Κεφάλαιο 10
Σχεδιασμός και Ανάπτυξη Δικτύων

Σύνοψη
Ανάλυση αναγκών, στόχων και περιορισμών ενός οργανισμού/επιχείρησης. Ανάλυση τεχνικών στόχων. Λογικός Σχεδιασμός: τοπολογία, μοντέλα για διευθυνσιοδότηση, επιλογή πρωτοκόλλων δρομολόγησης, ανάπτυξη στρατηγικών ασφάλειας και διαχείρισης. Σχεδιασμός του φυσικού δικτύου - περιπτώσεις. Δοκιμή του Σχεδιασμού, βελτιστοποίηση, τεκμηρίωση - περιπτώσεις.

Προαπαιτούμενη γνώση
Γνώση σε βασικά ζητήματα Δικτύων Υπολογιστών.

10.1. Πώς ξεκινάμε τον Σχεδιασμό ενός Δικτύου

Όπως είδαμε και στην Εισαγωγή, παρά τις γνώσεις και την εμπειρία που μπορεί να έχει κάποιος σε θέματα διαχείρισης δικτύων, ο σχεδιασμός παραμένει μία πολύ δύσκολη εργασία. Στο παρόν κεφάλαιο επιχειρούμε μία σύντομη επισκόπηση των βασικών προτάσεων επίλυσης του προβλήματος αυτού.

Υπάρχουν πολλές δυνατές μεθοδολογίες. Μάλιστα, πολλά από τα αντίστοιχα εργαλεία μοιάζουν να αποτελούν ένα παιχνίδι όπου ο σχεδιαστής καλείται απλά να ενώσει κάποιες τελείες που αντιπροσωπεύουν τους κόμβους του δικτύου, διανθίζοντας το σχέδιο με παραμέτρους για την χωρητικότητα της κυκλοφορίας, συγκεκριμένα μοντέλα δρομολογητών στους κόμβους, κλπ. Κάτι τέτοιο όμως είναι παραπλανητικό και άρα εσφαλμένο.

Γενικά, ως μεθοδολογία προτιμάται η προσέγγιση από-επάνω-προς-τα-κάτω (top-down). Εδώ, ο σχεδιασμός ξεκινά από το κορυφαίο επίπεδο του μοντέλου αναφοράς ISO OSI, και βαθμιαία επεκτείνεται προς τα χαμηλότερα επίπεδα. Ορισμένοι μάλιστα θεωρούν ότι στην κορυφή του μοντέλου αναφοράς πρέπει να τοποθετηθεί ένα όγδοο επίπεδο: οι πολιτικές στον χώρο εργασίας. Αυτό σημαίνει ότι ο σχεδιαστής θα πρέπει να κατανοεί τις πολιτικές (ακόμα και μικρο-πολιτικές) που υπάρχουν στην συγκεκριμένη εταιρεία ή οργανισμό, μια και αποτελούν σημαντικό μέρος των στόχων της εταιρίας και, επομένως, σημαντικό παράγοντα επιτυχίας του αποτελέσματος. Συνεπώς, ο σχεδιαστής πρέπει να διερευνήσει τις δομές της επιχείρησης και των ομάδων που δρουν σε αυτήν, ώστε να είναι σε θέση προσδιορίσει τους ανθρώπους-κλειδιά από όπου θα πάρει τις απαραίτητες πληροφορίες, οι οποίες θα του επιτρέψουν να σχεδιάσει το δίκτυο ώστε τελικά να παράσχει υπηρεσίες με επιτυχία. Οι βασικές φάσεις είναι τέσσερεις:

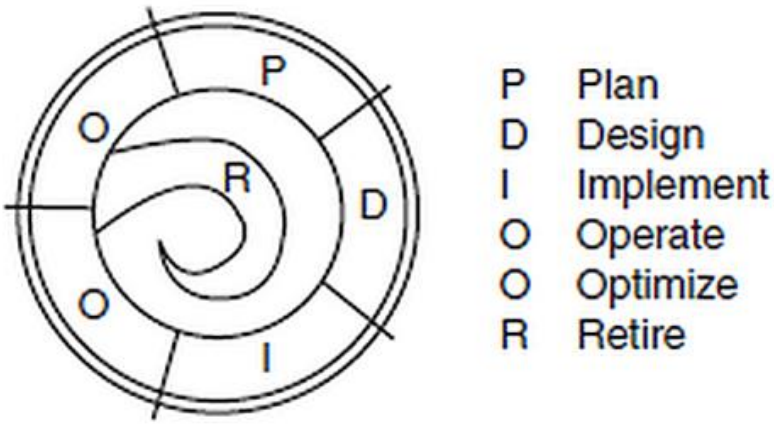
- Ανάλυση απαιτήσεων
- Ανάπτυξη του λογικού σχεδίου
- Ανάπτυξη του φυσικού σχεδίου
- Έλεγχος, βελτιστοποίηση και τεκμηρίωση του σχεδίου

Στην περίπτωση που το δίκτυο είναι πολύ μεγάλο, είναι σημαντικό να σχεδιασθεί αρθρωτά ώστε και το σχέδιο και η τελική του ανάπτυξη να είναι διαχειρίσιμα. Κάθε άρθρωμα (module) σχεδιάζεται χωριστά από τα υπόλοιπα.

Επίσης διακρίνουμε ότι υπάρχει *λογικό* και *φυσικό* σχέδιο. Το πρώτο έχει ως βάση ένα λογικό μοντέλο, το οποίο περιέχει τα βασικά δομικά στοιχεία, ταξινομημένα κατά την λειτουργία που επιτελούν. Άρα αφορά σχεδιασμό σε υψηλότερο επίπεδο (π.χ., έως το επίπεδο μεταφοράς του μοντέλου αναφοράς ISO OSI). Αντιθέτως, στο φυσικό σχέδιο αναπαρίστανται όλες οι φυσικές συσκευές και συγκεκριμένες τεχνολογίες που πρόκειται να χρησιμοποιηθούν.

Η Cisco από την πλευρά της έχει υιοθετήσει το λεγόμενο Plan Design Implement Operate Optimize (PDIOO) που περιλαμβάνει έξι φάσεις για την διάρκεια ζωής ενός δικτύου σε έναν κύκλο, όπως φαίνονται στην Εικόνα 10.1 (Oppenheimer, 2011):

- **Plan**: Εδώ προσδιορίζονται οι απαιτήσεις του δικτύου, οι περιοχές όπου θα εγκατασταθεί και οι χρήστες που θα ζητάν συγκεκριμένες δικτυακές υπηρεσίες
- **Design**: Εδώ ολοκληρώνεται το μεγαλύτερο μέρος του λογικού και του φυσικού σχεδίου, σύμφωνα με τις απαιτήσεις από την προηγούμενη φάση
- **Implement**: Εδώ αρχίζει η υλοποίηση του σχεδίου που προέκυψε από την προηγούμενη φάση, ενώ παράλληλα επαληθεύεται το σχέδιο
- **Operate**: Η λειτουργία του δικτύου αποτελεί το τελικό τεστ της αποδοτικότητας του σχεδίου. Επιτυγχάνεται με την παρακολούθησή του για ανίχνευση προβλημάτων απόδοσης και σφαλμάτων. Εάν προκύψουν, τροφοδοτούν την επόμενη φάση
- **Optimize**: Ουσιαστικά εδώ γίνεται προληπτική διαχείριση, αφού προσδιορίζονται και επιλύονται προβλήματα πριν προκληθούν διακοπές λειτουργίας. Εάν μάλιστα τα προβλήματα ή σφάλματα είναι πάρα πολλά, επιχειρείται επανασχεδιασμός του δικτύου. Το τελευταίο μπορεί να χρειασθεί και με την πάροδο του χρόνου, καθώς οι απαιτήσεις των χρηστών ή οι τεχνολογικές μεταβολές το επιβάλουν
- **Retire**: Εδώ έχουμε την απόσυρση ολόκληρου ή μέρους του δικτύου. Π.χ., παλαιότερα οι χρήστες μπορεί να συνδέονταν απομακρυσμένα μέσω απλής τηλεφωνικής κλήσεως (dial-in), κάτι που να μην θεωρείται πλέον απαραίτητο και άρα να καταργηθεί το τμήμα εκείνο του δικτύου που παρείχε την δυνατότητα αυτή



Εικόνα 10.1 *Κύκλος ζωής δικτύου κατά Cisco PDIOO.*

Κατά την πρώτη φάση είναι σημαντικό να υπάρξει επικοινωνία του σχεδιαστή με τον πελάτη ώστε να προσδιορισθούν οι βασικοί στόχοι από επιχειρηματικής πλευράς, καθώς και τα κριτήρια επιτυχίας, αλλά και οι συνέπειες αποτυχίας. Για παράδειγμα, θα είναι ορατές οι θετικές ή αρνητικές επιδόσεις του νέου δικτύου στην διοίκηση της επιχείρησης; Σε ποια έκταση κάποια αρνητική επίδοση ή αστοχία του δικτύου οδηγεί σε διακοπή της επιχειρηματικής δραστηριότητας;

Ιδιαίτερη προσοχή πρέπει να υπάρχει στο ότι πλέον τα τμήματα πληροφορικής σε μία εταιρεία είναι πιο προσανατολισμένα σε υπηρεσίες από ό,τι στο παρελθόν, ξοδεύοντας πιο πολύ χρόνο για ανάλυση και τεκμηρίωση των διεργασιών τους για την παροχή υπηρεσιών. Ο λόγος είναι ότι έτσι μειώνεται το κόστος παροχής υπηρεσιών στους τελικούς χρήστες, ενώ αποφεύγεται η σπατάλη σε τεχνολογίες που δεν παρέχουν αναγκαίες υπηρεσίες. Μάλιστα, στην Αγγλία έχει υπάρξει οργανωμένη προσπάθεια ορισμού πλαισίων και διεργασιών που βοηθούν έναν οργανισμό στην παροχή υπηρεσιών τεχνολογιών πληροφορικής (Information Technology – IT). Πιο συγκεκριμένα το United Kingdom Office of Government Commerce (OGC) έχει προχωρήσει στην έκδοση μίας σειράς πέντε σχετικών εγχειριδίων (Information Technology Infrastructure

Library – ITIL), με πιο πρόσφατη έκδοση εκείνη του 2011. Από το 2014, η σειρά ITIL ανήκει στην Axelos Ltd (Axelos, 2014), η οποία παρέχει και σχετικές μεθόδους εκπαίδευσης και πιστοποίησης.

Συνέπεια των παραπάνω είναι να καταγραφεί μία λίστα με τα διάφορα είδη των εφαρμογών και υπηρεσιών που χρησιμοποιούνται ή πρόκειται να χρησιμοποιηθούν, μαζί με τον βαθμό σπουδαιότητός τους. Για παράδειγμα, η υπηρεσία ηλεκτρονικού ταχυδρομείου μπορεί να θεωρηθεί ότι ανήκει στις σπουδαιότερες και συνεπώς ότι πρέπει να δοθεί ιδιαίτερο βάρος στην παροχή της, ακόμα και εάν υπάρξει μερική κατάρρευση του δικτύου. Φυσικά, θα πρέπει να τονισθεί στον πελάτη ότι κάθε υπηρεσία για την οποία επιθυμεί να παρέχεται απρόσκοπτα το κόστος θα είναι πιθανότατα πολύ μεγάλο.

Τέλος, εκτός από τα παραπάνω, σημαντικό βάρος πρέπει να δοθεί στην υποστήριξη χρηστών κινητών, στους περιορισμούς του προϋπολογισμού, αλλά και σε θέματα ασφάλειας και ανθεκτικότητας (π.χ., μέσω της εγγύησης για παροχή δικτυακών υπηρεσιών στο 99,99% του χρόνου). Επίσης, το συνηθέστερο είναι πλέον να σχεδιάζεται αναβάθμιση ενός υπάρχοντος δικτύου, παρά η δημιουργία ενός εντελώς νέου. Αυτό σημαίνει ότι πρέπει και να καταγραφεί το σύνολο των στοιχείων και υπηρεσιών που παρέχει το υπάρχον δίκτυο, αλλά και η αναβάθμιση να γίνει με την λιγότερη δυνατή (ή και καθόλου) διακοπή παροχής υπηρεσιών από το παλιό. Στην συνέχεια εξετάζουμε κάποια από τα θέματα αυτά πιο λεπτομερειακά.

10.2. Ανάλυση Τεχνικών Στόχων

Οι τεχνικοί στόχοι ενός νέου ή αναβάθμισης παλιού δικτύου είναι απαραίτητο να αναλυθούν, ώστε να βοηθήσουν στην πρόταση συγκεκριμένων δικτυακών τεχνολογιών με επιδόσεις που να ανταποκρίνονται στις προσδοκίες του πελάτη. Επειδή όμως η ανάλυση αυτή πρέπει να είναι όσο το δυνατόν σαφέστερη, συνήθως υιοθετούνται τα παρακάτω κριτήρια:

- **Κλιμάκωση:** Έχει να κάνει με τον βαθμό αύξησης του δικτύου, κυρίως σε πλήθος τερματικών κόμβων (υπολογιστών). Εν τούτοις, μπορεί να περιλαμβάνει και διασύνδεση με εξωτερικά δίκτυα ή εφαρμογές, καθώς και προσθήκη νέων εξυπηρετών. Επειδή κάτι τέτοιο δεν μπορεί να προβλεφθεί γενικά, πρέπει να αποτυπώνεται η επιθυμία του πελάτη σε συγκεκριμένο χρονικό ορίζοντα (π.χ., 2-5 έτη). Επειδή υπάρχουν περιορισμοί στην κλιμάκωση που οφείλονται στην φύση των διαφόρων τεχνολογιών δικτύωσης. Π.χ., δεν μπορεί κανείς να θεωρήσει ότι θα μπορεί να έχει κλιμάκωση για μεγάλο αριθμό χρηστών με την υιοθέτηση μεταγωγέων (switches) μόνον σε όλο το δίκτυο.
- **Διαθεσιμότητα:** Έχει να κάνει με το χρονικό διάστημα που το δίκτυο είναι διαθέσιμο στους χρήστες. Μπορεί να εκφράζεται με πολλούς τρόπους, συνηθέστερος εκ των οποίων είναι η χρήση ποσοστού ως προς κάποιο συγκεκριμένο χρονικό διάστημα. Π.χ., 98% σε μία εβδομάδα. Το ζήτημα της ανάνηψης από καταστροφή είναι διαφορετικό από την διαθεσιμότητα, αλλά σχετίζεται με αυτήν. Είναι δε σαφές ότι πρέπει να υπάρχει σχετικό σχέδιο, που να περιλαμβάνει ακόμα και σχετικές ασκήσεις για να διαπιστωθεί η αποτελεσματικότητά του και να υπάρχει η σχετική εκπαίδευση του προσωπικού.
- **Απόδοση Δικτύου:** Όπως είδαμε σε προηγούμενο κεφάλαιο, υπάρχουν διάφορες ποσοτικές μετρικές προκειμένου να καθορισθεί η απόδοση ενός δικτύου, και στην συνέχεια να αποτιμηθεί. Μερικές από αυτές είναι:
    - **Χωρητικότητα (capacity)** – η μέγιστη φυσική ικανότητα μεταφοράς πληροφορίας ενός δικτύου (συνήθως μετρούμενη σε bps)
    - **Ποσοστό χρήσης (utilization)**
    - **Ποσοστό βέλτιστης χρήσης (optimum utilization)** – ουσιαστικά το προηγούμενο μόλις πριν σημειωθεί κορεσμός
    - **Ρυθμαπόδοση (throughput)** – στο επίπεδο εφαρμογών συχνά καλείται *goodput*.
    - **Καθυστέρηση (delay)**
    - **Διακύμανση καθυστέρησης (delay variation)**
    - **Χρόνος απόκρισης (request time)** δικτυακής υπηρεσίας από την στιγμή που ζητήθηκε

- **Ασφάλεια:** Προφανώς από τους πλέον σημαντικούς τεχνικούς στόχους. Έχει να κάνει με την αντιμετώπιση απειλών με προέλευση όχι μόνον έξω, αλλά και μέσα από το δίκτυο. Δεν υπάρχει απόλυτη ασφάλεια και το κόστος για την διασφάλισή της μπορεί να είναι υπερβολικό. Συνήθως λοιπόν πρέπει να γίνουν κάποιοι συμβιβασμοί, ξεκινώντας από το στάδιο του σχεδιασμού.

  Το πρώτο βήμα περιλαμβάνει τον προσδιορισμό των δικτυακών στοιχείων που θεωρούνται σημαντικά, χρησιμοποιώντας μάλιστα συχνά και διαβάθμιση της σπουδαιότητάς τους. Εδώ δικτυακά στοιχεία θεωρούνται το υλικό, λογισμικό, αλλά και οι σχετικές εφαρμογές, τα διακινούμενα δεδομένα και η φήμη της εταιρείας. Για παράδειγμα, εάν κάποιος αλλάξει τις ιστοσελίδες της εταιρείας που είναι διαθέσιμες στο κοινό, ζημιώνει την εικόνα αξιοπιστίας που είχε η εταιρεία ως εκείνη την στιγμή.

  Το δεύτερο βήμα περιλαμβάνει την ανάλυση των πιθανών κινδύνων και των επιπτώσεών τους. Αυτή η διεργασία είναι ουσιαστικά διαρκής λόγω των ραγδαίων τεχνολογικών εξελίξεων και μεθόδων στον χώρο της Πληροφορικής. Η εκτίμηση του κάθε κινδύνου έχει να κάνει ακόμα και με το κόστος που θα είχε για την επιχείρηση εάν δεν ληφθεί κανένα σχετικό μέτρο. Αυτό θα πρέπει να ξεκαθαριστεί με τον πελάτη, ο οποίος ενδεχομένως να θεωρήσει ότι το κόστος προστασίας από έναν τέτοιο κίνδυνο είναι πολύ μεγαλύτερο από την αγνόησή του. Π.χ., εάν τα περισσότερα δεδομένα που μεταφέρουν φωνή υποκλαπούν, υπάρχει σημαντικό κόστος για την επιχείρηση και πόσο; Ο πελάτης μπορεί να θεωρήσει ότι δεν υπάρχει αξιόλογο κόστος, αφού κανένα σημαντικό επιχειρηματικό μυστικό δεν διακινείται με αυτόν τον τρόπο.
- **Διαχειρισιμότητα:** Ανάλογα με τις επιθυμίες του πελάτη, προκύπτουν και διαφορετικοί στόχοι ως προς την διαχειρισιμότητα του δικτύου. Είδαμε ήδη σε προηγούμενο κεφάλαιο τον όρο FCAPS (Fault, Configuration, Accounting, Performance, Security) του ISO για τις βασικές λειτουργίες που συνθέτουν την διαχειρισιμότητα ενός δικτύου.
- **Ευχρηστία:** Αυτή αναφέρεται στο πόσο εύχρηστο είναι το δίκτυο στους χρήστες, ενώ η διαχειρισιμότητα στο πόσο εύκολη είναι η διαχείρισή του για τους διαχειριστές. Για παράδειγμα, η τοποθέτηση κατάλληλων ιστοσελίδων, η εγκατάσταση υπηρεσίας DHCP για αποφυγή ανάγκης ρυθμίσεων στους υπολογιστές των χρηστών, κινητότητα μέσω υποστήριξης κινητών δικτύων, VPN, κλπ.
- **Προσαρμοστικότητα:** Πρόβλεψη για όσο το δυνατόν ευκολότερη υιοθέτηση νέων δικτυακών τεχνολογιών, προσαρμογή σε μεταβαλλόμενες μορφές δικτυακής κίνησης, απαιτήσεων QoS, κλπ.
- **Δυνατότητα κάλυψης κόστους:** Συχνά συναντάμε αυτόν τον όρο ως *cost-effectiveness*. Αν και έχει να κάνει κυρίως με τους επιχειρηματικούς στόχους, έχει και τεχνική χροιά. Για παράδειγμα, προκειμένου να μειωθεί το κόστος σε σχέση με τις παρεχόμενες υπηρεσίες:

  - Χρήση πρωτοκόλλου δρομολόγησης ώστε να ελαχιστοποιείται η κυκλοφορία WAN.
  - Χρήση ελαχίστων ή και μίας μόνον φυσικής μισθωμένης γραμμής ώστε να μεταφέρει και φωνή και δεδομένα.
  - Χρήση αυτόματης συμπίεσης για περιορισμό του όγκου της δικτυακής κυκλοφορίας.

Σε όλες τις περιπτώσεις όμως είναι χρήσιμο να δημιουργηθεί ένας κατάλογος με όλους τους παραπάνω τεχνικούς στόχους, καθώς και το σχετικό ποσοστό του κόστους για τον κάθε έναν από αυτούς. Έτσι θα είναι δυνατόν να καταδειχθεί στον πελάτη όχι μόνον τι μπορεί να επιτευχθεί τεχνικά, αλλά και πόσο στοιχίζει ως προς τον συνολικό προϋπολογισμό. Αυξάνοντας τις απαιτήσεις σε κάποιον στόχο είναι αναγκασμένος να αποδεχθεί μείωση των απαιτήσεων σε άλλους, ώστε το συνολικό κόστος να παραμείνει ίδιο.

10.3. Ανάλυση Υπάρχοντος Δικτύου

Επειδή συχνά ήδη υπάρχει εγκατεστημένο κάποιο δίκτυο, για το οποίο ουσιαστικά μας ζητείται να σχεδιάσουμε κάποια επέκταση ή αναβάθμιση, είναι απαραίτητο να συμπεριλάβουμε στα προηγούμενα και το ήδη υπάρχον δίκτυο.

Ουσιαστικά πρέπει να γίνει μία καταγραφή του υπάρχοντος δικτύου ή έλεγχος προηγούμενης καταγραφής, ώστε να επιβεβαιώσουμε, διορθώσουμε ή και να συμπληρώσουμε την καταγραφή αυτήν λαμβάνοντας υπ' όψιν τους στόχους και παραμέτρους που έχουμε θέσει.

Σε μεγάλο βαθμό αυτή η διαδικασία έχει ήδη περιγραφεί στο προηγούμενο κεφάλαιο, αφού τουλάχιστον κατά την αρχική αξιολόγηση ενός δικτύου, περιλαμβάνεται η τεκμηρίωση ως μία από τις βασικές ενέργειες. Επειδή όμως συνήθως γίνονται τροποποιήσεις ή επεκτάσεις σε ένα δίκτυο μεταξύ ριζικών αναδιαρθρώσεων, αλλά και επειδή είναι αναγκαίο να γίνεται αξιολόγηση ενός δικτύου σε τακτά χρονικά διαστήματα για ευνόητους λόγους, υπάρχει ήδη αρκετή σχετική τεκμηρίωση που καλύπτει την υπάρχουσα κατάσταση και μπορεί να χρησιμοποιηθεί ως βάση για τον σχεδιασμό του νέου δικτύου.

Στα πλαίσια αυτά περιλαμβάνεται και η καταγραφή των ροών κυκλοφορίας (traffic flows), αρχικά των υπαρχόντων, και στην συνέχεια των εκτιμώμενων μελλοντικών. Το άθροισμα των δεδομένων που διακινούνται από όλους τους κόμβους σε ένα χρονικό διάστημα ονομάζεται *φόρτος κυκλοφορίας* (*traffic load*) ή *προσφερόμενο φορτίο* (*offered load*). Στόχος μας είναι η χωρητικότητα του δικτύου μας να είναι αρκετά μεγάλη ώστε να μπορεί να το διακινήσει. Για να το πετύχουμε όμως, πρέπει πρώτα να εκτιμήσουμε σωστά αυτόν τον φόρτο.

Ένας γενικός, εμπειρικός οδηγός (Stallings, 2000) χρησιμοποιεί τις τιμές των παρακάτω παραμέτρων:

- Αριθμός απλών υπολογιστών.
- Μέσος χρόνος που ο υπολογιστής παραμένει αδρανής, μεταξύ αποστολής πλαισίων.
- Ο χρόνος που απαιτείται για την μετάδοση ενός μηνύματος από την στιγμή που θα επιτραπεί στον υπολογιστή να χρησιμοποιήσει το μέσο μετάδοσης (π.χ., Ethernet, WiFi).

Για παράδειγμα, εάν ένα δίκτυο προτείνεται να έχει χωρητικότητα 10 Mbps, έχοντας 1.000 υπολογιστές να μεταδίδουν πλαίσια των 8.000 bit κάθε δευτερόλεπτο, σημαίνει ότι το προσφερόμενο φορτίο είναι περίπου 16 Mbps. Συνεπώς η προτεινόμενη χωρητικότητα δεν επαρκεί.

