Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Κέντρα δεδομένων: Εισαγωγή και Ανάλυση προβλημάτων**
Ονοματεπώνυμο Φοιτητή	**Σοφία Μήττα**
Πατρώνυμο	**Θεόδωρος**
Αριθμός Μητρώου	**ΜΠΠΛ/ 09023**
Επιβλέπων	**Χρήστος Δουληγέρης, Καθηγητής**

Ημερομηνία Παράδοσης	**Ιούνιος 2012**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης Καθηγητής	Δέσποινα Πολέμη Επίκ. Καθηγήτρια	Δημήτρης Βέργαδος Επίκ. Καθηγητής

ΠΕΡΙΕΧΟΜΕΝΑ

1. Περίληψη

Τα κέντρα δεδομένων κατέχουν μέρα με την ημέρα ένα πολύ σημαντικό ρόλο στην επιστήμη της πληροφορικής αλλά και στην καθημερινή ζωή καθώς προσφέρουν χιλιάδες υπηρεσίες και εφαρμογές στις επιχειρήσεις, στην εκπαίδευση, στις επικοινωνίες αλλά και σε κυβερνητικά συστήματα. Η πρόοδος της τεχνολογίας και της πληροφορίας γεννά την ανάγκη για την συνεχή εξέλιξη και ανάπτυξη των κέντρων δεδομένων. Ειδικές βαθμίδες και οργανισμοί έχουν δημιουργηθεί για την κατηγοριοποίηση των κέντρων δεδομένων με βάση το μέγεθος τους και τις υπηρεσίες που προσφέρουν. Επιπλέον, οι οργανισμοί αυτοί θέτουν πρότυπα και κανόνες οι οποίοι πρέπει να τηρούνται για την ομαλή λειτουργία των κέντρων δεδομένων. Λαμβάνοντας υπόψη αυτούς τους παράγοντες τα κέντρα δεδομένων συνεχώς εξελίσσονται με αποτέλεσμα να παρατηρούνται διάφορα προβλήματα. Στην εργασία αυτή παρέχεται μία εισαγωγή στη έννοια των κέντρα δεδομένων, στις απαιτήσεις τους, στα χαρακτηριστικά τους και στα πιο συνηθισμένα προβλήματα τους. Συγκεκριμένα μελετούνται τα είδη των αρχιτεκτονικών που χρησιμοποιούνται, τα προβλήματα συμφόρησης , τα προβλήματα στο επίπεδο μετάδοσης, τα θέματα ενέργειας που προκύπτουν από τη χρήση τους αλλά και τα πιθανά προβλήματα ασφάλειας που μπορεί να εμφανιστούν και προτείνονται και τρόποι αντιμετώπισή τους. Η μεταπτυχιακή αυτή διατριβή αποτελεί μία εισαγωγική εργασία στο χώρο των κέντρων δεδομένων αφού καλύπτει τις βασικές πτυχές αυτών και μπορεί να χρησιμοποιηθεί για μελλοντική εργασία που θα έχει σαν σκοπό την εξειδίκευση και εκτενή ανάλυση κάποιου από τα παραπάνω θέματα.

Data centers are gradually gaining a significant share in computer science since they constitute the basis for a wide range of services and applications used in education, communications and government systems. Advances in technology as well as the rising complexity of information have set the need for constant evolution and development of data centers. Furthermore, it is important to mention that even specific grades/ratings and organizations have been established in order to classify data centers according to the size and the type of services offered. The role of these organizations is to set commonly agreed rules and standards to the smooth operation of data centers. However, it is obvious that the evolution of data centers has also caused a range of issues and problems that need to be addressed. The aim of this master thesis is to provide high-level information on the concept of data centers, focusing on their features and requirements as well as on the most commonly faced issues/problems. More specifically, presented information focuses on architectural types and aspects, congestion issues, security issues, the tcp incast as well as energy issues along with their respective proposed solutions. This thesis constitutes an introductory work on data centers covering key aspects, therefore providing a solid basis for future research.

2. Εισαγωγή

Στην παρούσα διπλωματική εργασία γίνεται μία ανάλυση/εισαγωγή στις βασικές αρχές των κέντρων δεδομένων και στα πιο συνήθη προβλήματα που αντιμετωπίζουν. Πιο συγκεκριμένα στο κεφάλαιο 1 υπάρχει μία περίληψη του θέματος της εργασίας τόσο στα ελληνικά τόσο και στα αγγλικά. Στο κεφάλαιο 2 γίνεται μία εισαγωγή στα κέντρα δεδομένων περιγράφοντας την ιστορία των κέντρων δεδομένων, την εξέλιξη τους με το πέρασμα του χρόνου φτάνοντας μέχρι τη σημερινή μορφή τους. Στο κεφάλαιο 3 περιγράφονται οι βασικές απαιτήσεις και οι προδιαγραφές που πρέπει να ικανοποιούν τα κέντρα δεδομένων έτσι ώστε να εξασφαλίζεται η ομαλή τους λειτουργία αλλά και η εξέλιξή τους. Συνεχίζοντας στο κεφάλαιο 4 γίνεται μία ανάλυση προβλημάτων που παρουσιάζονται στο επίπεδο μετάδοσης και προτείνονται λύσεις για την πρόληψη και αντιμετώπιση των προβλημάτων αυτών. Επιπλέον, στην ίδια ενότητα αναφέρονται και τα προβλήματα συμφόρησης που παρατηρούνται στους μεταγωγείς και αναλύονται τέσσερις βασικοί αλγόριθμοι του χρησιμοποιούνται για τον έλεγχο της συμφόρησης στους μεταγωγείς. Παρακάτω, στο κεφάλαιο 5 αναλύονται κάποιες από τις πιο γνωστές αρχιτεκτονικές των κέντρων δεδομένων. Στη συνέχεια, στο κεφάλαιο 6 ακολουθεί μία εκτενής ανάλυση σε θέματα ασφάλειας στα κέντρα δεδομένων. Θίγεται η ασφάλεια τόσο σε δικτυακό όσο και σε φυσικό επίπεδο και προτείνονται λύσεις για την εξασφάλισή της. Στην ενότητα 7 γίνεται μία αναφορά στα «πράσινα» κέντρα δεδομένων και πως μπορεί να επιτευχθεί η μείωση της ενέργειας που καταναλώνουν τα κέντρα δεδομένων μέσα από τη χρήση εναλλακτικών μορφών ενέργειας και ενεργειακών εξυπηρετητών. Η εργασία τελειώνει με κάποια συμπεράσματα και προτάσεις για εμπλουτισμό της στο μέλλον.

2.1 Εισαγωγή στα κέντρα δεδομένων- Ιστορία και Ορισμός

Τα πρώτα χρόνια της ανάπτυξης της τεχνολογίας των πληροφορικής, τα κέντρα δεδομένων αποτελούσαν τεράστιες αίθουσες με ηλεκτρονικούς υπολογιστές. Τα πρώιμα υπολογιστικά συστήματα ήταν πολύ δύσκολο να συντηρηθούν και να διαχειριστούν καθώς απαιτούσαν ένα ειδικό περιβάλλον λειτουργίας. Ήταν απαραίτητα πολλά καλώδια για να συνδεθούν όλα τους τα εξαρτήματα και πολλές μέθοδοι χρησιμοποιούνταν για να τα φιλοξενήσουν και να τα οργανώσουν όπως racks και υπερυψωμένα πατώματα. Επιπλέον, ένα μοναδικός υπολογιστής απαιτούσε μεγάλα ποσοστά ενέργειας για να λειτουργήσει και ταυτόχρονα έπρεπε να ψύχεται για να αποφεύγονται περιστατικά υπερθέρμανσης. Η ασφάλεια ήταν επίσης ένα σημαντικό θέμα διότι τα πρώτα κέντρα δεδομένων χρησιμοποιούνταν για στρατιωτικούς και κυβερνητικούς σκοπούς.

Κατά τη διάρκεια της άνθησης των μικροϋπολογιστής βιομηχανίας, η οποία παρατηρείται τη δεκαετία του 1980, οι υπολογιστές άρχισαν να αναπτύσσονται παντού, και σε πολλές περιπτώσεις χωρίς να δίνεται καθόλου σημασία στις λειτουργικές απαιτήσεις. Ωστόσο, η τεχνολογία της πληροφορικής (IT) άρχισε να αναπτύσσεται σε πολυπλοκότητα και οι εταιρείες είχαν πλέον επίγνωση της ανάγκης έλεγχου των πόρων της πληροφορικής. Με την έλευση του μοντέλου πελάτη-εξυπηρετητή (client-server), κατά τη διάρκεια της δεκαετίας του 1990, οι μικροϋπολογιστές (που σήμερα ονομάζεται "servers") άρχισαν παίρνουν θέση στα παλιά δωμάτια υπολογιστών. Η ανάγκη για φθηνό εξοπλισμό δικτύωσης, σε συνδυασμό με τα νέα πρότυπα για την καλωδίωση του δικτύου, κατέστησε δυνατό να χρησιμοποιηθεί ένας ιεραρχικός σχεδιασμός ο οποίος έθετε τους εξυπηρετητές σε ένα συγκεκριμένο χώρο εντός της εταιρείας. Η χρήση του όρου «data center», όπως εφαρμόζεται σε ειδικές διαμορφωμένες αίθουσες με ηλεκτρονικούς υπολογιστές, άρχισε να αποκτά μεγάλη δημοτικότητα.

Η έκρηξη των κέντρων δεδομένων ήρθε με την άφιξη της εμπορικής ανάπτυξης του διαδικτύου. Οι εταιρείες χρειαζόντουσαν γρήγορη σύνδεση στο διαδίκτυο (Internet) και ασταμάτητη λειτουργία όχι μόνο για την ανάπτυξη των συστημάτων τους αλλά και την εγκαθίδρυση της παρουσίας τους στο διαδίκτυο. Η εγκατάσταση ενός τέτοιου εξοπλισμού δεν ήταν βιώσιμη για τις μικρότερες εταιρείες. Πολλές εταιρείες άρχισαν να δημιουργούν μεγάλες εγκαταστάσεις, που ονομαζόντουσαν Internet κέντρα δεδομένων (IDCs), τα οποία παρείχαν στις επιχειρήσεις με μια σειρά από λύσεις για την εγκατάσταση και τη λειτουργία των συστημάτων τους. Νέες τεχνολογίες και πρακτικές σχεδιάστηκαν για τις λειτουργικές απαιτήσεις

αυτών των εργασιών οι οποίες μετανάστευσαν και προς τα ιδιωτικά κέντρα δεδομένων, και υιοθετήθηκαν σε μεγάλο βαθμό λόγω των πρακτικών αποτελεσμάτων τους.

Η σύγχρονη μορφή των κέντρων δεδομένων έχει τη μορφή μεγάλων εγκαταστάσεων που χρησιμοποιούνται για να στεγάσουν υπολογιστικά συστήματα, όπως υπολογιστές, εξυπηρετητές(servers), διακομιστές ιστοσελίδων(webservers), διακομιστές εφαρμογών(appli-servers), διακομιστές ηλεκτρονικής αλληλογραφίας(mail servers), μεταγωγείς (switches), δρομολογητές(routers), συσκευές αποθήκευσης δεδομένων και γενικότερα τέτοιου είδους εξοπλισμό (βλέπε Σχήμα 2). Στην ουσία, το κέντρο δεδομένων αποτελεί μία κεντρική αποθήκη, φυσική ή εικονική, για αποθήκευση, διαχείριση, διάδοση δεδομένων και ανταλλαγή ψηφιακών πληροφοριών που οργανώνεται γύρω από ένα συγκεκριμένο γνωστικό αντικείμενο ή μία συγκεκριμένη επιχείρηση. Οι υπηρεσίες που συνήθως παρέχουν τα κέντρα δεδομένων είναι η φιλοξενία ιστοσελίδων στο διαδίκτυο, intranet, υπηρεσίες που αφορούν τις τηλεπικοινωνίες και την τεχνολογία της πληροφορίας. Αναπόσπαστα συστατικά ενός κέντρου δεδομένων αποτελούν συνήθως οι συνδέσεις δικτύων, εφεδρικές και μη παροχές ηλεκτρικού ρεύματος, έλεγχοι περιβάλλοντος (πχ κλιματισμός, πυρασφάλεια) όπως και συστήματα ασφαλείας.

Στο Σχήμα 1 παρουσιάζεται η βασική δομή ενός κέντρου δεδομένων, η οποία αποτελείται από τρία επίπεδα. Το επίπεδο πυρήνα-αρχικό αποτελεί τη ραχοκοκαλιά του δικτύου και περιέχει τους τελικούς μεταγωγείς και μεγάλης ταχύτητας καλώδια όπως είναι οι οπτικές ίνες. Το επίπεδο αυτό δεν καθορίζει ούτε διευθύνει την κυκλοφορία του LAN. Επιπλέον, οι συσκευές αυτού του επιπέδου δεν πραγματοποιούν χειρισμό πακέτων. Αντίθετα, το επίπεδο αυτό συνδέεται με την ταχύτητα και εξασφαλίζει την αξιόπιστη μεταφορά των πακέτων. Ο παράγοντας κλειδί του επιπέδου αυτού είναι η αποτελεσματικότητα. Μερικά συστατικά του επιπέδου είναι οι μεταγωγείς για χρήση WAN, οι μεταγωγείς για χρήση LAN, T-1 και E-1 γραμμές, frame relay συνδέσεις, ATM δίκτυα, Switched Multimegabit Data Service (SMDS), όπως φαίνονται στο Σχήμα 2.

Το επίπεδο συνάθροισης περιλαμβάνει δρομολογητές και μεταγωγείς που βασίζονται σε LAN τριών επιπέδων. Το επίπεδο αυτό εξασφαλίζει ότι τα πακέτα διευθετούνται σωστά ανάμεσα στα υποδίκτυα και στα VLANs της επιχείρησης. Οι υπηρεσίες που προσφέρει αυτό το επίπεδο είναι:

- Φιλτράρισμα πακέτων (firewalling):Επεξεργάζεται τα πακέτα και ρυθμίζει τη μετάδοση τους με βάση την πηγή και τον προορισμό της πληροφορίας
- QoS: Ο δρομολογητής ή οι μεταγωγείς μπορούν να διαβάσουν τα πακέτα και να προτεραιοποιήσουν την παράδοση τους, με βάση τις πολιτικές που έχουν οριστεί.
- Παρέχει έλεγχο της μετάδοσης σε όλους τους υπολογιστές του υποδικτύου (broadcast) και της πολλαπλής διανομής (multicast).
- Επιτρέπει τη χρήση πρωτοκόλλων στις θύρες από και προς διαφορετικές αρχιτεκτονικές δικτύων.
- Το επίπεδο αυτό εκτελεί αναμονή και παρέχει διευθέτηση των πακέτων στην κίνηση του δικτύου.

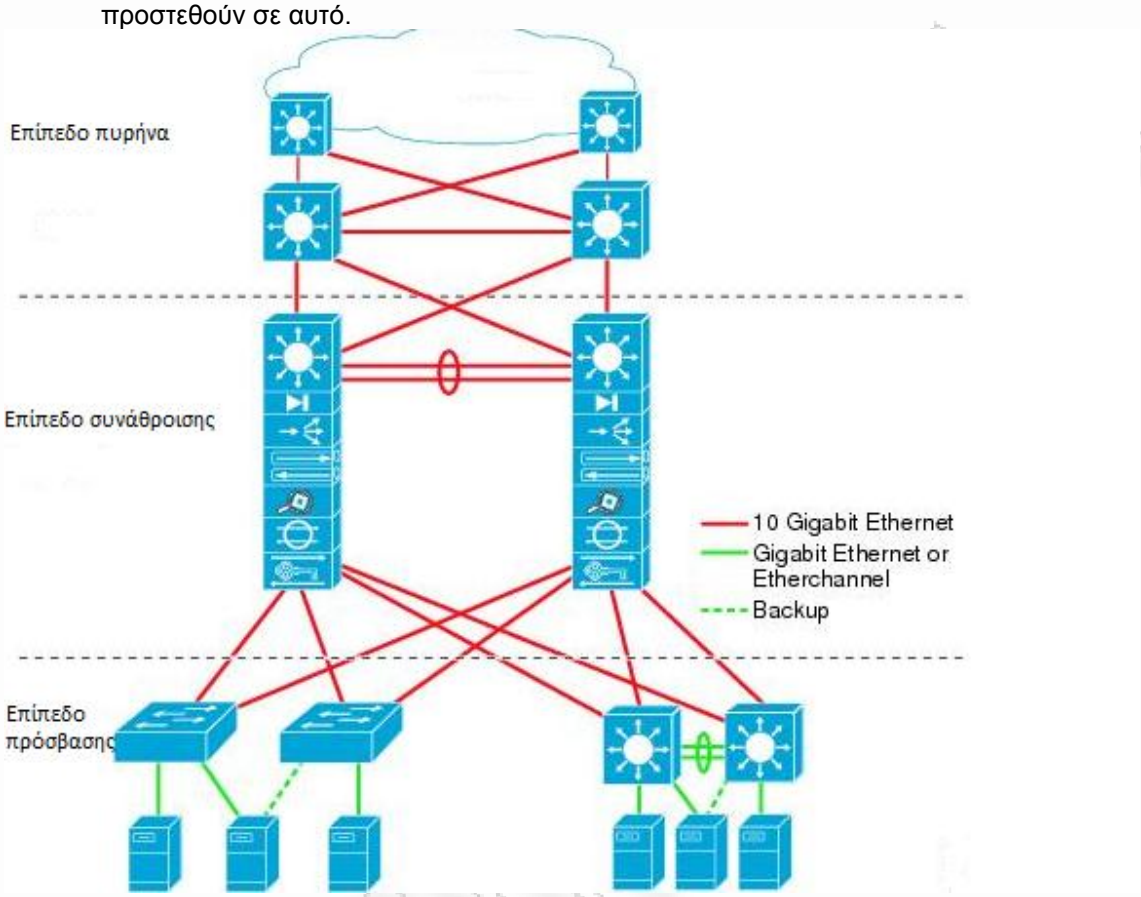
Το επίπεδο ασκεί έλεγχο στις μεταδόσεις του δικτύου, συμπεριλαμβάνοντας ότι έρχεται και ότι βγαίνει από το δίκτυο. Παρέχει τη δυνατότητα, εάν αυτό είναι αναγκαίο, περιορισμού και δημιουργίας περιοχών μετάδοσης μέσα από εικονικά δίκτυα LAN, και διεξάγει διάφορες εργασίες διαχείρισης.

Το επίπεδο πρόσβασης αποτελείται από διανομείς και μεταγωγείς και εστιάζει στη σύνδεση των κόμβων. Το επίπεδο αυτό εξασφαλίζει ότι τα πακέτα διανέμονται στους τελικούς χρήστες-υπολογιστές. Αποτελείται από υπολογιστές (desktops και laptops) και εξυπηρετητές όπως web servers, ftp servers,database servers κτλ.

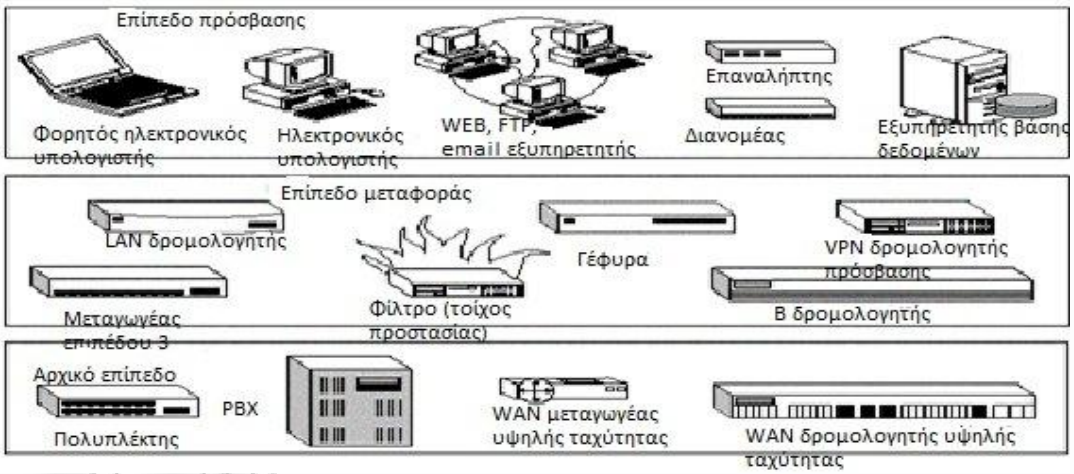
Τα προτερήματα του ιεραρχικού μοντέλου είναι:

- Υψηλή Απόδοση: Προσφέρει δίκτυα υψηλής απόδοσης, όπου μόνο ορισμένα στρώματα εμφανίζουν συμφόρηση.
- Αποτελεσματική διαχείριση και αντιμετώπιση προβλημάτων: Δίνει τη δυνατότητα αποτελεσματικής διαχείρισης του δικτύου απομόνωσης των αιτιών των προβλημάτων του δικτύου.
- Δημιουργία Πολιτικής: Εύκολη δημιουργία κανόνων και πολιτικών.
- Δυνατότητα επέκτασης: Εύκολη ανάπτυξη με τη διαίρεση του δικτύου σε λειτουργικές περιοχές.

- Πρόβλεψη Συμπεριφοράς: Κατά το σχεδιασμό ή τη διαχείριση ενός δικτύου, το μοντέλο αυτό επιτρέπει να προσδιοριστεί τι θα συμβεί με το δίκτυο, όταν νέες πιέσεις προστεθούν σε αυτό.



Σχήμα 1: Η δομή ενός κέντρου δεδομένων [23]



Σχήμα 2: Τα συστατικά ενός κέντρου δεδομένων [23]

Τα τελευταία χρόνια, ο σχεδιασμός, η ανάπτυξη και η λειτουργία των κέντρων δεδομένων πατάνε πάνω σε πειθαρχία. Τυποποιημένα έγγραφα από διαπιστευμένους επαγγελματικές ομάδες, όπως η Telecommunications Industry Association (TIA) , προσδιορίζουν τις απαιτήσεις για τη σχεδίαση των κέντρων δεδομένων. Γνωστές λειτουργικές μετρήσεις για τη διαθεσιμότητα του κέντρου δεδομένων μπορούν να χρησιμοποιηθούν για την αξιολόγηση των επιπτώσεων που θα υπάρξουν στις επιχειρήσεις σε περίπτωση διακοπής της λειτουργίας τους. Βέβαια, υπάρχει δρόμος ακόμα αναφορικά με την εξέλιξη κέντρων δεδομένων, για παράδειγμα η

σχεδίαση φιλικών προς το περιβάλλον κέντρα δεδομένων. Τα κέντρα δεδομένων είναι συνήθως πολύ ακριβά να κατασκευαστούν αλλά και στη συνέχεια να συντηρηθούν. Για παράδειγμα, το κέντρο δεδομένων της Amazon.com βρίσκεται στο Boardman, Oregon είναι 116.000 τετραγωνικά πόδια (10.800 m2) και κοστίσει μέχρι και 100 εκατομμύρια δολάρια.

