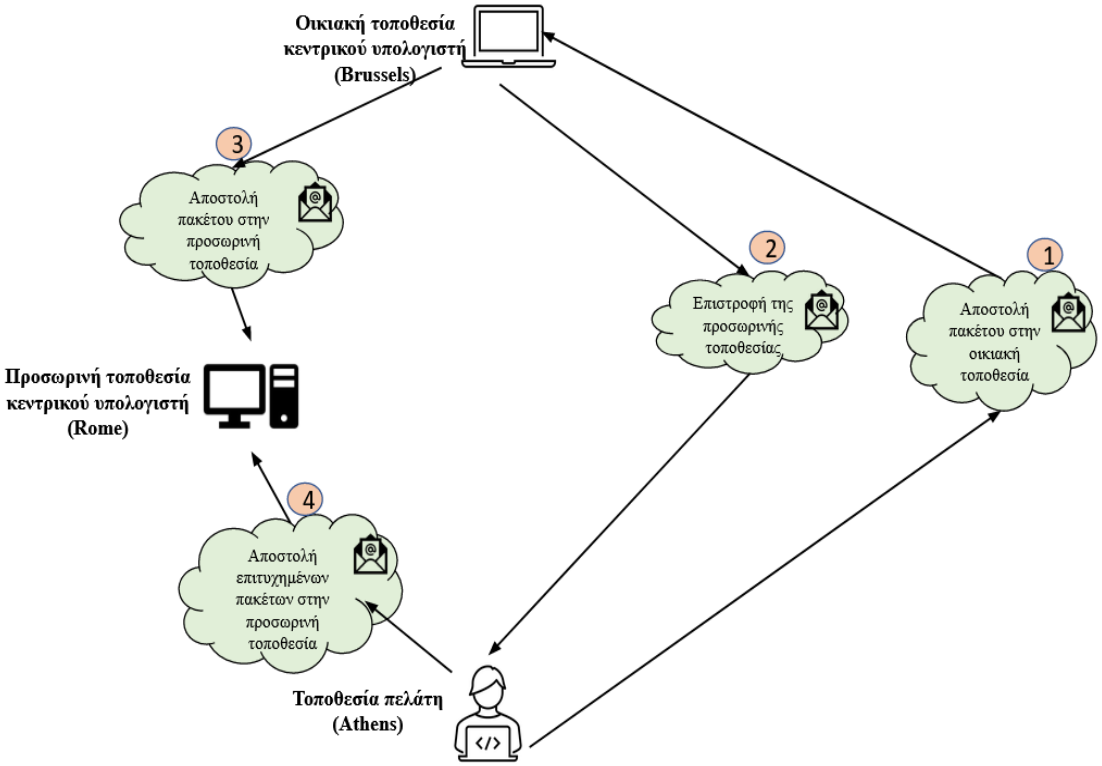
Υπάρχει μια αντιστάθμιση μεταξύ της αποστολής της απάντησης απευθείας στον κορμό του πελάτη εκκίνησης ή κατά μήκος της αντίστροφης διαδρομής των δεικτών προώθησης. Στην πρώτη περίπτωση, η επικοινωνία είναι ταχύτερη επειδή μπορεί να χρειαστεί να περάσουν λιγότερα ενδιάμεσα στάδια. Από την άλλη πλευρά, η αποστολή της απόκρισης κατά μήκος της αντίστροφης διαδρομής απαιτεί την προσαρμογή-δέσιμο (binding) όλων των ενδιάμεσων στελεχών!