Φυσικά, η παραπάνω προσέγγιση μπορεί να απέχει πολύ από την πραγματικότητα, εφόσον, για παράδειγμα, οι περισσότεροι υπολογιστές δεν επικοινωνούν με οποιονδήποτε άλλον τον περισσότερο χρόνο, αλλά μόνον με υπολογιστές που βρίσκονται στο ίδιο υποδίκτυο με αυτούς. Για αυτό άλλωστε γίνεται η χαρτογράφηση, όχι μόνον της τρέχουσας καταστάσεως, αλλά και της μελλοντικής με τις αντίστοιχες ροές κυκλοφορίας, ώστε να διαπιστωθεί με αρκετή ακρίβεια η πραγματικότητα.

Σε μεγάλα δίκτυα, με πολλούς χρήστες, είναι επίσης συχνά σκόπιμο να προσπαθούμε να υπολογίσουμε τον φόρτο κυκλοφορίας που θα επιφέρει μία δικτυακή εφαρμογή ή υπηρεσία. Εδώ χρειάζεται να εκτιμήσουμε, εκτός από τα παραπάνω, τον αριθμό των χρηστών που θα την χρησιμοποιούν ταυτόχρονα, αλλά και το αντίστοιχο ή αντίστοιχα πρωτόκολλα, ώστε να προσθέσουμε και τα byte ελέγχου (κεφαλίδες) που χρησιμοποιεί το κάθε ένα από αυτά. Π.χ., έχουμε 38 τέτοια byte εάν χρησιμοποιούμε Ethernet II, αφού αυτό περιλαμβάνει 8 byte για το προοίμιο (preamble), 14 για την κυρίως κεφαλίδα (MAC header), 4 για το CRC, και το ισοδύναμο των 12 byte για το διάστημα μεταξύ δύο διαδοχικών πλαισίων (Inter-Frame Gap). Εάν χρησιμοποιηθεί το IEEE 802.3 μαζί με το 802.2 (παραλλαγή του IEEE για το Ethernet), τότε τα αντίστοιχα byte γίνονται 46, επειδή επιπρόσθετα έχουμε το πεδίο LLC, 3 byte, και το SNAP, 5 byte (IEEE, 2012).

Η μελέτη για τον φόρτο λόγω των πρωτοκόλλων δρομολογήσεως δεν είναι τόσο σημαντική όταν έχουμε να κάνουμε με μικρά, σχεδόν τοπικά δίκτυα. Αντιθέτως, μπορεί να είναι σημαντική (λόγω φόρτου) για μεγάλα και πολύπλοκα δίκτυα τύπου WAN.

Η χρήση περισσοτέρων δρομολογητών μπορεί να μειώσει τον φόρτο κυκλοφορίας στο δίκτυο κορμού, περιορίζοντάς την κυρίως στα επί μέρους δίκτυα. Υπάρχει όμως μεγαλύτερο κόστος για την προμήθειά τους, διαχείριση για την σωστή τους ρύθμιση, καθώς και μεγαλύτερη καθυστέρηση στην διακίνηση πακέτων σε σχέση με έναν μεταγωγέα (switch). Εν τούτοις είναι χρήσιμοι και για μείωση προβλημάτων από εκπομπή και πολυεκπομπή, και σχετικών πρωτοκόλλων (π.χ., ARP).

Τέλος, χρειάζεται να γίνουν και έλεγχοι ως προς αρχιτεκτονικούς και άλλους περιβαλλοντικούς περιορισμούς, καθώς και έρευνα ως προς τους διαθέσιμους χώρους σε καμπίνες, την μέγιστη χωρητικότητα διακίνησης πληροφοριών και από τα καλώδια δικτύου, αλλά και τα ασύρματα δίκτυα για τυχόν προβλήματα.

10.4. Λογικός Σχεδιασμός Δικτύου

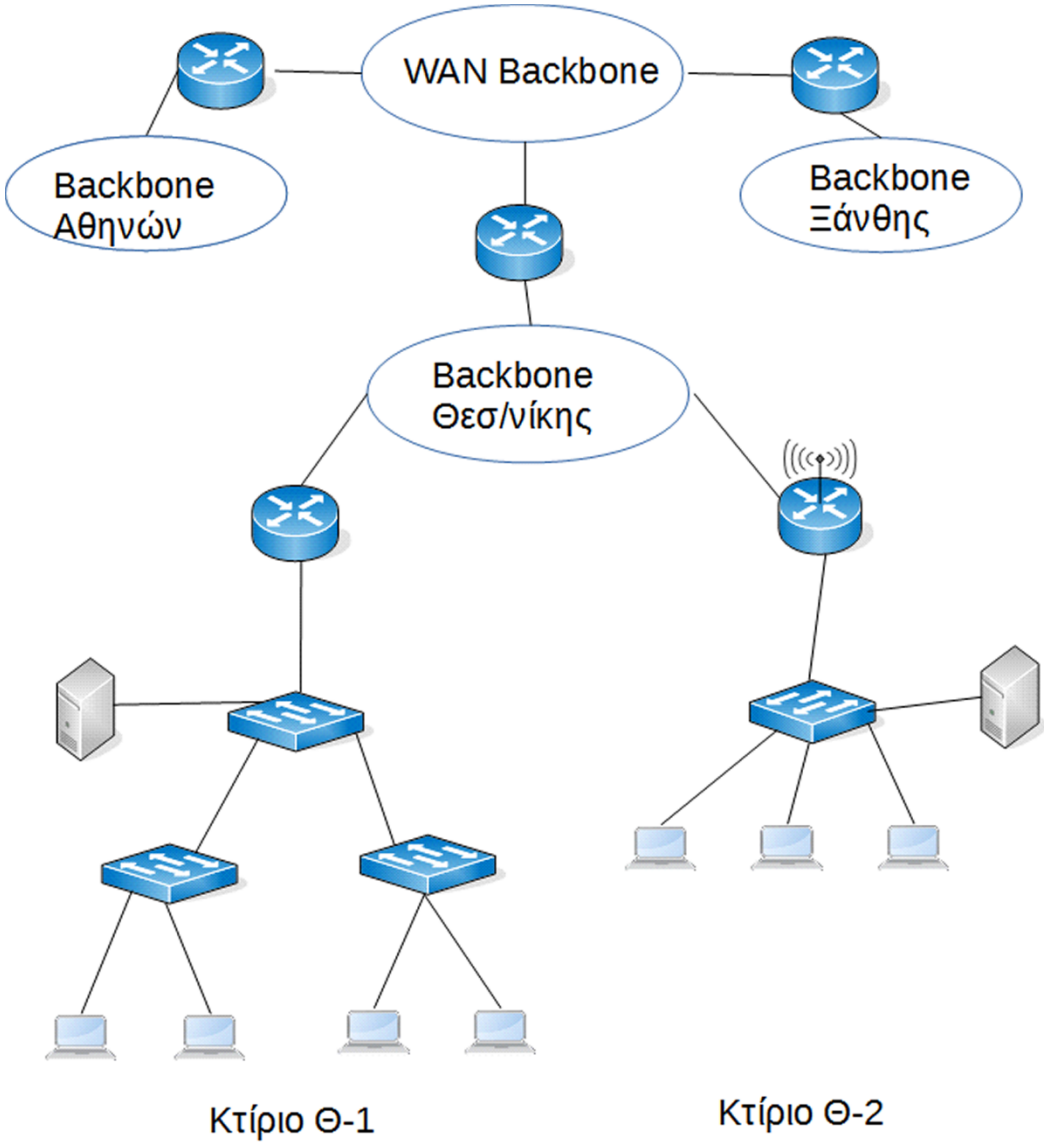
Ο λογικός σχεδιασμός ενός δικτύου υπολογιστών προηγείται πάντοτε του φυσικού σχεδιασμού. Συνοπτικά περιλαμβάνει τα παρακάτω, τα οποία και θα εξετάσουμε στην συνέχεια:

- Σχεδιασμό της τοπολογίας του δικτύου.
- Μοντέλα για διευθυνσιοδότηση.
- Επιλογή καταλλήλων πρωτοκόλλων για δρομολόγηση.
- Βασικούς κανόνες και διαδικασίες ασφάλειας.
- Βασικούς κανόνες και διαδικασίες διαχείρισης του δικτύου.

Όπως γνωρίζουμε, η τοπολογία ενός δικτύου δεν είναι παρά ένας χάρτης, ο οποίος περιλαμβάνει τουλάχιστον τα διάφορα τμήματα, στην πράξη υποδίκτυα, καθώς και τους κόμβους-σημεία διασύνδεσης των τμημάτων (συνήθως δρομολογητές). Στην περίπτωσή μας περιλαμβάνει και τις ομάδες χρηστών.

10.4.1. Η Ιεραρχική Προσέγγιση

Η εμπειρία έχει διδάξει ότι ο πιο ασφαλής τρόπος για να σχεδιάσουμε την τοπολογία είναι να ακολουθήσουμε μία διαδικασία επιπέδων από ‘επάνω-προς-τα-κάτω’, όπου κάθε επίπεδο περιλαμβάνει τα τμήματα ή στοιχεία του δικτύου που έχουν τον ίδιο τύπο λειτουργίας, ενώ στο ‘επάνω’ θεωρείται ότι πρέπει να τοποθετείται η ‘ραχοκοκαλιά’ του δικτύου, που διασυνδέει όλα τα επί μέρους τμήματα. Ένα τέτοιο παράδειγμα βλέπουμε στην Εικόνα 10.2.



Εικόνα 10.2 *Παράδειγμα σχεδιασμού τοπολογίας.*

Εδώ βλέπουμε ότι το δίκτυό μας έχει ένα τμήμα κορμού WAN (backbone), το οποίο διασυνδέει τα επί μέρους δίκτυα στις τρεις πόλεις όπου βρίσκονται τα καταστήματα της εταιρείας (Αθήνα, Θεσσαλονίκη, Ξάνθη), μέσω τριών δρομολογητών. Επίσης, εμφανίζεται λεπτομερέστερα το δίκτυο για το κατάστημα της Θεσσαλονίκης, για το οποίο κληθήκαμε να σχεδιάσουμε το δίκτυο. Βλέπουμε στην κορυφή του το τμήμα κορμού της Θεσσαλονίκης και τους δύο δρομολογητές (ο δεξιός είναι ασύρματος) μέσω των οποίων συνδέονται τα επί μέρους δίκτυα των δύο κτιρίων που υπάρχουν εκεί. Σε κάθε κτίριο υπάρχει ένας βασικός μεταγωγέας (switch) στον οποίον συνδέεται ένας εξυπηρέτης και οι σταθμοί εργασίας των χρηστών. Ειδικά για το κτίριο Θ-1 οι χρήστες είναι ίσως τόσοι πολλοί ή υπάρχουν κάποιες ιδιαίτερες συνθήκες (π.χ., διαφορετικοί όροφοι), που να δικαιολογούν την διαίρεσή του σε επί μέρους δίκτυα και αντίστοιχους μεταγωγείς.

Η γενική προσέγγιση είναι ότι ξεκινάμε με το *επίπεδο του πυρήνα* του δικτύου στην κορυφή (*core layer*), προχωρούμε με το επίπεδο στο οποίο γίνεται η *διανομή* της κυκλοφορίας σε επί μέρους δίκτυα (*distribution layer*), και ακολουθεί το *επίπεδο πρόσβασης* (*access layer*) μέσω του οποίου τα υποδίκτυα και οι λοιπές δικτυακές συσκευές διασυνδέονται μεταξύ τους.

Τα πλεονεκτήματα μίας τέτοιας ιεραρχικής και αρθρωτής προσέγγισης είναι σαφή και από άλλους τομείς. Τα βασικότερα έχουν να κάνουν με:

- Μείωση επιπτώσεων από πακέτα εκπομπής.

- Ευκολότερη εκτίμηση για τον όγκο και την διαδρομή για κάθε τύπου κυκλοφορίας.
- Καλύτερη επιλογή συσκευών διασύνδεσης δικτύων.
- Μείωση του συνολικού κόστους.
- Ευκολότερη κατανόηση του κάθε επί μέρους δικτύου και σχεδιασμός χωρητικότητός του.
- Ευκολότερος εντοπισμός σφαλμάτων και άλλων προβλημάτων.
- Ευκολότερη μεταβολή στον σχεδιασμό και ανάπτυξη του δικτύου κατά την διάρκεια ζωής του, αφού η όποια μεταβολή έχει επιπτώσεις που είναι ευκολότερο να κατανοηθούν.
- Ευκολότερη κλιμάκωση.

Γενικά, προτιμούμε μία μονο-επίπεδη τοπολογία όταν το δίκτυο είναι μικρό, αλλά πολύ-επίπεδη σε οποιαδήποτε άλλη περίπτωση. Στην πρώτη περίπτωση, το δίκτυο κορμού είναι ουσιαστικά ένας βρόγχος που διασυνδέει όλους τους δρομολογητές που διακινούν την δικτυακή κυκλοφορία από το επί μέρους δίκτυο προς δίκτυο κορμού και αντίστροφα, όπως φαίνεται στην Εικόνα 10.3.

Εικόνα 10.3 *Παράδειγμα δικτύου κορμού μονο-επίπεδης τοπολογίας.*

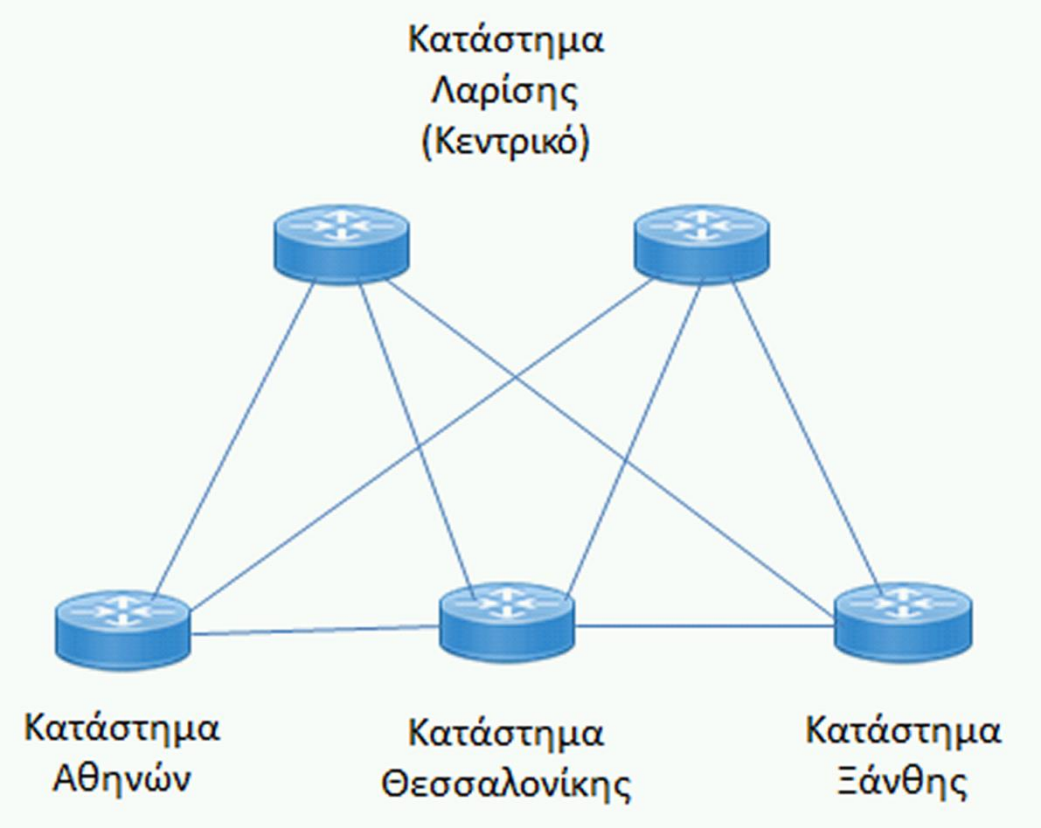
Ο λόγος που προτιμάται ένας βρόγχος είναι ότι το πλήθος αλμάτων (hop) που απαιτούνται μεταξύ των πλέον απομακρυσμένων κόμβων μειώνεται στο μισό. Η βασική εξαίρεση εμφανίζεται όταν το κόστος είναι υπερβολικά μεγάλο. Π.χ., στην Εικόνα 10.3, η ζεύξη των δρομολογητών 'Κατάστημα Αθηνών'-'Κατάστημα Ξάνθης' δεν θα υπήρχε.

Υπάρχει όμως και η περίπτωση της επιβολής πολύ-επίπεδης ιεραρχίας ακόμα και στο δίκτυο κορμού. Ένα τέτοιο παράδειγμα βλέπουμε στην Εικόνα 10.4, όπου επιπρόσθετα χρησιμοποιείται και πλεονασμός. Έτσι, το κεντρικό κατάστημα που αναμένεται να έχει μεγαλύτερη κυκλοφορία λόγω της σημασίας του, έχει δύο δρομολογητές αντί για έναν, προσφέροντας πλεονασμό που είναι χρήσιμος σε περίπτωση που ένας από τους δύο δρομολογητές καταρρεύσει.

Όπως γνωρίζουμε, ο μέγιστος πλεονασμός με N κόμβους προκύπτει όταν κάθε κόμβος συνδέεται απ' ευθείας με όλους τους άλλους. Το πλήθος των ζεύξεων όμως είναι N*(N-1)/2, που σημαίνει ότι αυξάνεται εκθετικά όσο αυξάνουμε το N. Το κόστος, επομένως, είναι απαγορευτικό. Για αυτό και προτιμάται συνήθως μία τοπολογία που είναι ιεραρχική και εμπεριέχει πλεονασμό ως έναν βαθμό (συνήθως μικρό).

Επιπλέον, επειδή η καθυστέρηση στην διακίνηση πακέτων είναι μεγαλύτερη στο δίκτυο κορμού (αφού συνήθως αντιστοιχεί σε ένα WAN), ο βασικός στόχος μας είναι η γρήγορη διακίνηση των πακέτων. Συνεπώς, προσπαθούμε να αποφύγουμε χρονοβόρες ενέργειες (εκτός εάν είναι άκρως απαραίτητες), όπως φιλτράρισμα πακέτων, κλπ., ενώ ταυτόχρονα επιδιώκουμε την όσο το δυνατόν ευκολότερη παρακολούθηση και διαχείρισή του, αφού χωρίς αυτό δεν υπάρχει επικοινωνία μεταξύ των επί μέρους δικτύων.

Ένα ακόμα πρόβλημα είναι και η διασύνδεση με δίκτυα άλλων εταιρειών ή και το Διαδίκτυο. Γενικά, είναι ευκολότερος ο σχεδιασμός και η διαχείριση τέτοιων περιπτώσεων, εφόσον η διασύνδεση λαμβάνει χώρα στο δίκτυο κορμού. Επίσης, έτσι διευκολύνεται και η υιοθέτηση πολιτικών ως προς την ασφάλεια, καθώς και ως προς την διακίνηση πακέτων που προέρχονται από άλλα δίκτυα.



Εικόνα 10.4 *Παράδειγμα δικτύου κορμού με ιεραρχική τοπολογία δύο επιπέδων και πλεονασμό.*

Σε όλες τις περιπτώσεις, ιδιαίτερη έμφαση πρέπει να δοθεί στην προσπάθεια απόκρυψης λεπτομερειών των δικτύων σε χαμηλότερο επίπεδο, από εκείνα σε υψηλότερο, όπως και το αντίστροφο. Κατ' αυτόν τον τρόπο η αρθρωτή μορφή του συνολικού δικτύου ενισχύεται, καθιστώντας τις τροποποιήσεις, διαχείριση και διακίνηση δεδομένων ευχερέστερη και πιο αποδοτική.

10.4.2. Cisco SAFE

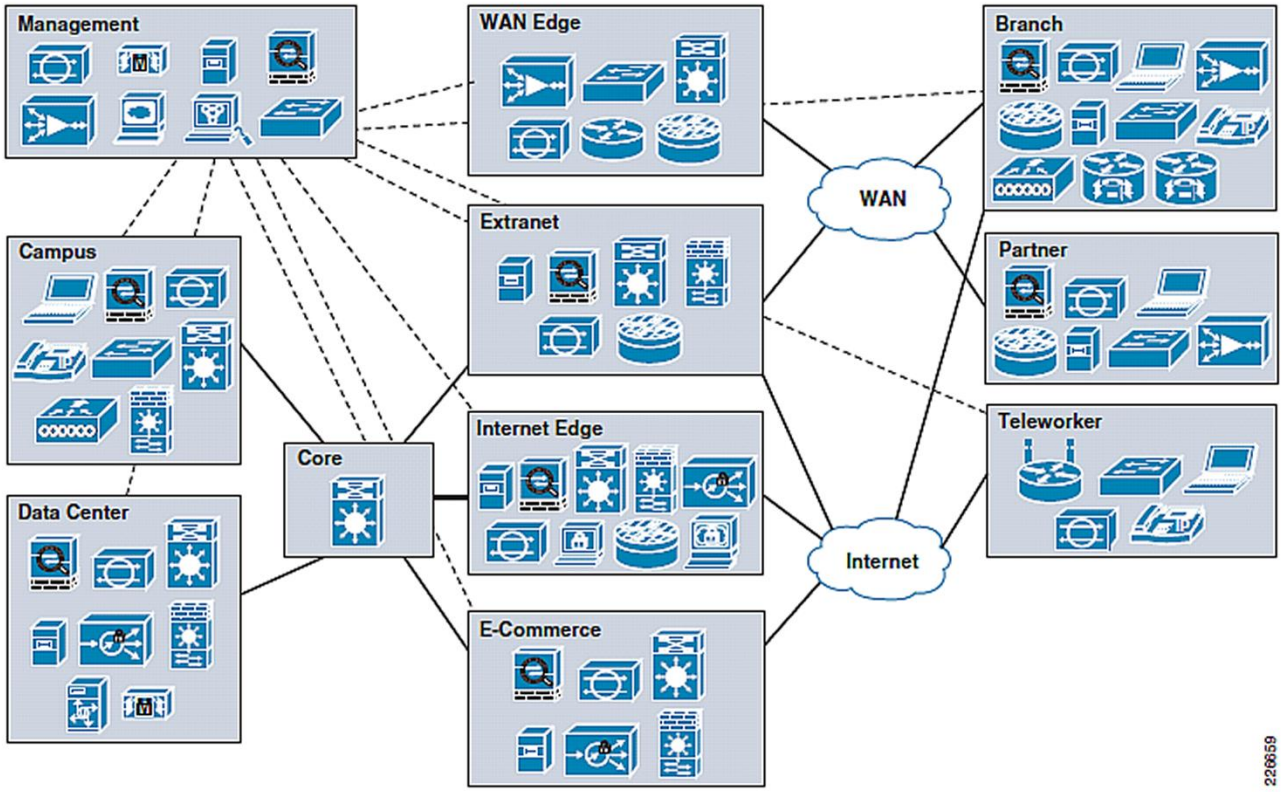
Δεδομένου ότι το πρόβλημα του σχεδιασμού ενός μεγάλου δικτύου υπολογιστών μπορεί να είναι εξαιρετικά πολύπλοκο, η Cisco επινόησε μία αρχιτεκτονική αναφοράς για τους σχεδιαστές, προκειμένου να βοηθήσει στην απλοποίηση του προβλήματος, διαθέτοντας τον σχετικό οδικό χάρτη στον ιστότοπό της (Chung et al., 2010). Αυτή η αρχιτεκτονική αναφοράς φέρει το όνομα SAFE, δεδομένου ότι η ασφάλεια έχει κρίσιμο ρόλο.

Η αρχιτεκτονική SAFE προσεγγίζει το πρόβλημα του σχεδιασμού ενός δικτύου με την ασφάλεια να προβλέπεται σε βάθος, μέσω πολλαπλών επιπέδων προστασίας, τα οποία τοποθετούνται στρατηγικά σε ολόκληρο το δίκτυο. Όλα τα επίπεδα αυτά προβλέπονται βάσει ενιαίας στρατηγικής για την προστασία του δικτύου ως σύνολο, αλλά και ως προς τα επί μέρους στοιχεία του. Η αρχιτεκτονική SAFE αποτελείται από τα παρακάτω κύρια αρθρώματα (modules), όπως φαίνονται και στην Εικόνα 10.5 (Σχήμα 1.3 στον σχετικό οδηγό της Cisco):

- **Core:** Ο πυρήνας του δικτύου. Διασυνδέει όλα τα άλλα αρθρώματα (modules). Παρέχει αξιόπιστη μεταφορά στα επίπεδα 2 και 3 του ISO OSI με υψηλή ταχύτητα. Συνήθως υλοποιείται με μεταγωγείς σε πλεονασμό.
- **Data center:** Αποτελείται από εξυπηρέτες, εφαρμογές και αποθηκευτικές συσκευές. Διασυνδέει τις συσκευές που το συνθέτουν μεταξύ τους, με δρομολογητές, μεταγωγείς, εξισορροποιητές φόρτου, συσκευές διανομής περιεχομένου, καθώς και συσκευές επιτάχυνσης εφαρμογών. Το κέντρο δεδομένων *δεν* είναι άμεσα προσπελάσιμο μέσω του Διαδικτύου.