3. Χαρακτηριστικά των κέντρων δεδομένων

3.1 Απαιτήσεις των κέντρων δεδομένων

Οι λειτουργίες των υπολογιστών είναι η πιο κρίσιμη πτυχή των οργανωτικών λειτουργιών. Ένα από τα πιο βασικά προβλήματα είναι η συνέχεια της επιχειρηματικής δραστηριότητας, οι εταιρίες βασίζονται στα πληροφοριακά τους συστήματα για την διευθέτηση των εργασιών τους. Εάν κάποιο σύστημα δεν είναι πλέον διαθέσιμο, οι λειτουργίες της εταιρείας μπορεί να μειωθούν ή και να σταματήσουν εντελώς. Είναι αναγκαίο να παρέχεται μία αξιόπιστη υποδομή για τις IT λειτουργίες, έτσι ώστε να ελαχιστοποιηθεί η οποιαδήποτε πιθανότητα διακοπής. Η ασφάλεια των συστημάτων και η ασφάλεια των πληροφοριών είναι επίσης ανησυχίες, και για το λόγο αυτό ένα κέντρο δεδομένων πρέπει να προσφέρει ένα ασφαλές περιβάλλον που να ελαχιστοποιεί τις πιθανότητες παραβίασης της ασφάλειας. Επομένως ένα κέντρο δεδομένων πρέπει να διατηρεί υψηλά πρότυπα για το υπολογιστικό περιβάλλον που φιλοξενεί.

Η αποτελεσματική λειτουργία ενός κέντρου δεδομένων απαιτεί την ισορροπημένη επένδυση τόσο στις εγκαταστάσεις όσο και στην στέγαση του εξοπλισμού. Το πρώτο βήμα είναι η δημιουργία ενός περιβάλλοντος κατάλληλου για την εγκατάσταση του εξοπλισμού. Η τυποποίηση μπορεί να αποφέρει εξοικονόμηση και αποδοτικότητα στο σχεδιασμό και την κατασκευή των τηλεπικοινωνιακών κέντρων δεδομένων.

Τυποποίηση σημαίνει ολοκληρωμένη δόμηση και ολοκληρωμένος μηχανολογικός εξοπλισμός. Τα τηλεπικοινωνιακά κέντρα δεδομένων θα πρέπει να σχεδιάζονται σε επαναλαμβανόμενες δομικές μονάδες εξοπλισμού και συναφών με την ενέργεια και την υποστήριξη (κλιματισμού) εξοπλισμού όπου αυτό είναι εφικτό. Η χρήση ειδικών κεντρικών συστημάτων απαιτεί πιο ακριβείς προβλέψεις των μελλοντικών αναγκών σχετικά με το κόστος κατασκευής αλλά και την απόκριση στις μελλοντικές ανάγκες.

Το κέντρο δεδομένων με «χαμηλό προφίλ» , γνωστό και ως ένα σκοτεινό ή ένα σκοτεινό κέντρο δεδομένων, είναι ένα κέντρο δεδομένων που, ιδανικά, έχει τα πάντα, αλλά έχει εξαλειφθεί η ανάγκη για άμεση πρόσβαση από το προσωπικό, εκτός από έκτακτες περιστάσεις. Λόγω της έλλειψης της ανάγκης σε προσωπικό, η είσοδος στο κέντρο δεδομένων, μπορεί να γίνει χωρίς φωτισμό. Όλες οι συσκευές έχουν πρόσβαση και διαχειρίζονται από απομακρυσμένα συστήματα, με τα αυτοματοποιημένα προγράμματα που χρησιμοποιούνται για την εκτέλεση εργασιών χωρίς επίβλεψη. Εκτός από την εξοικονόμηση ενέργειας, τη μείωση του κόστους λόγω έλλειψης προσωπικού και τη δυνατότητα εγκατάστασης του site μακριά από αστικά κέντρα, η δημιουργία ενός κέντρου δεδομένων με «χαμηλό προφίλ» μειώνει την απειλή των κακόβουλων επιθέσεων κατά της υποδομής.

Υπάρχει μια τάση για τον εκσυγχρονισμό των κέντρων δεδομένων, προκειμένου να επωφεληθούν από την απόδοση καθώς η ενεργειακή απόδοση αυξάνει με τη χρήση νεότερων εξοπλισμού πληροφορικής και ικανοτήτων, όπως το cloud computing. Η διαδικασία αυτή είναι επίσης γνωστή ως μετασχηματισμός του κέντρου δεδομένων. Οι οργανισμοί αντιμετωπίζουν ταχεία ανάπτυξη στην τεχνολογία της πληροφορίας αλλά τα κέντρα δεδομένων τους γερνούν. Η εταιρεία ερευνών International Data Corporation προσδιορίζει τη μέση ηλικία ενός κέντρου δεδομένων στα εννέα χρόνια. Η Gartner, μία άλλη εταιρεία ερευνών πιστεύει ότι ένα κέντρο δεδομένων ηλικίας επτά ετών θεωρείται απαρχαιωμένο. Πρόσφατη έρευνα που διενεργήθηκε το Μάιο του 2011 από οργανισμού έρευνας κέντρων δεδομένων, Uptime Institute, έδειξε ότι το τριάντα έξι τοις εκατό (36%) των μεγάλων εταιρειών αναμένεται να εξαντλήσει τη δυναμικότητα των κέντρων δεδομένων τους μέσα στους επόμενους δεκαοχτώ (18) μήνες. Ο μετασχηματισμός ενός κέντρου δεδομένων διενεργείται βήμα προς βήμα μέσα από ολοκληρωμένα έργα που διαρκούν αρκετό χρόνο. Αυτή η προσέγγιση διαφέρει από την κλασσική μέθοδο αναβάθμιση των κέντρων δεδομένων που γίνεται ακολουθώντας μία σειριακή λογική.

Τα πιο κοινά έργα που αφορούν τον μετασχηματισμό ενός κέντρου δεομένων έχουν να κάνουν με την τυποποίηση/ενοποίηση, την εικονικότητα, την αυτοματοποίηση και την ασφάλεια.

- Τυποποίηση/ενοποίηση: Ο σκοπός αυτού του έργου είναι η ελάττωση του αριθμού των κέντρων δεδομένων που μπορεί να έχει ένας μεγάλος οργανισμός. Κατά αυτόν τον τρόπο μειώνεται ο αριθμός του εξοπλισμού, του λογισμικού, των εργαλείων και διαδικασιών μέσα σε ένα κέντρο δεδομένων. Οι οργανισμοί αντικαθιστούν των παρωχημένο εξοπλισμό με πιο εξελιγμένο που προσφέρει μεγαλύτερες ικανότητες και αποδόσεις. Οι υπολογιστές, τα δίκτυα και ο τρόπος οργάνωσης του κέντρου δεδομένων ομαδοποιούνται ώστε να είναι πιο εύκολα διαχειρίσιμα.
- Εικονικότητα: Υπάρχει μία τάση στη χρήση IT εικονικών τεχνολογιών ώστε να αντικαθιστάται να ενοποιείται ο πολλαπλός εξοπλισμός των κέντρων δεδομένων όπως είναι οι εξυπηρετητές. Η εικονικότητα βοηθά στη μείωση των κεφαλαιακών και λειτουργικών εξόδων των κέντρων δεδομένων και στη μείωση της κατανάλωσης ενέργειας. Η Gartner βλέπει την εικονικότητα σαν καταλύτη στον εκσυγχρονισμό των κέντρων δεδομένων.
- Αυτοματοποίηση: Η αυτοματοποίηση στα κέντρα δεδομένων περιλαμβάνει αυτοματοποιημένες εργασίες όπως η παροχή, η ρύθμιση, η επιδιόρθωση, και η απελευθέρωση της διαχείρισης. Καθώς οι επιχειρήσεις διαθέτουν στο ενεργητικό τους λίγα άτομα με εξειδικευμένες IT ικανότητες , οι αυτοματοποιημένες εργασίες συμβάλουν δραστικά στην αύξηση της αποδοτικότητας των κέντρων δεδομένων.
- Ασφάλεια: Στα σύγχρονα κέντρα δεδομένων, η ασφάλεια των δεδομένων στα εικονικά συστήματα είναι ενσωματωμένη με την υπάρχουσα ασφάλεια των φυσικών υποδομών. Η ασφάλεια στο σύγχρονο πρέπει να λαμβάνει υπόψη τη φυσική ασφάλεια, την ασφάλεια των δικτύων και την ασφάλεια των δεδομένων και των χρηστών. [2]

3.2 Προκλήσεις στα κέντρα δεδομένων

Τα συμβατικά κέντρα δεδομένων κατασκευάζονται σύμφωνα με τη ιεραρχική τοπολογία δένδρου (tree-like). Καθώς όμως τα κέντρα δεδομένων μεγαλώνουν σε μέγεθος πολλά προβλήματα παρατηρούνται. Σε αυτή την ενότητα θα γίνει μία αναφορά στην δομή των κέντρων δεδομένων, συλλέγοντας τα σοβαρότερα προβλήματα τους και παρουσιάζοντας προδιαγραφές για νέες αρχιτεκτονικές των κέντρων δεδομένων. Αρκετές μελέτες έχουν δείξει τα βασικά προβλήματα των κοινών κέντρων δεδομένων που βασίζονται στην τοπολογία δένδρου.

- Επεκτασιμότητα: Καθώς οι ανάγκες για κέντρα δεδομένων μεγαλώνουν, τα σύγχρονα κέντρα δεδομένων πρέπει να υποστηρίζουν σταδιακή επεκτασιμότητα ώστε να φιλοξενήσουν μεγάλο αριθμό από εξυπηρετητές και όχι απλά μεγάλο αριθμό αλλά χιλιάδες εξυπηρετητές. Η κλασσική αρχιτεκτονική των κέντρων δεδομένων επιτρέπει τέτοιου είδους κλιμάκωση αντικαθιστώντας ή αναβαθμίζοντας το ήδη υπάρχον υλικό (hardware) με πιο προηγμένο. Παρόλα αυτά η στρατηγική είναι ακριβή και δύσκολη. Επομένως, νέες αρχιτεκτονικές πρέπει να προταθούν οι οποίες δε θα βασίζουν την επεκτασιμότητα τους στην αντικατάσταση του παλιού υλικού(hardware) με άλλο πιο εξελιγμένο.
- Στατική ανάθεση δικτύου: Στις αρχιτεκτονικές δένδρου των κέντρων δεδομένων, κάθε εφαρμογή αντιστοιχίζεται σε ένα εικονικό τοπικό δίκτυο (VLAN), με φυσικούς μεταγωγούς και δρομολογητές κάθε φορά που καλύπτουν συγκεκριμένους εξυπηρετητές που σχετίζονται με την εφαρμογή. Αυτή η απευθείας φυσική αντιστοίχιση της κάθε εφαρμογής σε μεταγωγούς και δρομολογητές προκαλεί στατικότητα στην ανάθεση των εξυπηρετητών. Σε ένα ιδανικό κέντρο δεδομένων κάθε εξυπηρετητής πρέπει να μπορεί να ανατεθεί σε οποιαδήποτε υπηρεσία δυναμικά συμφώνα με τις απαιτήσεις που προκύπτουν κάθε φορά.
- Επικοινωνία μεταξύ εξυπηρετητών: Η επικοινωνία μεταξύ των εξυπηρετητών περιορίζεται από το ποσοστό υπερκάλυψης , το οποίο μπορεί να υπολογιστεί απλά διαιρώντας το συνολικό εύρος ζώνης της σύνδεσης του εξυπηρετητή με το συγκεντρωτικό εύρος ζώνης σε επίπεδο μεταγωγέα. Το σύνηθες ποσοστό υπερκάλυψης είναι 2.5:1 μέχρι 8:1 σε μεγάλες συστοιχίες από εξυπηρετητές και το ποσοστό αυτό αυξάνεται στις αρχιτεκτονικές δένδρου.
- Κατακερματισμός και ευλυγισία πόρων: Σαν συνέπεια της ιεραρχικής φύσης της αρχιτεκτονικής των κέντρων δεδομένων και του μεγάλου ποσοστού υπερκάλυψης των εξυπηρετητών στο επίπεδο πυρήνα (core layer) και στο επίπεδο συνάθροισης (aggregation), οι πόροι κατακερματίζονται και απομονώνονται με συνέπεια τη μη δυνατή εκχώρηση των εξυπηρετητών στις εφαρμογές που τρέχουν στο κέντρο δεδομένων. Οι σχεδιαστές τείνουν να τοποθετούν τους διακομιστές τον έναν κοντά στον άλλον στην ιεραρχία γιατί η απόσταση στην ιεραρχία επηρεάζει την αποδοτικότητα και το κόστος

επικοινωνίας. Αν μία εφαρμογή ή μία υπηρεσία μεγαλώνει και χρειάζεται περισσότερους εξυπηρετητές, ο κατακερματισμός των πόρων την περιορίζει να χρησιμοποιήσει εξυπηρετητές από άλλες εφαρμογές. Ο κατακερματισμός των πόρων έχει σαν αποτέλεσμα τη μη αξιοποίηση των πηγών, που συνήθως περιορίζει την απόδοση ολόκληρου του κέντρου δεδομένων. Στην ιδανική αρχιτεκτονική των κέντρων δεδομένων, ο εξυπηρετητής μπορεί να τοποθετηθεί οπουδήποτε και να ανατεθεί σε οποιοδήποτε υπηρεσία , με αποτέλεσμα όλη η ομάδα των εξυπηρετητών να μπορούν να εξαπλωθούν ή να συρρικνωθούν δυναμικά για να ικανοποιήσουν τις συνεχείς μεταβαλλόμενες ανάγκες των ξεχωριστών υπηρεσιών.

- Αξιοπιστία και χρήση: Τα κλασσικά κέντρα δεδομένων πάσχουν από μικρή αξιοπιστία και χρήση. Πολλαπλά μονοπάτια δεν χρησιμοποιούνται επιτυχώς στις αρχιτεκτονικές δένδρου των κέντρων δεδομένων καθώς μόνο ένα μονοπάτι χρησιμοποιείται από το πρωτόκολλο Spanning Tree ανάμεσα στο επίπεδο 2 ακόμα και αν υπάρχουν πολλαπλά μονοπάτια ανάμεσα στους μεταγωγείς. Η κλασσική τοπολογία δένδρου προσφέρει δύο μονοπάτια το πολύ. Στο επίπεδο συνάθροισης και στο επίπεδο πυρήνα της αρχιτεκτονικής δένδρου η ευκαμψία του δικτύου είναι 1:1, που αντιστοιχεί στο 50% της μέγιστης χρήσης του κάθε μεταγωγέα και της κάθε σύνδεσης. Αυτού του τύπου η αρχιτεκτονική δικτύου χρησιμοποιήθηκε για αρκετά χρόνια στα κέντρα δεδομένων και αποδείχτηκε γρήγορα μη σταθερή. Ένα δυναμικό μοντέλο δικτύου κέντρου δεδομένων απαιτείται έτσι ώστε να αναπτύσσονται οι πόροι του δικτύου , όποτε και όταν αυτό χρειάζεται για να βελτιωθεί η αξιοπιστία των υπηρεσιών αλλά και να μεγιστοποιηθεί η χρήση των εξυπηρετητών.
- Ισορροπία δικτύου: Οι συνδέσεις στα κέντρα δεδομένων μπορούν να εξεταστούν μελετώντας το πρωτόκολλο Small Network Management Protocol. Οι συνδέσεις στο επίπεδο πυρήνα χρησιμοποιούνται περισσότερο από τις συνδέσεις στο ακραίο επίπεδο. Η κυκλοφορία πρέπει να κατανέμεται ομοιόμορφα σε όλα τα μονοπάτια του δικτύου στα βέλτιστα κέντρα δεδομένων.
- Ανοχή στα σφάλματα: Η ανοχή στα σφάλματα είναι βασική έννοια στα δίκτυα των κέντρων δεδομένων καθώς οι αποτυχίες στα δίκτυα των κέντρων δεδομένων είναι συνηθισμένες. Τα δίκτυα των κέντρων δεδομένων πρέπει αν είναι ανθεκτικά σε διάφορα είδη αποτυχιών των εξυπηρετητών, σε server racks αποτυχίες καθώς και σε αποτυχίες στις συνδέσεις και στους μεταγωγούς. Η υποδομή δένδρου του δικτύου κέντρων δεδομένων αντιμετωπίζει σημαντικά προβλήματα από την κατάρρευση ενός σημείου. Για παράδειγμα, η κατάρρευση ενός μεταγωγού στο επίπεδο πυρήνα μπορεί να καταστρέψει χιλιάδες χρήστες για αρκετές ώρες. Προσθέτοντας εφεδρικούς μεταγωγούς το πρόβλημα μπορεί να μετριαστεί , αλλά δεν θα λυθεί λόγω της χαμηλής σύνδεσης της κληρονομικής φύσης που παρατηρείται στις αρχιτεκτονικές δένδρου. Στις ιδανικές αρχιτεκτονικές δικτύου, όταν μία συσκευή καταρρέει , η απόδοση του συστήματος πρέπει να μειώνεται ομαλά και όχι κατακόρυφα. Η ανίχνευση του λάθους πρέπει να είναι γρήγορη και αποτελεσματική, το ίδιο και ο χρόνος επαναφοράς.
- Κόστος: Εκτιμάται ότι το κόστος σε ένα κέντρο δεδομένων με τοπολογία δένδρου είναι μία συνάρτηση του συνολικού αριθμού των τελικών υπολογιστών υποδοχής(end-hosts) με διαφορετικά ποσοστά υπερκάλυψης. Έχει βρεθεί ότι οι υπάρχουσες τεχνικές για την απόδοση μεγάλων επιπέδων εύρους ζώνης σε μεγάλες σε μεγάλες συστοιχίες επιφέρουν σημαντικό κόστος. Οι τελικοί μεταγωγείς που χρησιμοποιούνται από τα παραδοσιακά κέντρα δεδομένων που βασίζονται στην ιεραρχική τοπολογία επιβαρύνουν απαγορευτικά το κόστος για την επέκταση του μεγέθους της συστοιχίας. Το ιδανικό είναι το επεκτάσιμο εύρος ζώνης με λογικό κόστος.
- Κατανάλωση ενέργειας: Η κατανάλωση ενέργειας δεν λαμβάνεται υπόψη κατά τον σχεδιασμό της αρχιτεκτονικής δικτύου των κέντρα δεδομένων που βασίζονται στην τοπολογία δένδρου και ως εκ τούτου η κατανάλωση ενέργειας δεν είναι αποτελεσματική. Η υπερπροσφορά των πόρων των εξυπηρετητών στην ιεραρχική αρχιτεκτονική είναι ένας τεράστιος σωλήνας από ενέργεια και συστήματα ψύξης. Έρευνες έχουν δείξει ότι ένας ενεργειακά αποτελεσματικός εξυπηρετητής καταναλώνει το μισό από όλη την ενέργεια του, ακόμα και αν είναι ανενεργός [3].

3.3 Μέτρα/ σημεία αναφοράς των κέντρων δεδομένων

Υπάρχουν κάποια παγκοσμίως αποδεκτά μέτρα που χαρακτηρίζουν την απόδοση και την κατηγορία των κέντρων δεδομένων.