5.5.3 Οικιακή τοποθεσία

Η χρήση δεικτών μετάδοσης και προώθησης δημιουργεί προβλήματα επεκτασιμότητας. Η μετάδοση ή η πολλαπλή μετάδοση είναι δύσκολο να εφαρμοστεί αποτελεσματικά σε δίκτυα μεγάλης κλίμακας, ενώ οι μακριές αλυσίδες δεικτών προώθησης δημιουργούν προβλήματα απόδοσης και είναι επιρρεπείς στην καταστροφή συνδέσμων. Μια δημοφιλής προσέγγιση για την υποστήριξη φορητών οντοτήτων σε δίκτυα μεγάλης κλίμακας είναι η εισαγωγή μιας τοποθεσίας κατοικίας (home location), η οποία παρακολουθεί την τρέχουσα τοποθεσία μιας οντότητας. Στην πράξη, η τοποθεσία κατοικίας επιλέγεται συχνά ως το μέρος όπου δημιουργήθηκε μια οντότητα.

Κάθε κινητός κεντρικός υπολογιστής χρησιμοποιεί μια σταθερή διεύθυνση IP. Όλη η επικοινωνία σε αυτή τη διεύθυνση IP κατευθύνεται αρχικά στον πράκτορα κατοικίας του κεντρικού υπολογιστή κινητής τηλεφωνίας. Αυτός ο πράκτορας κατοικίας βρίσκεται σε κάποιο συγκεκριμένο τοπικό δίκτυο. Αυτό το τοπικο δίκτυο εντοπίζεται από τη διεύθυνση IP του κεντρικού υπολογιστή κινητής τηλεφωνίας. Πιο συγκεκριμένα, κοιτάμε τη διεύθυνση δικτύου που αντιστοιχεί το τοπικό δίκτυο μέσω της διεύθυνσης IP. Στην περίπτωση του IPv6, αυτό υλοποιείται ως στοιχείο επιπέδου δικτύου. Κάθε φορά που ο κεντρικός υπολογιστής κινητής τηλεφωνίας μετακινείται σε άλλο δίκτυο, ζητά μια προσωρινή διεύθυνση που μπορεί να χρησιμοποιήσει για επικοινωνία. Αυτή η προσωρινή διεύθυνση κατοικίας καταχωρείται στον πράκτορα κατοικίας.

Όταν ο πράκτορας κατοικίας λαμβάνει ένα πακέτο για τον κεντρικό υπολογιστή κινητής τηλεφωνίας, αναζητά την τρέχουσα τοποθεσία του κεντρικού υπολογιστή. Εάν ο κεντρικός υπολογιστής βρίσκεται στο τρέχον τοπικό δίκτυο, το πακέτο απλώς προωθείται. Διαφορετικά, “πακετάρεται” ως δεδομένα σε ένα πακέτο IP και αποστέλλεται στη προσωρινή διεύθυνση κατοικίας. Ταυτόχρονα, ο αποστολέας του πακέτου ενημερώνεται για την τρέχουσα τοποθεσία του κεντρικού υπολογιστή. Αυτή η αρχή φαίνεται στην Εικόνα 9. Σημειώστε ότι η διεύθυνση IP χρησιμοποιείται αποτελεσματικά ως αναγνωριστικό για τον κεντρικό υπολογιστή κινητής τηλεφωνίας.



Εικόνα 9 Η αρχή της Mobile IP.

Η προσέγγιση αυτή παρουσιάζει επίσης ένα μειονέκτημα σε δίκτυα μεγάλης κλίμακας. Συγκεκριμένα, για να επικοινωνήσει με μια φορητή οντότητα, ένας πελάτης πρέπει πρώτα να επικοινωνήσει με την κατοικία, η οποίο μπορεί να βρίσκεται σε εντελώς διαφορετική τοποθεσία από την ίδια την οντότητα. Το αποτέλεσμα είναι μια αύξηση του χρόνου επικοινωνίας.