- **Campus:** Το δίκτυο αυτό παρέχει πρόσβαση σε όλους τους χρήστες και συσκευές μίας γεωγραφικής τοποθεσίας. Μπορεί να περιλαμβάνει πολλαπλά κτίρια ή ορόφους. Παρέχει τοπικές υπηρεσίες δεδομένων, φωνής και βίντεο. Επίσης επιτρέπει την ασφαλή προσπέλαση του κέντρου δεδομένων για τους χρήστες του, καθώς και του Διαδικτύου.
- **Management:** Το δίκτυο διαχείρισης παρέχει υπηρεσίες παρακολούθησης, ανάλυσης, ταυτοποίησης και καταγραφής. Εδώ υπάρχουν σταθμοί διαχείρισης που υποστηρίζουν όλα τα σχετικά πρωτόκολλα.
- **WAN edge:** Το άκρο του WAN είναι εκείνο στο οποίο συγκεντρώνονται οι ζεύξεις του WAN, που συνδέουν γεωγραφικά απομακρυσμένα υποκαταστήματα της εταιρείας σε μία κεντρική τοποθεσία ή περιφερειακό σημείο συγκέντρωσης. Μπορεί να ανήκει στην εταιρεία, αλλά το πιο συνηθισμένο είναι ότι ανήκει σε κάποιον ISP.
- **Internet edge:** Το άκρο του Διαδικτύου είναι εκείνο που παρέχει συνδεσιμότητα του δικτύου της εταιρείας με το Διαδίκτυο. Ουσιαστικά ενεργεί ως μία πύλη της εταιρείας προς τον έξω κόσμο. Εκεί υπάρχουν κατάλληλες υποδομές, αλλά και υπηρεσίες, όπως VPN για απομακρυσμένη πρόσβαση, η πρόσβαση της εταιρείας από το Διαδίκτυο, καθώς και μία DMZ (DeMilitarized Zone). Όπως θυμόμαστε, στόχος της τελευταίας είναι να μην εκτίθεται το δίκτυο της εταιρείας απ' ευθείας στο Διαδίκτυο (για το οποίο δεν υπάρχει εμπιστοσύνη), αλλά μέσω αυτής της περιοχής, πίσω από την οποίαν πάντα προστίθεται ένα ακόμα επίπεδο ασφαλείας, ενώ οι υπολογιστές μέσα σε αυτήν έχουν περιορισμένη πρόσβαση στο υπόλοιπο δίκτυο της εταιρείας.
- **Branches:** Τα υποκαταστήματα παρέχουν συνδεσιμότητα σε χρήστες και συσκευές σε απομακρυσμένες γεωγραφικά τοποθεσίες. Ένα τέτοιο δίκτυο περιλαμβάνει τουλάχιστον ένα LAN και συνδέεται με τα κεντρικά μέσω ενός ιδιωτικού WAN (μισθωμένη γραμμή) ή μέσω του Διαδικτύου με την χρήση VPN, για λόγους ασφαλείας. Παρέχονται υπηρεσίες τοπικών δεδομένων, φωνής και βίντεο.
- **Extranet:** Αυτό επιτρέπει σε επιλεγμένες επιχειρήσεις, πελάτες και προμηθευτές να προσπελαύνουν ένα μέρος του δικτύου με την χρήση πρωτοκόλλων που παρέχουν ασφάλεια. Τυπικά παρέχονται υπηρεσίες VPN με απομακρυσμένη πρόσβαση, ανίχνευση και μετριασμός απειλών, οργανωμένος τερματισμός λειτουργίας για εξυπηρέτες και δικτυακές συσκευές, καθώς και πλεονασμός της αντίστοιχης τοπολογίας.
- **Partner site:** Οι δικτυακοί τόποι ή ιστότοποι συνεργατών δεν είναι παρά δίκτυα που ανήκουν σε συνεργάτες της εταιρείας, πελάτες και προμηθευτές. Έχουν πρόσβαση σε υπηρεσίες στο extranet μέσω ασφαλούς συνδέσεως, είτε μέσω WAN, είτε μέσω του Διαδικτύου.
- **E-Commerce:** Αυτό περιλαμβάνει εξυπηρέτες, εφαρμογές και δεδομένα που χρησιμοποιούνται στις αγοραπωλησίες προϊόντων. Σε πολύ μεγάλες εταιρείες περιλαμβάνονται φάρμες από εξυπηρέτες με φιλτράρισμα της κυκλοφορίας, εξισορρόπηση του φόρτου τους, καθώς και αυστηρές διαδικασίες ασφάλειας.
- **Teleworker:** Αυτό αντιστοιχεί σε ένα γραφείο υπαλλήλου της εταιρείας, ο οποίος εργάζεται εξ αποστάσεως. Οι σχετικές υπηρεσίες περιλαμβάνουν VPN εξ αποστάσεως, ασφάλεια για τον υπολογιστή εργασίας του υπαλλήλου, ασφαλή ασύρματη δικτύωση, καθώς και τηλεφωνία και βίντεο επάνω από IP.
- **Cisco SensorBase:** Αυτό αποτελείται από εξυπηρέτες συλλογής απειλών. Αυτοί λαμβάνουν ενημερώσεις από αναπτυχθέντες αισθητήρες απειλών, όπως για botnet, darknet, κακόβουλο λογισμικό (malware), κλπ. Στους αισθητήρες περιλαμβάνονται και τα συστήματα αποτροπής διεισδύσεων, εξυπηρέτες e-mail και οντότητες ασφάλειας ιστού.

Ένας άλλος χρήσιμος οδηγός για τον σχεδιασμό δικτύου σε μέγεθος μίας πανεπιστημιούπολης (που πιθανόν αποτελείται από πολλαπλά κτίρια σε μικρή απόσταση το ένα από το άλλο), είναι φυσικά να ακολουθήσουμε τον αλγόριθμο του STP (Spanning Tree Protocol), προκειμένου να σχηματισθεί η αρχική τοπολογία. Έτσι σχηματίζεται ως αφετηρία σχεδιασμού ένα δένδρο. Κατόπιν, μπορούμε να προσθέσουμε επιλεκτικά επιπρόσθετες ζεύξεις ή και κόμβους, προκειμένου να εισάγουμε πλεονασμό στην τελική τοπολογία.



Εικόνα 10.5 *Επισκόπηση υψηλού επιπέδου της αρχιτεκτονικής αναφοράς SAFE της Cisco.*

Επειδή τα διάφορα υποδίκτυα που απαρτίζουν το δίκτυο σε αυτήν την περίπτωση είναι σχετικά μικρά, η τάση είναι να χρησιμοποιούνται λίγοι δρομολογητές και περισσότεροι μεταγωγείς (switches). Προκειμένου να διευκολυνθεί η δρομολόγηση των πλαισίων, χρησιμοποιείται σε αυτούς το STP (Spanning Tree Protocol) και μάλιστα η νεότερη έκδοσή του (RSTP – Rapid STP) από το IEEE 802.1w (Cisco, 2006). Η γρήγορη σύγκλιση (convergence) είναι σημαντική, επειδή σε περιπτώσεις σφαλμάτων, ανακαλύπτονται αυτόματα οι νέες συντομότερες διαδρομές. Χαρακτηριστικά αναφέρεται ότι, ενώ με το παλαιότερο πρότυπο (802.1d) μπορεί να χρειαζόταν ακόμα και ένα λεπτό για να επιτευχθεί σύγκλιση σε κάποιο δίκτυο, ενώ με το νέο πρότυπο (802.1w) μερικές εκατοντάδες msec.

Ρυθμός Μετάδοσης Δεδομένων	**Κόστος Ζεύξης στο STP**		**Κόστος Ζεύξης στο RSTP**
	16-bit (Cisco)	**32-bit (IEEE 802.1d)**	**32-bit (IEEE 802.1w)**
100 kbps	-	200.000.000	200.000.000
1 Mbps	-	20.000.000	20.000.000
4 Mbps	-	5.000.000	5.000.000
10 Mbps	100	2.000.000	2.000.000
16 Mbps	-	1.250.000	1.250.000
100 Mbps	10	200.000	200.000
1 Gbps	4	20.000	20.000
10 Gbps	2	2.000	2.000
100 Gbps	-	200	200
1 Tbps	-	20	20
10 Tbps	-	2	2

Πίνακας 10.1 *Εξ ορισμού κόστη ζεύξεων των 16-bit (Cisco) και 32-bit (IEEE 802.1d) στα STP και RSTP (IEEE 802.1w).*

Η μεγάλη χρονική βελτίωση στην σύγκλιση οφείλεται στο ότι στην περίπτωση του STP κάθε θύρα που μαθαίνει διευθύνσεις MAC για να ενημερώσει κατάλληλα τον πίνακα διευθύνσεών της, περιμένει παθητικά για

σύγκλιση, πριν μεταπέσει σε κατάσταση προώθησης πλαισίων· αντίθετα, με το RSTP δεν χρειάζεται να περιμένει, ενώ υπάρχει και ένας μηχανισμός συγχρονισμού μεταξύ μεταγωγέων που υποστηρίζουν το RSTP.

Πιο συγκεκριμένα στο STP, ο μεταγωγέας με το μικρότερο ID εκλέγεται ως η ρίζα του δένδρου. Κάθε μεταγωγέας υπολογίζει το κόστος της διαδρομής (μεταξύ θυρών) ως την ρίζα. Προφανώς αυτό είναι μηδενικό για το μεταγωγέα-ρίζα. Το κόστος (για διακίνηση μέσω) μίας ζεύξης από μία θύρα, συνήθως ορίζεται από τον φυσικό ρυθμό μετάδοσης της ζεύξης (π.χ., οι τιμές στον Πίνακα 10.1), αλλά είναι δυνατόν ο διαχειριστής να ορίσει διαφορετικές τιμές για τα κόστη. Από όλες τις δυνατές διαδρομές, κάθε μεταγωγέας επιλέγει εκείνην που έχει το μικρότερο κόστος προς την ρίζα. Επίσης, για ένα ολόκληρο τμήμα δικτύου, οι αντίστοιχοι μεταγωγείς προσδιορίζουν την κατάλληλη θύρα ενός μεταγωγέα που οδηγεί προς την ρίζα του δένδρου (designated port), πάντα με το ελάχιστο κόστος για την διαδρομή.

Ως προς το θέμα της κλιμάκωσης, το STP και το RSTP λειτουργούν αρκετά καλά για μικρά δίκτυα. Η κατάσταση αλλάζει εάν είτε το αντίστοιχο δίκτυο είναι πολύ μεγάλο ή οι μεταγωγείς δεν έχουν αρκετή υπολογιστική ισχύ ή μνήμη, επειδή τότε οι πληροφορίες από τα αντίστοιχα πλαίσια, είτε δεν χωράν στην μνήμη του μεταγωγέα, είτε κάποια απορρίπτονται λόγω συμφόρησης. Δεν αναφέρουμε περισσότερες λεπτομέρειες, επειδή ξεφεύγουν από τον σκοπό του παρόντος.

Σήμερα, αυτά τα πρωτόκολλα είναι συνήθως ενεργοποιημένα εξ ορισμού, κυρίως επειδή ένας άπειρος τεχνικός μπορεί να συνδέσει έναν μεταγωγέα κατά λάθος, έτσι ώστε να δημιουργείται ένας φυσικός βρόγχος. Για λόγους κλιμάκωσης, αντιθέτως, προτιμάται η τοποθέτηση ενός ή περισσοτέρων δρομολογητών.

Τέλος, σήμερα προτιμάται η λύση των VLAN ώστε να χωρίζεται (λογικά) ένα φυσικό τμήμα δικτύου σε επί μέρους, οπότε ακόμα και πλαίσια εκπομπής (διεύθυνση προορισμού MAC `FF:FF:FF:FF:FF:FF` στο Ethernet) ή αγνώστου προορισμού, να μην προωθούνται παρά μόνον στα μέλη ενός VLAN από όπου ξεκίνησαν. Η επικοινωνία μεταξύ των VLAN απαιτεί την χρήση δρομολογητή. Σήμερα, είναι δυνατόν να έχουμε κάποιο VLAN που να επεκτείνεται σε περισσότερους από έναν φυσικούς μεταγωγείς, μέσω του προτύπου IEEE 802.1q (IEEE, 2014). Τα αντίστοιχα ισχύουν και στην περίπτωση ασυρμάτων δικτύων, εκτός από επιπρόσθετες λεπτομέρειες, όπως, για παράδειγμα, την τοποθέτηση ενός AP σε σημείο με την ελάχιστη παρεμβολή ή γενικά προβλήματα επικοινωνίας.

10.4.3. Διευθυνσιοδότηση

Και εδώ, όπως στα προηγούμενα, είναι σημαντικό το να χρησιμοποιηθεί μία δομημένη προσέγγιση για διευθυνσιοδότηση στο επίπεδο δικτύωσης. Ουσιαστικά αυτό αναφέρεται στις διευθύνσεις IP και τα διάφορα συμβολικά ονόματα που χρειάζεται να ανατεθούν.

Η εμπειρία αρκετών δεκαετιών έδειξε ότι, ακολουθώντας κάποιους κανόνες, διευκολύνεται η διαχείριση και η κλιμάκωση ενός δικτύου – αφού δεν πρέπει να λησμονούμε τις ενδεχόμενες ανάγκες για επέκταση ή τροποποίηση του δικτύου στην διάρκεια ζωής του. Συνοπτικά, οι κανόνες αυτοί είναι:

1. Σχεδιάζουμε ένα δομημένο μοντέλο διευθυνσιοδότησης, πριν την κανονική ανάθεση διευθύνσεων.
2. Αφήνουμε χώρο στο μοντέλο αυτό για επέκταση. Εάν δεν το κάνουμε, αργότερα θα χρειασθεί να αλλάξουμε τις διευθύνσεις σε πολλές συσκευές, κάτι το οποίο είναι και χρονοβόρο, αλλά και ενέχει κίνδυνο σφαλμάτων ή παραλείψεων.
3. Για να επιτύχουμε κλιμάκωση και διαθεσιμότητα, οι διευθύνσεις πρέπει να ανατίθενται σε ομάδες με ιεραρχικό τρόπο.
4. Η ανάθεση πρέπει να βασίζεται στο φυσικό δίκτυο και όχι στο εάν κάποιος κόμβος είναι μέλος μίας ομάδος. Είναι πιο πιθανό να μετακινηθεί, αλλάζοντας ομάδα κάποιο μέλος, παρά ένας φυσικός κόμβος.
5. Εάν υπάρχει αρκετά καλά εκπαιδευμένο προσωπικό, υπεύθυνο για τα επί μέρους δίκτυα, κλπ., είναι σκόπιμο να ανατίθεται σε αυτά τα άτομα η ανάθεση διευθύνσεων για τα τμήματα που υποστηρίζουν.
6. Χρήση δυναμικής διευθυνσιοδότησης για τα τερματικά συστήματα, παρά στατικής.
7. Για ακόμα μεγαλύτερη προσαρμοστικότητα σε νέες συνθήκες, αλλά και ασφάλεια, είναι σκόπιμο να χρησιμοποιούνται ιδιωτικές διευθύνσεις, μαζί με NAT.

Ξεκινώντας από τον πρώτο κανόνα, πρέπει να διευκρινίσουμε ότι ο όρος *δομημένο μοντέλο διευθυνσιοδότησης* σημαίνει ότι οι διευθύνσεις σε αυτό είναι ιεραρχικές και σχεδιασμένες. Αυτό σημαίνει ότι υπάρχει ιεραρχία σε αυτές, με συγκεκριμένο νόημα. Για παράδειγμα, οι διευθύνσεις IP αποτελούνται από δύο λογικά μέρη: το πρόθεμα (prefix) δικτύου και το επίθεμα (suffix) υπολογιστή. Εάν λοιπόν αναθέσουμε μία κατάλληλη διεύθυνση IP σε όλο το δίκτυο, και μετά προχωρήσουμε με υποδικτύωση (subnetting) για τα υποδίκτυα, έχουμε ακολουθήσει μία δομημένη προσέγγιση.

Εάν δεν ακολουθηθεί κάποιο δομημένο μοντέλο, μπορεί να εμφανισθούν προβλήματα όπως διπλότυπες (δύο ή περισσότερες ίδιες) διευθύνσεις για δίκτυα και υπολογιστές, ανεπαρκές πλήθος διευθύνσεων, διευθύνσεις που δεν μπορούν να χρησιμοποιηθούν και μένουν ανεκμετάλλευτες, ιδιωτικές διευθύνσεις που είναι μη δρομολογήσιμες στο Διαδίκτυο, κλπ.

Για την επίλυση αυτού του προβλήματος, πρέπει να υπάρχει μία καθολική, εταιρική πολιτική, η οποία να προκύψει από αποφάσεις σε κάποια σημαντικά ζητήματα:

- Θα χρησιμοποιηθούν ιδιωτικές ή δημόσιες διευθύνσεις; Για τις δημόσιες διευθύνσεις θα πρέπει να γίνει εκχώρηση, είτε από την αρμόδια προϊσταμένη αρχή κατόπιν αιτιολογημένης εκθέσεως, είτε από την εταιρεία-πάροχο του Διαδικτύου (ISP – Internet Service Provider). Στην μεν πρώτη περίπτωση οι διευθύνσεις ανήκουν στην εταιρεία μας, ενώ στην δεύτερη στον ISP. Εάν ανήκουν στον ISP, εφόσον σε κάποια στιγμή στο μέλλον αλλάξουμε ISP, θα πρέπει να αλλάξουμε και τις διευθύνσεις αυτές.
- Πόσα τερματικά συστήματα (υπολογιστές) θα έχουν πρόσβαση μόνον στο ιδιωτικό δίκτυο και πού βρίσκονται τα σύνορα μεταξύ ιδιωτικού δικτύου και εκείνου που έχει δημόσιες διευθύνσεις;
- Πόσα τερματικά συστήματα πρέπει να είναι ορατά από το δημόσιο δίκτυο και πώς γίνεται η αντιστοίχιση δημόσιας με ιδιωτική διεύθυνση;
- Ποιος είναι υπεύθυνος για την διευθυνσιοδότηση στο δίκτυο της εταιρείας μας;

Οι στατικές διευθύνσεις έχουν το πλεονέκτημα ότι διευκολύνουν την διαχείριση του δικτύου. Για αυτό και προτιμώνται για τον πυρήνα του δικτύου, δηλαδή για κόμβους όπως δρομολογητές, αλλά ακόμα και για μεταγωγείς που κανονικά δεν χρειάζονται διευθύνσεις IP (αφού λειτουργούν στο 2^{ο} επίπεδο). Οι δυναμικές πάλι (αυτόματη ανάθεση μέσω DHCP) έχουν το πλεονέκτημα ότι μειώνουν σημαντικά την ανάγκη για σχετικές ρυθμίσεις από τους διαχειριστές στα τερματικά συστήματα. Γενικά, ορισμένοι εμπειρικοί κανόνες μας λένε ότι:

- Για μεγάλο πλήθος τερματικών συστημάτων προτιμάται η δυναμική διευθυνσιοδότηση.
- Εάν υπάρχει σημαντική πιθανότητα αλλαγής των διευθύνσεων ή η αυτόματη απόδοση και άλλων πληροφοριών (όπως DNS), τότε και πάλι η δυναμική διευθυνσιοδότηση των τερματικών συστημάτων είναι προτιμότερη.
- Εάν η άμεση διαθεσιμότητα και η ασφάλεια είναι εξαιρετικά σημαντικές, προτιμάται η στατική διευθυνσιοδότηση, μια και δεν είναι αναγκαία η ύπαρξη αντίστοιχου εξυπηρέτη (DHCP), και κάθε συσκευή μπορεί να ταυτοποιηθεί άμεσα από την διεύθυνση IP που έχει. Το τελευταίο σημαίνει ότι μπορεί να γίνει εύκολα και παρακολούθηση της δικτυακής κίνησης της κάθε συσκευής.

Αν και το πρωτόκολλο DHCP παρουσιάσθηκε σε προηγούμενο κεφάλαιο, αξίζει να αναφερθεί ότι αυτό υποστηρίζει την δυναμική απόδοση διευθύνσεων, όχι μόνον επ' αόριστον, αλλά και για προκαθορισμένο από τον διαχειριστή χρονικό διάστημα. Επίσης υποστηρίζει και την περίπτωση μόνιμης διευθύνσεως IP (έστω και εάν είναι ιδιωτική) που έχει τοποθετήσει ο διαχειριστής. Αν και η τελευταία δυνατότητα χρησιμοποιείται σπάνια, είναι πολύ βολική όταν χρειάζεται. Τέλος, υπάρχει η δυνατότητα σε ορισμένους δρομολογητές να παίξουν τον ρόλο αναμεταδότη (relay), ώστε τερματικά συστήματα σε υποδίκτυα που δεν έχουν δικό τους εξυπηρέτη DHCP να μπορούν να επικοινωνήσουν με κάποιον στο συνολικό δίκτυο (συνήθως σε γειτονικό υποδίκτυο, επειδή η εκπομπή πακέτων είναι κάτι που πρέπει να χρησιμοποιείται με φειδώ).

Επίσης, με τις ιδιωτικές διευθύνσεις υπάρχει κίνδυνος να θεωρηθεί ότι δεν χρειάζεται να ακολουθηθεί ένα αυστηρά καθορισμένο ιεραρχικό μοντέλο διευθυνσιοδότησης. Ένα παράδειγμα αποτελεί η περιοχή ιδιωτικών διευθύνσεων `10.0.0.0`, που περιλαμβάνει τεράστιο πλήθος διευθύνσεων.

Ιδιαίτερη προσοχή χρειάζεται όταν χρησιμοποιείται NAT για επικοινωνία υπολογιστών σε περιοχές ιδιωτικών διευθύνσεων, με το Διαδίκτυο. Αφού όλη η κίνηση πρέπει να περνά μέσα από την συσκευή που προσφέρει αυτήν την υπηρεσία, θα πρέπει να δίδεται περισσότερη προσοχή στην ασφάλειά της, αλλά και στην ταχύτητα με την οποίαν διακινεί την σχετική κυκλοφορία. Διαφορετικά, μπορεί να αποτελέσει σημείο συμφόρησης.

Η ιεραρχία στην διευθυνσιοδότηση έχει και ένα ακόμα σημαντικό προσόν: επιτρέπει και την *ιεραρχική δρομολόγηση*. Σε μικρά δίκτυα κάτι τέτοιο μπορεί να είναι ασήμαντο, αλλά σε μεγάλα δίκτυα προσφέρει την δυνατότητα περίληψης δυνατών δρομολογίων (route summarization or aggregation). Έτσι, μειώνεται σημαντικά το πλήθος των σχετικών καταχωρήσεων στους πίνακες των δρομολογητών, όπως και τα πακέτα που περιγράφουν τις δυνατές πληροφορίες δρομολόγησης. Με την υιοθέτηση μίας τέτοιας ιεραρχίας, καθώς και μεταβλητής υποδικτύωσης (variable subnetting), οι περιοχές διευθύνσεων για τα διάφορα υποδίκτυα είναι διαδοχικές, διευκολύνοντας την περίληψη δρομολογίων, ενώ μειώνουν και την σπατάλη διευθύνσεων IP.

Όπως είδαμε στο κεφάλαιο 2, στην περίπτωση του IPv6 έχουμε διευθύνσεις Link-local (της μορφής `FE80::/10`) που έχουν νόημα μόνον σε ένα δίκτυο ή ζεύξη, για την ανάληψη διευθύνσεως μονοεκπομπής IPv6 όταν δεν χρησιμοποιείται DHCPv6. Αντίστοιχα, υπάρχουν και οι διευθύνσεις μονοεκπομπής με καθολική ισχύ (global) αποτελούμενες από τα τρία λογικά μέρη `<Global-routing-prefix>`, `<Subnet ID>`, `<Interface ID>`, καθώς και οι διευθύνσεις IPv6 με ενσωματωμένες διευθύνσεις IPv4 (για ευκολότερη μελλοντική μετάβαση στο IPv6). Υπάρχουν δύο τέτοιες προσεγγίσεις.

Στην πρώτη όλα τα αρχικά bit είναι '`0`', ενώ τα τελευταία 32 περιέχουν την διεύθυνση IPv4. Στην δεύτερη, τα 80 πρώτα από τα συνολικά 128 bit είναι '`0`', τα επόμενα 16 bit είναι '`1`', και τα τελευταία 32 περιέχουν την διεύθυνση IPv4. Απαιτείται επομένως αρκετή προσοχή για να μην δημιουργεί κάποιο πρόβλημα λόγω λανθασμένων υποθέσεων για τις μεταβατικές αυτές διευθύνσεις.

10.4.4. Ονοματοδοσία

Η ονοματοδοσία (συμβολικά ονόματα) πρέπει και αυτή να ακολουθεί κάποιους κανόνες, επειδή τα κατάλληλα ονόματα παίζουν σημαντικό ρόλο στην χρηστικότητα του δικτύου και, κατ' επέκταση, στην διαχειρισιμότητά του. Δεν χρειάζεται επομένως ο κάθε χρήστης να θυμάται συγκεκριμένες διευθύνσεις IP, αλλά ονόματα, κάτι που τον διευκολύνει.