1. Telecommunications Industry Association (TIA)
   Η TIA αποτελεί μία οργάνωση που αντιπροσωπεύει την παγκόσμια πληροφορία στη βιομηχανία της τεχνολογίας. Βοηθά στην ανάπτυξη σταθερών και προωθεί τις επαγγελματικές ευκαιρίες για παγκόσμια περιβαλλοντολογική κανονιστική συμμόρφωση. Με τη υποστήριξη των 600 μελών της, η TIA βελτιώνει το επαγγελματικό περιβάλλον για εταιρείες που ασχολούνται με τις τηλεπικοινωνίες, τα δίκτυα, την κινητή ασύρματη, την τεχνολογία των υπολογιστών και τη φιλική προς το περιβάλλον ανάπτυξη της τεχνολογίας.
2. TIA-942
   Δημοσιεύτηκε το 2005, το Telecommunications Infrastructure Standards για κέντρα δεδομένων ήταν το πρώτο πρότυπο που απευθυνόταν στην υποδομή και προοριζόταν για να χρησιμοποιείται από τους σχεδιαστές των κέντρων δεδομένων κατά τη διάρκεια του κτισίματος της υποδομής. Το TIA-942 καλύπτει το χώρο και τη σχεδίαση του site, την καλωδιακή υποδομή, την αξιοπιστία της βαθμίδας και τις περιβαλλοντολογικές θεωρήσεις.
   Το πρότυπο TIA-942 υιοθετήθηκε από την ANSI βασισμένο στην χρησιμότητα του για την αξιολόγηση των εφεδρειών και της διαθεσιμότητας του σχεδιασμού του κέντρου δεδομένων. Παρακάτω ακολουθεί μία σύντομη περιγραφή των βαθμίδων του προτύπου:
   Η βαθμίδα 1 είναι η βασική βαθμίδα, η οποία δεν περιέχει εφεδρικός εξοπλισμός (N) και προσφέρει διαθεσιμότητα 99.671%.
   - Ευαίσθητη στις απώλειες από προγραμματισμένες ή μη δραστηριότητες
   - Ένα και μοναδικό μονοπάτι για την παροχή ενέργειας και ψύξης
   - Για την εφαρμογή προληπτικής συντήρησης πρέπει να τερματιστούν όλες οι εργασίες
   - Ο ετήσιος χρόνος μη λειτουργίας αγγίζει τις 28.8 ώρες

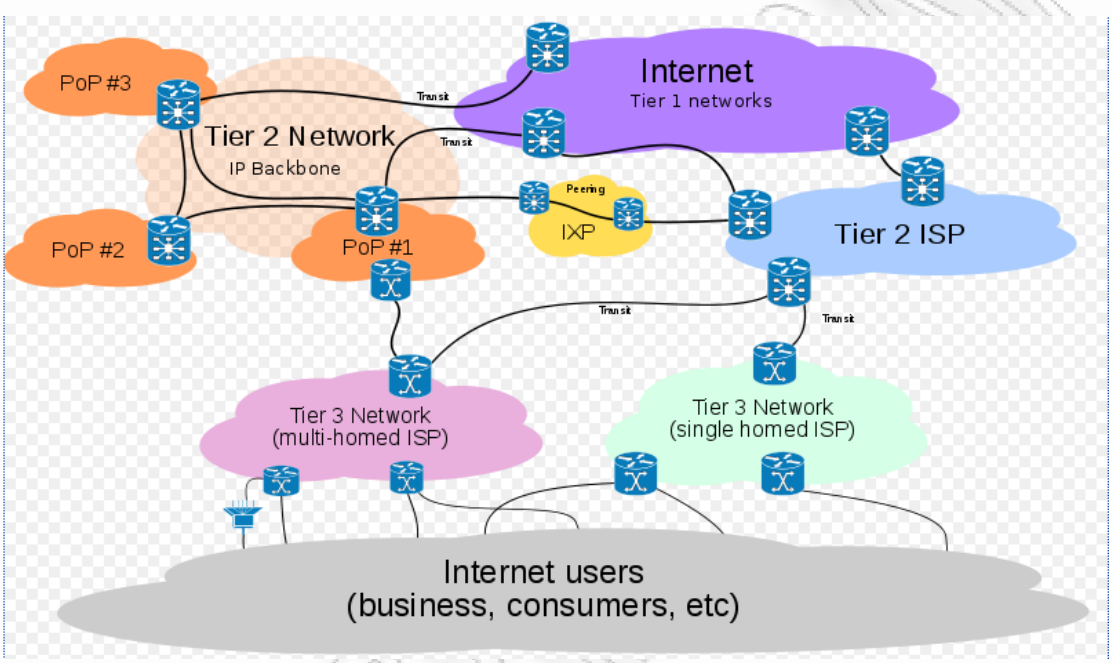
   Η βαθμίδα 2 έχει περιορισμένο εφεδρικός εξοπλισμός (N+1) και προσφέρει διαθεσιμότητα 99.741%.
   - Λιγότερο ευαίσθητο στις απώλειες από προγραμματισμένες ή μη δραστηριότητες
   - Ένα και μοναδικό μονοπάτι για την παροχή ενέργειας και ψύξης συμπεριλαμβανομένου και του εφεδρικού εξοπλισμού (N+1)
   - Περιλαμβάνει raised floor, UPS and generator
   - Ο ετήσιος χρόνος μη λειτουργίας αγγίζει τις 22.0 ώρες

   Η βαθμίδα 3 είναι παράλληλα διατηρήσιμη με N+1 και διαθεσιμότητα της τάξης του 99.982%.
   - Δίνει τη δυνατότητα σε προγραμματισμένες εργασίες (όπως προγραμματισμένη
   - προληπτική συντήρηση) χωρίς να διαλύει τις λειτουργίες του υλικού εξοπλισμού (μη προγραμματισμένα γεγονότα μπορούν να προκαλέσουν προβλήματα σε αυτή τη βαθμίδα)
   - Πολλαπλά μονοπάτια ενέργειας και ψύξης (βέβαια ένα μονοπάτι είναι ενεργό), εφεδρικός εξοπλισμός (N+1)
   - Ο ετήσιος χρόνος μη λειτουργίας αγγίζει τις 1.6 ώρες

   Η βαθμίδα 4 είναι ανεκτική στα λάθη καθώς προφέρει εφεδρικό εξοπλισμό (2N+1) και διαθεσιμότητα 99.995% διαθεσιμότητα
   - Οι προγραμματισμένες εργασίες δεν διαλύουν τις κρίσιμες λειτουργίες, όπως και ένα μη προγραμματισμένο συμβάν είναι ανεκτό από κέντρα δεδομένων που ανήκουν στη βαθμίδα 4 χωρίς ιδιαίτερες επιπτώσεις
   - Πολλαπλά μονοπάτια ενέργειας και ψύξης
   - Ο ετήσιος χρόνος μη λειτουργίας αγγίζει τις 0.4 ώρες

   Τα κέντρα δεδομένων που ανήκουν στη βαθμίδα 4 θεωρούνται πιο αποδοτικά και λιγότερο επιρρεπή σε αποτυχίες. Η βαθμίδα 4 είναι σχεδιασμένο για να φιλοξενήσει σημαντικούς εξυπηρετητές και πολύπλοκα συστήματα πληροφορικής, με υποσυστήματα που έχουν πλήρη χαρακτηριστικά εφεδρείας (ψύξη, δύναμη, συνδέσεις δικτύου, αποθήκευση κλπ) και

διαχωρισμένες ζώνες ασφαλείας. Σε σχέση με τη βαθμίδα3, η βαθμίδα 4 απαιτεί τη διπλάσια υποδομή και χώρο και κατ' επέκταση η κατασκευή καθώς και η λειτουργία του κοστίζουν περισσότερο. Συνεπώς, πολλοί οργανισμοί προτιμούν να λειτουργούν στη βαθμίδα 3 το οποίο πετυχαίνει μία ισορροπία ανάμεσα σε OPEX, CAPEX και διαθεσιμότητα. Τα κέντρα δεδομένων που υπόκεινται στη βαθμίδα 1 αποτελούν πιο απλές υλοποιήσεις και χρησιμοποιούνται από μικρές επιχειρήσεις ή καταστήματα. Οι διαφοροποιήσεις μεταξύ των βαθμίδων αναπαριστώνται γραφικά στο παρακάτω σχήμα:



Σχήμα 3: Αναπαράσταση του TIA προτύπου [2]

3. Uptime Institute

Είναι μια κερδοσκοπική οργάνωση που σχηματίζεται με την επίτευξη συνοχής στη βιομηχανία του κέντρου δεδομένων. Το ινστιτούτο Uptime παρέχει εκπαίδευση, συμβουλές, έρευνα, συνέδρια για τη βιομηχανία του κέντρου δεδομένων Αποτελεί παράδειγμα εταιρείας που έχει υιοθετήσει το TIA-942 πρότυπο αξιολόγησης ως πλαίσιο για την επίσημη πιστοποίηση των κέντρων δεδομένων. Ωστόσο, πρέπει να σημειωθεί ότι ένα κέντρο δεδομένων δεν είναι απαραίτητο να πιστοποιηθεί από το Ινστιτούτο Uptime, για να είναι συμβατό με το πρότυπο TIA-9.

4. Προβλήματα που αντιμετωπίζουν τα κέντρα δεδομένων

Ακολουθεί μία αναφορά σε δύο σημαντικά προβλήματα που αντιμετωπίζονται στα σύγχρονα κέντρα δεδομένων. Συγκεκριμένα στο TCP Incast και στη συμφόρηση που εμφανίζεται στους μεταγωγείς.

4.1 TCP Incast

Πριν προχωρήσουμε στο πρόβλημα, ακολουθεί μία μικρή περιγραφή του πρωτοκόλλου TCP.

4.1.1 Εισαγωγή στο TCP

Το πρωτόκολλο ελέγχου μετάδοσης σχεδιάστηκε ειδικά για την παροχή μιας από άκρου εις άκρο αξιόπιστης ροής byte μέσω ενός αναξιόπιστου διαδικτύου. Το διαδίκτυο διαφέρει από ένα μοναδικό δίκτυο επειδή τα διάφορα μέρη του μπορεί να έχουν εντελώς διαφορετική τοπολογία , εύρος ζώνης, μέγεθος πακέτων και άλλες παραμέτρους. Το TCP σχεδιάστηκε για να προσαρμόζεται δυναμικά στις ιδιότητες ενός διαδικτύου και να είναι ανθεκτικό σε πολλά είδη αστοχιών. Κάθε μηχανή που υποστηρίζει το TCP έχει μια οντότητα μεταφοράς TCP, η οποία λειτουργεί είτε ως διαδικασία βιβλιοθήκης είτε ως διεργασία χρήστη είτε ως τμήμα του πυρήνα . Σε όλες τις περιπτώσεις η οντότητα αυτή διαχειρίζεται τις ροές του TCP και τη διασύνδεση με το επίπεδο του IP. Μια οντότητα TCP δέχεται ροές δεδομένων χρήστη από τις τοπικές διεργασίες, τις διασπά σε τμήματα που δεν ξεπερνούν τα 64KB (στην πράξη , τα τμήματα συχνά περιέχουν 1460 byte δεδομένων έτσι ώστε να χωράνε , μαζί με τις κεφαλίδες IP και TCP, σε ένα μόνο πλαίσιο Ethernet), και στέλνει κάθε τμήμα ως ξεχωριστό αυτοδύναμο πακέτο IP. Επειδή τα αυτοδύναμα πακέτα πρέπει να παραδοθούν σωστά το TCP χρησιμοποιεί χρονόμετρα για αν μεταδίδει τα πακέτα όποτε χρειάζεται. Τα αυτοδύναμα πακέτα που φτάνουν πραγματικά στον προορισμό μπορεί και να φτάσουν με λάθος σειρά, έτσι είναι θέμα πάλι του TCP να τα επανασυναρμολογήσει με τη σωστή σειρά σε μηνύματα. Συνοπτικά, το TCP πρέπει να προσφέρει την αξιοπιστία που επιθυμούν οι περισσότεροι χρήστες. [3]

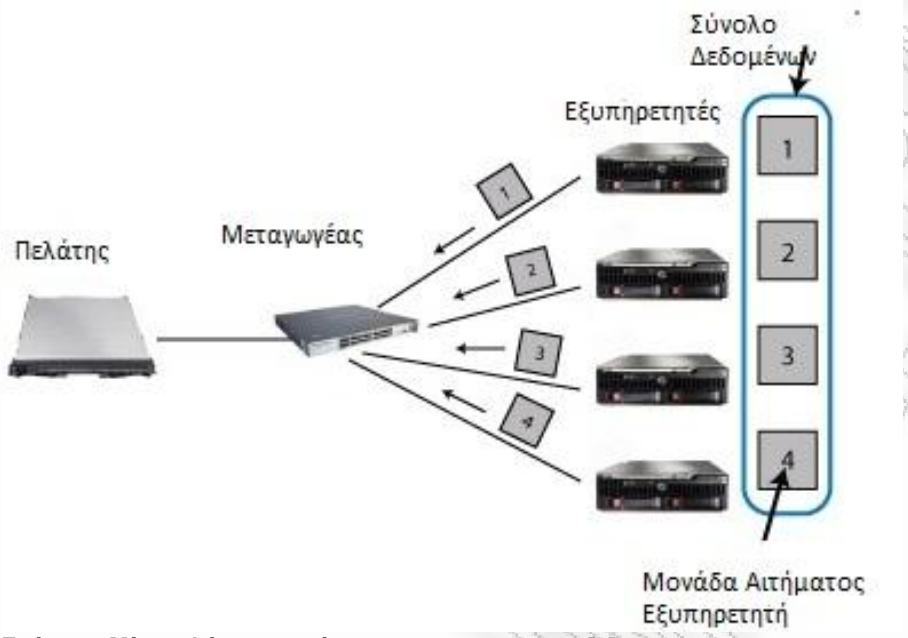
4.1.2 Το πρόβλημα

TCP Incast είναι μια κατάσταση κατά την οποία παρατηρείται δραματική μείωση της απόδοσης όταν πολλοί εξυπηρετητές επικοινωνούν με έναν μόνο παραλήπτη. Κατά τη διάρκεια της επικοινωνίας ο παραλήπτης στέλνει συνεχώς αιτήματα για παραλαβή δεδομένων από πολλούς εξυπηρετητές. Οι εξυπηρετητές μόλις λάβουν το αίτημα αρχίζουν να στέλνουν ταυτόχρονα μεγάλα μεγέθη πληροφοριών στον παραλήπτη με αποτέλεσμα η απόδοση του δέκτη στο επίπεδο εφαρμογής να καταρρέει και το μέγεθος στην πραγματικότητα να μικραίνει αρκετά σε σχέση με τις δυνατότητες της σύνδεσης. Προβλήματα στο επίπεδο μετάδοσης μπορούν να συμβούν σε πολλές εφαρμογές των κέντρων δεδομένων. Για παράδειγμα σε συστοιχία υπολογιστών αποθήκευσης(cluster storage), όταν οι κόμβοι αποθήκευσης απαντούν στα αιτήματα για δεδομένα, στην αναζήτηση στο διαδίκτυο , όταν πολλοί εξυπηρετητές απαντάνε σχεδόν ταυτόχρονα στα ερωτήματα αναζήτησης αλλά στην αυτόματη εκτέλεση σειράς προγραμμάτων (batch processing jobs).

Τα δεδομένα αφαιρούνται από ένα μεγάλο αριθμό εξυπηρετητών και αποθηκεύονται σαν ατομικό αίτημα εξυπηρέτησης πάνω σε κάθε εξυπηρετητή. Για να καταφέρει ένας πελάτης να έχει πρόσβαση σε ένα συγκεκριμένο σύνολο από δεδομένα χρειάζεται να πραγματοποιήσει συγχρονισμένες αναγνώσεις, στέλνοντας αιτήματα σε όλους τους εξυπηρετητές αποθήκευσης για το συγκεκριμένο σύνολο. Ο πελάτης δεν στέλνει επιπλέον αιτήματα για τα δεδομένα μέχρι να λάβει όλα τα δεδομένα για το τρέχον σύνολο. Οι εξυπηρετητές από την άλλη με το που λάβουν τα αιτήματα μεταφέρουν σχεδόν ταυτόχρονα την πληροφορία στον παραλήπτη μέσω Ethernet μεταγωγών. Οι μικρής χωρητικότητας Ethernet ενταμιευτές μπορεί να εξαντληθούν από τον συνεχή καταιγισμό κίνησης που θα έχει σαν αποτέλεσμα στην απώλεια πακέτων και λήξη του χρόνου αναμονής του TCP. Επομένως TCP Incast μπορεί να παρατηρηθεί κατά τη διάρκεια συγχρονισμένων αναγνώσεων συνόλων δεδομένων μέσου ενός αυξανόμενου αριθμού από εξυπηρετητές. Μία αναπαράσταση του προβλήματος φαίνεται στο Σχήμα 4 όπου ένας πελάτης ζητάει δεδομένα από πολλαπλούς εξυπηρετητές μέσω συγχρονισμένων αναγνώσεων.

Το TCP Incast μπορεί να προκληθεί από τις παρακάτω συνθήκες:

- Μεγάλο εύρος ζώνης , «αργά» δίκτυα που συνδέονται με Ethernet μεταγωγούς με μικρούς ενταμιευτές (buffers)
- Πελάτες που στέλνουν αιτήματα παράλληλα
- Εξυπηρετητές που ανταποκρίνονται με ένα τεμάχιο από σύνολο δεδομένων του κάθε αιτήματος



Σχήμα 4: Μία απλή αναπαράσταση του TCP Incast [9]

4.1.3 Λύσεις

Παρακάτω παρουσιάζονται [9] αρκετές μέθοδοι που έχουν κατά καιρούς προταθεί για την αποφυγή του προβλήματος του TCP Incast.

1) Μείωση του αριθμού των εξυπηρετητών ή μείωση στη μεταφορά των δεδομένων.
2) Περιορίζοντας τις απώλειες με τη χρήση μεταγωγών με μεγαλύτερους ενταμιευτές (buffers).
   Μειώνοντας το μέγεθος του ενταμιευτή στον Ethernet μεταγωγέα το TCP Incast μπορεί να καθυστερήσει να συμβεί. Υποστηρίζεται ότι διπλασιάζοντας το μέγεθος του ενταμιευτή στο μεταγωγέα Ethernet διπλασιάζεται ο αριθμός των εξυπηρετητών που στέλνουν ταυτόχρονα δεδομένα πριν παρατηρηθεί το φαινόμενο του TCP Incast. Παρόλα αυτά οι μεταγωγείς με μεγάλους ενταμιευτές εκτός του ότι κοστίζουν εξαντλούνται και γρήγορα όταν χρησιμοποιούνται σε συνδέσεις με μεγάλη ταχύτητα.
3) Περιορίζοντας το χρόνο σύνδεσης αυξάνοντας το μέγεθος της μονάδας αιτήματος εξυπηρετητή.
   Αυξάνοντας το μέγεθος της μονάδας αιτήματος εξυπηρετητή καθυστερείται η έναρξη του TCP Incast. Όμως, οι περισσότερες εφαρμογές ζητάνε δεδομένα σε μικρά τεμάχια της τάξης των 1-256KB οπότε η αύξηση της μονάδας αιτήματος εξυπηρετητή δεν έχει πάντα τα επιθυμητά αποτελέσματα. Επιπλέον, ένα μεγαλύτερο μέγεθος της μονάδας αιτήματος εξυπηρετητή μπορεί να αυξήσει το κλειδωμένο περιεχόμενο εξαιτίας των επικαλύψεων που προκύπτουν κατά το γράψιμο με αποτέλεσμα να εμφανίζεται μικρή απόδοση στο γράψιμο στις εφαρμογές του συστήματος αρχείων.
4) TCP παραλλαγές και TCP Slow Start
   Κατά καιρούς έχουν μελετηθεί διάφορες παραλλαγές του TCP, όπως το TCP Reno , το New Reno και το SACK. Κανένα όμως δεν βοηθάει στη λύση του προβλήματος του TCP Incast.. Επίσης ούτε η ελάττωση της αργής έναρξης του TCP περιορίζει το πρόβλημα.
5) Έλεγχος της ροής στο Ethernet
   Ο έλεγχος ροής στο Ethernet είναι αποτελεσματικός μόνο για τοπολογίες με μονό-μεταγωγείς, ενώ για τοπολογίες με πολλούς μεταγωγείς και πολλά επίπεδα καταρρέει εξαιτίας του ότι μπλοκάρει η αρχική γραμμή.
6) Έλεγχος συμφόρησης

Η εφαρμογή του αλγορίθμου QCN μπορεί να ελέγξει αποτελεσματικά και πολύ γρήγορα τους ρυθμούς σύνδεσης σε ένα κέντρο δεδομένων. Παρόλα αυτά όταν εμφανιστεί το TCP Incast η εφαρμογή του QCN δεν έχει τα επιθυμητά αποτελέσματα.

7) Λύση σε επίπεδο εφαρμογών
   Οι λύσεις που εφαρμόζεται σε επίπεδο εφαρμογών όπως ένα γενικό αίτημα προγραμμα-τισμού είναι πιθανές, αλλά απαιτούν πολύπλοκες τροποποιήσεις σε πολλές TCP εφαρμογές.
8) Μειώνοντας τον ελάχιστο χρονικό όριο αναμετάδοσης (RTO)
   Μειώνοντας την ελάχιστη τιμή του χρόνου αναμετάδοσης (RTO) από τα 200ms στα 200μs το πρόβλημα μειώνεται σημαντικά. Το θέμα είναι ότι τα περισσότερα συστήματα δεν διαθέτουν υψηλής ακρίβειας χρονόμετρα που απαιτούνται για τέτοιου είδους χαμηλούς χρόνους αναμετάδοσης.
9) Χρησιμοποιώντας ενταμιευτές μικρής χωρητικότητας.

4.2 Συμφόρηση

Ο μεγάλος αριθμός εισερχόμενων δεδομένων καθιστά τους μεταγωγείς πιθανούς χώρους για την εμφάνιση συμφόρησης στο δίκτυο. Συγκεκριμένα, η συμφόρηση παρατηρείται όταν το άθροισμα των δεδομένων τα οποία προορίζονται για έναν συγκεκριμένο παραλήπτη μέσα σε κάποιο χρονικό διάστημα, ξεπερνούν τη δυνατότητα του παραλήπτη σε αυτό το διάστημα. Από τη στιγμή που θα συμβεί οι προσωρινοί ενταμιευτές(buffers) αρχίζουν να γεμίζουν με αποτέλεσμα αν το φαινόμενο αυτό διαρκέσει για αρκετό διάστημα τα πακέτα να χαθούν και να μην φτάσουν στον παραλήπτη.

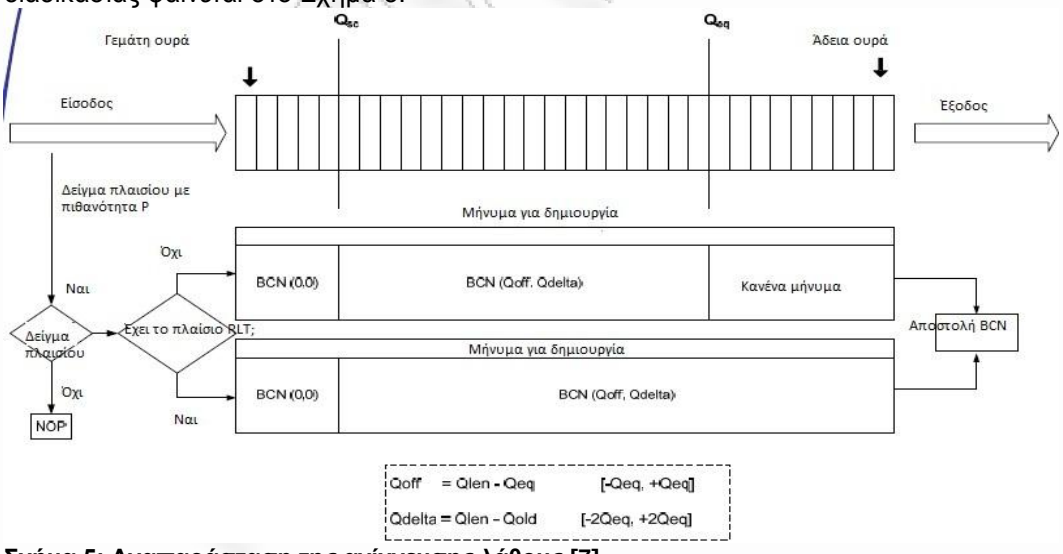
4.2.1 Αλγόριθμοι ελέγχου συμφόρησης

Διάφοροι αλγόριθμοι έχουν αναπτυχθεί για τη μείωση ή για την εξάλειψη των χαμένων πακέτων στους μεταγωγείς που εμφανίζουν συμφόρηση. Όλοι υποθέτουν ότι ο ανιχνευτής συμφόρησης ενσωματώνεται στο μεταγωγέα, ενώ η συμφόρηση συμβαίνει. Οι μεταγωγείς ανιχνεύουν τη συμφόρηση και δημιουργούν ένα μήνυμα συμφόρησης που ανατροφοδοτείται στην πηγή με βάση το υπολογιζόμενο μέτρο κυκλοφοριακής συμφόρησης, και οι ρυθμιστικές αρχές στις πηγές θα προσαρμόσουν το ρυθμό των μεμονωμένων ροών σύμφωνα με τα μηνύματα κυκλοφοριακής συμφόρησης που λαμβάνουν από μεταγωγείς. Παρακάτω ακολουθεί μία περιγραφή των αλγορίθμων αυτών.