Ένα ακόμα μειονέκτημα της προσέγγισης κατοικίας είναι η χρήση μιας σταθερής τοποθεσίας κατοικίας. Πρώτον, πρέπει να διασφαλιστεί ότι η τοποθεσία κατοικίας υπάρχει πάντα, διαφορετικά, η επικοινωνία με την οντότητα θα καταστεί αδύνατη. Τα προβλήματα επιδεινώνονται όταν μια μακρόβια οντότητα αποφασίζει να μετακομίσει μόνιμα σε ένα εντελώς διαφορετικό μέρος του δικτύου από την τοποθεσία κατοικίας (home location) της. Μια λύση σε αυτό το πρόβλημα είναι να γίνει καταχώρηση της κατοικίας σε μια κλασσική υπηρεσία ονομασίας, έτσι ώστε ο πελάτης να αναζητήσει την τοποθεσία κατοικίας στην υπηρεσία ονομασίας. Δεδομένου ότι η τοποθεσία κατοικίας μπορεί να θεωρηθεί ότι δεν αλλάζει συχνά και είναι σχετικά σταθερή, η τοποθεσία, η οποία επέστρεψε από την υπηρεσία ονομασίας, μπορεί να αποθηκευτεί στην προσωρινή μνήμη προς χρήση.

Βιβλιογραφικές αναφορές

[1] M. van Steen and A.S. Tanenbaum, Distributed Systems, 3rd ed., distributed-systems.net, 2017.

[2] Coulouris, J. Dollimore, T. Kindberg, G. Blair (2020), Κατανεμημένα Συστήματα, Έκδοση: 2η, Da Vinci M.E.Π.E.

[3] Κάβουρας Ι.Κ., Μήλης Ι.Ζ., Ρουκουνάκη Α.Α., Ξηλωμένος Γ.Β. (2011), Κατανεμημένα συστήματα σε Java, 3η έκδοση, Εκδόσεις Κλειδάριθμος ΕΠΕ.

[4] Sector, S., & Itu, O. F. (2008). ITU-T, Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.

[5] X.500 and LDAP. (n.d.). Retrieved October 3, 2022, from https://www.collectionscanada.gc.ca/iso/ill/document/ill_directory/X_500andLDAP.pdf

[6] Tuttle, S., Ehlenberger, A., Gorthi, R., Leiserson, J., Macbeth, R., Owen, N., Ranahandola, S., Storrs, M., & Yang, C. (2004). Understanding LDAP Design and Implementation LDAP concepts and architecture Designing and maintaining LDAP Step-by-step approach for directory Front cover (p. 774). ibm.com/redbooks. https://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf

[7] https://ldap.com (πρόσβαση 8/10/2022)

[8] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/ (πρόσβαση 8/10/2022)

Κριτήρια αξιολόγησης

Ερώτηση 1

Η ομάδα εργασίας είναι ο όρος της Microsoft για μηχανήματα Windows που συνδέονται μέσω δικτύου client-server;

α. Σωστό

β. Λάθος

Ερώτηση 2

Ο χώρος ονομάτων DNS Διαδικτύου είναι διαμερισμένος, τόσο οργανωτικά όσο και γεωγραφικά

α. Μόνο οργανωτικά.

β. Μόνο γεωγραφικά.

γ. Οργανωτικά και γεωγραφικά.

Ερώτηση 3

Ένας τομέας είναι μια ομάδα αντικειμένων, όπως χρήστες ή συσκευές, που μοιράζονται διαφορετική βάση δεδομένων Active Directory.

α. Σωστό

β. Λάθος

Ερώτηση 4

Οι τομείς μπορεί να χρησιμοποιηθούν για να φιλοξενήσουν πολύ περισσότερους υπολογιστές από ό,τι ομάδες εργασίας.

α. Σωστό

β. Λάθος

Ερώτηση 5

Το DNS έχει τις εξής δυνατότητες:

α. Μετάφραση ονομάτων σε διευθύνσεις IP.

β. Εντοπισμό εξυπηρετητών email .

γ. Αντικατάσταση των αρχείων αντιστοίχισης.

δ. Όλα τα παραπάνω

Ερώτηση 6

Το OpenLDAP είναι ένας κατάλογος LDAP ανοιχτού κώδικα που βασίζεται σε

α. Debian.

β. Apache.

γ. Red Hat.