Τα πρώτα ζητήματα που πρέπει να διευκρινισθούν είναι:

- Οι κατηγορίες των δικτυακών οντοτήτων που χρειάζονται συμβολικά ονόματα. Π.χ., δρομολογητές, μεταγωγείς, υπολογιστές, εκτυπωτές, κλπ.
- Εάν γενικά τα τερματικά συστήματα πρέπει να έχουν συμβολικά ονόματα.
- Ποια είναι η δομή των διαφόρων ονομάτων, καθώς και εάν κάποιο τμήμα του ονόματος σχετίζεται με τον τύπο της αντίστοιχης συσκευής.
- Ποιος αναλαμβάνει την διαχείριση της ονοματοδοσίας, καθώς και το πού και πώς αποθηκεύονται αυτά, και είναι μετά προσπελάσιμα.
- Πώς γίνεται η ανάθεση ονόματος σε κάποια συσκευή (ιδίως υπολογιστή) κάθε φορά που εκκινεί.
- Εάν η προηγούμενη διαδικασία γίνεται με δυναμικό τρόπο.
- Πόσος πλεονασμός πρέπει να υπάρχει για την υπηρεσία αυτή και με ποιον τρόπο.
- Εάν με το συγκεκριμένο μοντέλο πρόκειται να επηρεασθεί ο όγκος της κυκλοφορίας και η ασφάλεια.

Μερικοί γενικοί κανόνες για τα ονόματα, προέρχονται από την εμπειρία. Έτσι, τα ονόματα πρέπει να είναι συνήθως σύντομα, διακριτά μεταξύ τους και με νόημα. Για παράδειγμα, ένα όνομα εξυπηρέτη όπως το '`e-mail_web_server`' μπορεί να είναι σαφές, αλλά είναι αρκετά μεγάλο για να μπορεί να είναι εύκολη η χρήση του αφού χρειάζεται να πληκτρολογηθούν κάθε φορά τόσοι χαρακτήρες.

Από την άλλη, εάν υποθέσουμε ότι κάθε όνομα ξεκινά πάντα με 2-3 χαρακτήρες που υποδηλώνουν τον τύπο του (π.χ., '`rt`' για router, '`sw`' για switch, '`srv`' για server), υπάρχει μεγάλη διευκόλυνση στην κατανόηση. Το ίδιο και εάν υπάρχει κάποιος σύντομος κώδικας για τοποθεσία, π.χ., '`gd1`' θα μπορούσε να σημαίνει 'πύργος ΓΔ, 1ος όροφος'.

Είναι σημαντικό να αποφεύγεται η διαφοροποίηση μεταξύ κεφαλαίων και μικρών γραμμάτων, αφού είναι δύσκολο να θυμόμαστε ποια γράμματα πρέπει να γράφονται με κεφαλαία και να μην υπάρχουν κενά.

Υπάρχει η περίπτωση να έχουμε μία συσκευή, με πολλαπλές συνδέσεις, σε κάθε μία εκ των οποίων έχει αποδοθεί ξεχωριστή διεύθυνση IP. Σε αυτήν την περίπτωση είναι σκόπιμο να αποδίδεται το ίδιο όνομα για όλες τις αντίστοιχες διευθύνσεις IP.

Από την άλλη, εάν κάποιος βλέπει ένα συμβολικό όνομα από το οποίο καταλαβαίνει άμεσα ότι πρόκειται για κάποιον σημαντικό δικτυακό κόμβο, τότε υπάρχει μεγαλύτερη πιθανότητα να προσπαθεί να διεισδύσει σε αυτόν.

Δεν θα επεκταθούμε περισσότερο στο ζήτημα αυτό, μια και είναι αρκετά γνωστό από την εισαγωγή στην ονοματοδοσία κατά DNS, καθώς και από τον στατικό τρόπο ονοματοδοσίας κάθε υπολογιστή για τον εαυτό του, κάτι που εξαρτάται και από το τοπικό λειτουργικό σύστημα (π.χ., αρχείο '`/etc/hosts`' στο Linux).

10.4.5. Πρωτόκολλα Δρομολόγησης

Τα πρωτόκολλα δρομολόγησης αποτελούν με την σειρά τους σημαντικό παράγοντα για την ομαλή και αποδοτική λειτουργία ενός δικτύου. Συνεπώς, η επιλογή των καταλλήλων πρωτοκόλλων δρομολόγησης είναι κρίσιμο ζήτημα.

Προκειμένου να διευκολυνθούμε στην επιλογή αυτή, χρειάζεται να λάβουμε υπ' όψιν ορισμένες παραμέτρους, βάσει των αναγκών ή στόχων που έχουν τεθεί. Εμπειρικά, ορισμένα τέτοια γενικά ζητήματα μπορούν να είναι τα εξής:

- Ποιοι είναι οι στόχοι.
- Ποιες είναι οι επιλογές που υπάρχουν και πόσο καλά ανταποκρίνονται στους στόχους.
- Ποιες είναι οι θετικές ή αρνητικές επιπτώσεις από την όποια επιλογή κάνουμε.
- Ποια είναι η εμπειρία από την υιοθέτηση κάποιας από τις επιλογές στο παρελθόν (εφόσον υπάρχει).
- Ποιο το σχετικό κόστος και η εκτιμώμενη αντίδραση του πελάτη.

Τα παραπάνω ζητήματα μπορούν να συγκεκριμενοποιηθούν περισσότερο. Π.χ., οι στόχοι μπορούν να διαχωρισθούν σε εκείνους που θεωρούμε κρίσιμους και σε εκείνους που δεν θεωρούμε ως τέτοιους και οι δύο αυτές ομάδες να αναλυθούν περισσότερο. Στην πρώτη ομάδα θα μπορούσαμε να συμπεριλάβουμε στόχους όπως το ότι το πρωτόκολλο δρομολόγησης πρέπει να είναι προτυποποιημένο και ευρέως διαθέσιμο στους δρομολογητές, να έχει δυνατότητα κλιμάκωσης, να είναι εύκολο στην διευθέτηση και διαχείριση, καθώς και να είναι γρήγορη η σύγκλισή του. Στην δεύτερη ομάδα θα μπορούσαμε να συμπεριλάβουμε στόχους όπως το να μην δημιουργεί μεγάλο όγκο κυκλοφορίας, να μην είναι 'κλειστό' πρωτόκολλο έστω και μερικώς, να προσφέρει δυνατότητες για εξισορρόπηση φόρτου, ελέγχου πακέτων σε βάθος, ο βαθμός συνεργασίας μεταξύ διαφορετικών πρωτοκόλλων που λειτουργούν ταυτόχρονα σε γειτονικά μέρη του δικτύου, κλπ.

Τα αντίστοιχα ισχύουν και για τους μεταγωγείς (switches). Εδώ βέβαια οι δυνατές επιλογές είναι λιγότερες, αλλά πάλι αρκετές ώστε να χρειάζονται μελέτη. Π.χ., οι μεταγωγείς λειτουργούν στο επίπεδο ζεύξης δεδομένων (2), και άρα είναι διαφανείς ως προς το αμέσως ανώτερο επίπεδο (και τους δρομολογητές). Ο τρόπος λειτουργίας τους είναι επίσης *store-and-forward*. Επομένως, πρώτα λαμβάνουν ολόκληρο το πλαίσιο, το ελέγχουν για σφάλματα, και εάν όλα είναι καλά το αποθηκεύουν προσωρινά πριν το προωθήσουν στις κατάλληλες εξόδους τους. Υπάρχει όμως σε ορισμένους και ο τρόπος λειτουργίας *adaptive cut-through*. Εδώ, ο μεταγωγέας εξετάζει τα πρώτα byte του πλαισίου ενώ το λαμβάνει και αμέσως μόλις προσδιορίσει την κατάλληλη έξοδο το προωθεί προς αυτήν, έστω και εάν δεν έχει ολοκληρώσει την λήψη του. Αυτός ο τρόπος λειτουργίας επιταχύνει την προώθηση πλαισίων, αλλά έχει το μειονέκτημα ότι εάν ένα πλαίσιο είναι εσφαλμένο, προωθείται εσφαλμένο αντίγραφό του. Υπάρχουν και άλλες δυνατότητες, όπως π.χ., ο τρόπος διαχείρισης πληροφοριών για VLAN με την χρήση πλαισίων IEEE 802.1q, κλπ.

Δεν θα επεκταθούμε περισσότερο, επειδή αυτά τα ζητήματα, είτε έχουν ήδη εξετασθεί, είτε ξεφεύγουν από τους σκοπούς του παρόντος κειμένου.

10.4.6. Ασφάλεια

Όπως προαναφέρθηκε η ασφάλεια παίζει σήμερα κρίσιμο ρόλο στα δίκτυα υπολογιστών, εμφανιζόμενη ως ζήτημα σε όλες τις φάσεις, από τον σχεδιασμό, έως και την λήξη της ζωής ενός δικτύου. Εδώ θα εξετάσουμε την ασφάλεια μόνον από την πλευρά του σχεδιασμού ενός δικτύου.

Επειδή η ασφάλεια δεν είναι κάτι το στατικό που σχεδιάζεται και υλοποιείται σε μία μόνον φάση, κατά τον σχεδιασμό ενός δικτύου πρέπει να σχεδιασθεί και το πώς θα γίνει η διαχείρισή του από πλευράς ασφάλειας. Σε όλα αυτά προστίθεται πάντα και το σχετικό κόστος, το οποίο θα πρέπει να συζητηθεί (μαζί με εναλλακτικές προτάσεις) με τον πελάτη, προκειμένου να καταλήξουμε σε κάτι αποδεκτό.

Ο σχεδιασμός, επομένως, πρέπει να περιλαμβάνει κάποια ζητήματα ασφάλειας που μπορούν να εξετασθούν και να επιλυθούν πριν την ανάπτυξη του δικτύου, αλλά και ορισμένα ζητήματα που πρέπει να μπορούν να αντιμετωπισθούν κατά την διάρκεια λειτουργίας του δικτύου.

Στην πρώτη κατηγορία περιλαμβάνονται ο σχεδιασμός και, κατά το δυνατόν, απομόνωση τμημάτων του δικτύου προκειμένου να είναι δύσκολο σε έναν εισβολέα να επιτύχει πλήρη ανατροπή του δικτύου επειδή κατάφερε να εισβάλει σε ένα μέρος του. Επίσης, περιλαμβάνονται και ζητήματα αρχικής εξασφάλισης κάθε μέρους του, καθώς και παρακολούθησης της δικτυακής δραστηριότητας για τον όσο το δυνατόν ταχύτερο εντοπισμό ύποπτης δραστηριότητας. Εδώ έχουμε και ζητήματα διαχείρισης κρίσεων, αλλά και διάρθρωσης και κατάλληλης εκπαίδευσης του προσωπικού.

Στην δεύτερη κατηγορία έχουμε ζητήματα που αφορούν την ανίχνευση και αντιμετώπιση ύποπτων περιστατικών κατά την διάρκεια λειτουργίας του δικτύου, καθώς και διαρκούς εκπαίδευσης και επιμόρφωσης όχι μόνον του προσωπικού διαχείρισης του δικτύου, αλλά και των χρηστών.

Η σπουδαιότητα των παραπάνω είναι τόσο σημαντική ώστε να προχωρήσει το Network Working Group του IETF στην έκδοση δύο οδηγών:

- Οδηγός ασφάλειας για δικτυακές τοποθεσίες (sites), με την νεότερη ως RFC 2196 (Fraser, 1997).
- Οδηγός ασφάλειας για χρήστες, ως RFC 2504 (Guttman, Leong, & Malkin, 1999).

Ο πρώτος αναφέρει ως βασική προσέγγιση τα παρακάτω βήματα για ένα σχέδιο ασφάλειας δικτύου:

1. Προσδιορισμός του τι προσπαθούμε να προστατεύσουμε.
2. Προσδιορισμός για το ποιο είναι αυτό από το οποίο προσπαθούμε να προστατεύσουμε το προηγούμενο.
3. Προσδιορισμός του πόσο πιθανές είναι οι απειλές.
4. Υλοποίηση μέτρων που θα προστατεύσουν τους πόρους μας με αποδοτικό τρόπο ως προς το κόστος.
5. Διαρκής εξέταση και αναθεώρηση της διεργασίας, με βελτίωση κάθε φορά που ανακαλύπτεται κάποια αδυναμία.

Ο οδηγός αυτός επικεντρώνεται στα πρώτα τέσσερα βήματα. Στα πρώτα δύο βήματα προσδιορίζουμε τους πόρους που θέλουμε να προστατεύσουμε, καθώς και τις σχετιζόμενες απειλές. Πόροι μπορεί να είναι υλικό, λογισμικό, δεδομένα, αλλά επίσης και κείμενα τεκμηρίωσης, άνθρωποι-κλειδιά, και προμήθειες. Βασικές απειλές θεωρούνται:

- Η μη εξουσιοδοτημένη πρόσβαση σε πόρους και πληροφορίες.
- Μη προμελετημένη ή/και μη εξουσιοδοτημένη αποκάλυψη πληροφοριών.
- Denial of Service.

Για να δημιουργήσουμε ένα κατάλληλο σχέδιο ασφάλειας χρειάζεται να προσδιορίσουμε τους στόχους της ασφάλειας, με τους αναπόφευκτους σχετικούς συμβιβασμούς:

- *Προσφερόμενες υπηρεσίες έναντι παρεχόμενης ασφάλειας*. Κάθε παρεχόμενη ασφάλεια ενέχει και τους δικούς της κινδύνους ασφάλειας. Ανάλογα με το τι είναι πιο σημαντικό, οι διαχειριστές μπορεί να αποφασίσουν την μη προσφορά κάποιας υπηρεσίας προς τους χρήστες.

- *Ευκολία χρήσης έναντι ασφάλειας*. Π.χ., ένα σύστημα χωρίς χρήση password θα ήταν το πλέον εύχρηστο, αλλά δεν θα είχε καμία ασφάλεια. Αντιθέτως, η πρόσβαση μέσω κωδικών μίας χρήσεως θα το έκανε πιο δύσχρηστο, αλλά πιο ασφαλές.
- *Κόστος ασφάλειας έναντι κινδύνου απώλειας*. Υπάρχουν πολλά είδη κόστους για την ασφάλεια, που δεν είναι μόνον χρήματα. Π.χ., χρόνος, αποδοτικότητα, ευχρηστία, απώλεια ιδιωτικότητος και δεδομένων, υπηρεσιών, φήμης, κλπ.

Κατόπιν μπορούμε να προχωρήσουμε μία Πολιτική Ασφάλειας. Δεν θα επεκταθούμε εδώ περισσότερο, επειδή ήδη αναφερθήκαμε σε αυτήν διεξοδικά σε προηγούμενο κεφάλαιο.

10.5. Φυσικός Σχεδιασμός Δικτύου

Ο φυσικός σχεδιασμός έχει να κάνει με την επιλογή συγκεκριμένων τεχνολογιών LAN και WAN. Σε αυτές περιλαμβάνονται η καλωδίωση, τα πρωτόκολλα των χαμηλοτέρων δύο επιπέδων (αφού εξαρτώνται από την τεχνολογία που επιλέγεται), και τα ενεργά στοιχεία στο εσωτερικό του δικτύου (μεταγωγείς και δρομολογητές). Οι δυνατές επιλογές είναι πολλές και δεν υπάρχει μία τεχνολογία που να καλύπτει άριστα όλες τις ανάγκες. Προφανώς οι τελικές επιλογές επηρεάζονται από τις αποφάσεις που έχουν προηγηθεί στις προηγούμενες φάσεις.

Η πρώτη επιλογή έχει να κάνει με την τοπολογία της καλωδίωσης. Διάφορες εταιρείες έχουν δημοσιεύσει οδηγούς για το πώς πρέπει να γίνεται, αλλά ο πιο διαδεδομένος σήμερα είναι εκείνος των TIA /EIA (Telecommunications Industry Association / Electronics Industry Alliance), γνωστός ως πρότυπο TIA/EIA-568 Rev. C (TIA/EIA, 2012). Σημειωτέον ότι η TIA είναι τμήμα της EIA, καθώς και ότι συχνά εμφανίζεται και ως EIA/TIA-568. Για μία επισκόπηση του εκτενούς αυτού οδηγού ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει και στο σχετικό κείμενο της εταιρείας Anixter (2013).

Σε γενικές γραμμές, μπορούμε να πούμε ότι υπάρχουν δύο βασικές μορφές καλωδίωσης. Στην πρώτη (κεντρικοποιημένη) σχεδόν όλα τα καλώδια τερματίζουν σε έναν χώρο (όπως, π.χ., στην τοπολογία αστέρος). Στην δεύτερη μπορούν να τερματίζουν σε διαφορετικούς χώρους (κατανεμημένη).

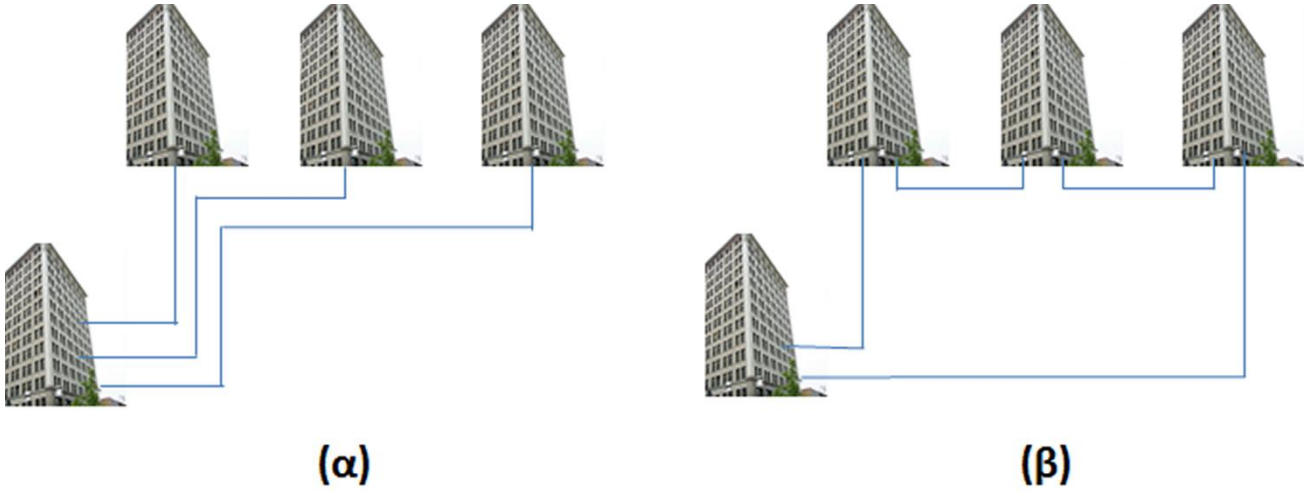
Σε κάθε κτίριο μπορεί να χρησιμοποιηθεί οποιαδήποτε μορφή από τις παραπάνω, αν και για τα μεγάλα κτίρια προτείνεται η δεύτερη μορφή για ευνόητους λόγους – κυρίως όμως για διαθεσιμότητα, μια και εάν κοπεί κάποιο καλώδιο, δεν παύει η επικοινωνία στα επί μέρους δίκτυα. Φυσικά η πολυπλοκότητα της διαχείρισης μπορεί να είναι αυξημένη.

Η βασική ιδέα είναι ότι έχουμε σε κάθε κτίριο, μία ή περισσότερες οριζόντιες καλωδιώσεις ανά όροφο που τερματίζουν (συνήθως με τοπολογία αστέρος) σε κατάλληλα ικριώματα, μέσα σε καμπίνες επικοινωνιών. Μέσα σε αυτές τοποθετούνται και οι αντίστοιχοι μεταγωγείς με τους οποίους διασυνδέονται. Επίσης, υπάρχει και μία κατακόρυφη καλωδίωση που διασυνδέει όλους τους μεταγωγείς σε κάθε όροφο (άμεσα ή μέσω κάποιου επιπρόσθετου μεταγωγέα ή δρομολογητή) μεταξύ τους και τελικά με έναν δρομολογητή για περαιτέρω διασύνδεση. Ένα τέτοιο παράδειγμα μπορεί κανείς να δει από την τεκμηρίωση του δικτύου του Πανεπιστημίου Μακεδονίας (Κέντρο Υπολογιστών & Δικτύων, 2012).

Εφόσον έχουμε πολλά κτίρια που διασυνδέονται μεταξύ τους, όπως προαναφέρθηκε, υπάρχει η δυνατότητα να ακολουθήσουμε την κεντρικοποιημένη ή την κατανεμημένη μορφή.

Όπως φαίνεται από την Εικόνα 10.6, στην πρώτη περίπτωση όλα τα καλώδια καταλήγουν απ' ευθείας στο κεντρικό κτίριο που φαίνεται κάτω αριστερά, σχηματίζοντας μία τοπολογία αστέρος. Στην δεύτερη περίπτωση (κατανεμημένη μορφή), κάθε κτίριο διασυνδέεται με δύο καλώδια με τα δύο γειτονικά του κτίρια, σχηματίζοντας μία τοπολογία δακτυλίου.

Αν και υπάρχουν αρκετές τεχνολογίες, σήμερα προτιμάται η καλωδίωση με UTP (Unshielded Twisted Pair), εξ αιτίας του λόγους απόδοση ως προς κόστος. Πιο συγκεκριμένα αν και επιτρέπεται η κατηγορία UTP-5e (enhanced) κατ' ελάχιστον, προτείνεται η κατηγορία UTP-6 που επιτρέπει εύρος ζώνης τουλάχιστον 200 MHz, και επομένως υποστηρίζει Ethernet (100 Mbps και 1 Gbps) και ATM.



Εικόνα 10.6 *Καλωδίωση κτιρίων με (α) κεντρικοποιημένη, (β) κατανεμημένη μορφή.*

Η χρήση οπτικών ινών είναι τεχνολογικά προτιμότερη, αλλά το κόστος συνεχίζει να είναι τόσο μεγάλο, ώστε ακόμα και εταιρείες το αποφεύγουν, χρησιμοποιώντας το μόνον στην κατακόρυφη καλωδίωση, την καλωδίωση μεταξύ κτιρίων ή κρισίμων χώρων (όπως, π.χ., δίκτυο διασύνδεσης με το Διαδίκτυο ή με εξυπηρέτες που έχουν ανάγκη για δυνατότητα διακίνησης μεγάλης κυκλοφορίας).

Στα τοπικά δίκτυα υπάρχουν διάφορες ενσύρματες τεχνολογίες, με προεξάρχουσα εκείνη του Ethernet. Γενικά, οι παράγοντες που επηρεάζουν την επιλογή είναι:

- Οι υπάρχουσες πολιτικές για εγκεκριμένες τεχνολογίες.
- Η τεχνική αρτιότητα του προσωπικού.
- Οι οικονομικοί περιορισμοί.
- Σχέδια επεκτάσεως ή αναβάθμισης του δικτύου.

Ως προς τις συσκευές διασύνδεσης (δρομολογητές και μεταγωγείς), υπάρχουν αρκετά κριτήρια τα οποία πρέπει να λαμβάνονται υπ’ όψιν, όπως τα παρακάτω:

- Ταχύτητα επεξεργασίας πακέτων.
- Μέγεθος μνήμης.
- Καθυστέρηση που εισάγει η συσκευή κατά την διαχείριση πακέτων.
- Αριθμός διαθέσιμων φυσικών θυρών.
- Διαθέσιμες τεχνικές για την διαχείριση ουρών.
- Τεχνολογίες δικτύωσης που υποστηρίζονται.
- Ευχέρεια στην διευθέτηση και διαχείριση.
- Υποστήριξη πολιτικών QoS.
- Υποστήριξη VLAN.
- Υποστήριξη μηχανισμών ασφαλείας και ελέγχου ή φιλτραρίσματος πακέτων.
- Συμβατότητα με άλλες συσκευές.
- Η φήμη του κατασκευαστή, καθώς και δημοσιευμένα τεστ απόδοσης από ανεξάρτητους φορείς.
- Ανθεκτικότητα σε διάφορες αστοχίες (π.χ., πλεονασμός τροφοδοτικών, κλπ.).
- Τεκμηρίωση.
- Δυνατότητα εύκολης εκπαίδευσης και αναβάθμισης λογισμικού.
- Κόστος προμήθειας και εγκατάστασης.
- Κόστος, ευκολία και ταχύτητα προμήθειας ανταλλακτικών.
- Κόστος, δυνατότητα και ευκολία αναβάθμισης υλικού και υποστηριζόμενων τεχνολογιών.
- Κόστος και διάρκεια εγγύησης.