4.2.1.1 Αλγόριθμος BCN

Ο αλγόριθμος BCN λειτουργεί σε τρεις φάσεις: ανιχνεύει το λάθος, το σηματοδοτεί και στη συνέχεια ακολουθεί η αντίδραση της πηγής.

Κατά την ανίχνευση του λάθους χρησιμοποιούνται δύο κατώτατα όρια για την αναφορά των ανεκτών επιπέδων συμφόρησης στο μεταγωγέα. Το Q_{eq} που αντιπροσωπεύει το μήκος της ουράς σε κατάσταση ισορροπίας και το Q_{sc} που αντιπροσωπεύει το μήκος της ουράς σε κατάσταση συμφόρησης. Η δειγματοληψία των εισερχόμενων πακέτων στο μεταγωγέα γίνε-ται με πιθανότητα P_m. Το μέγεθος της συμφόρησης υπολογίζεται ως $e_i = -(Q_{off}(t) + w*Q_{\delta}(t))$, *όπου* $Q_{off} = q(t) - Q_{eq}$, $Q_{\delta} = Q_a - Q_d$, $q(t)$ υποδηλώνει το στιγμιαίο μέγεθος της ουράς, Q_a και Q_d υποδηλώνουν τον αριθμό των αφιχθέντων και εξερχόμενων πακέτων μεταξύ δύο συνεχόμενων δειγματοληψιών. Το w είναι μία μη αρνητική σταθερά, βάρος. Η αναπαράσταση αυτής της διαδικασίας φαίνεται στο Σχήμα 5.



Σχήμα 5: Αναπαράσταση της ανίχνευσης λάθους [7]

Η διαδικασία της σηματοδότησης έχει ως εξής: Τα αφιχθέντα πακέτα στο μεταγωγέα δειγματοληπτούνται με πιθανότητα P_m και για κάθε πακέτο το μήνυμα BCN ανταπόκρισης γεννάται με βάση τα παρακάτω χρησιμοποιώντας την ετικέτα 802.1Q :

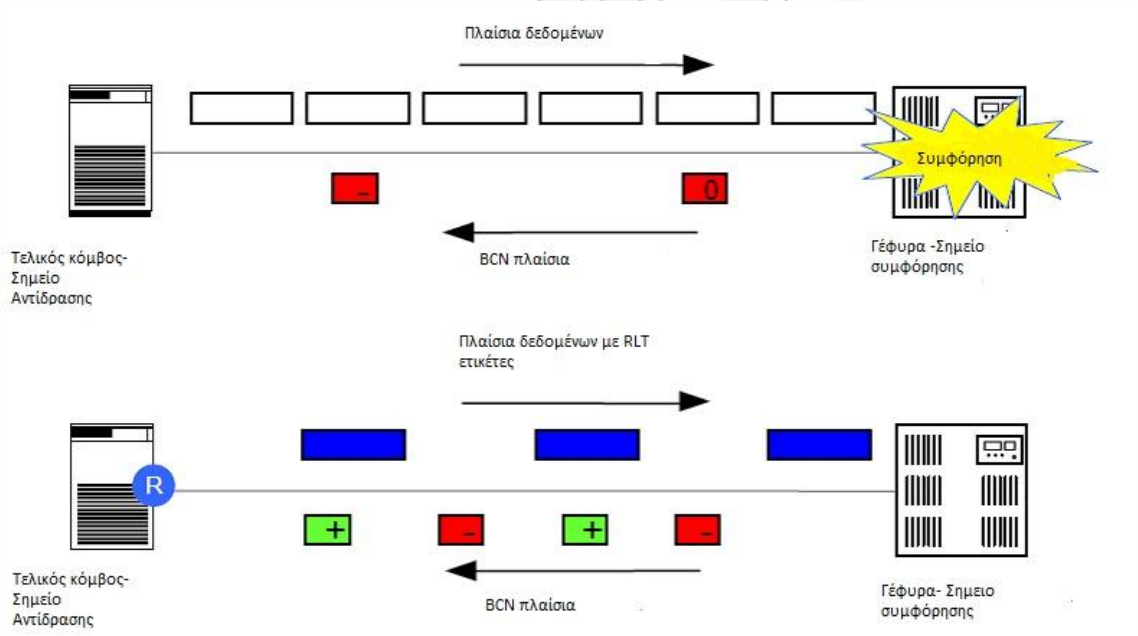
Αν το πακέτο δεν περιέχει ετικέτα ρυθμιστή ταχύτητας τότε:

1. *Αν $q(t) < Q_{eq}$, δεν στέλνεται κανένα μήνυμα BCN*
2. *Αν $Q_{eq} < q(t) < Q_{sc}$, στέλνεται κανονικό μήνυμα BCN*
3. *Αν $q(t) > Q_{sc}$, στέλνεται BCN μήνυμα διακοπής (STOP)*

Αν το πακέτο περιέχει ετικέτα ρυθμιστή ταχύτητας τότε:

1. *Αν $q(t)<Q_{eq}$, και το CPID πεδίο στην ετικέτα 802.1Q, το οποίο αντιπροσωπεύει μοναδικό αριθμό (ID) για το σημείο συμφόρησης, ταιριάζει με τον μοναδικό αριθμό του μεταγωγέα, τότε αποστέλλεται θετικό BCN μήνυμα.*
2. *Αν $Q_{eq} < q(t)< Q_{sc}$, στέλνεται κανονικό BCN μήνυμα*
3. *Αν $q(t)> Q_{sc}$, στέλνεται BCN μήνυμα διακοπής (STOP)*

Η διαδικασία της σηματοδότησης παρουσιάζεται γραφικά στο Σχήμα 6.

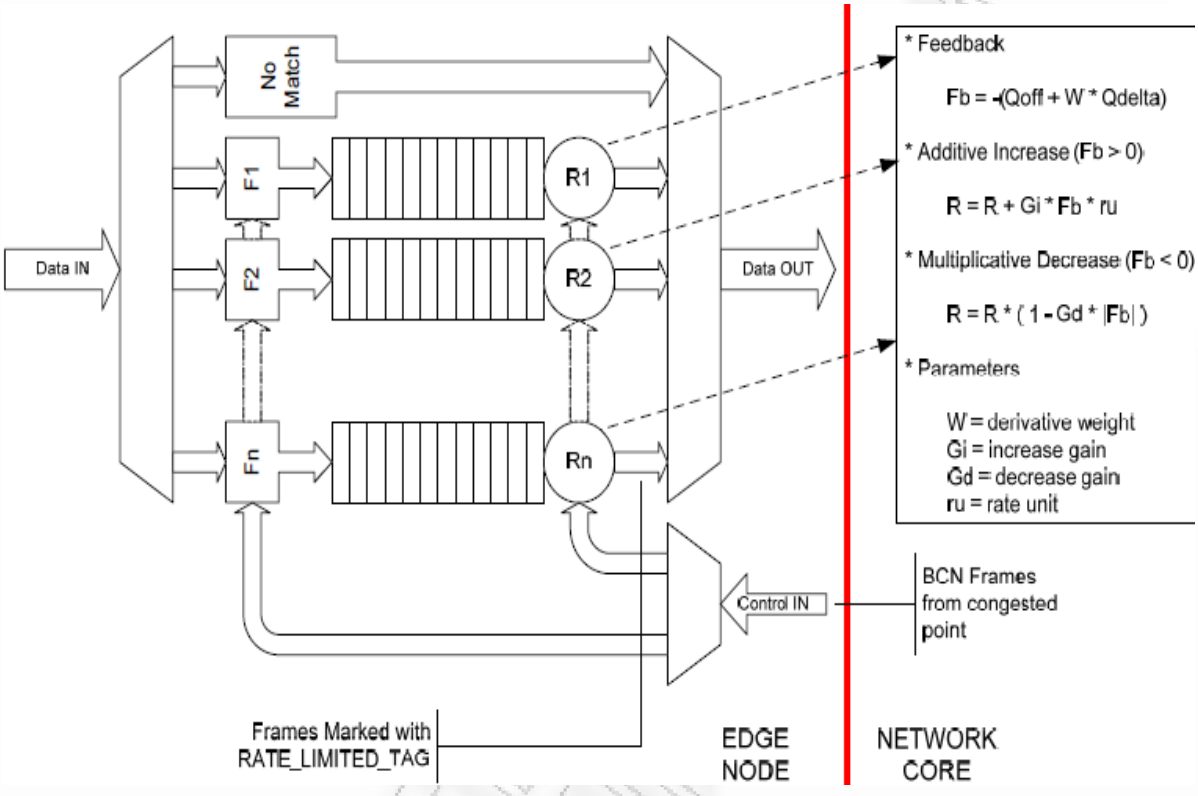


Σχήμα 6: Αναπαράσταση της σηματοδότησης [7]

Μόλις η πηγή λάβει μήνυμα διακοπής (STOP) ο ρυθμιστής ταχύτητας αντιδρά σταματώντας να στέλνει πακέτα για κάποια περίοδο και επανέρχεται αργότερα με ρυθμό C/K, όπου C είναι η δυνατότητα της σύνδεσης και K είναι μία σταθερά που εξαρτάται από τον αριθμό των ροών που υπάρχουν στο δίκτυο. Μόλις η πηγή λάβει ένα κανονικό μήνυμα BCN ο ρυθμιστής ταχύτητας προσαρμόζει τον ρυθμό του χρησιμοποιώντας τον αλγόριθμο AIMD (Additive Increase and Multiplicative Decrease) όπως φαίνεται παρακάτω:

$$ri = \begin{cases} ri + GieiRu, & \alpha v\ ei > 0 \\ ri\ (1 + Gdei), & \alpha v\ ei < 0 \end{cases}$$

Όπου το Ru αναπαριστά τον αύξοντα ρυθμό , και τα Gi και Gd υποδηλώνουν την πρόσθετη αύξηση και την πολλαπλασιαστική μείωση αντίστοιχα [9]. Η απεικόνιση της αντίδρασης φαίνεται στο Σχήμα 7.



Σχήμα 7: Απεικόνιση της αντίδρασης [7]

4.2.1.2 Αλγόριθμος QCN

Ο αλγόριθμος QCN αποτελείται από δύο μέρη: τις δυναμικές του μεταγωγέα ή του σημείου συμφόρησης (CP) και τις δυναμικές ελέγχου της κίνησης στο δίκτυο (RL) ή του σημείου αντίδρασης (RP). Στο CP, ο ενταμιευτής του μεταγωγού συνδέεται σε μία επικαλυφθείσα σύνδεση, εξετάζει όλα τα εισερχόμενα πακέτα και στη συνέχεια ανατροφοδοτεί το επίπεδο της σοβαρότητας της συμφόρησης πίσω στην πηγή που έστειλε τα πακέτα. Ενώ στα RP, RL η πηγή μειώνει το ρυθμό αποστολής της βασισμένη στο μήνυμα συμφόρησης που θα πάρει από το CP και αυξάνει το ρυθμό της εθελοντικά για να ανακτήσει το χαμένο εύρος ζώνης και να αναζητήσει επιπλέον διαθέσιμο εύρος ζώνης.

Ο αλγόριθμος που χρησιμοποιείται στο σημείο συμφόρησης λειτουργεί ως εξής [9]: Ο σκοπός του CP είναι να διατηρεί τη χωρητικότητα του ενταμιευτή σε ένα λειτουργικό σημείο, Q_{eq}. Το CP ελέγχει τα εισερχόμενα πακέτα με μία πιθανότητα εξαρτώμενη από τη σοβαρότητα της συμφόρησης F_b. Το F_b υπολογίζεται ως εξής $F_b = -Q_{off} + w*Q_\delta$ όπου Q_{off} και Q_δ ορίζονται όπως και στον BCN αλγόριθμο. Το w είναι μία μη-αρνητική σταθερά, που θεωρείται ότι είναι το δύο(2) για την έναρξη της εφαρμογής. Το F_b καλύπτει έναν συνδυασμό από την υπέρβαση του μεγέθους της ουράς Q_{off} και από την υπέρβαση του ρυθμού Q_δ. Όντως , το Q_δ είναι παράγωγο του μεγέθους της ουράς , ίσο με τον εισερχόμενο ρυθμό και μικρότερο από τον εξερχόμενο ρυθμό. Επομένως, όταν το F_b προκύπτει αρνητικό είτε οι ενταμιευτές είτε η σύνδεση είτε και τα δύο έχουν υπερκαλυφθεί και ένα μήνυμα συμφόρησης που περιέχει την τιμή του F_b στέλνεται στην πηγή. Ειδάλλως καμία ανταπόκριση-ενημέρωση δεν στέλνεται.

Ο αλγόριθμος που χρησιμοποιείται στο σημείο αντίδρασης λειτουργεί ως εξής: Ο αλγόριθμος RP προσαρμόζει το ρυθμό αποστολής μειώνοντας το ρυθμό αποστολής βασισμένος στο μήνυμα συμφόρησης που θα πάρει από το CP, και αυξάνοντάς τον στη συνέχεια για να ανακτήσει το χαμένο εύρος ζώνης. Η μείωση του ρυθμού ακολουθεί μετά τη λήψη του

συγκεκριμένου μηνύματος με αποτέλεσμα ο τρέχων ρυθμός (CR) και ο επιθυμητός ρυθμός (TR) να ανανεώνονται ως εξής:

TR = CR

CR = CR (1 – Gd |Fb|)

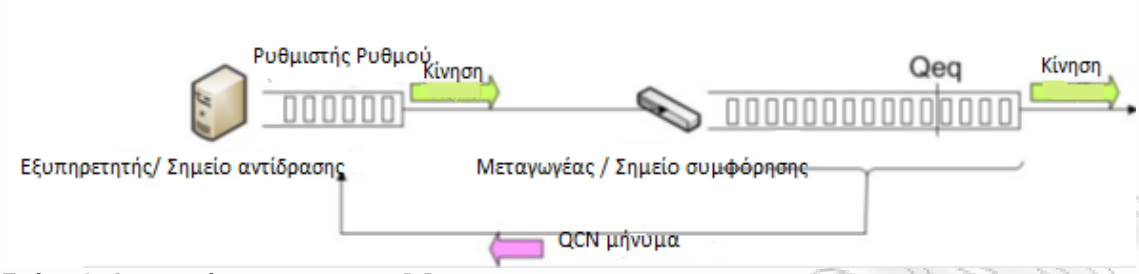
Όπου η σταθερά Gd επιλέγεται με τέτοιο τρόπο ώστε ο ρυθμός αποστολής να μη μπορεί να μειωθεί περισσότερο από 50% και επομένως *Gd*|Fbmax|=1/2*, όπου Fbmax δηλώνει τη μέγιστη τιμή του Fb.

Ακολουθεί περιγραφή για τον τρόπο που γίνεται η μείωση του ρυθμού: Ο μετρητής των bytes, Byte Counter (*BC*) και ο χρονοδιακόπτης αύξησης ρυθμού(Rate Increaser Timer), εισάγονται στο RP για την αύξηση του ρυθμού. Ο BC είναι ένας μετρητής στο RP για τη μέτρηση του αριθμού των bytes που μεταδίδονται από το RL. Όπως ένα ρολόι στο RP που ασχολείται με τη χρονομέτρηση του ρυθμού μείωσης , ο Rate Increase Timer εισάγεται για να επιτρέπει τη γρήγορη ανάκτηση του εύρους ζώνης, όταν ο ρυθμός αποστολής είναι πολύ μικρός ενώ το διαθέσιμο εύρος ζώνης γίνεται τεράστιο. Ο ρυθμός αυξάνει στο RP και έχει σαν αποτέλεσμα τις φάσεις γρήγορης ανάκτησης (Fast Recover, FR) και ενεργής αύξησης (Active Increase, AI).Ο μετρητής byte επαναφέρεται κάθε φορά που παρατηρείται μείωση του ρυθμού και εισάγει τη FR κατάσταση. Στην FR κατάσταση, ο μετρητής byte μετρά τα bytes που μεταδίδονται από το RL και αυξάνει τον κύκλο του BC κατά 1 όταν τα bytes που μεταδίδονται είναι ίσα με BC_THRESHOLD. Μετά από κάθε κύκλο, το RL αυξάνει το ρυθμό για να ανακτήσει κάποιο από το εύρος ζώνης που έχασε στην προηγούμενη μείωση του ρυθμού μετάδοσης. Μετά από FR_THRESHOLD κύκλους (όπου FR_THRESHOLD είναι μία μεταβλητή που επιλέγεται να είναι ίση με 5 κύκλους σε), ο BC εισάγει την κατάσταση AI για να μεταδώσει BC_THRESHOLD/2 bytes δεδομένων σε κάθε κύκλο του μετρητή byte.

Ο χρονοδιακόπτης αύξησης του ρυθμού λειτουργεί όμοια με τον BC. Στην FR κατάσταση, ο χρονομετρητής ολοκληρώνει έναν κύκλο των T ms (το T έχει διάρκεια ίση με 10 ms). Μετά από FR_THRESHOLD κύκλους, εισάγει την AI κατάσταση όπου κάθε κύκλος ορίζεται σε T/2 ms. Ο byte και ο timer μετρητής αποφασίζουν από κοινού την αύξηση του ρυθμού στο RL. Μετά την άφιξη του μηνύματος, ο καθένας λειτουργεί ανεξάρτητα και εκτελούν τους αντίστοιχους κύκλους στο FR .

Οι μετρητές byte και timer καθορίζουν την κατάσταση στο RL και ο ρυθμός αποστολής ανανεώνεται ως εξής:

1) Το RL είναι στο FR αν και μόνο αν ο byte και ο μετρητής timer είναι στο FR. Σε αυτή την περίπτωση όταν είτε ο byte counter ή ο rate increase timer συμπληρώνει έναν κύκλο , ο TR παραμένει ως έχει ενώ ο CR διαμορφώνεται ως εξής:
   CR = ½ (CR+TR)
2) Το RL είναι στο AI αν και μόνο αν είτε ο μετρητής byte είτε ο μετρητής timer είναι στο AI. Σε αυτή την περίπτωση, όταν είτε ο byte counter ή ο byte timer ολοκληρώσουν έναν κύκλο, το TR και το CR ανανεώνονται ως εξής:
   $TR = TR + R_{AI}$
   CR = ½ (CR + TR)
   Όπου R_{AI} είναι μία σταθερά που συνήθως έχει την τιμή 5 Mbps
3) Το RL είναι στη φάση Hyper-Active Increase όταν μαζί ο BC και ο Rate Increaser Timer είναι στο AI. Σε αυτή την περίπτωση, TR και CR ανανεώνονται ως εξής :
   $TR = TR + R_{HAI} *(min (BC\_cycle, Timer\_cycle) - FR\_THRESHOLD)$
   CR = ½ (CR + TR),
   Όπου η σταθερά R_{HAI} είναι ίση με 50 Mbps. Άρα η αύξηση του TR στην HAI φάση συμβαίνει σε πολλαπλάσια των 50 Mbps. Είναι πολύ σημαντικό να σημειωθεί ότι το RL πάει στη κατάσταση HAI μόνο αφότου σταλούν τουλάχιστον 5BC_THRESHOLD πακέτα και αφού περάσουν 5T ms από τη λήψη του τελευταίου μηνύματος συμφόρησης. Έτσι διασφαλίζεται ότι η μείωση του ρυθμού συμβαίνει μόνο όταν το RL προσδώσει στο δίκτυο επαρκή δυνατότητα.



Σχήμα 8: Αναπαράσταση του QCN [9]

4.2.1.3 Αλγόριθμοι FECN και E-FECN

Ο αλγόριθμος FECN [9] είναι ένας βρόχος με σταθερό ρυθμό ανατροφοδότησης του μηχανισμού ελέγχου. Όλες οι ροές αρχικοποιούνται με το μέγιστο ρυθμό. Οι πηγές περιοδικά εξετάζουν την κατάσταση συμφόρησης κατά μήκος της διαδρομής προς τον προορισμό. Το πεδίο του ρυθμού στο μήνυμα-εξέτασης τροποποιείται κατά μήκος του μονοπατιού προώθησης από τους μεταγωγείς, εάν το διαθέσιμο εύρος ζώνης σε κάθε μεταγωγέα στο μονοπάτι προώθησης είναι μικρότερο από την τιμή του ρυθμού στο μήνυμα. Όταν οι πηγές λάβουν τα μηνύματα-εξέτασης που επιστρέφουν από τον προορισμό, ο ρυθμιστής προσαρμόζει το ρυθμό αποστολής όπως υποδεικνύεται στο λαμβανόμενο μήνυμα. Όλες οι ροές αντιμετωπίζονται ισότιμα στο FECN δεδομένου ότι ο ίδιος ρυθμός δημοσιεύεται από το μεταγωγέα. Το FECN χρησιμοποιεί το ρυθμό με βάση τον αισθητήρα φορτίου για την ανίχνευση της συμφόρησης. Στο σημείο συμφόρησης, ο μεταγωγέας περιοδικά μετρά τη μέση τιμή άφιξης Ai και το στιγμιαίο μήκος ουράς qi, όπου i είναι ο δείκτης του διαστήματος μέτρησης. Ο αποδεκτός φόρτος μπορεί να μετρηθεί ως

$\rho_i = \frac{Ai}{f(qi)\,x\,C}$, όπου C είναι η δυνατότητα της σύνδεσης και f (q_i) είναι μία συνάρτηση ελέγχου της ουράς υπερβολή η οποία εξασφαλίζει σταθερό μήκος ουράς και ορίζεται παρακάτω:

$$f(qi) = \begin{cases} \dfrac{aQeq}{(a-1)qi + Qeq} \\ \max\left(c, \dfrac{bQeq}{(b-1)qi + Qeq}\right), \end{cases} \quad \begin{matrix} \text{εάν } qi \leq Qeq \\ \text{αλλίως} \end{matrix}$$

όπου a, b, c είναι μεταβλητές . Για $q < Q_{eq}$, $f(q) > 1$, η συνάρτηση ελέγχου ουράς προσπαθεί να αυξηθεί στο ρυθμό δημοσίευσης. Για $q > Q_{eq}$, $f(q) < 1$ η συνάρτηση ελέγχου ουράς προσπαθεί να μειώσει το ρυθμό δημοσίευσης.