δ. Windows

ε. Oracle

Ερώτηση 7

Η αρχιτεκτονική του πρωτοκόλλου LDAP αποτελείται από έναν πελάτη-διακομιστή που επικοινωνεί μέσω του μοντέλου δικτύωσης:

α. UDP/IP

β. OSI

γ. TCP/IP

δ. Κανένα από τα παραπάνω

Ερώτηση 8

Το LDAP προσδιορίζει τα αντικείμενα με ένα μοναδικό-ή ...

α. Αριθμό

β. Όνομα

γ. Διεύθυνση IP

δ. Κανένα από τα παραπάνω

Ερώτηση 9

Το πρωτόκολλο X.500 χρησιμοποιεί την υποδομή δημόσιου κλειδιού X.509 (PKI) η οποία χρησιμοποιεί ψηφιακά πιστοποιητικά για τον έλεγχο ταυτότητας.

α. Σωστό

β. Λάθος

Ερώτηση 10

Το DNS έχει την δυνατότητα αντικατάστασης αρχείων αντιστοίχισης.

α. Σωστό

β. Λάθος

Ερώτηση 11

Το DNS έχει τη δυνατότητα εντοπισμού ενός email server.

α. Σωστό

β. Λάθος

Ερώτηση 12

Σε μια τυπική συνεδρία X.500 ο πελάτης συνδέεται και ζητά πρόσβαση στο διακομιστή και ο διακομιστής ολοκληρώνει τη δέσμευση.

α. Σωστό

β. Λάθος

Ερώτηση 13

Η μορφή xxxx:xxxx00:xxxx:000:0000 αποτελεί μορφή …

α. URL

β. URN

γ. URM

δ. ipv4

Ερώτηση 14

Το DNS αντιστοιχίζει τα ονόματα τομέα με τα χαρακτηριστικά ενός κεντρικού υπολογιστή, δηλαδή τη διεύθυνση IP

α. Σωστό

β. Λάθος

Ερώτηση 15

Ένα πιστοποιητικό χρησιμοποιεί κρυπτογράφηση για να επιτρέπει σε έναν χρήστη να ανταλλάσσει πληροφορίες μέσω του Διαδικτύου με ασφάλεια με δημόσιο κλειδί.

α. Σωστό

β. Λάθος

Ερώτηση 16

Όταν μια οντότητα μετακινείται από το Α στο Β, αφήνει πίσω στο Α μια αναφορά στη νέα θέση της στο Β, Αυτή η τεχνική αφορά …

α. Οικιακή τοποθεσία

β. Δείκτες προώθησης

γ. Multicast

δ. Broadcast

Ερώτηση 17

Στους δείκτες προώθησης, μια αλυσίδα για μια οντότητα υψηλής κινητικότητας μπορεί να γίνει τόσο μεγάλη που ο εντοπισμός αυτής της οντότητας να ...

α. γίνεται εξαιρετικά εύκολος

β. είναι απαγορευτικά δαπανηρός

γ. δεν επηρεάζει την διαδικασία

δ. γίνεται από διαφορετική αλυσίδα

Ερώτηση 18

Ένα από τα πλεονεκτήματα της προσέγγισης κατοικίας είναι η χρήση μιας σταθερής τοποθεσίας κατοικίας.

α. Σωστό

β. Λάθος

Ερώτηση 19

Η χρήση ψευδωνύμων κατά τη διαχείριση του DNS, σε περίπτωση που η διαχείριση περάσει σε άλλο μηχάνημα διακομιστή, προσφέρει τη δυνατότητα να αλλάξουν τα ονόματα και οι διευθύνσεις από τα δύο μηχανήματα.

α. Σωστό

β. Λάθος

Ερώτηση 20

Ο χώρος ονομάτων DNS έχει τα εξής χαρακτηριστικά

α. Χρησιμοποιεί τον χαρακτήρα της τελείας για διαχωρισμο

β. Υποστηρίζει μέχρι 63/255 χαρακτήρες ανά ακμή/διαδρομή.

γ. Είναι ένα κατευθυνόμενο δέντρο με ρίζα

δ. Όλα τα παραπάνω