Για την περίπτωση μεγαλυτέρων δικτύων ή εκείνων που εκτείνονται σε μεγάλες γεωγραφικές αποστάσεις (π.χ., εταιρικά υποκαταστήματα), επιπρόσθετα ζητήματα έχουν να κάνουν με τεχνολογίες WAN, μισθωμένες γραμμές, και δυνατότητες άμεσης πρόσβασης από εξωτερικά δίκτυα ή το Διαδίκτυο.

10.6. Παράδειγμα Σχεδιασμού Δικτύου

Έστω ότι μας έχει ανατεθεί ο σχεδιασμός για την αναβάθμιση του δικτύου στο Πανεπιστήμιο Βερτίσκου. Αυτό το πανεπιστήμιο είναι μικρό, αποτελούμενο από τέσσερα μεγάλα κτίρια (‘Α’, ‘Β’, ‘Γ’, και ‘Δ’), των πέντε ορόφων το κάθε ένα. Τα κτίρια αυτά συνδέονται μεταξύ τους σε ένα ενιαίο οικοδόμημα, στο ισόγειο και τον πρώτον όροφο, όπου βρίσκονται αμφιθέατρα και γραμματείες των διαφόρων σχολών/τμημάτων, το εστιατόριο, καθώς και το κέντρο υπολογιστών και δικτύων.

Το προσωπικό αποτελείται από περίπου 100 διδάσκοντες σε όλες τις βαθμίδες, 40 τεχνικούς και 100 διοικητικούς υπαλλήλους. Υπάρχουν 2 σχολές, με 2 τμήματα η κάθε μία (συνολικά 4 τμήματα) και περίπου 4.000 φοιτητές σε όλα τα έτη σπουδών, περίπου 200 στα διάφορα μεταπτυχιακά προγράμματα που προσφέρονται, καθώς και 60 φοιτητές ως υποψήφιοι διδάκτορες. Δεν υπάρχουν φοιτητικές εστίες.

Λόγω της πρόσφατης αύξησης στον αριθμό των φοιτητών του πρώτου έτους κατά 50%, ο αριθμός των φοιτητών έχει αυξηθεί, και αναμένεται σε βάθος χρόνου να φθάσει τους 7.500. Ήδη υπάρχουν παράπονα ότι το υφιστάμενο προσωπικό στο κέντρο υπολογιστών και δικτύων, που αποτελείται από τον διευθυντή και άλλους έξι τεχνικούς, δεν επαρκεί για τις αυξημένες ανάγκες, ενώ επίσης υπάρχουν παράπονα για την απόδοση και αξιοπιστία του δικτύου. Ιδιαίτερα παράπονα έχουν οι φοιτητές που έχουν αυστηρά καθορισμένες προθεσμίες για ηλεκτρονική υποβολή εργασιών, επειδή συχνά προσπαθούν να παραδώσουν τις εργασίες τους εμπρόθεσμα, αλλά τελικά αυτές εμφανίζονται ως εκπρόθεσμα υποβληθείσες από το σύστημα.

Ένα άλλο ζήτημα είναι η υποστήριξη ασύρματης δικτύωσης, επειδή συχνά τα τμήματα ή οι φοιτητές τους, εγκαθιστούν διάφορα AP (Access Point), χωρίς προηγούμενη ενημέρωση και έγκριση από το κέντρο υπολογιστών και δικτύων. Αυτό ανησυχεί τον διευθυντή του τελευταίου, επειδή υπάρχουν ζητήματα αξιοπιστίας και ασφάλειας.

Βάσει των όσων αναπτύχθηκαν στις προηγούμενες ενότητες, προχωράμε στον σχεδιασμό του νέου δικτύου.

10.6.1. Επιχειρηματικοί Στόχοι

Το πανεπιστήμιο επιθυμεί να συνεχίζει να προσελκύει όσο το δυνατόν περισσότερους φοιτητές, όχι μόνον για να αυξήσει τον συνολικό αριθμό των φοιτούντων, αλλά και για να έχει δυνατότητες αυξημένης επιλογής ανάμεσα στους αιτούντες, κάτι που μπορεί να το χρησιμοποιήσει διαφημιστικά για περαιτέρω βελτίωση της φήμης του.

Μετά από σχετική συζήτηση με την διοίκηση του πανεπιστημίου καθορίσθηκαν οι επιχειρηματικοί στόχοι που είναι οι παρακάτω:

- Αύξηση των προπτυχιακών φοιτητών από 4.000 (για τέσσερα έτη σπουδών) σε 7.000 στα επόμενα τρία έτη, καθώς και διπλασιασμός των μεταπτυχιακών φοιτητών.
- Βελτίωση της αποδοτικότητας του προσωπικού και αύξηση του διαθέσιμου χρόνου τους για συμμετοχή σε ερευνητικά προγράμματα με συμμετοχή και άλλων πανεπιστημίων.
- Βελτίωση της αποδοτικότητας των φοιτητών και εξάλειψη του προβλήματος της ηλεκτρονικής υποβολής εργασιών.
- Παροχή πρόσβασης στο δίκτυο, αλλά και στο Διαδίκτυο, στους φοιτητές μέσω των φορητών τους υπολογιστών και με ασύρματο τρόπο.
- Να επιτρέπεται σε επισκέπτες να έχουν ασύρματη πρόσβαση στο Διαδίκτυο μέσω του δικτύου του πανεπιστημίου, χρησιμοποιώντας τις φορητές τους συσκευές.
- Προστασία του δικτύου από εισβολείς, αλλά και από κακόβουλους χρήστες.
- Απορρόφηση του σχετικού κρατικού κονδυλίου που δόθηκε για την αναβάθμιση του δικτύου, με προθεσμία έως το τέλος του επόμενου έτους. Διαφορετικά, τα χρήματα αυτά χάνονται.

10.6.2. Τεχνικοί Στόχοι

Το κέντρο υπολογιστών και δικτύων συνέταξε έναν κατάλογο με τεχνικούς στόχους, στην προσπάθεια να αντιμετωπισθούν τα προβλήματα που έχουν διαπιστωθεί κατά την λειτουργία του τρέχοντος δικτύου:

- Επανασχεδιασμός της διευθυνσιοδότησης κατά IP.
- Αύξηση της χωρητικότητας της σύνδεσης με το Διαδίκτυο για να υποστηριχθούν οι μελλοντικές αυξημένες ανάγκες και σε όγκο κυκλοφορίας, αλλά και σε τύπους εφαρμογών.
- Παροχή ενός ασφαλούς, ιδιωτικού ασυρμάτου δικτύου για χρήση από τους φοιτητές, με σύνδεση στο δίκτυο του πανεπιστημίου, και μέσω του τελευταίου με το Διαδίκτυο.
- Παροχή ενός ανοικτού ασυρμάτου δικτύου για τους επισκέπτες, ώστε να μπορούν να προσπελάσουν το Διαδίκτυο.
- Χρόνο απόκρισης τουλάχιστον 200 msec για διαδραστικές εφαρμογές (περιλαμβάνεται και η τηλε-συνεδρίαση).
- Εγγύηση διαθεσιμότητας του δικτύου κατά 99,9% του χρόνου με μέσο χρόνο διόρθωσης βλάβης τεσσάρων (4) ωρών.
- Μέγιστη δυνατή προστασία από κακόβουλους χρήστες και εισβολείς από το Διαδίκτυο.
- Επιλογή και εγκατάσταση εργαλείων διαχείρισης δικτύου, ώστε να βελτιωθεί η αποδοτικότητα του κέντρου υπολογιστών και δικτύων, αλλά και ο μέσος χρόνος αντίδρασης σε διάφορα σχετικά συμβάντα.
- Δυνατότητα κλιμάκωσης του δικτύου για μελλοντική εκτεταμένη χρήση πολυμεσικών εφαρμογών.

10.6.3. Δικτυακές Εφαρμογές

Επί του παρόντος, το προσωπικό και οι φοιτητές του Πανεπιστημίου Βερτίσκου χρησιμοποιούν το δίκτυο για τους παρακάτω τύπους εφαρμογών:

- Εφ-1: *Εργασίες στα πλαίσια των μαθημάτων*. Οι περισσότεροι φοιτητές χρησιμοποιούν τους διαθέσιμους εκτυπωτές για τις εργασίες τους και τους εξυπηρέτες αρχείων στο κέντρο υπολογιστών και δικτύων, είτε για να τις αποθηκεύουν προσωρινά, είτε για να τις υποβάλλουν ηλεκτρονικά, ανάλογα με το τι τους έχει ζητήσει ο κάθε διδάσκων. Οι διδάσκοντες από την πλευρά τους συνήθως χρησιμοποιούν τους διαθέσιμους πόρους για να στέλνουν διορθωμένες εργασίες ηλεκτρονικά στους φοιτητές, βαθμούς στην γραμματεία του κάθε τμήματος, κλπ.
- Εφ-2: *e-mail*. Χρησιμοποιείται ευρέως από όλους τους χρήστες.
- Εφ-3: *web*. Χρησιμοποιείται ευρέως από όλους τους χρήστες μέσω διαφόρων τυπικών φυλλομετρητών, είτε για αναζητήσεις και έρευνα στο Διαδίκτυο, είτε για άλλες συνηθισμένες υπηρεσίες, ενώ συχνή είναι η χρήση εφαρμογών κοινωνικής δικτύωσης ή παιχνιδιών, κυρίως από φοιτητές.
- Εφ-4: *Εξ αποστάσεως εκπαίδευση*. Το πανεπιστήμιο οργανώνει εκπαιδευτικά και ενημερωτικά σεμινάρια σε συνεργασία με άλλους φορείς στα πλαίσια της Διά Βίου Εκπαίδευσης. Υπάρχει δυνατότητα απλής παρακολούθησης και για τους τακτικούς χρήστες του πανεπιστημίου. Επίσης, ενοικιάζει κάποιους χώρους του ορισμένα Σαββατοκύριακα για χρήση από φοιτητές του Ανοικτού Πανεπιστημίου Πολυδενδρίου.
- Εφ-5: *Πληροφοριακό σύστημα φοιτητών*. Χρησιμοποιείται κυρίως από το διοικητικό προσωπικό και τους φοιτητές. Οι μεν πρώτοι εγγράφουν και διαχειρίζονται τον προσωπικό φάκελο του κάθε φοιτητή, ενώ οι δεύτεροι το χρησιμοποιούν για ενημέρωση, εγγραφές σε προγράμματα σπουδών, μαθήματα, εργαστήρια, κλπ.
- Εφ-6: *Πληροφοριακό σύστημα βιβλιοθήκης*. Χρησιμοποιείται από σχεδόν όλους τους χρήστες για δανεισμό βιβλίων, αναζήτηση, ενημέρωση, κλπ.
- Εφ-7: *Πληροφοριακά συστήματα διοίκησης*. Επί μέρους πληροφοριακά συστήματα, από δέσμευση αιθουσών για μαθήματα, κλπ., έως χρήση από το γραφείο προσωπικού, το γραφείο προμηθειών, κλπ.

- Εφ-8: *Σύστημα για διακίνηση και αποθήκευση μεγάλου όγκου δεδομένων*. Χρησιμοποιείται από το τμήμα καλών τεχνών, αλλά και από τα τμήματα φυσικής και οικονομικών, για επεξεργασία μεγάλου όγκου δεδομένων που αφορούν πολύπλοκους υπολογισμούς μοντέλων ή λεπτομερειακές προσομοιώσεις.

10.6.4. Ομάδες Χρηστών

Οι ομάδες χρηστών στο δίκτυο του Πανεπιστημίου Βερτίσκου είναι οι παρακάτω, στον Πίνακα 10.2. Παρατίθενται το πλήθος, η τοποθεσία, οι τύποι εφαρμογών που χρησιμοποιούν, καθώς και το εκτιμώμενο μελλοντικό τους πλήθος. Ως προς το πλήθος αναγράφεται ο αριθμός των ταυτόχρονων χρηστών και ο συνολικός αριθμός των χρηστών της κάθε ομάδος, εφόσον έχει να κάνει με χρήση υπολογιστών στο πανεπιστήμιο. Σημειωτέον ότι αναγράφονται μόνον οι τύποι εφαρμογών που έχουν να κάνουν με το δίκτυο. Π.χ., η παρακολούθηση εργαστηριακών μαθημάτων δεν αναφέρεται εφόσον δεν χρησιμοποιείται κατά κύριο λόγο το δίκτυο. Επίσης δεν αναφέρονται ως ξεχωριστή ομάδα οι διαχειριστές του δικτύου.

Ομάδες Χρηστών	Πλήθος ανά Ομάδα		Τοποθεσία της Ομάδος	Τύποι Εφαρμογών της Ομάδος
	Τρέχον	Μελλοντικό		
Χρήστες υπολογιστών στο Κέντρο υπολογιστών & δικτύων	100	150	1ος Όροφος, Κτίριο Α	Εργασίες, e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης, εκτύπωση εργασιών
Χρήστες βιβλιοθήκης	30	100	Ισόγειο, Κτίριο Α	Εργασίες, e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης
Τμήμα Φυσικής	120	200		Εργασίες, e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης, εκτύπωση εργασιών, διακίνηση μεγάλου όγκου δεδομένων
Τμήμα Μαθηματικών	120	200		Εργασίες, e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης, εκτύπωση εργασιών
Τμήμα Οικονομικών	120	200		Εργασίες, e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης, εκτύπωση εργασιών, διακίνηση μεγάλου όγκου δεδομένων
Τμήμα Καλών Τεχνών	120	200		Εργασίες, e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης, εκτύπωση εργασιών, διακίνηση μεγάλου όγκου δεδομένων
Διοικητικοί και Τεχνικοί υπάλληλοι	140	150	Σε όλο το πανεπ/μιο	e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης, όλες οι εφαρμογές πληροφοριακών συστημάτων
Επισκέπτες	20	400	Κτίριο Β, Βιβλιοθήκη (1ος όροφος, Κτίριο Α)	e-mail, web, χρήση των υπηρεσιών βιβλιοθήκης
Εξωτερικοί χρήστες	Δεκάδες	Χιλιάδες από το	Διαδίκτυο	Web του πανεπιστημίου, χρήση των υπηρεσιών βιβλιοθήκης

Πίνακας 10.2 *Ομάδες χρηστών του δικτύου μας.*

10.6.5. Εξυπηρέτες του Δικτύου

Στην συνέχεια καταγράφουμε τους εξυπηρέτες που υπάρχουν στο πανεπιστήμιο, όπως φαίνεται στον Πίνακα 10.3.

Εξυπηρέτης	Τοποθεσία	Τύποι Εφαρμογών	Ομάδες Χρηστών
Εξυπηρέτης υπηρεσιών βιβλιοθήκης, Linux	Κέντρο υπολογιστών και δικτύων, Data Center	Υπηρεσίες βιβλιοθήκης	Όλες
Εξυπηρέτης αρχείων, Linux (NFS)	Κέντρο υπολογιστών και δικτύων, Data Center	Εργασίες	Όλες εκτός των υπαλλήλων, επισκεπτών και εξωτερικών χρηστών
Εξυπηρέτης Εκτυπώσεων, Linux	Κέντρο υπολογιστών και δικτύων, Data Center	Εργασίες	Από όλους τους χρήστες. Η εκτύπωση γίνεται συνήθως σε τοπικό εκτυπωτή του χρήστη, όπου είναι εξουσιοδοτημένος.
Εξυπηρέτης Web, Linux	Κέντρο υπολογιστών και δικτύων, Data Center	Web του πανεπιστημίου	Όλες
Εξυπηρέτης e-mail, Linux	Κέντρο υπολογιστών και δικτύων, Data Center	e-mail	Όλες
Εξυπηρέτης Πληροφοριακών Συστημάτων, Windows	Κέντρο υπολογιστών και δικτύων, Data Center	Όλες οι εφαρμογές πληροφοριακών συστημάτων	Διοικητικοί και Τεχνικοί υπάλληλοι με εξουσιοδότηση ανά υπηρεσία
Εξυπηρέτης DNS, Linux	Κέντρο υπολογιστών και δικτύων, Data Center	DNS	Όλες
Εξυπηρέτης LDAP, Linux	Κέντρο υπολογιστών και δικτύων, Data Center	LDAP	Όλες
Εξυπηρέτης DHCP, Windows	Κέντρο υπολογιστών και δικτύων, Data Center	DHCP	Διαχειριστές Δικτύου
Εξυπηρέτης Διαχείρισης Δικτύου, Linux	Κέντρο υπολογιστών και δικτύων, Data Center	Διαχείριση	Διαχειριστές Δικτύου

Πίνακας 10.3 *Τρέχοντες εξυπηρέτες στο δίκτυό μας.*

10.6.6. Τρέχουσα Κατάσταση του Δικτύου

Εδώ αποτυπώνουμε την τοπολογία του δικτύου (κυρίως κορμού), δημιουργώντας την Εικόνα 10.7.

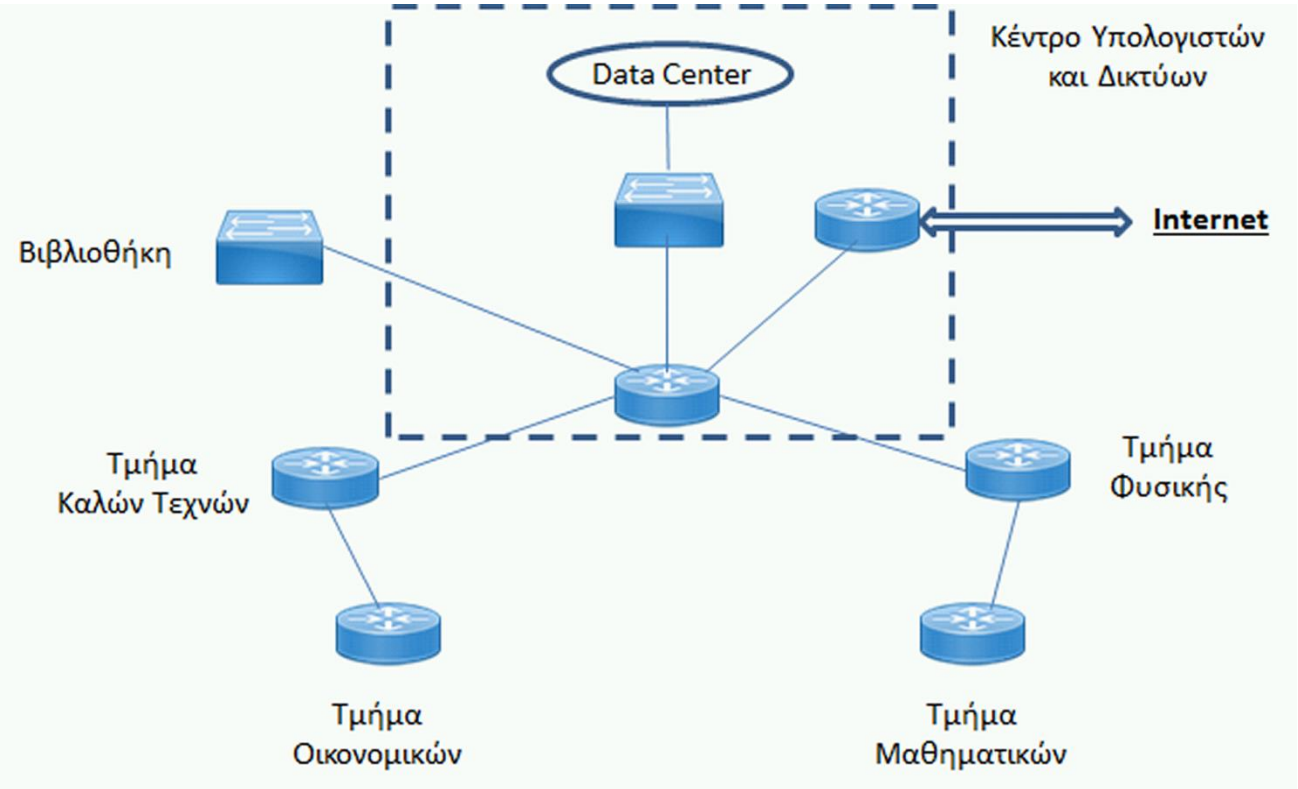
Όπως βλέπουμε, το δίκτυο κορμού αποτελείται από τέσσερεις δρομολογητές (έναν στην βάση κάθε πύργου) και έναν στο Κέντρο υπολογιστών και δικτύων. Ο τελευταίος συνδέεται επίσης με έναν δρομολογητή που παρέχει την διασύνδεση με το Διαδίκτυο, καθώς και δύο μεταγωγείς που διασυνδέουν την βιβλιοθήκη και το Data Center όπου βρίσκονται οι βασικοί εξυπηρέτες του πανεπιστημίου. Υπάρχουν και άλλοι μεταγωγείς των 24 ή 48 θυρών σε κάθε όροφο του κάθε πύργου (για κάθε τμήμα), καθώς και σε κάθε εργαστήριο, αλλά δεν χρειάζεται να απεικονισθούν εδώ. Όλες οι συνδέσεις είναι Ethernet των 100 Mbps, εκτός από την ζεύξη προς το Διαδίκτυο που είναι οπτική ίνα με ATM στα 16 Mbps.

Η διευθυνσιοδότηση κατά IP, έχει γίνει με στατικές διευθύνσεις, από ομάδες τέτοιων διευθύνσεων που έχουν σχεδόν εξαντληθεί.

Ως προς τα χαρακτηριστικά της κυκλοφορίας των δικτυακών εφαρμογών, από μεν ελαστικότητα σε χρόνο είναι οι περισσότερες που μεταφέρουν αρκετόν όγκο δεδομένων. Ωστόσο, υπάρχουν και ορισμένες, όπως η εξ αποστάσεως εκπαίδευση, που είναι ευαίσθητες ως προς την χρονική καθυστέρηση, ενώ μεταφέρουν μεγάλο όγκο δεδομένων όταν πρόκειται για βίντεο.

Επίσης, και από την Εικόνα 10.7, αλλά και από μετρήσεις της κυκλοφορίας, βλέπουμε ότι υπάρχει ένα σημείο συμφόρησης μέσα στο δίκτυο, το οποίο είναι ο δρομολογητής του κέντρου υπολογιστών και δικτύων, ο οποίος διασυνδέει όλα τα επί μέρους δίκτυα μεταξύ τους. Επίσης, ορισμένες φορές και ο δρομολογητής που διασυνδέει το δίκτυο με το Διαδίκτυο παρουσιάζει συμφόρηση, η οποία όμως έχει να κάνει όχι με τον ίδιο, αλλά με την σχετικά μικρή χωρητικότητα της σύνδεσης αυτής.

Σημειωτέον ότι οι δρομολογητές των τμημάτων Καλών Τεχνών και Φυσικής, διακινούν σχεδόν διπλάσια κίνηση σε σχέση με τους δρομολογητές των άλλων τμημάτων επειδή τα τελευταία διακινούν τα δεδομένα τους μέσω των δύο πρώτων. Επίσης, υπάρχει μία μόνον δυνατή διαδρομή από τον δρομολογητή του κάθε τμήματος προς τον ‘κεντρικό’ δρομολογητή.



Εικόνα 10.7 *Τοπολογία του υπάρχοντος δικτύου.*

10.6.7. Σχεδιασμός του Νέου Δικτύου

Ουσιαστικά εδώ έχουμε να κάνουμε με ανασχεδιασμό και αναβάθμιση του υπάρχοντος δικτύου. Χρησιμοποιώντας την στρατηγική του αρθρωτού (modular) σχεδιασμού. Οι βασικές ενέργειες είναι:

- Βελτιστοποίηση της διευθυνσιοδότησης IP.
- Αναβάθμιση της σύνδεσης με το Διαδίκτυο.
- Μείωση της μέσης κυκλοφορίας με το Διαδίκτυο ανά φοιτητή.
- Μείωση της συμφόρησης στον ‘κεντρικό’ δρομολογητή.
- Δημιουργία στοιχειώδους πλεονασμού στο εσωτερικό δίκτυο κορμού.
- Παροχή ασύρματης (WiFi) δικτύωσης με αυξημένο επίπεδο ασφάλειας.

Εδώ θα αναφερθούμε στις ενέργειες αυτές περιληπτικά, χωρίς να επεκταθούμε και σε άλλες που επίσης θα έπρεπε να γίνουν, αλλά που καλύφθηκαν από τις γενικές αρχές σχεδιασμού στις προηγούμενες ενότητες.