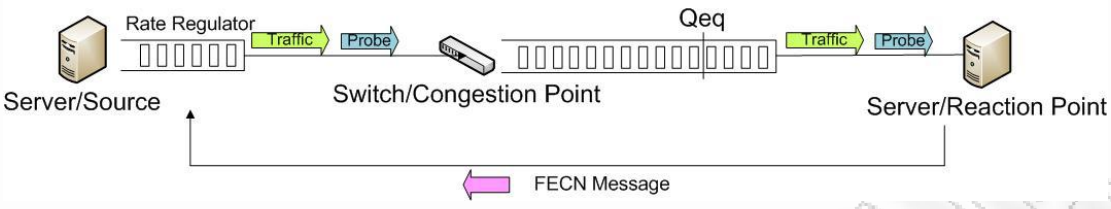
Η κατανομή εύρους ζώνης μπορεί να υπολογιστεί ως:

$r_{i+1} = \frac{ri}{\rho i} = \frac{Cf(qi)}{\frac{Ai}{ri}}$

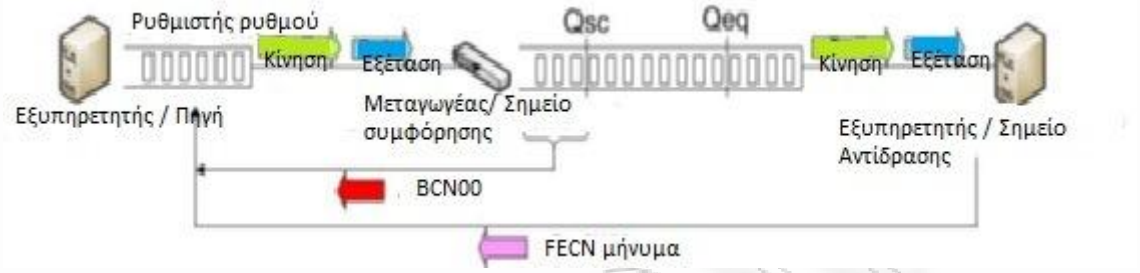
όπου C $f(q_i)$ θα μπορούσε να θεωρηθεί ως το διαθέσιμο αποτελεσματικό

εύρος ζώνης, και $N = \frac{Ai}{ri}$ είναι ο πραγματικός αριθμός των ροών. Αν $r_{i+1} < r$ όπου r είναι η τιμή του ρυθμού στα μηνύματα, τότε η τιμή του ρυθμού στο μήνυμα-εξέτασης ορίζεται με r_{i+1}

Οι E-FECN λειτουργίες είναι σχεδόν ίδιες όπως αυτές στο FECN. Η διαφορά στο E-FECN είναι ότι οι μεταγωγείς μπορούν απευθείας να ανατροφοδοτήσουν την πηγή κάτω από σοβαρή κυκλοφοριακή συμφόρηση ($Q(t) > Q_{sc}$). Κάτω από σοβαρή συμφόρηση, ο μεταγωγέας στέλνει ένα ειδικό μήνυμα BCN00. Μόλις ο ρυθμιστής ταχύτητας στην πηγή λάβει αυτό το μήνυμα μειώνει τον αρχικό ρυθμό αποστολής του.



Σχήμα 9: Αναπαράσταση του FECN [9]



Σχήμα 10: Αναπαράσταση του E-FECN [9]

4.2.2 Σύγκριση των αλγορίθμων ελέγχου συμφόρησης

Παρακάτω, ακολουθεί μία σύγκριση των αλγορίθμων ελέγχου συμφόρησης που περιγράφηκαν στην ενότητα 4.2.1:

1. Δικαιοσύνη
   Έρευνες έχουν δείξει ότι ο BCN επιτυγχάνει μία σχετική δικαιοσύνη. Δεν μπορεί να χαρακτηριστεί απόλυτα δίκαιος ή άδικος αλγόριθμος. Η δικαιοσύνη στους FECN και E-FECN εξασφαλίζεται από την ανακάλυψη του αλγορίθμου συμφόρησης στο μεταγωγέα καθώς επιτυγχάνει το ίδιο ποσοστό σε όλες τις ροές που περνούν από το μεταγωγέα. Στον QCN, το μήνυμα της ανταπόκρισης στέλνεται μόνο στην πηγή του απλού πακέτου και επομένως ο QCN επιτυγχάνει και αυτός σχετική δικαιοσύνη όπως συμβαίνει και με τον BCN.
2. Έλεγχος ανταπόκρισης
   Ο QCN και ο FECN χρησιμοποιούν προς τα πίσω ανταπόκριση ελέγχου. Ο FECN παρέχει προς τα εμπρός ανταπόκριση και ο αλγόριθμος E-FECN χρησιμοποιεί προς τα εμπρός έλεγχο της συμφόρησης μαζί με BCN00 μηνύματα για να ενημερώσει την πηγή ότι υπάρχει συμφόρηση στον εξυπηρετητή και συγκεκριμένα στο μεταγωγέα.
3. Υπερκάλυψη
   Η υπερκάλυψη στον αλγόριθμο BCN είναι υψηλή και απρόβλεπτη. Ομοίως και στον αλγόριθμο QCN η υπερκάλυψη είναι ένας παράγοντας που δε μπορεί να προβλεφθεί, ωστόσο είναι μικρότερη σε σχέση με την υπερκάλυψη που παρατηρείται στον αλγόριθμο BCN καθώς υπάρχει μόνο αρνητικό μήνυμα που στέλνεται για να μειωθεί ο ρυθμός αποστολής και η πιθανότητα δειγματοληψίας είναι ανάλογη με το δείκτη συμφόρησης. Η υπερκάλυψη FECN είναι μικρή και προβλέψιμη γιατί το μήνυμα FECN στέλνεται περιοδικά με αμελητέο χάσιμο φορτίου της τάξης των 20 bytes. Η υπερκάλυψη στο E- FECN είναι μεγαλύτερη από το FECN εξαιτίας του μηνύματος BCN00 που εμπλέκεται στον E- FECN αλγόριθμο.
4. Ο ρυθμός της σύγκλισης σε επίπεδο δικαιοσύνης
   Ο αλγόριθμος BCN είναι αργός στη σύγκλιση και πετυχαίνει μακροπρόθεσμα δικαιοσύνη. Οι αλγόριθμοι FECN και E- FECN μπορούν να επιτύχουν εξαιρετικό επίπεδο δικαιοσύνης μέσα σε μικρό χρονικό διάστημα καθώς όλες οι πηγές λαμβάνουν την ίδια ανταπόκριση.
5. Ρύθμιση της συμφόρησης
   Ο ρυθμός της πηγής στους αλγορίθμους BCN και QCN μπορεί να μειωθεί γρηγορότερα από ότι στον αλγόριθμο FECN γιατί το μήνυμα στους πρώτους στέλνεται κατευθείαν από το σημείο

συμφόρησης ενώ το μήνυμα εξέτασης στον αλγόριθμο FECN πρέπει να κάνει ολόκληρο ταξίδι μέχρι να επιστρέψει πίσω στην πηγή. Η ταχύτητα ρύθμισης της συμφόρησης βελτιώνεται στον αλγόριθμο E-FECN καθώς υπάρχει η δυνατότητα της χρήσης του μηνύματος BCN00 όταν υπάρχει αρκετή συμφόρηση.

6. Ταλάντωση της απόδοσης
   Ο αλγόριθμος BCN επιφέρει μεγάλες ταλαντώσεις στην απόδοση. Οι αλγόριθμοι FECN και E-FECN δεν επιφέρουν μεγάλες ταλαντώσεις στην απόδοση της πηγής. Η ταλάντωση της απόδοσης βελτιώνεται στον αλγόριθμο QCN με το ρυθμό αύξησης να καθορίζεται από τον μετρητή byte και τον increase timer στην πηγή.
7. Αισθητήρας φορτίου
   Οι αλγόριθμοι BCN και QCN στέλνουν τις δυναμικές των ουρών πίσω στις πηγές, ενώ ο FECN χρησιμοποιεί έναν ρυθμό βασισμένο στο φορτίο για να ανιχνεύσει τη συμφόρηση.
8. Αποτυχία της σύνδεσης
   Αν η σύνδεση χαθεί οι αλγόριθμοι BCN, QCN, E-EFCN μπορούν να χρησιμοποιήσουν ένα ενημερωτικό μήνυμα το οποίο το αποστέλλουν στην πηγή για να την ενημερώσουν να ελαττώσει ή και ακόμα να σταματήσει τη μετάδοση πακέτων. Από την άλλη ο αλγόριθμος FCEN δεν έχει τη δυνατότητα να ενημερώσει την πηγή με αποτέλεσμα αυτή να διατηρεί τον ίδιο ρυθμό αποστολής και κατά συνέπεια τα πακέτα να χάνονται. Για τη αντιμετώπιση αυτού του προβλήματος εισάγεται ένα χρονικό όριο ανίχνευσης έτσι ώστε οι πηγές να στέλνουν με χαμηλότερο ρυθμό κατά τη διάρκεια της αποσύνδεσης.
9. Γρήγορη εκκίνηση
   Στους αλγορίθμους BCN και QCN, οι πηγές αρχικοποιούνται με το μεγαλύτερο δυνατό ρυθμό και τον μειώνουν όταν λάβουν αρνητικό μήνυμα από το μεταγωγέα. Στον αλγόριθμο FECN, οι πηγές ξεκινούν με χαμηλό ρυθμό και ανακτούν σταθερούς ρυθμούς όσο επιστρέφουν επανειλημμένοι έλεγχοι.
10. Αριθμός των ρυθμιστών ρυθμού
    Ο αλγόριθμος FECN χρειάζεται τόσους ρυθμιστές όσες είναι οι ταυτόχρονες ροές. Εξαιτίας της εισαγωγής του μηνύματος BCN00 κάτω από συγκεκριμένη συμφόρηση, ο αριθμός των ρυθμιστών του ρυθμού ποικίλει.[9]

5. Οι αρχιτεκτονικές των κέντρων δεδομένων

Οι αρχιτεκτονικές που χρησιμοποιούνται για τα κέντρα δεδομένων χωρίζονται σε δύο κατηγορίες. Η μία βασίζεται στους μεταγωγείς οι οποίοι παρέχουν εσωτερική επικοινωνία και δρομολόγηση με έξυπνο τρόπο. Η δεύτερη κατηγορία βασίζεται στους εξυπηρετητές, οι οποίοι με πολλαπλές network interface card (nic) θύρες, συμμετέχουν επίσης στην επικοινωνία και στη δρομολόγηση της πληροφορίας. Παρακάτω παρουσιάζονται οι πιο πρόσφατες αρχιτεκτονικές:

5.1 Switch-Centric αρχιτεκτονικές

5.1.1 Αρχιτεκτονική Monsoon

Η αρχιτεκτονική Monsoon καθιστά τα δίκτυα των κέντρων δεδομένων ευρέως διαθέσιμα για cloud υπηρεσίες όπου μεγάλος αριθμός εξυπηρετητών συνεργάζονται για να ανταπεξέλθουν σε μεγάλους όγκους δουλειάς.

Η αρχιτεκτονική αυτή μειώνει το κόστος της δικτυακής υποδομής ενώ ταυτόχρονα αυξάνει τη δυνατότητα υποστήριξης του εύρους ζώνης και τη λειτουργικότητα των απαιτήσεων των κέντρων δεδομένων. Τα δύο βασικά χαρακτηριστικά της αρχιτεκτονικής Monsoon είναι το μεγάλο επίπεδο2 του δικτύου που ενώνει όλους τους εξυπηρετητές μέσα στο κέντρο δεδομένων καθώς και οι ευέλικτοι τρόποι με τους οποίους μοιράζονται τα αιτήματα στους εξυπηρετητές. Από μία προοπτική υψηλού επιπέδου αρχιτεκτονικής, οι διαφορές ανάμεσα το επίπεδο2 (Ethernet) και στο επίπεδο3 (IP) συρρικνώνονται, όταν ειδικά όλο το δίκτυο βρίσκεται σε ένα μοναδικό κτίριο, όπως το κέντρο δεδομένων. Παρόλα αυτά, υπάρχει ένας αριθμός από πρακτικούς παράγοντες που οδηγούν την αρχιτεκτονική Monsoon να συνδέει όλους τους εξυπηρετητές μέσω ενός μοναδικού χώρου στο επίπεδο Ethernet. Πρώτα από όλα είναι το κόστος, το πρέπει να ελαττώνεται όσο το περισσότερο γίνεται. Δεύτερον, υπάρχει ανάγκη για περιορισμός του κατακερματισμού των εξυπηρετητών: με ιεραρχικές διευθύνσεις, οι εξυπηρετητές που χρησιμοποιούνται για να επεκτείνουν μία εφαρμογή πρέπει να τοποθετούνται στην ίδια δικτυακή ιεραρχία με την εφαρμογή. Με ένα τεράστιο χώρο επίπεδων διευθύνσεων, μία ομάδα από ελεύθερους εξυπηρετητές μπορεί να μοιράζεται από πολλές εφαρμογές. Το τρίτο σημαντικό σημείο είναι ότι πρέπει να σημειώνονται όσο το δυνατόν μικρότερες αναταραχές. Συγκεκριμένα οι υπάρχουσες εφαρμογές, τα συστήματα διαχείρισης και οι πολιτικές ασφαλείας κάνουν εκτενή χρήση των IP διευθύνσεων. Εφαρμόζοντας την αρχιτεκτονική Monsoon κάτω από το επίπεδο IP, αυτά τα συστήματα μπορούν να λειτουργούν κανονικά χωρίς τροποποιήσεις. Συνδυάζοντας, λοιπόν, τους τρεις αυτούς παράγοντες, το επίπεδο Ethernet αποδεικνύεται ξεκάθαρα νικητής, αφού τρέχει κάτω από το IP, είναι φθηνότερο σε κόστος και έχει καλύτερες αποδόσεις στην προώθηση πληροφοριών βασισμένο στις επίπεδες διευθύνσεις. Μία Ethernet θύρα έχει σχεδόν το μισό κόστος από μια IP θύρα και είναι γνωστό πως τα κέντρα δεδομένων περιέχουν εκατοντάδες χιλιάδες θύρες.

Όλοι οι εξυπηρετητές συνδέονται στο επίπεδο2 δίκτυο το οποίο είναι σχεδιασμένο να έχει πλήρη προσβασιμότητα χωρίς να υπερκαλύπτονται οι συνδέσεις , δηλαδή κάθε εξυπηρετητής μπορεί να επικοινωνεί με όποιον άλλο εξυπηρετητή με ταχύτητα 1Gbps. Το επίπεδο IP του Monsoon δικτύου συνδέει το κέντρο δεδομένων στο δίκτυο και χρησιμοποιεί το Equal Cost Multipath για να διασπείρει τα μηνύματα που λαμβάνει από το διαδίκτυο σε όλους τους δρομολογητές πρόσβασης. Όταν τα αιτήματα εισάγονται στην περιοχή του επιπέδου Ethernet, οι δρομολογητές του επιπέδου πρόσβασης χρησιμοποιούν συνεπές hashing για να στείλουν τα αιτήματα στη δημόσια εικονική(virtual) IP κάθε εφαρμογής για όλους τους εξυπηρετητές που δρουν σαν ισορροπιστές φορτίου(load balancers) της εφαρμογής. Τελικά οι ισορροπιστές φορτίου διαδίδουν τα αιτήματα χρησιμοποιώντας μια συνάρτηση κατανομής του φόρτου που εξαρτάται από την κάθε εφαρμογή.

Η ικανότητα του Monsoon να διαδίδει τα πακέτα που προορίζονται για μία IP διεύθυνση πάνω από το σύνολο των εξυπηρετητών σημαίνει ότι οι ισορροπιστές φορτίου μπορούν να διαχωριστούν από τους απλούς εξυπηρετητές χωρίς να τη χρήση υψηλής απόδοσης υλικού. Το γεγονός αυτό σημαίνει εξοικονόμηση κόστους και προσθήκη ευελιξίας. Πρέπει να σημειωθεί ότι, γενικά, οι ισορροπιστές φορτίου χρειάζονται υποστήριξη από υλικό για να διατηρήσουν τον υψηλό ρυθμό δεδομένων, όμως στην περίπτωση του Monsoon τα αιτήματα στέλνονται στους

εξυπηρετητές, ο φόρτος σε κάθε εξυπηρετητή μπορεί να διατηρηθεί σε τέτοιο επίπεδο όπου η προώθηση να γίνεται σε επίπεδο λογισμικού. Όταν το προσφερόμενο φορτίο ξεκινά να κατακλύζει τους ρυθμιστές φορτίου, επιπλέον εξυπηρετητές μπορούν να βοηθήσουν ώστε να μειώσουν αυτόν το φόρτο. Αυτό το κόστος είναι μικρότερο από ένα ισοδύναμο ισορροπιστή φορτίου σε επίπεδο υλικού. Επιπλέον, η χρήση απλών εξυπηρετητών ως ισορροπιστές φορτίου τους καθιστά πλήρως προγραμματιζόμενους, με αλγορίθμους που είναι συντονισμένοι με τις τρέχουσες εφαρμογές των κέντρων δεδομένων και όχι με τους αλγορίθμους που προσφέρουν οι έμποροι για το firmware. Η αρχιτεκτονική αυτή προσφέρει κάθε φορά ανάκτηση απέναντι σε αποτυχίες στον κάθε δρομολογητή πρόσβασης, ισορροπιστή φορτίου ή εξυπηρετητή στο κέντρο δεδομένων. Η λειτουργία κάθε εξυπηρετητή παρακολουθείται συνεχώς και όταν ένα πρόβλημα ανιχνευθεί, τότε ο εξυπηρετητής αποσύρεται και δε στέλνονται πλέον νέα αιτήματα σε αυτόν. [16]

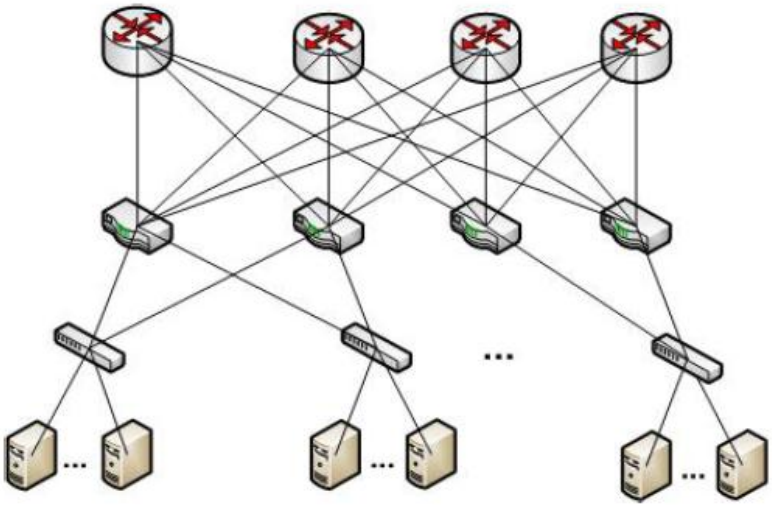
5.1.2 Αρχιτεκτονική VL2

Η εικονική αρχιτεκτονική στο επίπεδο Ethernet (Virtual Layer2) χρησιμοποιεί επίπεδη (flat) διευθυνσιοδότηση για να επιτρέψει τα στιγμιότυπα υπηρεσιών να τοποθετηθούν οπουδήποτε μέσα στο δίκτυο. Επιπλέον, χρησιμοποιεί Valiant Load Balancing (VLB) για εξαπλώσει την κίνηση μέσα στα μονοπάτια του δικτύου και το τελικό σύστημα βασίζεται στην ανάλυση της διεύθυνσης για να κλιμακωθεί σε μεγάλο κέντρο δεδομένων.

Η VL2 είναι μία αρχιτεκτονική τριών επιπέδων , που έχει πολλές ομοιότητες με την τυπική αρχιτεκτονική των κέντρων δεδομένων, όπως φαίνεται και στο Σχήμα 12. Η βασική διαφορά είναι ότι η τοπολογία εφαρμόζεται με τους μεταγωγείς που ανήκουν στο ακραίο και στο επίπεδο συνάθροισης. Ο μεγάλος αριθμός από μονοπάτια ανάμεσα σε κάθε δυάδα από ενδιάμεσους μεταγωγείς βοηθά στην ομαλή υποβάθμιση του εύρους ζώνης στις περιπτώσεις που η σύνδεση χάνεται.

Η αρχιτεκτονική VL2 χρησιμοποιεί δύο διαφορετικών κατηγοριών IPs: τις IP διευθύνσεις που προσδιορίζουν την τοποθεσία (location-specific,LAs) και στις IP διευθύνσεις που προσδιορίζουν την εφαρμογή (application-specific, AAs). Η υποδομή του δικτύου λειτουργεί χρησιμοποιώντας τις LAs, όλοι οι μεταγωγείς και οι διεπαφές εκχωρούνται σε LAs και οι μεταγωγείς τρέχουν ένα πρωτόκολλο που βασίζεται στην IP διεύθυνση που διαδίδει μόνο εκείνα τα LAs. Αυτό επιτρέπει στους μεταγωγείς να ανακτούν την ολοκληρωμένη τοπολογία όπως και να προωθούν τα πακέτα ενθυλακωμένα με τα LAs μέσα από τα συντομότερα μονοπάτια. Από την άλλη, οι εφαρμογές χρησιμοποιούν AAs, που διατηρούνται αναλλοίωτες χωρίς να εξαρτώνται από το πώς αλλάζουν οι θέσεις των εξυπηρετητών. Κάθε AA συσχετίζεται με ένα LA από το TOR μεταγωγέα στον οποίο συνδέεται ο εξυπηρετητής. Η αντιστοιχία μεταξύ AAs και LAs αυτή αποθηκεύεται σε φάκελο της VL2.

Από τη στιγμή που η υποδομή του δικτύου λειτουργεί χρησιμοποιώντας μόνο LAs ενώ οι εφαρμογές λειτουργούν χρησιμοποιώντας AAs, ο VL2 agent σε κάθε εξυπηρετητή χρειάζεται να παγιδεύει και να ενθυλακώνει τα πακέτα με την LA διεύθυνση του ακραίου μεταγωγέα στον προορισμού. Μόλις το πακέτο φτάσει στον τελικό μεταγωγέα του προορισμού, ο μεταγωγέας το μεταφέρει στον προορισμό AA που εμπεριέχει την εσωτερική κεφαλίδα. Η VL2 διατηρεί κατάλογο για την αναζήτηση και ενημέρωση των αντιστοιχήσεων των διευθύνσεων από LA σε AA [8].