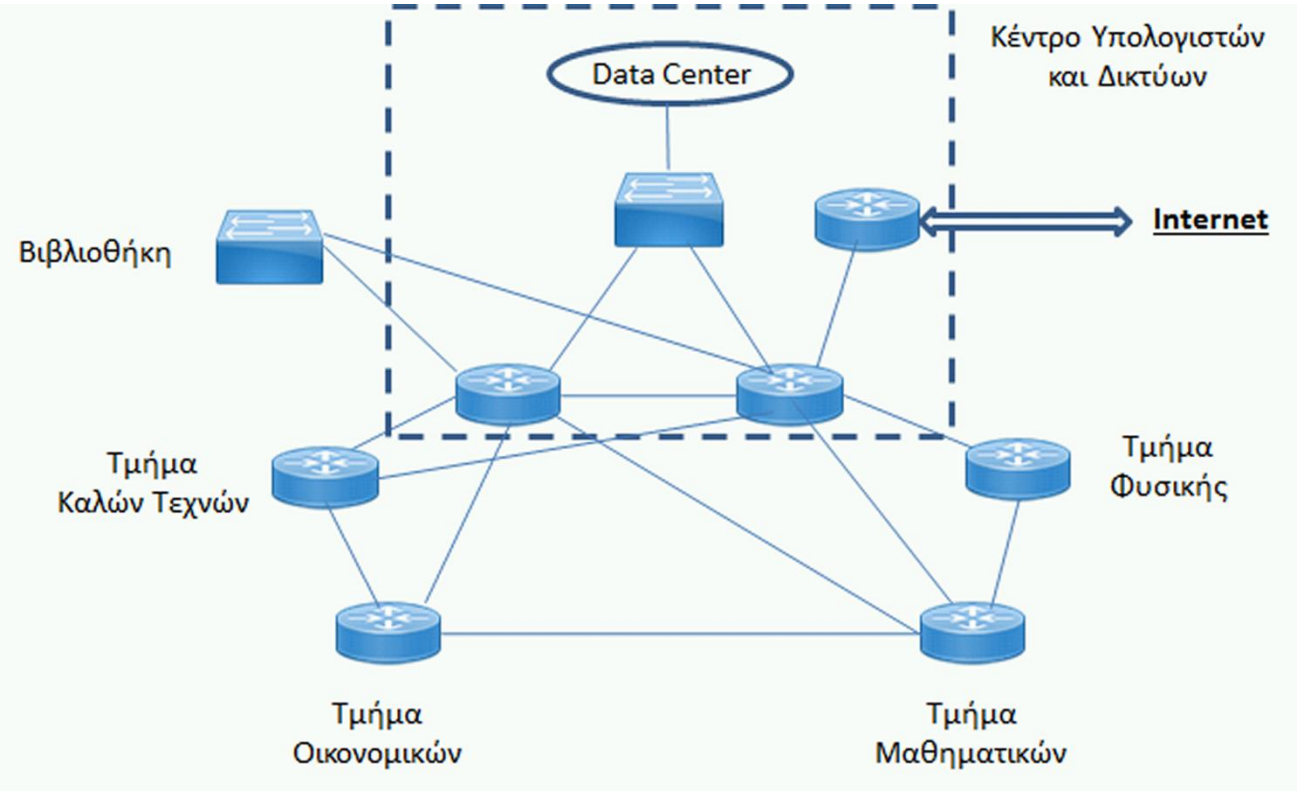
Ξεκινώντας με την βελτιστοποίηση της διευθυνσιοδότησης IP, εφόσον έχουν εξαντληθεί οι στατικές, δημόσιες διευθύνσεις IP που μας είχαν εκχωρηθεί, η μία λύση είναι να ζητήσουμε και άλλες τέτοιες από την προϊσταμένη αρχή. Καλύτερη όμως (και αμεσότερη) λύση είναι να χρησιμοποιήσουμε ιδιωτικές διευθύνσεις σε όλο σχεδόν το δίκτυό μας. Σε αυτήν την περίπτωση θα πρέπει να γίνει αναδιάταξη των διευθύνσεων IP, κρατώντας τις στατικές, δημόσιες διευθύνσεις για τους εξυπηρέτες που βρίσκονται στο Data Center του κέντρου υπολογιστών και δικτύων, καθώς και για τους δρομολογητές. Σε όλα τα άλλα τμήματα και γραφεία – ακόμα και στην βιβλιοθήκη – τα επί μέρους δίκτυα θα έχουν ιδιωτικές διευθύνσεις IP. Το ίδιο θα ισχύει και για τα ασύρματα τοπικά δίκτυα. Αυτό σημαίνει ότι όλοι οι εξυπηρέτες (εκτός των DHCP) θα βρίσκονται στο Data Center, ακόμα και αυτοί που παρέχουν, για παράδειγμα, τις υπηρεσίες Web, με τους αντίστοιχους ιστοτόπους.

Η αναβάθμιση της σύνδεσης με το Διαδίκτυο θα πρέπει να μελετηθεί, λαμβάνοντας υπ’ όψιν και την μελλοντική αύξηση της κυκλοφορίας. Πηγαίνοντας όμως στα 32 Mbps και με την χρήση καταλλήλων εξυπηρετών proxy, θα μειωθεί αρκετά.

Το τελευταίο μπορεί να οδηγήσει και σε μείωση της κυκλοφορίας στο εσωτερικό δίκτυο κορμού, με την τοποθέτηση πέντε υπολογιστών, από έναν σε κάθε τμήμα και έναν στην βιβλιοθήκη, οι οποίοι και θα αποτελούν τους proxy servers για υπηρεσίες web (http). Προφανώς θα τους ανατεθεί από μία ιδιωτική διεύθυνση IP, η οποία όμως θα είναι στατική (π.χ., πάντα η πρώτη διαθέσιμη ανά υποδίκτυο). Επίσης, οι δρομολογητές των τμημάτων θα πρέπει να φιλτράρουν όλη την εξερχόμενη κυκλοφορία HTTP, ώστε καμία αντίστοιχη αίτηση να μην επιτρέπεται να προωθείται, εάν δεν έχει ως αφετηρία τον αντίστοιχο εξυπηρέτη proxy HTTP.

Με όλα τα παραπάνω, αναμένεται μείωση του μέσου όρου της τρέχουσας κίνησης προς τον κεντρικό δρομολογητή ανά φοιτητή. Από εκεί και μετά, θα πρέπει να γίνει αναβάθμιση/αντικατάσταση του δρομολογητή αυτού.

Πλεονασμός στο δίκτυο κορμού μπορεί να γίνει, κατ' ελάχιστον, με την προσθήκη ζεύξης μεταξύ των δρομολογητών των τμημάτων Οικονομικών και Μαθηματικών. Περαιτέρω πλεονασμός μπορεί να επιτευχθεί, με αντικατάσταση του κεντρικού δρομολογητή από δύο διαφορετικούς (αλλά ισοδύναμους) δρομολογητές, αλλά και σύνδεση από τον δρομολογητή του κάθε τμήματος, και με τους δύο κεντρικούς δρομολογητές απ' ευθείας. Ενδεχομένως μάλιστα, θα ήταν σκόπιμο να υιοθετηθεί το OSPF για το δίκτυο κορμού, λόγω των δυνατοτήτων του ως προς την εξισορρόπηση φόρτου. Ο πλεονασμός είναι σημαντικός και για αποφυγή κατάρρευσης ενός δικτύου, εάν καταρρεύσει ένας κόμβος (Buchanan, 2002).



Εικόνα 10.8 *Σχέδιο για την νέα τοπολογία του δικτύου.*

Ένα παράδειγμα πλεονασμού φαίνεται στην Εικόνα 10.8, όπου δεν έχουμε μεν το τέλειο γράφημα, αλλά έχουμε υψηλό βαθμό πλεονασμού. Στην εικόνα αυτήν δεν εμφανίζονται τα Access Points για τα ασύρματα δίκτυα, όπως και οι εξυπηρέτες του Data Center χωρίζονται σε δύο λογικά μέρη. Το πρώτο παραμένει όπως και πριν ιδιωτικό και όχι άμεσα προσπελάσιμο από το Διαδίκτυο. Το δεύτερο όμως (που βρίσκεται και σε ξεχωριστό υποδίκτυο) περιλαμβάνει όλους τους εξυπηρέτες που πρέπει να είναι ορατοί από το Διαδίκτυο. Ο διαχωρισμός αυτός έχει γίνει ώστε το τελευταίο υποδίκτυο να ανήκει στην λεγόμενη DMZ (DeMilitarized Zone), έτσι ώστε εάν γίνει μη εξουσιοδοτημένη διείσδυση σε κάποιον από τους εξυπηρέτες, το πρόβλημα ασφάλειας να μην επεκταθεί άμεσα στο υπόλοιπο δίκτυο. Στην DMZ τοποθετούνται επομένως εξυπηρέτες όπως ο DNS, Web (κεντρικός, αλλά και όλων των τμημάτων και εργαστηρίων), FTP, καθώς και e-mail.

Τέλος, ως προς την παροχή WiFi προβλέπεται ότι η κίνηση θα φιλτράρεται ώστε να επιτρέπεται μόνον αυτή που αντιστοιχεί σε DNS, HTTP, POP (κατά προτίμηση όμως POPS), καθώς και DHCP. Επίσης θα πρέπει να είναι κρυμμένο και το SSID του κάθε Access Point από τα πλαίσια τύπου beacon για να δυσκολεύει την εύκολη διείσδυση, και φυσικά όλη η κυκλοφορία κρυπτογραφημένη.

10.7. Ανάπτυξη Δικτύου

Αφού γίνει ο σχεδιασμός του δικτύου και εγκριθεί από τον πελάτη, το επόμενο βήμα φαίνεται να είναι η υλοποίησή του. Δεν είναι όμως έτσι. Το κόστος σε χρήμα και χρόνο είναι μεγάλο και τις περισσότερες φορές δεν υπάρχει η δυνατότητα (πέρα από την διάθεση) να γίνεται ο πλήρης έλεγχος ως προς την πραγματική απόδοση του νέου δικτύου, αφού τεθεί σε λειτουργία.

Συνεπώς, το επόμενο βήμα είναι *να δοκιμασθεί* το νέο σχέδιο πριν υλοποιηθεί στην πράξη. Το πώς θα ελεγχθεί διεξοδικά το σχέδιο, μέσα σε εύλογο χρονικό διάστημα, και με μικρό κόστος, είναι τεράστιο ζήτημα. Εδώ θα κάνουμε μόνον μία σύντομη επισκόπηση. Οι βασικές μέθοδοι και εργαλεία για τον έλεγχο του σχεδίου μας εξαρτώνται από τους στόχους που είχαν τεθεί αρχικά. Συνήθως όμως περιλαμβάνουν τα παρακάτω:

- Επαλήθευση ότι το σχέδιο ικανοποιεί τους βασικούς επιχειρηματικούς και τεχνικούς στόχους.
- Επαλήθευση ότι οι τεχνολογίες που επελέγησαν ανταποκρίνονται στις παραμέτρους και στόχους του σχεδίου.
- Επαλήθευση ότι υπάρχει πάροχος που θα παράσχει την υπηρεσία που ζητάμε μέσα στα πλαίσια του κόστους που έχουμε εκτιμήσει.
- Εντοπισμός τυχόν προβλημάτων συνδεσιμότητας ή συμφόρησης.
- Έλεγχος του προβλεπόμενου πλεονασμού.
- Σενάρια κατάρρευσης ζεύξεων και κόμβων, και εκτίμηση των επιπτώσεών τους στην απόδοση του δικτύου.
- Καθορισμός κάποιων τεστ (εάν δεν υπάρχουν ήδη) για δημόσια αξιολόγηση του σχεδίου, ώστε να εγκριθεί από τον πελάτη.
- Έγκριση από τον πελάτη (και ει δυνατόν από το αρμόδιο προσωπικό διαχείρισης) για το σχέδιο.
- Καθορισμός φάσεων δοκιμαστικής λειτουργίας.
- Εκτίμηση χρόνου εργασιών για την εγκατάσταση και δοκιμαστική λειτουργία.

Ως προς την επιλογή των επί μέρους δικτυακών στοιχείων – ιδίως μεταγωγέων και δρομολογητών – εκτός από τις προδιαγραφές τους και δημοσιευμένα αποτελέσματα αξιολόγησης και ελέγχων των κατασκευαστών, είναι χρήσιμο να ανατρέξουμε σε ανεξάρτητους φορείς ή οργανισμούς που έχουν ήδη κάνει παρόμοιους ελέγχους. Έτσι, βεβαιώνουμε άμεσα και στον μέγιστο δυνατό βαθμό ότι η επιλογή μας θα ανταποκριθεί στο έργο για το οποίο την προορίζουμε.

Από εκεί και μετά, υπάρχουν δύο βασικοί τρόποι που γενικά μπορούν να χρησιμοποιηθούν για τον έλεγχο του σχεδίου μας πριν προχωρήσουμε στην υλοποίησή του.

Ο πρώτος έχει να κάνει με την προσομοίωση ενός μοντέλου του νέου δικτύου. Το βασικό πλεονέκτημα είναι ότι μία τέτοια προσέγγιση έχει χαμηλό κόστος, αλλά η ακρίβεια των αποτελεσμάτων εξαρτάται από την ακρίβεια του μοντέλου και των συνθηκών που προσομοιώνονται. Δεν θα επεκταθούμε περισσότερο, δεδομένου ότι υπήρξε διεξοδική παρουσίαση σε προηγούμενο κεφάλαιο.

Ο δεύτερος τρόπος στηρίζεται στην υλοποίηση ενός πρωτοτύπου. Αυτό είναι ένα κατάλληλο, πραγματικό δίκτυο, το οποίο πλησιάζει ως έναν βαθμό το σχέδιο του νέου μας δικτύου, χωρίς όμως και να είναι το ίδιο, ώστε να μπορούμε να ελέγξουμε το ορθόν της λειτουργικότητας του νέου δικτύου. Εφόσον πρόκειται για πραγματικό δίκτυο, περιλαμβάνει την δέσμευση και χρήση πραγματικού δικτυακού υλικού, το οποίο πρέπει να είναι, είτε διαθέσιμο, είτε να μπορούμε να το προμηθευθούμε για τους σκοπούς μας. Μπορεί δε να είναι ένα δίκτυο σε ένα εργαστήριο ή και ενσωματωμένο στο αρχικό δίκτυο που επιχειρούμε να αναβαθμίσουμε. Φυσικά, στην τελευταία περίπτωση θα πρέπει να ληφθούν επιπρόσθετες προφυλάξεις και να υπάρξει έγκαιρη και ενδελεχής ενημέρωση των χρηστών για ενδεχόμενα προβλήματα. Ακόμα και τότε όμως, ο χρόνος πειραματισμού δεν μπορεί να είναι μεγάλος – ιδίως όταν υπάρχουν εμφανείς ενδείξεις προβλημάτων στους χρήστες – μια και η αρχική ανεκτικότητα δίνει την θέση της σε απόρριψη, εφόσον συνεχίζουν να υπάρχουν προβλήματα.

Οι έλεγχοι που πρέπει να πραγματοποιηθούν πρέπει να έχουν μελετηθεί και καταγραφεί λεπτομερειακά από πριν, ώστε να υπάρχει ο μέγιστος βαθμός οργάνωσης και συγκροτημένης προσπάθειας. Εννοείται πως οι έλεγχοι πρέπει να είναι προσαρμοσμένοι στους στόχους που είχαν τεθεί. Για παράδειγμα, εάν ένας στόχος ήταν ότι ο οποιοσδήποτε υπολογιστής στο εσωτερικό δίκτυο θα πρέπει να έχει την απόκριση από ένα αίτημα στην εφαρμογή εξυπηρέτη για δέσμευση αιθουσών σε 2 το πολύ δευτερόλεπτα, είναι ανάγκη να πραγματοποιηθούν σχετικές μετρήσεις κατά τις ώρες λειτουργίας αιχμής του δικτύου.

Μερικά κλασικά τεστ με τις αντίστοιχες μετρήσεις είναι τα παρακάτω:

- Χρόνος απόκρισης δικτυακής εφαρμογής.
- Ρυθμαπόδοση συγκεκριμένων εφαρμογών.
- Διαθεσιμότητα – Εδώ συνήθως γίνονται μετρήσεις για τουλάχιστον ένα εικοσιτετράωρο, ώστε να μετρηθούν πιθανά σφάλματα, καθυστερήσεις ή και μη απαντήσεις – ιδίως σε συνθήκες υψηλού φόρτου του δικτύου, σε εργάσιμες ημέρες.
- Έλεγχος για το εάν οι παλαιότερες δικτυακές εφαρμογές και υπηρεσίες λειτουργούν κανονικά ή έχουν ξαφνικά προβλήματα.

Εάν απαιτείται η εγκατάσταση νέου υλικού ή λογισμικού ή ο προγραμματισμός νέου προκειμένου να πραγματοποιηθούν οι μετρήσεις, πρέπει όλα αυτά να ολοκληρώνονται προτού ξεκινήσει η διαδικασία. Παράλληλα πρέπει να καταγραφούν εκ των προτέρων όλα τα τεστ που πρόκειται να διεξαχθούν, με αναλυτικό τρόπο περιγραφής, καθώς και των ορίων των τιμών των αντίστοιχων μετρικών, που θεωρούμε ότι εκφράζουν επιτυχημένο αποτέλεσμα.

Έτσι, θα μπορούμε να εκτιμήσουμε το κόστος για την προμήθεια των κατάλληλων εργαλείων, αλλά και του χρόνου που απαιτείται για την ολοκλήρωση του ελέγχου.

Συνηθισμένους τύπους τέτοιων εργαλείων εξετάσαμε εν πολλοίς στα προηγούμενα κεφάλαια. Αυτοί περιλαμβάνουν γεννήτριες δικτυακής κίνησης, εργαλεία διαχείρισης δικτύου, καθώς και αναλυτές δικτυακής κίνησης.

Μετά από την πραγματοποίηση των παραπάνω, ενδεχομένως να χρειάζεται μία ενδιάμεση φάση: αυτή της επιδιόρθωσης των προβλημάτων που έχουν ανιχνευθεί, καθώς και του σχεδίου του νέου δικτύου. Στην συνέχεια, ίσως χρειάζεται να επαναληφθούν τα τεστ προκειμένου να επιβεβαιωθεί το επιθυμητό επίπεδο λειτουργικότητας και η ορθότητα του σχεδιασμού.

Εφόσον κάτι τέτοιο συμβεί, το νέο σχέδιο οριστικοποιείται και μαζί με τα αποτελέσματα των ελέγχων παρουσιάζεται στον πελάτη για την τελική έγκριση.

Κατόπιν, προχωράμε στην προμήθεια και εγκατάσταση του νέου εξοπλισμού και λογισμικού, έχοντας προηγουμένως ενημερώσει τους χρήστες για οποιαδήποτε ενέργεια υπάρχει πιθανότητα εμφάνισης προβλημάτων, καθώς και για το αναμενόμενο χρονικό διάστημα ολοκλήρωσης της ενέργειας αυτής.

Με την ολοκλήρωση της υλοποίησης του σχεδίου μας, προχωράμε στην δοκιμαστική λειτουργία του νέου δικτύου, με ελέγχους ορθής λειτουργίας, έχοντας και πάλι ενημερώσει τους χρήστες σχετικά. Η φάση αυτή είναι παρόμοια με τα όσα αναφέρθηκαν λίγο παραπάνω. Παράλληλα προχωράμε στην τεκμηρίωση του δικτύου μας.

Τέλος, μπορεί να υπάρχει και μία φάση, κατά την οποία ενδεχομένως να προσπαθήσουμε να βελτιώσουμε την απόδοση του νέου μας δικτύου, με τεχνικές όπως πολυεκπομπή IP, traffic engineering, κλπ.

10.8. Συγκεντρωτισμός και Αποκέντρωση

Όπως σε όλες τις μορφές οργάνωσης ενός συστήματος, έτσι και στην διαχείριση δικτυακών συστημάτων υπάρχουν δύο βασικές κατηγορίες για την δόμηση της ιεραρχίας.

Η πρώτη κατηγορία έχει ως βασικό χαρακτηριστικό τον συγκεντρωτισμό. Εδώ έχουμε ένα σημείο, άνθρωπο ή οντότητα που αποτελεί το κέντρο του ελέγχου. Για παράδειγμα, μπορεί να έχουμε δύο ή περισσότερους εξυπηρέτες DNS, αλλά όλοι ελέγχονται από μία οντότητα.

Η δεύτερη κατηγορία έχει ως βασικό χαρακτηριστικό την αποκέντρωση. Εδώ ο έλεγχος κατανέμεται σε περισσότερες οντότητες. Για παράδειγμα, αντί να υπάρχει ένας ή δύο εξυπηρέτες DNS για το Πανεπιστήμιο Μακεδονίας (όπως σήμερα), θα μπορούσαν να υπάρχουν επιπρόσθετοι εξυπηρέτες DNS σε κάθε τμήμα του

πανεπιστημίου. Τότε, υπεύθυνος για κάθε επί μέρους εξυπηρέτη DNS θα ήταν και διαφορετικός διαχειριστής, ο οποίος θα ανήκε στο τεχνικό προσωπικό του κάθε τμήματος.

Με λίγα λόγια, με τον συγκεντρωτισμό ο κύριος στόχος είναι να βελτιώσουμε την αποδοτικότητα της διαχείρισης, εκμεταλλευόμενοι την δυνατή οικονομία κλίμακος και πετυχαίνοντας μεγαλύτερη αξιοπιστία με την μείωση των περιπτώσεων σφαλμάτων, αφού δεν επεμβαίνουν πολλοί στην διαχείριση.

Από την άλλη, με την αποκέντρωση προσπαθούμε να βελτιώσουμε την ταχύτητα και την ευελιξία της διαχείρισης, αυξάνοντας τον τοπικό έλεγχο.

Ποια είναι καλύτερη; Δεν υπάρχει απόλυτα καλή ή κακή, αλλά εξαρτάται από την κάθε περίπτωση. Με την αποκέντρωση έχουμε μία συνομοσπονδία, όπου κάθε επί μέρους 'περιοχή' του συστήματος είναι εν πολλοίς ανεξάρτητη, υποχρεωμένη να υπακούει σε ελάχιστους κανόνες ως προς τις σχέσεις της με τις γειτονικές 'περιοχές' ευθύνης.

Με την συγκέντρωση (ή κεντρικοποιημένη προσέγγιση) προχωράμε στην συνένωση των επί μέρους ομάδων για να επιτύχουμε μία ενιαία τάξη για το γενικότερο καλό. Αλλά είναι μία διαδικασία ισοπέδωσης, αφού δεν μπορούν να υπάρχουν διπλά συστήματα με διαφορές ως προς την φιλοσοφία και τις ενέργειες διαχείρισης.

Στην συνέχεια εξετάζουμε τους καταλληλότερους τρόπους για να προχωρήσουμε από την μία, στην άλλη κατηγορία.

10.8.1. Οι Βασικές Αρχές για Συγκεντρωτική ή Αποκεντρωμένη Αναδιοργάνωση

Για να προχωρήσουμε στην αναδιοργάνωση της διαχείρισης ενός συστήματος, είτε προς συγκέντρωση, είτε προς αποκέντρωση, πρέπει να υπάρχουν σημαντικοί λόγοι και προϋποθέσεις. Τέτοιοι λόγοι και προϋποθέσεις μπορούν να είναι οι παρακάτω (Limoncelli, Hogan, & Chalup, 2007):

- *Επίλυση προβλήματος*. Σημαίνει ότι θα πρέπει να γνωρίζουμε το ακριβές πρόβλημα που προσπαθούμε να επιλύσουμε. Επίσης θα πρέπει να το μεταφέρουμε με σαφή τρόπο στους λοιπούς διαχειριστές της ομάδος μας, όχι μόνον για να το γνωρίζουν, αλλά και για να πουν την γνώμη τους. Εάν, τελικά, δεν επιλύουμε κάποιο συγκεκριμένο πρόβλημα ή δεν είναι πραγματικά αναγκαίο, καλό είναι να σταματήσουμε και να μην προχωρήσουμε.
- *Κίνητρο*. Ποιο είναι το πραγματικό κίνητρο; Είναι τεχνικής φύσεως ή έχει να κάνει με εσωτερική πολιτική; Προσπαθούμε να βελτιώσουμε την καθημερινότητα της διαχείρισης ή την δική μας (κάτι απόλυτα φυσιολογικό); Ή μήπως προσπαθούμε να αποκτήσουμε καλύτερη εικόνα στα μάτια της Διοίκησης;
- *Εμπειρία*. Μερικές φορές η εμπειρία, παρά συγκεκριμένες μετρήσεις, είναι αυτό που χρειάζεται. Οι εμπειρικοί κανόνες άλλωστε προκύπτουν ακριβώς έτσι.
- *Συμμετοχή χρηστών*. Η γνώμη και οι προσδοκίες των χρηστών ενός συστήματος μπορεί να μην είναι ο αποκλειστικός κανόνας που οδηγεί έναν διευθυντή ή διαχειριστή, αλλά πρέπει να λαμβάνονται σοβαρά υπ' όψιν, αφού η αναδιοργάνωση έχει συνήθως επιπτώσεις που τους αφορούν.
- *Ρεαλισμός*. Ουσιαστικά είναι το «μη δίνετε υποσχέσεις που δεν μπορείτε να τηρήσετε». Εάν, για παράδειγμα, ένας νέος δρομολογητής υπόσχεται να βελτιώσει αποδοτικά την απόδοση του δικτύου μας, επειδή έτσι ισχυρίζεται ο κατασκευαστής, αλλά υπό την προϋπόθεση ότι θα προχωρήσουμε σε συγκεντρωτισμό του δικτυακού ελέγχου, μπορεί να μην προκύψει κάτι τέτοιο στην πράξη. Αλλά ακόμα και εάν προκύψει κάτι τέτοιο, να οφείλεται στην αναδιοργάνωση και όχι στον νέο δρομολογητή.
- *Ισορροπία*. Ως συνήθως, η βέλτιστη επιλογή βρίσκεται σε κάποιο σημείο μεταξύ των άκρων. Ποιο είναι το σημείο ισορροπίας μεταξύ συγκεντρωτισμού και αποκέντρωσης είναι δύσκολο να βρεθεί. Ενίοτε δεν είναι και σταθερό, αλλά μετατοπίζεται ανάλογα με τις συνθήκες. Οπωσδήποτε όμως δεν πρέπει να φθάνουμε και εμείς στα άκρα ως προς την προσπάθεια να βρούμε αυτό το σημείο. Πιο συγκεκριμένα, είναι σφάλμα να μην κάνουμε απολύτως τίποτε, αλλά εξ ίσου και το να είμαστε τελειομανείς, αναζητώντας το τέλειο. Πρέπει να προχωρούμε με τις παρούσες και επικείμενες (σε μικρό χρονικό διάστημα) συνθήκες και ανάγκες, και όχι να σχεδιάζουμε για το απώτερο μέλλον, αναβάλλοντας διαρκώς την τελική απόφαση.

- *Πρόσβαση*. Το να έχουμε έναν συγκεντρωτικό τρόπο για όλα τα ζητήματα είναι χρήσιμο επειδή η τυποποίηση βοηθά στην αποφυγή παρεξηγήσεων και σφαλμάτων. Από την άλλη όμως, ο συγκεντρωτικός τρόπος οδηγεί σε μονολιθική αντιμετώπιση, ενώ συνήθως δεν υπάρχει μία προσέγγιση που να επιλύει τα πάντα αποδοτικά. Άλλωστε, ποτέ δεν ανήκουν όλοι οι χρήστες σε μία και μόνον κατηγορία.
- *Καθόλου πίεση*. Η αναθεώρηση της οργάνωσης σε περισσότερη συγκέντρωση ή αποκέντρωση είναι όπως η δημιουργία και παροχή μίας νέας υπηρεσίας. Συνεπώς χρειάζεται μεγάλη προσοχή, έλεγχοι και συντονισμός για να πετύχει. Άρα χρειάζεται να γίνεται ομαλά και όχι υπό καθεστώς πιέσεως.
- *Βεβαιότητα 110%*. Κάθε νέο σύστημα ή υπηρεσία δεν κερδίζει άμεσα την εμπιστοσύνη των χρηστών του. Και επειδή η αρχή είναι το ήμισυ του παντός, πρέπει να διασφαλίσουμε ότι θα φανεί να επιτυγχάνει με την πρώτη. Διαφορετικά θα υπάρξουν επιπτώσεις, με μεγαλύτερη εκείνη που έχει να κάνει με την φήμη μας. Άπαξ και καταρρακωθεί, είναι πολύ δύσκολο να την επαναφέρουμε στην προηγούμενη κατάσταση.
- *Δικαίωμα αρνησικυρίας (βέτο)*. Αν και πρέπει να ακούμε τους χρήστες, ο έλεγχος ως δικαίωμα, αλλά και ως ευθύνη, ανήκει στους διαχειριστές. Η δομή της εταιρείας σαφώς επηρεάζει την απόφαση για περισσότερη συγκέντρωση ή αποκέντρωση. Τα μεγαλύτερα εμπόδια δεν είναι τεχνικής φύσεως, αλλά οι αποφάσεις της διοίκησης και η πολιτική. Ακόμα πιο δύσκολα είναι τα πράγματα όταν υπάρχει έλλειψη εμπιστοσύνης. Πάντως, ο τελικός στόχος είναι η παροχή υπηρεσιών υψηλού επιπέδου στους χρήστες.

Στις επόμενες ενότητες θα δούμε πιο αναλυτικά τις κύριες περιπτώσεις κατά τις οποίες είναι συνήθως σκόπιμο να εξετάσουμε την σκοπιμότητα μετάβασης από αποκεντρωμένη οργάνωση σε πιο συγκεντρωτική, καθώς και το αντίστροφο.

10.8.2. Από Αποκεντρωμένη σε Συγκεντρωτική Οργάνωση

Κάθε διαχειριστής έχει την (φυσιολογική) ανθρώπινη τάση να βρίσκει ευκαιρίες για να κεντρικοποιήσει τις διάφορες διαδικασίες και υπηρεσίες. Βέβαια, αυτός ο συγκεντρωτισμός δεν βελτιώνει κατ' ανάγκην την απόδοση. Εν τούτοις, δίδει την ευκαιρία για εισαγωγή οικονομίας κλίμακος σε διάφορες διαδικασίες. Στην πραγματικότητα, αυτό που βελτιώνει την απόδοση είναι η τυποποίηση, που συνήθως είνα παρα-προϊόν της κεντρικοποίησης.

Η μείωση κόστους προέρχεται από την υπόθεση ότι θα υπάρχει μικρότερη επιβάρυνση σε σχέση με το συνολικό κόστος από τις επιβαρύνσεις για κάθε υπο-ενέργεια που εκτελείται αποκεντρωμένα για να μας δώσει το ίδιο ισοδύναμο τελικό αποτέλεσμα. Για παράδειγμα, είναι ευκολότερο για κάποιον διαχειριστή να διαχειρίζεται πολλούς δρομολογητές του ιδίου μοντέλου, της ίδιας εταιρείας, αντί για διάφορα μοντέλα από πολλές εταιρείες.

Η ψυχολογία παίζει σημαντικό ρόλο. Εάν αφαιρέσουμε τον έλεγχο από έναν διαχειριστή, θα το δεχθεί ή θα προσπαθήσει να υποσκάψει την προσπάθεια; Θα πεισθούν οι εμπλεκόμενοι ότι η νέα οργάνωση θα είναι καλύτερη από την προηγούμενη;

Επιλέγοντας κατάλληλες υπηρεσίες για συγκεντρωτική οργάνωση ως προς την διαχείριση, οι πιθανότητες επιτυχίας είναι μεγαλύτερες. Μερικά τέτοια παραδείγματα είναι τα παρακάτω:

- *Διαχείριση κατανεμημένων συστημάτων*. Π.χ., κάθε τμήμα του Πανεπιστημίου Μακεδονίας έχει τον δικό του εξυπηρέτη web, καθώς και έναν αριθμό από μεταγωγείς (switches) ορόφων. Αντί να είναι διαφορετικού τύπου και να διαχειρίζονται πλήρως από το τοπικό προσωπικό, οι μεν εξυπηρέτες web είναι του ιδίου τύπου και με ίδια ή παρόμοια διευθέτηση, ενώ οι μεταγωγείς ορόφων ελέγχονται αποκλειστικά από το κέντρο διαχείρισης δικτύων του πανεπιστημίου. Εάν χρειασθεί αναβάθμιση του λογισμικού στους εξυπηρέτες μπορεί να γίνει η ίδια σε όλους. Αυτό σημαίνει οικονομία σε χρόνο.
- *Εδραίωση υπηρεσιών σε λιγότερους υπολογιστές*. Για λόγους αξιοπιστίας κάθε υπηρεσία μπορεί να προσφέρεται από διαφορετικό υπολογιστή. Για να μειώσουμε τα έξοδα, όμως, μπορούμε να εγκαταστήσουμε περισσότερες υπηρεσίες σε έναν ισχυρό υπολογιστή. Με την έλευση των Storage Area Network (SAN) άλλαξε η μορφή του αποθηκευτικού χώρου. Δεν έχει πλέον ο

κάθε υπολογιστής-εξυπηρέτης τον δικό του αποθηκευτικό χώρο (που μπορεί να είναι εν μέρει γεμάτος), αλλά υπάρχει ένας κοινός (μέσω του δικτύου εδικού σκοπού όπως ένα SAN), οπότε η χρήση του είναι συνολικά πιο αποδοτική όταν χρησιμοποιείται από πολλαπλούς υπολογιστές. Η εικονικοποίηση των εξυπηρετών (server virtualization) άλλαξε το τοπίο ακόμα περισσότερο, αφού τώρα μπορεί να φορτώνεται ένας εικονικός εξυπηρέτης για κάποιο χρονικό διάστημα και μετά να τερματίζεται, μειώνοντας το κόστος σε σχέση με ένα αποκλειστικό μηχάνημα για μία εταιρία. Από την άλλη, ο συνδυασμός των παραπάνω οδήγησε σε ένα σύμπλεγμα από εικονικούς υπολογιστές, οι οποίοι μπορούν να μετακινούνται από το λογισμικό διαχείρισης σε διάφορους φυσικούς υπολογιστές του συμπλέγματος για λόγους εξισορρόπησης φόρτου. Η συντήρηση και διαχείριση τέτοιου κεντρικοποιημένου συστήματος είναι σχετικά μικρότερη σε κόστος (οποιασδήποτε μορφής) σε σχέση με ένα αποκεντρωμένο.

- *Εξειδίκευση*. Όταν γίνεται αναθεώρηση της οργάνωσης της διαχείρισης, ο στόχος μπορεί να είναι η μείωση κόστους. Από την άλλη όμως μπορεί να υπάρχει ανάγκη για εξειδικευμένη τεχνική κατάρτιση για υποστήριξη, είτε διαφορετικών ομάδων χρηστών, είτε υλικού και λογισμικού. Εάν όμως, το τελευταίο προχωρήσει στα άκρα, μπορεί να καταλήξει στο να υπάρχουν πάρα πολλά μέλη στην τεχνική ομάδα, το καθένα εκ των οποίων ειδικεύεται μόνον σε ένα αντικείμενο. Επομένως η μείωση του κόστους δεν είναι τόσο σημαντική όπως φαινόταν πριν την αναδιοργάνωση.
- *Κοινές προμήθειες και κοινά αγαθά*. Όταν υπάρχει συγκεντρωτική οργάνωση διαχείρισης, τότε μπορεί να επιτευχθεί οικονομία κλίμακος και από το γεγονός ότι οι προμήθειες εξοπλισμού γίνονται από ένα κεντρικό σώμα σε μεγαλύτερες ποσότητες, άρα (συνήθως) σε καλύτερες τιμές ή όρους προμήθειας εν γένει. Όταν μάλιστα ένα μέρος του εξοπλισμού δεν είναι κάτι το εξωτικό, αλλά κάτι που πλέον χρησιμοποιούν ως κοινό αγαθό πολλοί χρήστες, τότε αποτελεί καλό υποψήφιο για συγκέντρωση της διαχείρισής του. Ένα τέτοιο παράδειγμα μπορεί να είναι ο αποθηκευτικός χώρος όλων των χρηστών υπολογιστών σε ένα πανεπιστήμιο, όπου όλοι χρησιμοποιούν ένα SAN μέσω του τοπικού δικτύου.

10.8.3. Από Συγκεντρωτική σε Αποκεντρωμένη Οργάνωση

Εδώ έχουμε την ακριβώς αντίθετη προσέγγιση. Συνηθισμένο επιχείρημα είναι ότι με σωστή αποκέντρωση επιτυγχάνεται ταχύτερος χρόνος απόκρισης. Άλλα επιχειρήματα είναι η ευελιξία που προέρχεται από την αυτονομία, παροχή εξειδικευμένης υποστήριξης κοντά στις τοπικές ανάγκες («μπορεί να μην είναι οι καλύτεροι τεχνικοί, αλλά είναι *οι δικοί μας* τεχνικοί»), ο 'εκδημοκρατισμός' της οργάνωσης ή απλά η σχετική ανεξαρτησία.

Ορισμένοι καλοί υποψήφιοι για αναθεώρηση της οργάνωσης διαχείρισης από συγκεντρωτική σε αποκεντρωμένη, είναι οι παρακάτω:

- *Ανοχή σε σφάλματα*. Εάν υπάρχει ένα κεντρικό σημείο ελέγχου, τότε αποτελεί και μοναδικό σημείο αποτυχίας. Για παράδειγμα, εάν διακοπεί η δικτυακή επικοινωνία με το Data Center όπου υπάρχει ο κοινός αποθηκευτικός χώρος και κύριοι εξυπηρέτες ενός συγκεντρωτικά οργανωμένου συστήματος, δεν θα υπάρχει πρόσβαση των χρηστών στα αρχεία τους, στο e-mail, κλπ.
- *Εξατομίκευση*. Ορισμένες ομάδες χρηστών μπορεί να έχουν ορισμένες ιδιαιτερότητες σε σχέση με τους υπόλοιπους που χρειάζονται σταθερότητα. Για παράδειγμα, μία ερευνητική ομάδα που έχει να κάνει με πειραματισμούς σε δικτυακή τεχνολογία.
- *Καλύτερη ανταπόκριση σε αιτήματα χρηστών*. Μπορεί κάποιες φορές αρκετοί χρήστες να παραπονούνται ως προς το επίπεδο ή μορφή υποστήριξης που λαμβάνουν, αποτεινόμενοι σε ένα κεντρικό helpdesk. Μετά από εξέταση των παραπόνων, ίσως προκύψει ότι το να υπάρχουν επί μέρους helpdesk σε διάφορα τμήματα (π.χ., πανεπιστημίου), καλύπτει ταχύτερα και αποδοτικότερα τα αιτήματα αυτά σε μεγάλο βαθμό. Επιπλέον, η εμπειρία που αποκτάται από την φύση των αιτημάτων είναι προσαρμοσμένη καλύτερα και στις τοπικές ανάγκες.

Άλλα επιχειρήματα μπορεί να περιλαμβάνουν την διαφοροποίηση ως εναλλακτική μορφή παροχής υπηρεσιών. Για παράδειγμα, εάν προκύψει κάποιος ιός ή 'τρύπα' στο λειτουργικό σύστημα των δρομολογητών

μίας εταιρίας μέσω του οποίου κακόβουλοι χρήστες ή εισβολείς οδηγούν τους δρομολογητές στο να σταματήσουν να λειτουργούν, το υπόλοιπο δίκτυο μπορεί να συνεχίσει να λειτουργεί κανονικά επειδή ένα μέρος του χρησιμοποιεί δρομολογητές με άλλο λειτουργικό σύστημα.

10.8.4. Webmaster

Υπάρχουν πολλές δικτυακές υπηρεσίες οι οποίες μπορούν να θεωρηθούν σημαντικές. Ανάμεσά τους ξεχωρίζει η υπηρεσία ιστού, λόγω της δημοτικότητάς της, αλλά και της ποικιλίας των μορφών πληροφορίας και δεδομένων που μπορούν να διακινηθούν μέσω αυτής.

Εδώ ο ρόλος του λεγόμενου webmaster είναι πρωταρχικός. Ο webmaster διαχειρίζεται το περιεχόμενο του ιστοτόπου, όπως ο εκδότης ενός περιοδικού. Αυτός είναι εκείνος που καθορίζει την πολιτική του ιστοτόπου. Συχνά υπάρχει σύγχυση με τον διαχειριστή του υπολογιστή όπου βρίσκεται ο εξυπηρέτης, αλλά και με τον διαχειριστή του εξυπηρέτη ιστού αυτού καθαυτού.

Ο πρώτος είναι αυτός που είναι υπεύθυνος για τον ίδιο τον υπολογιστή, το λειτουργικό του σύστημα, καθώς και τις άδειες ή εξουσιοδοτήσεις που παρέχει ώστε κάποιοι ειδικοί χρήστες να μπορούν να εγκαταστήσουν κάποιο λογισμικό και να χρησιμοποιήσουν αντίστοιχο αποθηκευτικό χώρο.

Ο δεύτερος είναι εκείνος που εγκαθιστά το λογισμικό του εξυπηρέτη ιστού και είναι υπεύθυνος για την καλή του λειτουργία, αναβάθμιση και συχνά δημιουργία αντιγράφων ασφαλείας. Αυτός δημιουργεί ανάμεσα στα άλλα και έναν λογαριασμό για τον webmaster, ο οποίος είναι υπεύθυνος για το περιεχόμενο του ιστοτόπου όπως αναφέρθηκε παραπάνω.

Η σύγχυση οφείλεται στο ότι σε μικρούς σχετικά ιστοτόπους, οι τρεις παραπάνω ρόλοι μπορεί να υλοποιούνται από ένα πρόσωπο.

Εάν συμβαίνει κάτι τέτοιο, ο φόρτος μπορεί να υπερβολικός εφόσον επιτρέπεται σε χρήστες να αναρτούν δικό τους περιεχόμενο, εάν η ανάρτηση γίνεται από τον webmaster μετά από αποστολή του περιεχομένου από τους χρήστες.

Ένας τρόπος για να μειωθεί αυτός ο φόρτος είναι η ανάρτηση αυτή καθαυτή να γίνεται από τους ίδιους τους χρήστες. Η δομή του ιστοτόπου, ο ακριβής χώρος σε αυτόν όπου θα γίνονται οι αναρτήσεις των χρηστών, καθώς και οι όποιες διαδικασίες και δικλείδες ασφαλείας, θα πρέπει να δημιουργηθούν από τον webmaster. Από εκεί και μετά όμως τα υπόλοιπα θα γίνονται αυτόματα, χωρίς να χρειάζεται η παρέμβασή του.

Στην δυσάρεστη όμως περίπτωση που ένας webmaster πρέπει να κάνει και τις αναρτήσεις ιστοσελίδων είναι σκόπιμο να δημιουργηθεί και συμφωνηθεί μία σχετική πολιτική περί του τι επιτρέπεται να αναρτάται, ώστε να μην βρεθεί προ δυσάρεστων εκπλήξεων αργότερα. Παράδειγμα τέτοιων εκπλήξεων είναι ο χρόνος του αιτήματος ανάρτησης (π.χ., λίγο πριν την λήξη του εργάσιμου ωραρίου) και η διάρκειά του (μπορεί να χρειάζεται και ώρες). Ένα άλλο ζήτημα φυσικά είναι και η ευθύνη για το περιεχόμενο που αναρτάται.

Και εδώ, όπως και σε άλλες υπηρεσίες, απαιτείται η ύπαρξη SLA, μαζί με αντίστοιχη παρακολούθηση για να διαπιστώνεται η συμμόρφωση με αυτήν. Φυσιολογικά, πρέπει να υπάρχει μνεία και περιόδων με αντίστοιχες διαδικασίες για συντήρηση. Η απόδοση συνήθως μετράται στον μέσο χρόνο που χρειάσθηκε για να εξυπηρετηθεί το αίτημα για κάποια ιστοσελίδα, εφόσον υπήρχε συγκεκριμένος φόρτος στο σύστημα.

Το λογισμικό ενός εξυπηρέτη ιστού δεν είναι πάντοτε της ιδίας μορφής, αφού μπορεί να εστιάζεται στην παροχή δεδομένων διαφορετικής μορφής. Έτσι, εάν προορίζεται για παροχή συνηθισμένων ιστοσελίδων ή έστω δυναμικών ιστοσελίδων με δεδομένα από συνδεδεμένη βάση δεδομένων, είναι πολύ διαφορετικός ως στόχος, σε σχέση με την περίπτωση που αντιστοιχεί σε παροχή πολυμεσικού περιεχομένου (π.χ., βίντεο). Στην τελευταία περίπτωση μπορεί να υπάρχουν διαδοχικές αιτήσεις για το ίδιο βίντεο, οπότε δεν ανακτάται όλο το βίντεο για αποστολή για κάθε αίτηση, αλλά μπορεί να γίνει βελτιστοποίηση με ταυτόχρονη εξυπηρέτηση των αιτήσεων, π.χ., με chaining, patching ή και με caching. Ειδικά για βιντεοροή (video streaming) συνηθίζεται πλέον και η τεχνική DASH όπως είδαμε σε προηγούμενο κεφάλαιο.

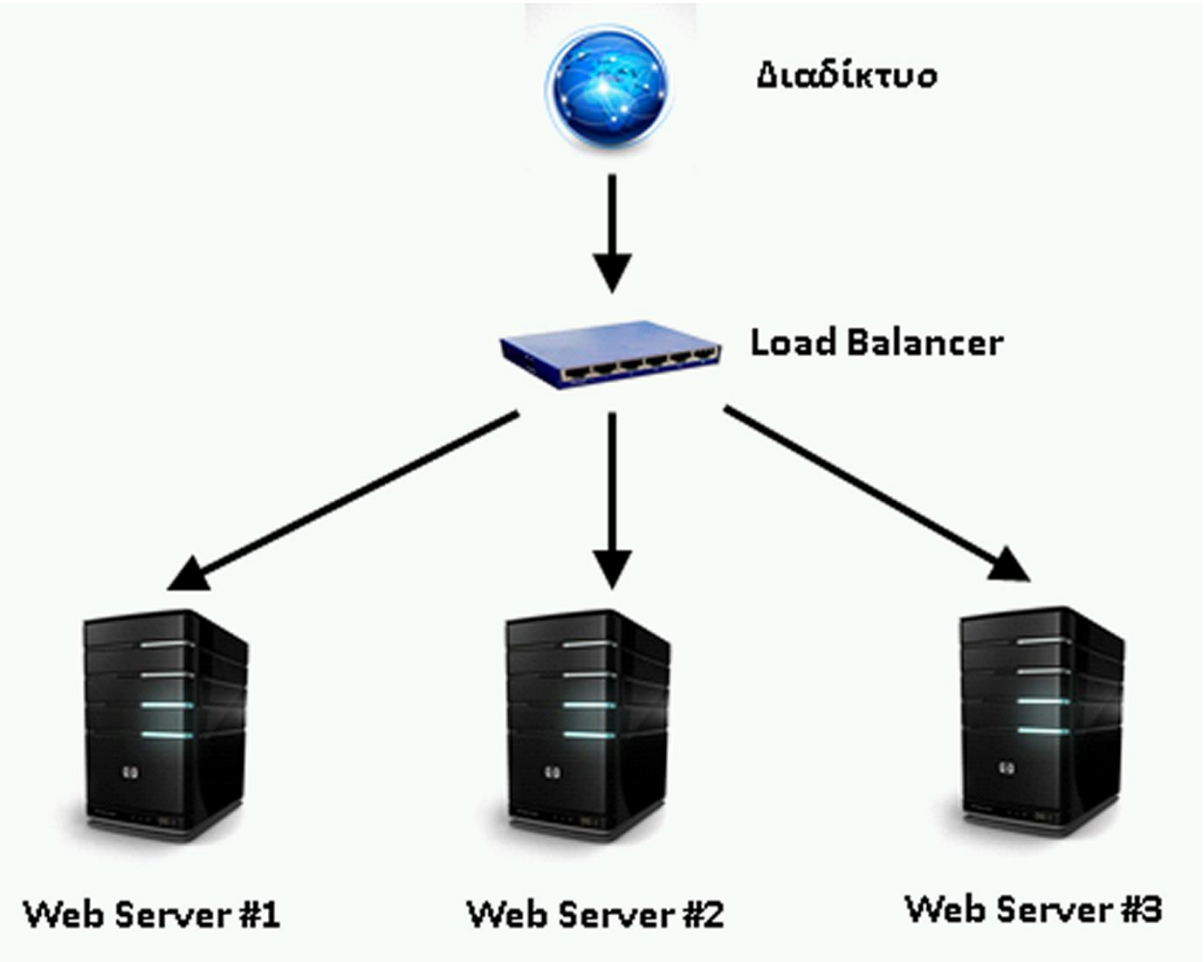
Μία αξιοσημείωτη δυνατότητα είναι ότι τα σημερινά λειτουργικά συστήματα γενικής χρήσης επιτρέπουν την ανάθεση πολλαπλών διευθύνσεων IP στην ίδια φυσική σύνδεση, αλλά επίσης και ταυτόχρονα την ύπαρξη πολλών ενεργών δικτυακών διεπαφών (άρα και συνδέσεων). Αυτό διευκολύνει την συνύπαρξη πολλαπλών ιστοτόπων στον ίδιο υπολογιστή-εξυπηρέτη. Εάν χρειασθεί να μεταφέρουμε τους ιστοτόπους σε άλλον υπολογιστή, η μεταφορά είναι πολύ εύκολη. Αυτή η δυνατότητα καθίσταται ευκολότερη πλέον σήμερα λόγω της ύπαρξης λογισμικού εξυπηρετών ιστού, όπως ο Apache (Apache Software Foundation, 2015), που υποστηρίζουν την συνύπαρξη πολλών εικονικών ιστοτόπων.