Σχήμα 12: Αναπαράσταση της VL2 αρχιτεκτονικής [9]

5.1.3 Αρχιτεκτονική Portland

Η αρχιτεκτονική Portland χαρακτηρίζεται από επεκτασιμότητα και από δρομολόγηση δευτέρου επιπέδου που είναι ανεκτική σε λάθη. Απευθύνεται στο περιβάλλον των κέντρων δεδομένων Portland και αναθέτει τις εσωτερικές ψευδό MAC διευθύνσεις σε όλους τους τελικούς υπολογιστές υποδοχής ώστε να κωδικοποιεί τις τοποθεσίες τους στην τοπολογία. Οι ψευδό MAC διευθύνσεις ενεργοποιούν αποτελεσματικές και αποδεδειγμένες προωθήσεις μηνυμάτων με τη χρήση μικρού αριθμού επιπέδων μεταγωγών.

Η τοπολογία Portland κατασκευάζεται βασισμένη στη fat-tree τοπολογία. Οι μεταγωγείς που ανήκουν στο ακραίο επίπεδο και στο επίπεδο συνάθροισης τοποθετούνται σε ένα pod και διαμορφώνουν ένα διμερή γράφο και οι μεταγωγείς στο επίπεδο του πυρήνα μαζί με τα pods διαμορφώνουν μία δεύτερη τοπολογία στην οποία κάθε μεταγωγέας συνδέεται με ένα pod.

- Η θέση των ψευδό-MAC διευθύνσεων και ο διαχειριστής (fabric manager) τους

Η βάση για αποτελεσματική προώθηση και δρομολόγηση καθώς και η μετάβαση σε εικονική μηχανή (virtual machine) στο Portland είναι η ιεραρχική PMAC διεύθυνση. Σε κάθε τελικό υπολογιστή υποδοχής εκχωρείται μία μοναδική PMAC διεύθυνση, η οποία κωδικοποιεί την τοποθεσία του κάθε τελικό υπολογιστή υποδοχής στην τοπολογία. Η PMAC διεύθυνση ακολουθεί τη μορφή pod: position:port:vmid, όπου το pod (αποτελείται από 16 bits) αναπαριστά τον αριθμό των pods στον αρχικό μεταγωγέα , το position (αποτελείται από 8bits) είναι ο αριθμός της θέσης του στο pod, port (8bits) είναι ο αριθμός της θύρας που συνδέεται ο υπολογιστής υποδοχής, και το vmid(16bits) χρησιμοποιείται για πολλαπλές εικονικές μηχανές στην ίδια φυσική μηχανή. Οι ακραίοι μεταγωγείς κάνουν το ταίριασμα ανάμεσα στις πραγματικές MAC διευθύνσεις και στις PMAC ώστε να διατηρούν τις MAC διευθύνσεις χωρίς τροποποιήσεις στους τελικούς υπολογιστές υποδοχής. Ο αριθμός του pod και ο αριθμός της θέσης σε κάθε pod ανακτάται από τους ακραίους μεταγωγείς μέσω του πρωτοκόλλου Location Discovery Protocol (LDP). Όταν ένας ακραίος μεταγωγέας ανιχνεύει μία νέα MAC διεύθυνση, δημιουργεί μία εγγραφή στον τοπικό PMAC πίνακα ταιριάζοντας το AMAC με PMAC και ταυτόχρονα επικοινωνεί αυτό το ταίριασμα στο fabric manager , ο οποίος είναι μία διαδικασία χρήστη σε συγκεκριμένη μηχανή για την παροχή συνδρομής σε ARP ανάλυση. Ο διαχειριστής διατηρεί πληροφορίες για την διαμόρφωση του δικτύου, όπως για παράδειγμα η τοπολογία και τη χρησιμοποιεί για να ανταποκρίνεται στα ARP αιτήματα. Όταν ένας τελικός υπολογιστής υποδοχής μεταδίδει ένα ARP αίτημα, ο ακραίος μεταγωγέας που συνδέεται απευθείας με αυτόν θα διακόψει το ARP αίτημα για μία IP στη MAC διεύθυνση και προωθεί το αίτημα στο fabric manager. Ο διαχειριστής με τη σειρά του ελέγχει τον PMAC πίνακα για να δει να υπάρχει μία εγγραφή διαθέσιμη για την τρέχουσα IP. Εάν ναι, επιστρέφει μία PMAC διεύθυνση στον ακραίο μεταγωγέα, ειδάλλως ο fabric manager επιστρέφει τη μετάδοση σε όλους τους τελικούς υπολογιστές υποδοχής για ανάκτηση του ταιριάσματος προωθώντας το ARP αίτημα σε κάθε

μεταγωγέα που ανήκει στο επίπεδο του πυρήνα, όπου διανέμεται σε όλα τα pods και τελικά σε όλους τους ακραίους μεταγωγείς. Ο τελικός υπολογιστής υποδοχής θα απαντήσει με το AMAC του, το οποίο θα ξαναγραφεί από τον ακραίο μεταγωγέα στον κατάλληλο PMAC πριν προωθηθεί στο ζητούμενο υπολογιστή υποδοχής και στο fabric manager.

- Δρομολόγηση

Οι μεταγωγείς στο Portland χρησιμοποιούν τις θέσεις στην τοπολογία για να πραγματοποιούν πιο αποτελεσματική δρομολόγηση. Το Portland χρησιμοποιεί των αριθμό των pod και τον αριθμό των μεταγωγών για τους ακραίους μεταγωγείς, τους μεταγωγείς συνάθροισης και τους μεταγωγείς του πυρήνα. Οι μεταγωγείς στο Portland στέλνουν περιοδικά ένα LDM στις θύρες τους για να ανταλλάσουν πληροφορία με τους άλλους μεταγωγείς. Το μήνυμα αυτό περιέχει όλη την πληροφορία για τους μεταγωγείς, τον αριθμό του pod, τον αριθμό της θέσης, το επίπεδο του δένδρου και τη θύρα ενός μεταγωγέα. Το κλειδί πίσω από τα LDPs είναι το γεγονός ότι οι ακραίοι μεταγωγείς λαμβάνουν LDPs μόνο από θύρες που είναι συνδεδεμένες με μεταγωγείς συνάθροισης. Εάν ένας μεταγωγέας ακούει LDP μηνύματα από θύρες μικρότερες από το μισό από τις συνολικές του θύρες, τότε αποφασίζει ότι είναι μεταγωγέας του ακραίου επιπέδου. Οι μεταγωγείς του επιπέδου συνάθροισης ρυθμίζουν το επίπεδό τους μόλις μάθουν ότι κάποιες από τις θύρες τους συνδέονται με μεταγωγείς του ακραίου επιπέδου.

Τέλος, όταν οι μεταγωγείς του πυρήνα μάθουν το επίπεδό τους μόλις επιβεβαιώσουν ότι όλες οι θύρες τους συνδέονται στους μεταγωγείς συνάθροισης. Οι μεταγωγείς συνάθροισης βοηθούν στην ανάθεση μία μοναδικής θέσης στους ακραίους μεταγωγείς του κάθε pod. Το LDP αξιοποιεί το διαχειριστή για την ανάθεση μοναδικών αριθμών pods σε όλους τους μεταγωγείς του ίδιου pod. Οι μεταγωγείς του πυρήνα μαθαίνουν τον αριθμό του pod από τους απευθείας συνδεδεμένους μεταγωγείς συνάθροισης. Όταν προωθείται ένα πακέτο, οι μεταγωγείς του πυρήνα ανιχνεύουν τον αριθμό του pod στον PMAC προορισμό για να αποφασίσουν την κατάλληλη θύρα εξόδου. Οι μεταγωγείς συνάθροισης μαθαίνουν τον αριθμό της θέσης από όλους τους απευθείας συνδεδεμένους μεταγωγείς συνάθροισης. Οι μεταγωγείς συνάθροισης καθορίζουν αν το πακέτο κατευθύνεται για τον υπολογιστή υποδοχής στο ίδιο pod ή όχι. Αν ναι το πακέτο θα προωθηθεί στην θύρα εξόδου που αντιστοιχεί στην θέση εισόδου της PMAC. Ειδάλλως, προωθείται σε οποιαδήποτε σύνδεση του μεταγωγέα συνάθροισης στο επίπεδο του πυρήνα. Το πρωτόκολλο προώθησης που χρησιμοποιείται στο Portland είναι δεν περιέχει βρόχους επανάληψης. Το πακέτο προωθείται πάντα σε έναν μεταγωγέα συνάθροισης ή σε ένα μεταγωγέα πυρήνα και μετά προς τα κάτω στο μοναδικό προορισμό. Παροδικές επαναλήψεις και καταιγίδες από εκπομπές αποφεύγονται διασφαλίζοντας ότι μόλις το πακέτο ξεκινήσει να ταξιδεύει προς τα κάτω δεν υπάρχει πιθανότητα να ταξιδεύσει πίσω στην τοπολογία. Το LDP επιβλέπει την κατάσταση του μεταγωγέα και της σύνδεσης στα Portland δίκτυα. Αν περάσει κάποιος χρόνος χωρίς τη λήψη LDM, ο μεταγωγέας θεωρεί ότι η σύνδεση έχει αποτύχει. Ο μεταγωγέας που ανιχνεύει την παραπάνω κατάσταση ενημερώνει τον διαχειριστή για τις αποτυχίες και ο διαχειριστής διατηρεί έναν πίνακα από λογικά λάθη με την πληροφορία της κάθε σύνδεσης για όλη την τοπολογία και τον ενημερώνει κάθε φορά με τη νέα πληροφορία. Στο τέλος, ο διαχειριστής ενημερώνει όλους τους μεταγωγείς που επηρεάζονται από την αποτυχία, πάνω στην οποία επαναϋπολογίζουν μεμονωμένα τους δικούς τους πίνακες προώθησης βασισμένοι στην τοπολογία που διαμορφώνεται κάθε φορά.[17]

5.1.4 Αρχιτεκτονική SPAIN

Η αρχιτεκτονική SPAIN έχει σχεδιαστεί για να βελτιώσει τη διχοτόμηση του εύρους ζώνης παρέχοντας πολλαπλά μονοπάτια μικρού κόστους και μεταγωγείς Ethernet πάνω σε αυθαίρετες τοπολογίες. Το SPAIN συγχωνεύει ένα σύνολο από προϋπολογισμένα μονοπάτια, και μέσα από ένα σύνολο δένδρων κάθε δένδρο ταιριάζεται με ένα ξεχωριστό VLAN. Η αρχιτεκτονική SPAIN αποτελείται από τρεις φάσεις: τον υπολογισμό του μονοπατιού, την εγκατάσταση του μονοπατιού και τέλος την επιλογή του μονοπατιού. Τα πρώτα δύο βήματα τρέχουν offline και το τελικό βήμα τρέχει online στους τελικούς υπολογιστές υποδοχής. Το SPAIN είναι ανεκτικό σε σφάλματα και αυτό συμβαίνει γιατί παρέχει πολλαπλά μονοπάτια ανάμεσα σε κάθε ζευγάρι από υπολογιστές υποδοχής.

- Υπολογισμός μονοπατιού

Ο σκοπός του υπολογισμού του μονοπατιού είναι να υπολογίσει ένα σύνολο από μονοπάτια χωρίς επαναλήψεις που συνδέουν ζευγάρια από τελικούς υπολογιστές υποδοχής μέσα από την

υπάρχουσα τοπολογία του δικτύου. Ο μηχανισμός της SPAIN αρχιτεκτονικής διατηρεί την υπάρχουσα τοπολογία και ρυθμίζει τους μεταγωγείς με τα κατάλληλα VLANs. Το SPAIN αξιοποιεί το πρωτόκολλο LINK-Layer-Discovery για να αποφασίσει προγραμματισμένα πλέον την τοπολογία ολόκληρου του επιπέδου Ethernet. Η ανάθεση του VLAN πραγματοποιείται χρησιμοποιώντας το SNMP(Simple Network Management Protocol) πρωτόκολλο στο SPAIN.

- Εγκατάσταση μονοπατιού

Το SPAIN ταιριάζει το προϋπολογισμένο σύνολο μονοπατιού μέσα στο ελάχιστο σύνολο από VLANs στο βήμα της εγκατάστασης μονοπατιού. Έχει αποδειχθεί ότι το πρόβλημα της ελαχιστοποίησης του VLAN, δηλαδή της ανάθεσης μονοπατιών στο μικρότερο αριθμό από VLANs, είναι NP δύσκολο. Ένας άπληστος VLAN-packing ευρετικός αλγόριθμος έχει αναπτυχθεί για να επεξεργάζεται τα μονοπάτια που υπολογίζονται σειριακά στον υπολογισμό μονοπατιού και συνθέτουν το ελάχιστο αριθμό από VLANs. Εξαιτίας της σειριακής επεξεργασίας κάθε μονοπατιού από το σύνολο μονοπατιών, ο ευρετικός αλγόριθμος δεν έχει καλές αποδόσεις. Για να αυξηθεί η επεκτασιμότητα του αλγορίθμου ένας παράλληλος αλγόριθμος ανά προορισμό που υπολογίζει τα VLANs έχει προταθεί. Αυτός ο αλγόριθμος υπολογίζει ένα σύνολο από υπογράφους ανά προορισμό και μετά αυτοί οι υπογράφοι από διαφορετικές πηγές ενώνονται για να ελαττώσουν τον συνολικό αριθμό των VLANs που απαιτούνται.

- Επιλογή μονοπατιού

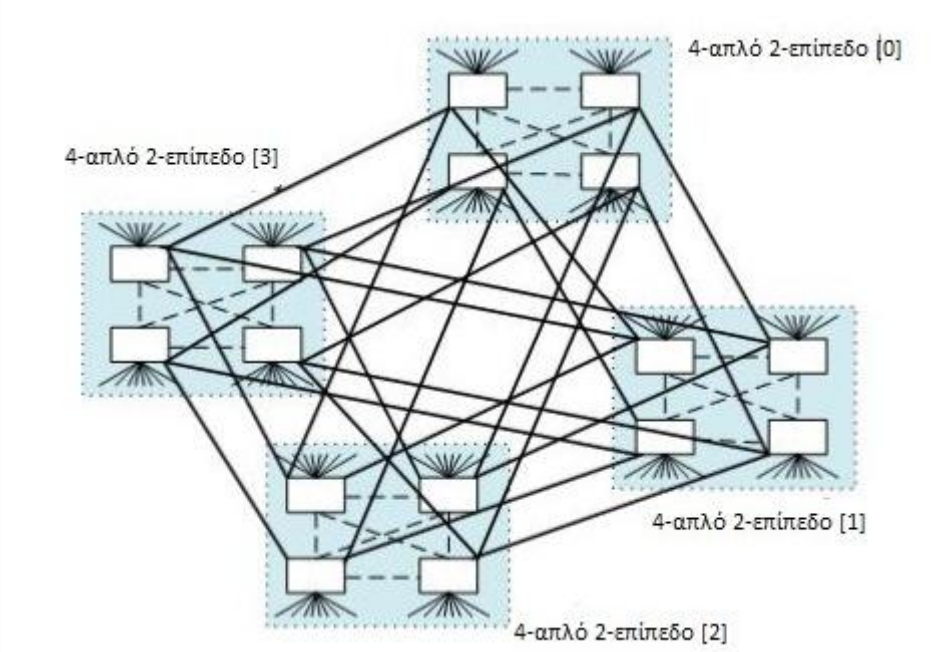
Η μεγάλη διχοτόμηση του SPAIN επιτυγχάνεται εξαπλώνοντας την κίνηση μέσα από πολλαπλά VLANs. Το SPAIN απαιτεί αλλαγές στο λογισμικό του τελικού υπολογιστή υποδοχής για να αποφασίσει αποτελεσματικά την εξάπλωση του φορτίου μέσα στο δίκτυο και να ενεργοποιήσει την επανεπιλογή του VLAN για τη ροή. Όταν η ροή ξεκινά, ο τελικός υπολογιστής υποδοχής βρίσκει ένα σύνολο από χρησιμοποιούμενα VLANs για να φτάσει στον ακραίο μεταγωγέα στον οποίο συνδέεται ο προορισμός. Στη συνέχεια ο τελικός υπολογιστής υποδοχής τυχαία επιλέγει ένα VLAN για τη νέα ροή.[18]

5.1.5 Αρχιτεκτονική Energy Proportional

Η κατανάλωση ενέργειας ώθησε το ενδιαφέρον για την ανάπτυξη ενός ενεργειακά αποτελεσματικού κέντρου δεδομένων. Η τοπολογία flattened butterfly (FBFLY) έχει εξαιρετικές ενεργειακές αποδόσεις αναλογικά με τις άλλες αρχιτεκτονικές των κέντρων δεδομένων.

- Δομή του Flattened Butterfly

Η flattened butterfly είναι ένα πολυδιάστατο απευθείας δίκτυο όπου κάθε διάσταση είναι πλήρως συνδεδεμένη με ένα FBFLY. Μία πλειάδα (x, y, z) μπορεί να χρησιμοποιηθεί για να περιγράψει ένα y-πλό z-επίπεδο με x κόμβους ανά μεταγωγέα στη flattened butterfly δομή. Ένα (x, y, z) (z>2) FBLY δίκτυο μπορεί να χτιστεί με y (x,y,z-1) FBLY δίκτυα συνδέοντας κάθε μεταγωγέα σε κάθε (x, y, z-1) FBFLY δίκτυο με τους ομότιμους μεταγωγείς του.
Παράδειγμα : Έστω ότι έχουμε μία 3-διάστατη, 4-πλή 3-επίπεδη FBFLY τοπολογία δικτύου. Σε κάθε 4-το 2-επίπεδο FBFLY δίκτυο οι μεταγωγείς είναι πλήρως συνδεδεμένοι. Το 3-διάστατο, 4-στο 3-επίπεδο FBFLY δίκτυο χτίζεται με 4 2-διάστατα 4-τα 2 επίπεδα FBLY δίκτυα συνδέοντας κάθε 2-διάστατο 4-το 2-επίπεδο FBFLY δίκτυο με τα ομότιμα του στις 3 άλλες ομάδες. Το (8,4,3) FBFLY δίκτυο φιλοξενεί 128 εξυπηρετητές με 16 μεταγωγείς το καθένα με 14 θύρες.



Σχήμα 13: Αναπαράσταση από μία τρισδιάστατη 4-πλή 3-επιπέδη FBFLY τοπολογία [9]

- Χαρακτηριστικά της αρχιτεκτονικής Flattened Butterfly

Τα χαρακτηριστικά της FBFLY αρχιτεκτονικής δικτύου μπορούν να συνοψιστούν παρακάτω:
Επεκτασιμότητα: Ένα FBFLY μπορεί να επεκταθεί εκθετικά με βάση τον αριθμό των διαστάσεων. Ένα (x,y,z) flatted butterfly δίκτυο μπορεί να φιλοξενήσει xy^{z-1} εξυπηρετητές και y^{z-1} μεταγωγείς. Κάθε μεταγωγέας έχει x+(y-1)(z-1) θύρες.
Τοπική διαμόρφωση: Στη flattened butterfly τοπολογία, η πρώτη διάσταση μπορεί να χρησιμοποιεί μικρές ηλεκτρικές συνδέσεις. Γενικά, ο αριθμός των φθηνών καλωδίων που χρησιμοποιούνται σε ένα (x, y, z) FBFLY δίκτυο είναι $y^{(z-2)}$(x*y+ y*(y-1)/2). [19]

5.2 Server-Centric αρχιτεκτονικές

5.2.1 Αρχιτεκτονική FiConn

Η FiConn είναι μία καινούργια δομή διασύνδεσης των εξυπηρετητών η οποία εφαρμόζει μία επεκτάσιμη και υψηλής αποτελεσματικότητας δομή για κοινούς εξυπηρετητές οι οποίοι έχουν δύο Ethernet θύρες και κοινούς μεταγωγείς. Η αρχιτεκτονική αυτή παίρνει σαν δεδομένο ότι οι κοινοί εξυπηρετητές που χρησιμοποιούνται στα σημερινά κέντρα δεδομένων, συνήθως διαθέτουν δύο ενσωματωμένες Ethernet θύρες, μία για τη σύνδεση δικτύου και μία άλλη εφεδρική. Ο FiConn αλγόριθμος χρησιμοποιεί δρομολόγηση η οποία εκμεταλλεύεται όλες τις διαθέσιμες δυνατότητες της σύνδεσης βασισμένος στις δυναμικές της σύνδεσης και ισορροπεί τη χρήση διαφορετικών συνδέσεων για να αναπτύξει ολόκληρη την απόδοση του δικτύου.

- Αρχιτεκτονική FiConn

Η FiConn αρχιτεκτονική ορίζει μία αναδρομική δομή του δικτύου σε επίπεδα. Ένα $FiConn_k$ επιπέδου k αποτελείται από πολλά $FiConn_{k-1}$ επιπέδου (k-1). Κάθε εξυπηρετητής μπορεί να οριστεί από μία (k+1)-άδα , $[\alpha_{k,....,} \alpha_{1,}\alpha_0]$, όπου α_0 ορίζει το s στο δικό του $FiConn_{0,}$ και το α_l με (1 ≤ l ≤ k) ορίζει το $FiConn_l$ περιλαμβάνοντας το s στο δικό του $FiConn_{l.}$ Σε ένα $FiConn_k$ υπάρχουν $u_k = a_0 + \Sigma^k_{l=1} (\alpha_l * N_{l-1})$ εξυπηρετητές σε ένα $FiConn_{k,}$,όπου N_l είναι ο συνολικός αριθμός των εξυπηρετητές στο $FiConn_{l.}$ Όταν κατασκευάζεται ένα υψηλού επιπέδου FiConn, το χαμηλό επίπεδο FiConn οργανώνει τη χρήση των μισών από τις διαθέσιμες εφεδρικές θύρες για διασυνδέσεις και εφαρμόζει ένα πλέγμα από $FiConn_{k-1}$ ενότητες.
Το $FiConn_0$ είναι η βασική κατασκευαστική μονάδα, η οποία αποτελείται από n εξυπηρετητές και ένα n-θύρο μεταγωγέα συνδέοντας n εξυπηρετητές. Αν υπάρχουν b εξυπηρετητές με διαθέσιμες εφεδρικές θύρες στο $FiConn_{k-1}$, ο αριθμός των $FiConn_{k-1}$ στο $FiConn_k$, το g_k είναι ίσο με b/2 $FiConn_{k-1}$ χρησιμοποιώντας τις εφεδρικές θύρες , μία για κάθε $FiConn_{k-1.}$

- Δρομολόγηση στο FiConn

Στην αρχιτεκτονική FiConn προτείνεται μία άπληστη προσέγγιση με άλμα προς άλμα (hop-by-hop) εγκατάσταση σε κάθε μονοπάτι που είναι ενήμερο για την κίνηση σε κάθε ενδιάμεσο εξυπηρετητή. Κάθε εξυπηρετητής ψάχνει να ισορροπήσει τον όγκο της κίνησης ανάμεσα στις δύο εξερχόμενες συνδέσεις που έχει. Συγκεκριμένα, ο εξυπηρετητής πηγή επιλέγει πάντα την εξερχόμενη σύνδεση με το μεγαλύτερο διαθέσιμο εύρος ζώνης για να προωθήσει την κίνηση. Για τον ενδιάμεσο εξυπηρετητή επιπέδου-l, εάν η εξερχόμενη σύνδεση χρησιμοποιεί TOR είναι η σύνδεση του επιπέδου l και το διαθέσιμο εύρος ζώνης του επιπέδου 0 είναι μεγαλύτερο, η σύνδεση επιπέδου l προσπερνιέται διαλέγοντας τυχαία ένα τρίτο $FiConn_{l-1}$ στο $FiConn_l$ για να μεταφέρει την κυκλοφορία ειδάλλως η κίνηση δρομολογείται από το TOR.

- Χαρακτηριστικά της αρχιτεκτονικής FiConn

Το FiConn δίκτυο χαρακτηρίζεται από τις παρακάτω ιδιότητες:
Επεκτασιμότητα**:** Έστω ότι ο αριθμός των εξυπηρετητών στο FiConn , είναι N και μεγαλώνει εκθετικά με τα FiConn επίπεδα. Αν ορίσουμε ότι ο συνολικός αριθμός των εξυπηρετητών στο $FiConn_k$ είναι ίσος με $N_{k,}$ όπου $N_k \geq 2^{k+2} * (n/4^{2k})$ όπου n είναι ο αριθμός των εξυπηρετητών στο $FiConn_{0.}$
Βαθμός: ο μέσος βαθμός ενός κόμβου του εξυπηρετητή στο $FiConn_k$ είναι $2- 1/2^k$
Διάμετρος: Η διάμετρος του FiConn είναι O(logN), η οποία είναι μικρή και μπορεί να υποστηρίξει εφαρμογές σε πραγματικό χρόνο. Το άνω όριο της διαμέτρου του $FiConn_k$ είναι $2^{k+1} -1.$
Συνδέσεις επιπέδου l: Ο αριθμός των συνδέσεων επιπέδου l στο $FiConn_k$ ορίζεται από $L_{l,}$, όπου*:* $L_l = 4 * L_l +1$, *εάν* $l=0$

$L_l = 2 * L_l +1$, *εάν* $0< l < k$

Ανοχή σε σφάλματα: Η διχοτόμηση του εύρους του FiConn είναι O(N= logN), υπονοώντας ότι το FiConn μπορεί να αντισταθεί αποτελεσματικά στα λάθη των συνδέσεων. Το κατώτερο όριο είναι $N_k / (4*2^k)$, όπου N_k είναι ο συνολικός αριθμός των εξυπηρετητών στο $FiConn_{k.}$
Κόστος: Ο αριθμός των μεταγωγών που χρησιμοποιούνται στο FiConn είναι αρκετά μικρός. Για την κατασκευή ενός κέντρου δεδομένων με N εξυπηρετητές με n-θυρους μεταγωγείς, ο αριθμός των μεταγωγών που χρειάζονται με το Fat-Tree είναι 5N/n, ενώ ο αριθμός στο FiConn είναι N/n.
Δρομολόγηση: Το μέγιστο μέγεθος του μονοπατιού δρομολόγησης ανάμεσα σε οποιοδήποτε servers είναι $2*3^k-1$. [20]

5.2.2 Αρχιτεκτονική DPillar

Η DPillar αρχιτεκτονική χρησιμοποιεί απλούς δίθυρους εξυπηρετητές PC και plug-and-play Ethernet μεταγωγείς για την ανάπτυξη μίας επεκτάσιμης αρχιτεκτονικής διασύνδεσης του κέντρου δεδομένων. Ένα από τα πιο σημαντικά χαρακτηριστικά του DPillar είναι ότι το κέντρο δεδομένων μπορεί να επεκταθεί χωρίς καμία φυσική αναβάθμιση των ήδη υπαρχόντων εξυπηρετητών.

- Η αρχιτεκτονική

Όπως αναφέρθηκε και παραπάνω, ένα DPillar δίκτυο χτίζεται με δίθυρους εξυπηρετητές και n-θυρους μεταγωγείς Ethernet, οι οποίοι οργανώνονται σε k στήλες από εξυπηρετητές [H_0, H_1, ….H_{k-1}] και k στήλες από μεταγωγείς [S_0, S_1, ….S_{k-1}]. Οι στήλες των εξυπηρετητών και οι στήλες των μεταγωγέων τοποθετούνται εναλλάξ γύρω από ένα κύκλο: η στήλη εξυπηρετητή H_i γειτνιάζει με τη στήλη μεταγωγέα S_i και τη $S_{(i+k-1)\%k}$ και η στήλη μεταγωγέα S_i γειτνιάζει με τις στήλες των εξυπηρετητών H_i και $H_{(i+k-1)\%k}$, όπου το σύμβολο % την γνωστή μαθηματική πράξη μόντουλο. Κάθε εξυπηρετητής στο DPillar μπορεί να οριστεί με μία μοναδικό σύμβολο (C, v^{k-1},…, v^0) , όπου C (0 ≤ C ≤ k-1), είναι ο δείκτης της στήλης του εξυπηρετητή και v^i είναι ένας ακέραιος ανάμεσα σε 0 και (n/2-1). Αυτοί οι εξυπηρετητές που έχουν τα ίδια σύμβολα εκτός του v^C (v^{k-1}, …v^C,.. v^0), στη στήλη H_C του εξυπηρετητή και $H_{(C+1)\%k}$ συνδέονται στη στήλη μεταγωγέα S_C. Ένα DPillar δίκτυο μπορεί να αναπαρασταθεί μοναδικά από μία πλειάδα (n,k), όπου n είναι ο αριθμός των θυρών του μεταγωγέα και k είναι ο αριθμός των στηλών του εξυπηρετητή.

- Η δρομολόγηση

Η δρομολόγηση πακέτου και η διαδικασία προώθησης στο DPillar μπορεί να χωριστεί σε δύο φάσεις στη σπειροειδή φάση και στη φάση δαχτυλίδι. Στη σπειροειδή φάση το πακέτο στέλνεται από την πηγή εξυπηρετητή σε έναν ενδιάμεσο εξυπηρετητή του οποίου η ετικέτα είναι ίδια με την ετικέτα του εξυπηρετητή προορισμού. Στη φάση δαχτυλίδι, το πακέτο προωθείται στον προορισμό από έναν ενδιάμεσο εξυπηρετητή Οι αποτυχίες, συμπεριλαμβανομένων των αποτυχιών των εξυπηρετητών και των μεταγωγέων στα δίκτυα των κέντρων δεδομένων είναι πολύ κοινές και επομένως το DPillar περιέχει ένα σχήμα δρομολόγησης ανεχτικό στα σφάλματα για να προσπερνά ένα μεγάλο εύρος από αποτυχίες στο DPillar. Το πρωτόκολλο Hello χρησιμοποιείται για να ανακαλύψει τα λάθη της σύνδεσης. Ο εξυπηρετητής A για παράδειγμα υποθέτει ότι ο εξυπηρετητής B, δεν είναι απευθείας προσπελάσιμος αν δεν ακούει το Hello μήνυμα του για κάποιο συγκεκριμένο διάστημα. Είναι σχετικά απλό να προσπεράσεις μία αποτυχία στη φάση δαχτυλίδι αλλάζοντας την κατεύθυνση από τη δεξιόστροφη κατεύθυνση στην αριστερόστροφη, ή και το αντίστροφο. Για να αποφεύγονται οι συνεχείς προσπάθειες προώθησης του μηνύματος, το πακέτο μπορεί μία μόνο φορά να αλλάξει την κατεύθυνση προώθησης του ειδάλλως απορρίπτεται. Στη σπειροειδή φάση, ο εξυπηρετητής μπορεί να ανοίξει τούνελ στο πακέτο ώστε να προσπεράσει όλους τους προβληματικούς εξυπηρετητές. Συνέχεια Προσπαθεί να προσπερνά τους προβληματικούς εξυπηρετητές στέλνοντας το πακέτο σε έναν προσβάσιμο εξυπηρετητή στην πρώτη γειτονική δεξιόστροφη στήλη. Αν δεν το καταφέρει να στείλει το πακέτο σε κανέναν εξυπηρετητή από τη γειτονική δεξιόστροφη στήλη, ο εξυπηρετητής θα προωθήσει το πακέτο σε μία γειτονική αριστερόστροφη στήλη για να ξεπεράσει τις αποτυχίες.

- Χαρακτηριστικά της αρχιτεκτονικής DPillar

Τα χαρακτηριστικά του DPillar δικτύου συνοψίζονται παρακάτω:

Επεκτασιμότητα: Ένα (n,k) DPillar δίκτυο μπορεί να φιλοξενήσει $k(n/2)^k$ εξυπηρετητές.

Κόστος: Ένα (n,k) DPillar δίκτυο χτίζεται με $k(n/2)^{k-1}$ μεταγωγέων . Το μέσο κόστος για να συνδέσεις ένα εξυπηρετητή σε ένα DPillar δίκτυο είναι $2(U_s/n + U_c)$, όπου U_s είναι ι τιμή της μονάδας ενός n-θυρου μεταγωγέα και U_c είναι η τιμή της μονάδας για ένα Ethernet καλώδιο.

Πλάτος της διχοτόμησης: Το πλάτος της διχοτόμησης ενός (n,k) Dpillar δικτύου είναι κοντά στο $(n/2)^k$.

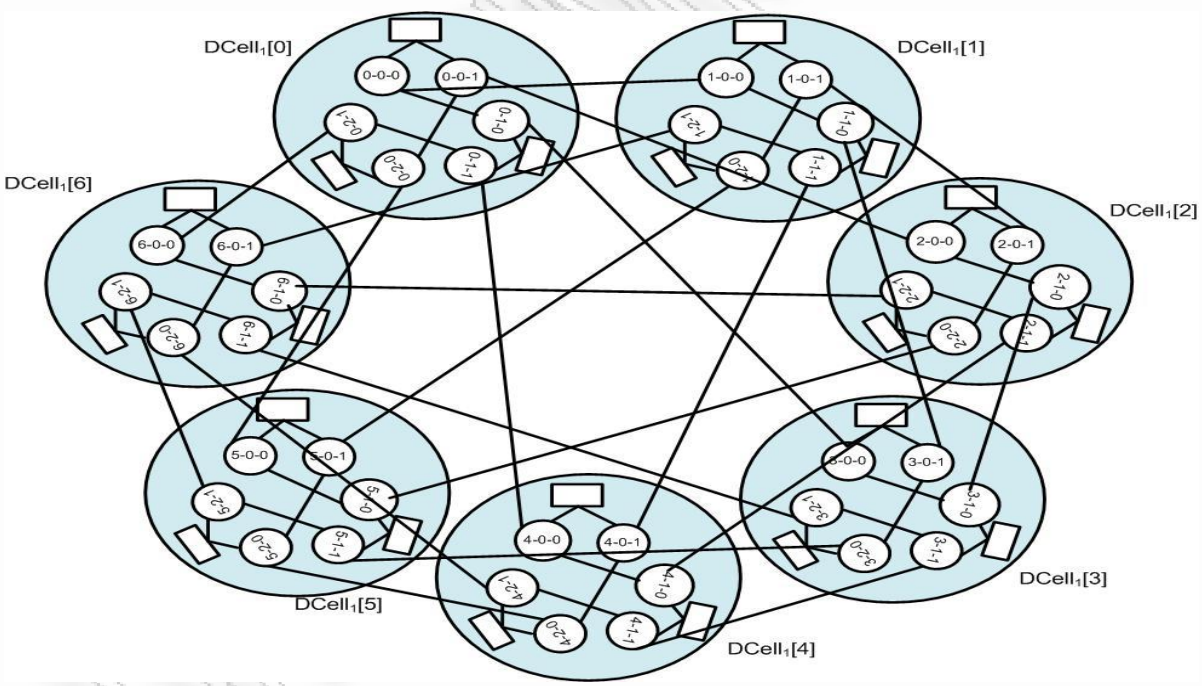
Διανομή της κυκλοφορίας: Σε τέτοιου είδους επικοινωνίες, που όλοι οι εξυπηρετητές στέλνουν σε όλους τους εξυπηρετητές, μία σύνδεση ενός εξυπηρετητή με ένα μεταγωγέα κουβαλάει το πολύ 3k(N-1)/2 ροές.

Μεγαλύτερο μονοπάτι: Το μεγαλύτερο μονοπάτι σε ένα(n,k) DPillar δίκτυο χρησιμοποιώντας έλιξ και δρομολόγηση δαχτυλίδι δύο φάσεων είναι k + [k/2]. [20]

5.2.3 Αρχιτεκτονική DCell

Η αρχιτεκτονική DCell αποτελείται έχει τέσσερα βασικά χαρακτηριστικά. Πρόκειται για μία επεκτάσιμη δικτυακή δομή, με έναν αποτελεσματικό και κατανεμημένο αλγόριθμο δρομολόγησης που εκμεταλλεύεται τη δομή του DCell, μία δρομολόγηση που παρουσιάζει ανεκτικότητα σε πολλές κατηγορίες λαθών και με ένα σχήμα τέτοιο που επιτρέπει τη σταδιακή επέκταση του μεγέθους του κέντρου δεδομένων.Το DCell απασχολεί εξυπηρετητές με πολλαπλές θύρες δικτύου και μικρούς μεταγωγείς για τη δημιουργία μιας αναδρομικής δομής. Τα DCells που είναι υψηλού επιπέδου κατασκευάζονται αναδρομικά εφαρμόζοντας έναν πλήρως συνδεδεμένο γράφο με πολλά DCells χαμηλού επιπέδου.

Ένα $DCell_k$ (k>0) [9] επιπέδου k κατασκευάζεται από $g_k = t_{k-1}$ $DCell_{k-1}$στοιχεία, όπου t_{k-1} είναι ο συνολικός αριθμός των εξυπηρετητών σε ένα DCellk-1. Επομένως, ο συνολικός αριθμός σε ένα $DCell_k$ είναι $t_k = t_{k-1}g_k = t_{k-1}(t_{k-1}+1)$, k>0 . Το βασικό επίπεδο είναι $DCell_0$ το οποίο αποτελεί τον κορμό για την ανάπτυξη DCells υψηλότερων επιπέδων. Για να διευκολυνθεί η κατασκευή του DCell,σε κάθε εξυπηρετητή στο $DCell_k$ του εκχωρείται μία (k+1)-άδα $[a_k, a_{k-1}, \ldots, a_1, a_0]$ όπου $a_i < g_i$ $(0< i \leq k)$ που δηλώνει σε ποιο $DCell_{i-1}$ τοποθετείται ο εξυπηρετητής, και a0 < n δηλώνει το δείκτη του εξυπηρετητή στο $DCell_0$. Κάθε εξυπηρετητής προσδιορίζεται από ένα μοναδικό ID uid_k, που παίρνει τιμές από $[0, t_k)$. Το ταίριασμα ανάμεσα στο μοναδικό ID και στην (k+1)-άδας του είναι μία αντιστοιχία. Το ID uid_k μπορεί να υπολογιστεί ως εξής:
$uid_k = a^0 + \sum_{j=1}^{k}\{a_j \; x \; t_j - 1\}$.Ένας εξυπηρετητής στο DCell συμβολίζεται ως $[a_k, uid_{k-1}]$, όπου a_k είναι ο δείκτης του $DCell_{k-1}$ στον οποίο αυτός ο εξυπηρετητής ανήκει και uid_{k-1} είναι το μοναδικό id του εξυπηρετητή μέσα στο $DCell_{k-1}$. Παρακάτω φαίνεται ένα παράδειγμα από ένα DCell2 δίκτυο όπου n=2 . Αν υπάρχουν δύο εξυπηρετητές στη βασική δομή του $DCell_0$, θα χρειαστούν 3 $DCell_0$ στοιχεία για να χτιστεί ένα $DCell_1$ για να χτιστεί μία $DCell_1$ δομή και 7 $DCell_1$ στοιχεία για να δημιουργηθεί ένα $DCell_2$ δίκτυο.



Σχήμα 14: Ένα $DCell_2$ δίκτυο αποτελείται από 7 $DCell_1$ δίκτυα και κάθε $DCell_1$ αποτελείται από 3 $DCell_0$s [9]

- Δρομολόγηση

Τα βασικά πρωτόκολλα δρομολόγησης στη DCell αρχιτεκτονική είναι το DCellRouting και το DCell Fault–Tolerant Routing (DFR). Τα δύο αυτά πρωτόκολλα εκμεταλλεύονται τη δομή του DCell για τη δρομολόγηση. Το DCellRouting είναι το βασικό πρωτόκολλο δρομολόγησης στο DCell χωρίς καμία αποτυχία ενώ το DFR έχει σχεδιαστεί για να διαχειρίζεται αποτελεσματικά

διάφορες αποτυχίες εξαιτίας του υλικού (hardware), του λογισμικού (software) και διάφορα προβλήματα ενέργειας.Το πρωτόκολλο DCellRouting είναι ένας απλός και αποτελεσματικός αλγόριθμος δρομολόγησης που εκμεταλλεύεται την αναδρομική δομή του DCell. Ο σχεδιασμός του ακολουθεί μία προσέγγιση διαίρει-και-βασίλευε. Σε ένα $DCell_k$ δίκτυο, κάθε εξυπηρετητής ορίζεται από μία (k+1)-άδα, και κατά αυτόν τρόπο είναι πολύ εύκολο να εξετάσουμε το βρούμε το ίδιο πρόθεμα [a_k, a_{k-1}, …, a_l] στο οποίο ανήκουν ο εξυπηρετητής πηγή και ο εξυπηρετητής προορισμός. Στο επίπεδο l, $DCell_l$-1 στοιχεία συνθέτουν έναν γράφο και επομένως το μονοπάτι του DCellRouting μπορεί να χωριστεί σε δύο υπομονοπάτια ένα στον προορισμό $DCell_{l-1}$ και ένα άλλο υπομονοπάτι ανάμεσα στην πηγή $DCell_{l-1}$ και στον προορισμό $DCell_{l-1}$. Το άνω όριο του μήκους του μονοπατιού είναι 2^{k+1}-1 και η διάμετρος του $DCell_k$ δικτύου είναι 2^{k+1}-1. Ο αλγόριθμος αυτός δεν υπολογίζει το ελάχιστο δυνατό μονοπάτι αλλά οι επιδόσεις του είναι αρκετά καλές και αγγίζουν αυτές των αλγορίθμων εύρεσης του συντομότερου μονοπατιού.Το πρωτόκολλο DCell Fault-tolerant Routing (DFR) είναι ένα κατανεμημένο πρωτόκολλο που χρησιμοποιεί το DCellRouting και το DCellBroadcast. Ένας εξυπηρετητής στο DCell δίκτυο θα μεταδώσει το πακέτο σε όλους του τους (k+1) γείτονες, όταν μεταδίδει ένα πακέτο στο $DCell_k$ χρησιμοποιεί το DCellBroadcast. Ο DFR ασχολείται με την τοπική αναδρομολόγηση, την κατάσταση των τοπικών συνδέσεων, τις διευθύνσεις των συνδέσεων και τις αποτυχίες των εξυπηρετητών. Η τοπική αναδρομολόγηση χρησιμοποιείται για να παίρνονται επί τόπου αποφάσεις για αναδρομολόγηση των πακέτων για να ξεπερνιούνται προβληματικές συνδέσεις στο DCellRouting. Παρόλα αυτά μια τέτοια αντιμετώπιση δεν εξασφαλίζει την αποφυγή επαναλαμβανόμενων βρόγχων καθώς η δρομολόγηση βασίζεται μόνο στην DCell τοπολογία και δεν χρησιμοποιεί κάποιο μηχανισμό για την κατάσταση των κόμβων ή των συνδέσεων. Στο DCell, κάθε κόμβος γνωρίζει την κατάσταση όλων των εισερχόμενων και εξερχόμενων συνδέσεων χρησιμοποιώντας το DCellBroadcast για να μεταδώσει την κατάσταση των συνδέσεων κάθε κόμβου (k+1) ή όταν αντιλαμβάνεται κάποια αποτυχία σύνδεσης. Εάν ένα ολόκληρο rack έχει πρόβλημα η απευθείας αναδρομολόγηση και η κατάσταση της σύνδεσης μπορούν να οδηγήσουν σε μία ατέρμονη αναδρομολόγηση μέσα στο προβληματικό rack. Σε αυτή την περίπτωση ο αλγόριθμος έχει τη δυνατότητα να προσπερνά το αποτυχημένο rack.

- DCell χαρακτηριστικά

Τα χαρακτηριστικά του DCell δικτύου αναφέρονται παρακάτω:

Επεκτασιμότητα: Ο αριθμός των εξυπηρετητών σε ένα DCell μπορεί να διπλασιάζεται εκθετικά όσο αυξάνεται ο αριθμός των κόμβων. Ο συνολικός αριθμός των εξυπηρετητών είναι $t_k = g_k\, g_{k-1} \dots . g_1 g_0 t_0 = t_0 \prod_{i=0}^{k} g_i$ και $(n+\frac{1}{2})^{2^k} - \frac{1}{2} < t_k < (n+1)^{2^k} - 1\ (k > 0)$, όπου n είναι ο συνολικός αριθμός των εξυπηρετητών στο $DCell_0$

Φυσική συνδεσιμότητα: Κάθε εξυπηρετητής στο $DCell_k$ συνδέεται με k+1 συνδέσεις.

Ανοχή στα σφάλματα: Εξαιτίας της πλούσιας φυσικής συνδεσιμότητας και του κατανεμημένου πρωτοκόλλου ανοχής σφαλμάτων , παρουσιάζει μεγάλη ανοχή σε σφάλματα.