Τέλος, η κλιμάκωση μίας επιτυχημένες υπηρεσίας ιστού είναι κάτι που αργά ή γρήγορα καθίσταται αναγκαία. Υπάρχουν δύο βασικές κατηγορίες κλιμάκωσης:

- **Οριζόντια κλιμάκωση**. Εδώ έχουμε την δημιουργία ενός ή περισσοτέρων αντιγράφων της υπηρεσίας, κατανέμοντας στην συνέχεια τον φόρτο σε όλα τα αντίγραφα. Εάν, για παράδειγμα, έχουμε δύο αντίγραφα του ιδίου ιστοτόπου σε δύο υπολογιστές-εξυπηρέτες, κάθε ένας θα δέχεται τις μισές από τις συνολικές αιτήσεις http. Πώς όμως επιτυγχάνεται αυτή η κατανομή αυτόματα;

  Εδώ μας βοηθά η υπηρεσία DNS, όπου για το ίδιο συμβολικό όνομα υπολογιστή (π.χ., '`www.uom.gr`') έχουμε δύο διευθύνσεις IP. Εάν επιστρέφονται με τυχαία σειρά για κάθε σχετικό αίτημα (ή μία διεύθυνση IP, αλλά εναλλάξ), τότε χρησιμοποιείται η πρώτη από τις διευθύνσεις αυτές από τον πελάτη για να στείλει το σχετικό αίτημα. Αυτό φθάνει στον αντίστοιχο υπολογιστή και έτσι κατανέμεται ο συνολικός φόρτος.

  Αν και απλή, αυτή η μέθοδος παρουσιάζει το μειονέκτημα ότι η επιστρεφόμενη διεύθυνση IP μπορεί να αποθηκεύεται σε σχετική cache του υπολογιστή-πελάτη. Άρα η κατανομή δεν γίνεται εξ ίσου. Επίσης, εάν σταματήσει να λειτουργεί ο ένας υπολογιστής-εξυπηρέτης, οι μισές αιτήσεις θα κατευθύνονται (λόγω DNS) σε αυτόν. Εάν πάλι χρειάζεται να γίνει συντήρηση, θα πρέπει να αφαιρείται η σχετική διεύθυνση από το DNS.



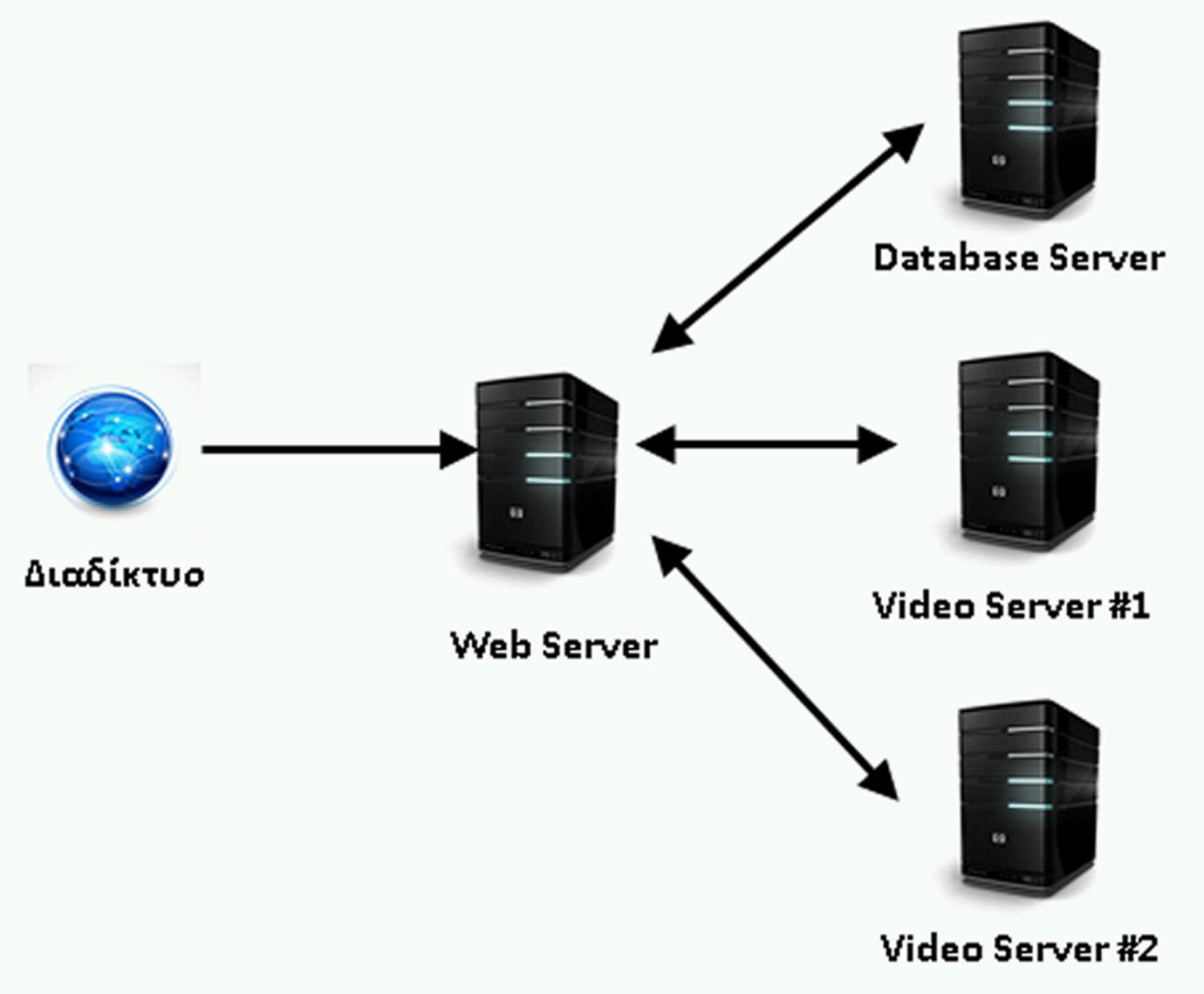
Εικόνα 10.9 *Παράδειγμα οριζόντιας κλιμάκωσης υπηρεσίας ιστού.*

Για τους παραπάνω λόγους, η πιο ενδεδειγμένη – αλλά ακριβότερη – λύση είναι η χρήση ενός εξειδικευμένου υπολογιστή που ονομάζεται *load balancer*, όπως φαίνεται στην Εικόνα 10.9,

όπου κάθε εξυπηρέτης έχει από ένα αντίγραφο του ιδίου ιστοτόπου. Για λόγους αξιοπιστίας χρησιμοποιούνται σε ζεύγη (εάν καταρρεύσει ο ένας, συνεχίζει να λειτουργεί ο άλλος). Τοποθετούνται μεταξύ των πελατών και των εξυπηρετών εν είδη proxy. Ο φυλλομετρητής (browser) του πελάτη στέλνει το αίτημά του στην διεύθυνση του load balancer. Κατόπιν, ο load balancer το προωθεί σε έναν από τους εξυπηρέτες ιστού με διαφανή τρόπο και κάνει το ίδιο για την αντίστοιχη απόκριση. Επίσης, παρακολουθεί τον κάθε εξυπηρέτη, ώστε εάν καταρρεύσει να μην του προωθεί αιτήσεις, ενώ μπορεί να εκτιμά και ποιος εξυπηρέτης έχει τον μικρότερο φόρτο ώστε να κάνει ακόμα καλύτερη κατανομή.

- **Κατακόρυφη κλιμάκωση.** Εδώ η κλιμάκωση δεν αφορά όλον τον ιστότοπο, αλλά μόνον εκείνα τα μέρη που αντιστοιχούν σε περισσότερο φόρτο. Για παράδειγμα (βλ. Εικόνα 10.10), εάν ο ιστότοπος ουσιαστικά είναι μία ταινιοθήκη, το μεγαλύτερο μέρος του φόρτου έχει να κάνει με την μετάδοση των διαφόρων βίντεο και όχι με τις λοιπές ιστοσελίδες. Συνεπώς, τα αρχεία βίντεο θα μπορούσαν να τοποθετηθούν σε ξεχωριστούς υπολογιστές-εξυπηρέτες, με λογισμικό που εξειδικεύεται σε υπηρεσίες βιντεοροής. Μάλιστα, θα μπορούσε να υπάρχει περαιτέρω διάκριση για τα πολύ μικρά βίντεο (trailer) και για τις πλήρεις ταινίες.

Εννοείται φυσικά, ότι μπορούν να υπάρχουν και συνδυασμοί των παραπάνω. Αν και είναι επίσης σημαντικό ζήτημα, δεν επεκτεινόμαστε εδώ σε θέματα ασφάλειας, όπως ασφαλών συνδέσεων, κρυπτογραφίας, ψηφιακών πιστοποιητικών και προστασίας από ιούς και άλλο κακόβουλο λογισμικό.



Εικόνα 10.10 *Παράδειγμα κατακόρυφης κλιμάκωσης υπηρεσίας ιστού.*

10.8.5. Αποθετήριο Λογισμικού

Το αποθετήριο λογισμικού αποτελεί και αυτό μία πολύ σημαντική υπηρεσία που μπορεί να προσφέρει η ομάδα διαχείρισης, όχι μόνον στα μέλη της, αλλά και στο σύνολο των χρηστών του συστήματος. Το αποθετήριο λογισμικού μπορεί να περιέχει μερικές δεκάδες έως και μερικές εκατοντάδες λογισμικού. Το λογισμικό αυτό μπορεί να προέρχεται από τους κατασκευαστές του σχετικού εξοπλισμού (π.χ., drivers συσκευών) ή ακόμα και από διάφορα μέρη από το Διαδίκτυο, αλλά και από τα μέλη της διαχειριστικής ομάδος. Σε όλες τις περιπτώσεις είναι νόμιμο και δωρεάν.

Η ευθύνη της αναζήτησης, διαλογής, δοκιμής, ταξινόμησης και συμπερίληψης αυτού του λογισμικού, ανάμεσα στην πληθώρα που υπάρχει στο Διαδίκτυο, είναι εξαιρετικά μεγάλη και ανήκει στους διαχειριστές. Αυτοί είναι υπεύθυνοι και για την περιοδική ενημέρωση ή αντικατάστασή του.

Η σπουδαιότητά του προκύπτει από το ότι διευκολύνει αφάνταστα κάθε χρήστη του συστήματος κατά την αντιμετώπιση διαφόρων προβλημάτων ή ζητημάτων με την άμεση ανεύρεση του κατάλληλου εργαλείου, χωρίς να χρειάζεται να σπαταλήσει πολύτιμο χρόνο για την ανεύρεσή του. Μάλιστα, μπορεί να μειώσει και το πλήθος αιτημάτων υποστήριξης προς τους διαχειριστές, καθώς και τον χρόνο για την υποστήριξη κάθε χρήστη. Για παράδειγμα, μπορεί κάποιο λογισμικό να είναι ένα διαγνωστικό εργαλείο, το οποίο αυτόματα αναζητεί κάποιους τύπους προβλημάτων στον υπολογιστή του χρήστη και τους επιλύει. Έτσι μειώνεται το πλήθος σχετικών αιτημάτων υποστήριξης.

Ανάλογα με την περίπτωση, μπορεί το λογισμικό αυτό να μην χρειάζεται να εγκατασταθεί στον υπολογιστή του χρήστη, αλλά να εκτελείται απ' ευθείας από το αποθετήριο λογισμικού. Οπωσδήποτε όμως χρειάζεται σωστή ταξινόμηση, καθώς και καλή τεκμηρίωση, ώστε να μπορεί εύκολα ο κάθε χρήστης να καταλάβει την χρησιμότητα, αλλά και τον τρόπο χρήσης του κάθε λογισμικού.

Συνήθως, τοποθεσίες με μικρό μέγεθος δεν έχουν τέτοιο αποθετήριο λογισμικού θεωρώντας ότι είναι περιττό. Στην πράξη όμως πάντα προκύπτει κάποια στιγμή που χρειάζεται ένα λογισμικό που θα έλυνε ένα σχετικά συνηθισμένο πρόβλημα πολύ γρήγορα, αλλά που επειδή δεν είναι διαθέσιμο πρέπει να αναλώσει πολύ χρόνο ο χρήστης για την αναζήτησή του, χωρίς να είναι συχνά αρκετά βέβαιος ή έμπειρος για να εκτιμήσει την χρησιμότητά του.

Γενικά, για να είναι πραγματικά χρήσιμο το αποθετήριο λογισμικού, θα πρέπει να έχει γίνει μία «έρευνα αγοράς». Αυτό σημαίνει ότι πρέπει να έχει γίνει μία έρευνα για το τι πραγματικά χρειάζεται ή προσδοκά να βρει ο χρήστης στις περισσότερες των περιπτώσεων και μετά να προχωρήσουμε στον εμπλουτισμό της.

Φυσική συνέπεια μίας επιτυχημένης τράπεζας λογισμικού είναι η αυξημένη χρήση της, αλλά και η ανάγκη διασφάλισής της από κακόβουλες επιθέσεις, επειδή εάν μολυνθεί, θα μολύνει στην συνέχεια και μεγάλο μέρος των υπολογιστών των χρηστών.

Προκειμένου να εμπλουτισθεί μπορεί να επιτρέπεται για λόγους οικονομίας ανθρωπίνων πόρων και χρόνου σε χρήστες να τοποθετούν αντίστοιχο λογισμικό.

Επομένως, όπως είδαμε σε ανάλογες περιπτώσεις έως τώρα χρειάζεται η δημιουργία σχετικής πολιτικής για την υπηρεσία αυτή:

- Ποιοι επιτρέπεται να κατασκευάζουν και να τοποθετούν πακέτα λογισμικού;
- Ποιοι είναι εκείνοι που εγκρίνουν κάτι τέτοιο κατά περίπτωση (εάν υπάρχουν);
- Τι γίνεται εάν τα άτομα που είναι υπεύθυνα για το λογισμικό λείπουν για αρκετό διάστημα ή εγκαταλείψουν την εταιρεία;
- Ποια λειτουργικά συστήματα υποστηρίζονται; Μήπως πρέπει να έχουμε ένα ξεχωριστό αποθετήριο λογισμικού για κάθε ένα;
- Υπάρχει συγκεκριμένη φόρμα για τον τρόπο με τον οποίον θα πρέπει να γίνεται η ανάρτηση;
- Πώς και από ποιον γίνεται η ανάρτηση ενημερωμένων εκδόσεων λογισμικού;
- Πώς και υπό ποίες συνθήκες γίνεται η διαγραφή από το αποθετήριο λογισμικού;
- Πώς και από ποιον γίνεται η διαχείριση τυχόν σφαλμάτων στο λογισμικό; Από κάποιον διαχειριστή ή απλά μέσω αναφορών από χρήστες που τα διαπίστωσαν;
- Ποιον αφορά το αποθετήριο λογισμικού; Όλους τους χρήστες ή συγκεκριμένες κατηγορίες;
- Ποια είναι η διαδικασία μέσω της οποίας οι χρήστες μπορούν να ζητήσουν την προσθήκη νέου λογισμικού στην τράπεζα; Υπάρχει κάποια επιτροπή για τον σκοπό αυτόν;

Προφανώς η πολιτική αυτή πρέπει να δημοσιοποιείται κατάλληλα ώστε να ενημερωθούν όλοι οι ενδιαφερόμενοι.

10.8.6. Εξωτερικές Αναθέσεις

Μία εξωτερική ανάθεση είναι απλά η διαδικασία κατά την οποία σε μία οντότητα (συνήθως εταιρία) εκτός της δικής μας εταιρίας (ή οργανισμού), αναθέτουμε κάποιες τεχνικές λειτουργίες έναντι αντιτίμου. Ουσιαστικά αποτελεί μία μορφή συγκέντρωσης.

Ένα τέτοιο παράδειγμα είναι κάποιο συμβόλαιο εγγύησης καλής λειτουργίας που μπορεί να έχουμε με μία εταιρία από όπου προμηθευθήκαμε κάποιους δρομολογητές, ότι μέσα σε 8 το πολύ ώρες από τότε που αναφέρθηκε κάποιο πρόβλημα σε αυτούς, θα το έχουν επιλύσει, είτε επισκευάζοντας, είτε αντικαθιστώντας τους προβληματικούς δρομολογητές.

Πιο κλασικά παραδείγματα όμως είναι η ανάθεση δημιουργίας ιστοτόπου, υπηρεσίες απομακρυσμένης πρόσβασης, κλπ. Μία εξωτερική ανάθεση μπορεί να μειώσει το κόστος επειδή ίσως δεν χρειαζόμαστε τέτοιες υπηρεσίες συνέχεια ή με μεγάλο ρυθμό, αλλά και επειδή έτσι μπορεί να μειωθεί η ένταση που θα προέκυπτε, εάν αυτές οι υπηρεσίες ανατίθεντο σε εσωτερικά τμήματα της εταιρίας, λόγω μικροπολιτικής.

Ενώ, γενικά, θεωρείται από πολλούς καλή λύση, στην πραγματικότητα χρειάζεται ιδιαίτερη προσοχή, επειδή μία τέτοια εταιρία δεν είναι υποχρεωμένη να κάνει οτιδήποτε δεν ορίζεται με σαφήνεια στην σχετική σύμβαση. Εάν η εξωτερική ανάθεση αφορά νέες τεχνικές δεξιότητες, οι εκπρόσωποι της εν λόγω εταιρίας θα έχουν μεγαλύτερες τεχνικές ικανότητες, άρα ίσως και μεγαλύτερη ισχύ στις σχετικές διαπραγματεύσεις.

Ταυτόχρονα, για να δηλωθούν ρητά οι απαιτήσεις μας στην σύμβαση θα πρέπει να έχουμε κατανοήσει πολύ καλά τις τεχνικές μας ανάγκες. Εάν όμως η διοίκηση της εταιρίας μας γνώριζε αρκετά καλά τι χρειάζονταν και μπορούσε να το μεταδώσει στο υπάρχον τεχνικό προσωπικό της εταιρίας μας, τότε ίσως δεν θα χρειαζόταν να γίνει εξωτερική ανάθεση.

Τέλος, υπάρχουν και αρκετές περιπτώσεις που η εξωτερική ανάθεση αποφασίζεται από εταιρίες όταν η υποδομή τους (π.χ., δικτυακή) έχει χειροτερεύσει τόσο πολύ ώστε να αποφασίζεται μία τέτοια λύση, ως λύση κατεπείγουσας ανάγκης. Αυτή η τελευταία περίπτωση συνήθως εγκυμονεί περισσότερα προβλήματα αφού συχνά γίνεται υπό καθεστώς πανικού.

Γενικά, μία λογική προσέγγιση είναι παρόμοια με την προμήθεια ενός νέου προϊόντος: μελετάμε στον σχετικό Τύπο για την προσέγγιση αυτή, ενώ ερχόμαστε σε επαφή με αντίστοιχα άτομα από άλλες εταιρείες που έχουν ήδη επιλέξει κάτι τέτοιο, προκειμένου να μας μεταδώσουν τις εμπειρίες τους.

Εφόσον προχωρήσουμε σε μία τέτοια λύση πρέπει οπωσδήποτε να συμπεριλαμβάνουμε στην σχετική σύμβαση τον πλήρη κύκλο τέτοιων υπηρεσιών: σχεδιασμό, εγκατάσταση, συντήρηση, υποστήριξη, απόσυρση, ακεραιότητα σχετικών δεδομένων και ανάνηψη από καταστροφές. Επίσης θα πρέπει να συμπεριλαμβάνονται μετρήσιμες παράμετροι SLA και οι σχετικές ποινές για μη τήρηση των συμφωνηθέντων. Προφανώς, οι απαιτήσεις για την σύναψη τέτοιων συμβάσεων είναι υψηλές, αφού οι διαπραγματεύσεις είναι συνήθως δύσκολες.

Ιδιαίτερη προσοχή χρειάζεται στην συχνή πρακτική τέτοιων εταιριών να περιλαμβάνουν όχι μόνον τις εργασίες που καλύπτονται από την κανονική σύμβαση, αλλά και επιπρόσθετες εργασίες με την σχετική κοστολόγηση. Εδώ οι εργασίες ή υπηρεσίες του τελευταίου τύπου συνήθως είναι αρκετά γενικά ορισμένες, ενώ το αναγραφόμενο κόστος υπερβολικά μεγάλο. Εννοείται πως δεν θα πρέπει να έχει καμία σχέση με τέτοιες εταιρείες οποιοσδήποτε από το εμπλεκόμενο (στις διαπραγματεύσεις) προσωπικό της δικής μας εταιρίας.

Στην περίπτωση εξωτερικής ανάθεσης, ο αναθέτων γίνεται ουσιαστικά ο επιστάτης που διασφαλίζει την ποιότητα της παρεχόμενης υπηρεσίας.

Άλλο ζήτημα είναι ότι εάν η αμοιβή της εταιρίας αυτής είναι, για παράδειγμα, ‘το πολύ’ 100.000 Ευρώ για δύο έτη, θα κάνει οτιδήποτε σε αυτό το διάστημα προκειμένου να εμποδίσει την αμοιβή της να πέσει κάτω από το ανώτατο αυτό ποσό.

Επίσης, εάν φέρει κάποιο προσωπικό για καθημερινές εργασίες και είμαστε ευχαριστημένοι με αυτό μετά από έξι μήνες, δεν σημαίνει ότι το προσωπικό αυτό θα συνεχίσει για όλο το διάστημα της σύμβασης. Αντιθέτως, μπορεί να αλλάζει το προσωπικό αυτό, όποτε και όπως θέλει, εφόσον τηρεί τους όρους της σύμβασης με εμάς.

Βιβλιογραφία/Αναφορές

Apache Software Foundation. (2015). Apache HTTP Server [Software]
Available from https://httpd.apache.org/

Anixter Inc. (2013). *Anixter Standards Reference Guide*.
Retrieved from https://www.anixter.com/content/dam/Anixter/Guide/12H0001X00-Anixter-Standard-Ref-Guide-ECS-US.pdf

Axelos Ltd. (2015, June 12). *Axelos Global Best Practice, ITIL® Qualifications*. [Web page].
Retrieved from https://www.axelos.com/qualifications/

Buchanan, R. (2002). *Disaster Proofing Information Systems: A Complete Methodology for Eliminating Single Points of Failure*. New York, NY: McGraw-Hill Education.

Chung, J., Pueblas, M., Nadimi, A., Hamilton D., & Farrington S. (2010). *Cisco SAFE Reference Guide*.
Revised: July 8, 2010. Retrieved from:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html

Cisco (2006, October 24). *Understanding Rapid Spanning Tree Protocol (802.1w)*.
Retrieved from: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.pdf

Fraser, J. *Editor* (September, 1997). *RFC 2196, Site Security Handbook*.
Retrieved from https://tools.ietf.org/html/rfc2196

Guttman, E., Leong, L., & Malkin, G. (February, 1999). *RFC 2504, Users' Security Handbook*.
Retrieved from https://tools.ietf.org/html/rfc2504

IEEE (2012, December 28). *802.3-2012 – IEEE Standard for Ethernet*. [Web page].
Retrieved from http://standards.ieee.org/findstds/standard/802.3-2012.html

IEEE (2014). *802.1Q-2014 - IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks*. [Web page].
Retrieved from http://standards.ieee.org/findstds/standard/802.1Q-2014.html

Limoncelli, T., Hogan, C., & Chalup, S. (2007). *The Practice of System and Network Administration, 2nd Edition*. Boston, MA: Pearson Education, Inc.

Oppenheimer, P. (2011). *Top-Down Network Design, 3rd Edition*. Indianapolis: Cisco Systems, Inc.

Stallings, W. (2000). *Local and Metropolitan Area Networks, 6th Edition*. New York: Pearson.

TIA/EIA. (August, 2012). *TIA-568 SET Revision C*.
Retrieved from
https://global.ihs.com/doc_detail.cfm?&rid=TIA&item_s_key=00378460&item_key_date=870731&input_doc_number=TIA-568&input_doc_title=

Κέντρο Υπολογιστών & Δικτύων. (2012). *Καλωδίωση Δικτύου*. Πανεπιστήμιο Μακεδονίας.
Retrieved from http://www.cnc.uom.gr/network/domi/genika.htm

Κριτήρια αξιολόγησης

Κριτήριο αξιολόγησης 1

Τι είναι το PDIOO της Cisco και ποιες είναι οι φάσεις που περιλαμβάνει;

Κριτήριο αξιολόγησης 2

Ένας πελάτης ζητά ποσοστό λειτουργίας του δικτύου του 99,5%. Για πόσο χρόνο μπορεί το δίκτυό του να μην λειτουργεί κανονικά μέσα σε διάστημα μίας εβδομάδος;

Κριτήριο αξιολόγησης 3

Ποιες είναι οι διαφορές μεταξύ του λογικού και του φυσικού σχεδιασμού ενός δικτύου;

Κριτήριο αξιολόγησης 4

Τι είναι το SAFE της Cisco;

Κριτήριο αξιολόγησης 5

Ποιοι είναι οι βασικοί λόγοι ή προϋποθέσεις για να προχωρήσουμε σε αναδιοργάνωση της διαχείρισης ενός δικτύου, είτε προς την συγκεντρωτική, είτε προς την αποκεντρωμένη μορφή;