Δικτυακή χωρητικότητα: Η αρχιτεκτονική αυτή εμφανίζει μεγάλη δικτυακή χωρητικότητα [22].

5.2.4 Αρχιτεκτονική BCube

Η BCube αρχιτεκτονική παρουσιάζει πολλά κοινά με την DCell αρχιτεκτονική που περιγράψαμε προηγουμένως. Τα BCube δίκτυα αποτελούνται από πολλούς μικρό-μεταγωγείς και οι εξυπηρετητές είναι εξοπλισμένοι με πολλές θύρες δικτύου. Η υποδομή του BCube δεν παρέχει μόνο «ένα- προς- ένα» εύρος ζώνης αλλά επιπλέον επιταχύνει την «ένα-προς-πολλά» και «πολλά-προς-πολλά» κίνηση.

Υπάρχουν δύο τύποι συσκευών στο BCube: εξυπηρετητές με πολλαπλές θύρες και μεταγωγείς που συνδέουν ένα σταθερό αριθμό από εξυπηρετητές. Το BCude αποτελεί μία αναδρομική δομή. Συγκεκριμένα, το $BCube_0$ αποτελείται από n $BCube_0$s και από n n-θυρους μεταγωγείς. Ένα $BCube_1$ αποτελείται από n $BCube_0$s και από n n-θυρους μεταγωγείς. Πιο γενικά, ένα $BCube_k$ (με k≥1) αποτελείται από n $BCude_{k-1}$s και n^k n-θυρους μεταγωγείς. Κάθε εξυπηρετητής στο $BCude_k$ έχει k+1 θύρες οι οποίες αριθμούνται από το επίπεδο 0 μέχρι το επίπεδο 1. Είναι εύκολο να δει κανείς ότι ένα $BCude_k$ έχει n^{k+1} εξυπηρετητές και k+1 επίπεδα από μεταγωγείς ,όπου κάθε τέτοιο επίπεδο έχει n^k n-θύρους μεταγωγείς. Η κατασκευή του $BCube_k$ έχει ως εξής: Αρχίζουμε την αρίθμηση του n $BCude_{k-1}$s από το 0 μέχρι το n-1 και οι εξυπηρετητές σε κάθε $BCube_{k-1}$ από το 0 μέχρι το n^{k-1}. Στη συνέχεια συνδέουμε τη θύρα επιπέδου k του i-οστού εξυπηρετητή(i € [0, n^k - 1]) στο j-στο $BCube_{k-1}$ (j € [0, n - 1]) με την j-στη θύρα από το i-στο μεταγωγέα του επιπέδου k. Αυτό που γενικά ισχύει είναι ότι κάθε i-στη θύρα από ένα μεταγωγέα <l, s_{k-1}, s_{k-2}..s_0> συνδέεται με l επίπεδο του εξυπηρετητή $s_{k-1}s_{k-2}..s_l s_{l-1}..s_0$. Η κατασκευή του BCude εξασφαλίζει ότι οι μεταγωγείς συνδέονται μόνο με τους εξυπηρετητές και ποτέ απευθείας με τα άλλους μεταγωγείς. Κατά συνέπεια, οι μεταγωγείς μπορούν να θεωρηθούν σαν δοκοί που συνδέουν γειτονικούς εξυπηρετητές μεταξύ τους. Με 8-θυρους μικρούς μεταγωγείς μπορούν να υποστηριχθούν μέχρι και 4096 σε ένα $BCube_3$. Επομένως η αρχιτεκτονική BCube ικανοποιεί το στόχο μας για τη χρήση μόνο απλών μεταγωγεών και αφήνει όλη τη λογική της δρομολόγησης να ικανοποιηθεί από τους εξυπηρετητές. Η υποδομή του BCube συνδέεται στενά με το Hypercude. Δηλαδή σε ένα BCube δίκτυο αν αντικαταστήσουμε κάθε μεταγωγέα και τις n συνδέσεις του με ένα πλήρες πλέγμα n x (n-1), το οποίο συνδέει απευθείας τους εξυπηρετητές, προκύπτει ένα γενικευμένο Hypercube. Συγκρίνοντας αυτές τις δύο αρχιτεκτονικές ο αριθμός των θυρών του εξυπηρετητή στο BCube είναι k+1 και ο αντίστοιχος αριθμός στο HyperCube είναι (n-1)(k+1). Είναι φανερό πως ο πρώτος είναι μικρότερος από τον δεύτερο. Αυτό συνεπάγεται ότι μπορούμε να μειώσουμε τον αριθμό των θυρών από 28 σε 4 όταν n = 8 και k = 3. Το κόστος που προκύπτει από αυτή την αλλαγή είναι K+1 επίπεδα από μεταγωγείς, αποτέλεσμα επιθυμητό λόγω τις μικρής αξίας των μικρό-μεταγωγέων.

- BCube δρομολόγηση πηγής

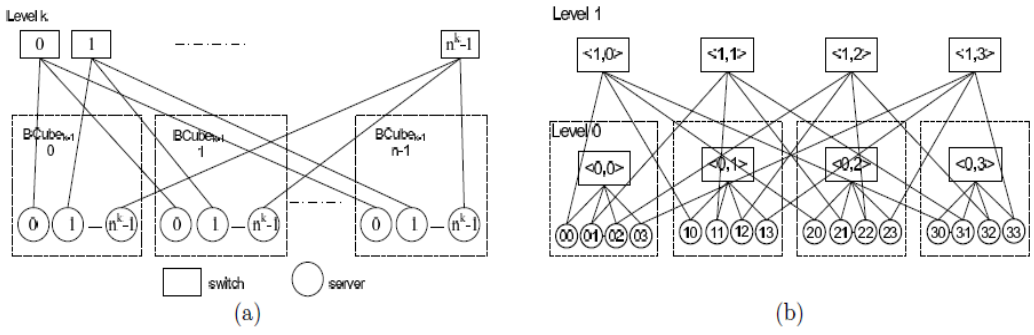
Στο BCR ο εξυπηρετητής πηγή αποφασίζει ποιο μονοπάτι πρέπει να διασχίσει ένα πακέτο σύμφωνα με το δίκτυο αλλά με το μονοπάτι που φαίνεται στην επικεφαλίδα του πακέτου. Επιλέγουμε source routing για δύο λόγους. Πρώτον, η πηγή μπορεί να ελέγξει το μονοπάτι δρομολόγησης χωρίς το συντονισμό από τους ενδιάμεσους εξυπηρετητές. Δεύτερον οι ενδιάμεσοι εξυπηρετητές δεν εμπλέκονται στην δρομολόγηση απλά προωθούν τα πακέτα βασισμένοι στην επικεφαλίδα κάθε πακέτου. Στο BSR μία ροή μπορεί να αλλάξει το μονοπάτι της χρησιμοποιώντας ένα μονοπάτι κάθε φορά έτσι ώστε να αποφεύγεται το πρόβλημα του πακέτου εκτός λειτουργίας. Η ροή είναι μία ακολουθία πακέτων που έχουν τις ίδιες τιμές για ένα υποσύνολο πεδίων τις επικεφαλίδας του πακέτου. Μία διπλή ροή αντιμετωπίζεται σαν δύο ξεχωριστές ροές , καθώς οι συνθήκες του δικτύου ανάμεσα σε αντίθετες κατευθύνσεις μπορεί να είναι διαφορετικές. Όταν μία ένα ροή έρχεται , η πηγή στέλνει πακέτα σε πολλαπλά διαφορετικά μονοπάτια. Οι ενδιάμεσοι εξυπηρετητές επεξεργάζονται τα πακέτα για να καλύψουν την απαιτούμενη πληροφορία πχ το μικρότερο διαθέσιμο εύρος ζώνης των συνδέσεων. Ο προορισμός επιστρέφει μία σύντομη απάντηση στην πηγή. Όταν η πηγή λαμβάνει απαντήσεις , χρησιμοποιεί μία ένα μέτρο για επιλέξει το καλύτερο μονοπάτι, για παράδειγμα αυτό με το μεγαλύτερο διαθέσιμο εύρος ζώνης. Όταν η πηγή επιλέγει το μονοπάτι για μία ροή, δεν κρατάει τα πακέτα. Η πηγή αρχικά χρησιμοποιεί ένα προεπιλεγμένο μονοπάτι από το παράλληλο σύνολο μονοπατιών. Μόλις ολοκληρωθεί η επιλογή του μονοπατιού και ένα καλύτερο μονοπάτι επιλεγεί , η πηγή αλλάζει τη ροή στο νέο μονοπάτι. Η αλλαγή μονοπατιού μπορεί προσωρινά να φέρει το πακέτο εκτός λειτουργίας. Επειδή αυτή η διαδικασία διαρκεί για λίγο, η αλλαγή μονοπατιού επιφέρει προβλήματα επίδοσης στο δίκτυο.

- Η διαδικασία επιλογής μονοπατιού

Η διαδικασία αυτή αποτελείται από τρία μέρη , τα οποία περιγράφουν πως οι πηγή , οι ενδιάμεσοι και οι εξυπηρετητές προορισμός αλληλεπιδρούν. Όταν η πηγή εφαρμόζει Path selection, χρησιμοποιεί αρχικά το Build Path set για να ανακτήσει κ+1 παράλληλα μονοπάτια και την συνέχεια διερευνά αυτά τα μονοπάτια. Παρόλα αυτά αν ένα μονοπάτι δεν είναι διαθέσιμο, η πηγή χρησιμοποιεί το Breadth First Search (BFS) αλγόριθμο για να βρει ένα άλλο παράλληλο μονοπάτι. Η πηγή πρώτα διαγράφει τα υπάρχοντα παράλληλα μονοπάτια και τις αποτυχημένες συνδέσεις από τον $BCube_k$ γράφο, και μετά χρησιμοποιεί BFS για την αναζήτηση μονοπατιού. Όταν οι συνδέσεις έχουν τα ίδια βάρη, BFS είναι αλγόριθμος δρομολόγησης του συντομότερου μονοπατιού. Το νέο μονοπάτι που βρίσκεται είναι παράλληλο με τα υπάρχοντα μονοπάτια , καθώς όλα τα υπάρχοντα μονοπάτια διαγράφονται πριν το BFS. Όταν ο BFS δεν μπορεί να βρει ένα μονοπάτι ξέρουμε ότι ο αριθμός των παραλλήλων μονοπατιών είναι μικρότερος του k+1.Ο BFS λειτουργεί πολύ γρήγορα για ένα BCube με χιλιάδες εξυπηρετητές. Όταν ο ενδιάμεσος εξυπηρετητής λάβει ένα πακέτο και επόμενος σταθμός δεν είναι διαθέσιμος επιστρέφει ένα μήνυμα αποτυχίας στην πηγή. Αλλιώς , ενημερώνει το διαθέσιμο πεδίο εύρους ζώνης του πακέτου αν το διαθέσιμο εύρος ζώνης του είναι μικρότερο από την υπάρχουσα τιμή. Το διαθέσιμο του εύρος ζώνης είναι η μικρότερη διαθέσιμη τιμή για τις εισερχόμενες και εξερχόμενες συνδέσεις. Αυτός ο έλεγχος γίνεται γιατί δύο παρακείμενοι εξυπηρετητές A και B στο BCube συνδέονται έμμεσα μέσω ενός Σ μεταγωγέα. Επομένως το διαθέσιμο εύρος ζώνης της εξερχόμενης σύνδεσης του A δεν είναι απαραίτητα ίσο με το εύρος ζώνης της εισερχόμενης σύνδεσης του B. Όταν ο εξυπηρετητής προορισμός λάβει το πακέτο ελέγχει με τη σειρά του να το εύρος ζώνης της εισερχόμενης σύνδεσης είναι μικρότερο από την τιμή που φέρει το πακέτο. Στη συνέχει στέλνει την τιμή αυτή πίσω στην πηγή με ένα μήνυμα απάντησης. Όλοι οι εξυπηρετητές διατηρούν μία βάση με τις αποτυχημένες συνδέσεις σύμφωνα με τα μηνύματα αποτυχίας των μονοπατιών. Μία σύνδεση σβήνεται από τη βάση σε περίπτωση που ο εξυπηρετητής λάβει επιτυχημένη απάντηση που να περιέχει αυτή τη σύνδεση.

- Προσαρμογή μονοπατιού

Κατά τη διάρκεια της ροής των δεδομένων, η πορεία της μπορεί να αλλάξει εξαιτίας των πολλαπλών αποτυχιών όπως και η κατάσταση του δικτύου μπορεί να αλλάξει δραματικά. Η πηγή εφαρμόζει path selection περιοδικά για να προσαρμοστεί στις αποτυχίες του δικτύου και στις δυναμικές συνθήκες του δικτύου. Όταν ένας εξυπηρετητής βρει ότι το επόμενο άλμα(hop) του πακέτου δεν είναι διαθέσιμο , στέλνει μήνυμα απόρριψης πίσω στην πηγή. Όσο υπάρχουν άλλα διαθέσιμα μονοπάτια η πηγή δεν ψάχνει απευθείας στο δίκτυο όταν το μήνυμα λαμβάνεται. Αντίθετα, αλλάζει τη ροή σε ένα από τα διαθέσιμα μονοπάτια που έχει βρει από προηγουμένη αναζήτηση. Όταν ο χρόνος αναζήτησης λήξει, η πηγή εφαρμόζει ένα άλλο γύρο εύρεσης μονοπατιού και προσπαθεί να διατηρήσει τα κ+1 παράλληλα μονοπάτια. Αυτός ο σχεδιασμός απλοποιεί την εφαρμογή αποφεύγοντας τη συσσώρευση πακέτων. Όταν πολλαπλές ροές ανάμεσα σε δύο εξυπηρετητές φτάνουν ταυτόχρονα μπορούν να επιλέξουν το ίδιο μονοπάτι. Το χειρότερο σενάριο μπορεί να συμβεί όταν μετά την επιλογή μονοπατιού λήξει ο χρόνος και αλλάξουν και οι δύο σε άλλο μονοπάτι ταυτόχρονα. Για να μετριαστεί αυτό το σύμπτωμα απλά προστίθεται μία μικρή τυχαία σταθερά στο χρονικό όριο ώστε να το αυξήσει [23].



Σχήμα 15: (a)Το BCube είναι μία δομή που αποτελείται από επίπεδα. Ένα BCubek κατασκευάζεται από n BCubek¡1 and n^k n-θύρους μεταγωγείς. (b) Ένα BCube1 με n = 4. Σε αυτό το BCube1 δίκτυο, κάθε εξυπηρετητής έχει δύο θύρες.

6. Ασφάλεια των κέντρων δεδομένων

Τα κέντρα δεδομένων περιέχουν πολλές εφαρμογές που διαχειρίζονται πολύ σημαντικά δεδομένα με αποτέλεσμα να γίνονται συχνά στόχος ηλεκτρονικών επιθέσεων. Οι εξυπηρετητές στα κέντρα δεδομένων αποτελούν σημαντικό στόχο κακόβουλων επιθέσεων και πρέπει να προστατεύονται. Οι επιθέσεις αυτές μπορεί να οδηγήσουν στην κλοπή εμπιστευτικών και σημαντικών πληροφοριών αλλά και σε ζημιές σε επιχειρήσεις που ασχολούνται με το ηλεκτρονικό εμπόριο αλλά και με άλλες εφαρμογές. Τόσα τα LANs αλλά και τα SANs πρέπει να εξασφαλίσουν τη μείωση της πιθανότητας σε τέτοια περιστατικά. Τα SAN παραδοσιακά θεωρούνται πιο ασφαλή καθώς οι αναπτύξεις τους περιορίζονται σε ένα περιορισμένο σύνολο του κτιρίου, σε ένα δηλαδή απομονωμένο δίκτυο . Παρόλο τούτου είναι δεν είναι δύσκολο να διαταραχτεί η ασφάλεια των υπολογιστών που συνδέονται στο SAN όπως για παράδειγμα όταν δίνεται μη εξουσιοδοτημένη πρόσβαση σε δεδομένα του δικτύου , ή όταν παρακάμπτονται τα firewalls και άλλα συστήματα ανίχνευσης κακόβουλων επιθέσεων αν χρησιμοποιείται η IP του καναλιού οπτικής ίνας.

Γενικά , δεν είναι ασυνήθιστο ένα SAN δίκτυο να εκτείνεται έξω από το χώρο του κέντρου δεδομένων για τη συνέχιση της επιχειρηματικότητας αλλά και για σκοπούς ανάκτησης των πληροφοριών σε σενάρια καταστροφής (disaster recovery). Η υιοθέτηση τέτοιων τεχνολογιών όπως το Small Computer System Interface πάνω στην IP(iSCSI) και το κανάλι των οπτικών ινών πάνω από την IP (FCIP), οι οποίες χρησιμοποιούν το TCP/IP για τη μεταφορά , γεννούν την ανάγκη της ασφάλειας του δικτύου των κέντρων δεδομένων καθώς μεταφέρονται ευαίσθητες πληροφορίες.

Παρακάτω θα εξετάσουμε μερικές τεχνολογίες που χρησιμοποιούνται σε επίπεδο μεταγωγέων στα κέντρα δεδομένων αλλά και λύσεις που καθιστούν τους εξυπηρετητές λιγότερο ευάλωτους σε αυτές τις απειλές.

6.1 Δικτυακές επιθέσεις και ασφάλεια δικτύου

Βασικό κομμάτι για την αντιμετώπιση των κακόβουλων επιθέσεων αποτελεί η κατηγοριοποίηση των επιθέσεων και η κατανόηση των κινδύνων που ελλοχεύει η κάθε επίθεση. Ουσιαστικά, υπάρχουν δύο είδη επιθέσεων : η κλοπή δεδομένων και η μετάδοση ιών. Το πρώτο είδος επίθεσης αποσκοπεί στην κλοπή σημαντικών πληροφοριών ενώ η δεύτερη επίθεση στην αποδιοργάνωση των εφαρμογών έτσι ώστε να μην μπορούν να χρησιμοποιηθούν

6.2 Κλοπή δεδομένων

Οι επιθέσεις αυτές απευθύνονται στην κλοπή εμπιστευτικών πληροφοριών και ξεκινούν σαρώνοντας εξονυχιστικά το σύστημα στόχο. Ένα hacker μπορεί να χρησιμοποιήσει ένα κοινό εργαλείο όπως το nmap για αντλήσει πληροφορίες σχετικά με το λειτουργικό σύστημα του στόχου αλλά και για τις υπηρεσίες που έχουν ρυθμιστεί από τον εξυπηρετητή. Η επόμενη φάση είναι ο εντοπισμός των αδυναμιών του συστήματος εξ αποστάσεως. Στη συνέχεια ο εισβολέας εγκαθιστά ένα παράνομο λογισμικό στο σύστημα στόχο το οποίο εκτελεί ανεπιθύμητες λειτουργίες (trojan). Κατά αυτόν τρόπο ο εισβολέας ελέγχει τον εξυπηρετητή στο κέντρο δεδομένων και από αυτόν τον εξυπηρετητή μπορεί να έχει πρόσβαση σε όλα τις μονάδες που αποθηκεύουν ευαίσθητα δεδομένα ή να εγκαταστήσει άλλα εργαλεία επίθεσης που θα του δώσουν πρόσβαση σε όλους τους εξυπηρετητές στο εσωτερικό του κέντρου δεδομένων. Σε αυτό το σημείο ο εισβολέας μπορεί να λειτουργήσει είτε πάνω στο LAN είτε στο SAN. Εάν, ο εξυπηρετητής που κινδυνεύει συνδέεται στο LAN , ο εισβολέας μπορεί να χρησιμοποιήσει το επίπεδο2 (Ethernet) για να επιτεθεί όπως να πλαστογραφήσει το ARP ή μέσω των MAC διευθύνσεων να υποκλέψει τις IP. Εάν ο υπό κίνδυνο εξυπηρετητής συνδέεται στο SAN με ένα δίαυλο κεντρικού υπολογιστή, ο εισβολέας μπορεί δυνητικά να αποκτήσει πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο SAN μέσω επιθέσεων χρησιμοποιώντας πλαστά ονόματα (WWNs) ή να αποκτήσει πρόσβαση σε άλλους εξυπηρετητές που χρησιμοποιούν IP πάνω στο κανάλι της οπτικής ίνας. Μία άλλη γνωστή τακτική για τον έλεγχο του εξυπηρετητή είναι η TCP εισβολή. Οι εξυπηρετητές των οποίων το ISN (αρχικός αριθμός της ακολουθίας ,

initial sequence number) είναι προβλέψιμο μπορούν να ελεγχτούν από έναν απομακρυσμένο υπολογιστή συνδυάζοντας την εύρεση του ISN και την πλαστογράφηση της IP [4].

6.2.1 Ιοί

Μερικές από αυτές τις επιθέσεις έχουν στόχο να εμποδίζουν την πρόσβαση των χρηστών στις εφαρμογές. Αυτό που κάνουν είναι να γεννούν μεγάλα ποσά κίνησης και αιτήματα σύνδεσης μέσα (SYN flood, ping flood) με αποτέλεσμα οι εξυπηρετητές να αντιμετωπίζουν έλλειψη πόρων και να μην μπορούν να εξυπηρετήσουν. Οι ιοί μπορούν να αναπαράγονται χωρίς ανθρώπινη παρέμβαση επιδεινώνοντας έτσι το πρόβλημα. Θεωρούνται εξαιρετικά επικίνδυνα λόγω του γρήγορου ρυθμού εξάπλωσης. Για παράδειγμα μπορούν να διπλασιάζονται κάθε 8.5 δευτερόλεπτα και να γενούν κίνηση τέτοια ώστε μία σύνδεση του 1Gbps να φτάνει στο σημείο κορεσμού της σε λιγότερο από ένα λεπτό. Κάθε ιός έχει διαφορετικά χαρακτηριστικά (πχ ευαισθησία) αλλά μοιράζονται και ομοιότητες. Αν για παράδειγμα μελετήσουμε έναν ιό συγκεκριμένα μπορεί να μας βοηθήσει να καταλάβουμε πώς να προστατεύουμε τους εξυπηρετητές και από τους άλλους ιούς. Για παράδειγμα, ο Code Red στέλνει TCP αιτήματα σύνδεσης για τη θύρα 80 σε τυχαίες διευθύνσεις IP αναζητώντας έναν ευάλωτο υπολογιστή υποδοχής. Ο Code Red εκμεταλλεύεται έναν υπερχειλισμένο ενταμιευτή στην ουδέτερη υπερχείλιση ευπαθή στον Microsoft Internet Information Services (IIS) (Microsoft Security Bulletin MS01-033). Αφού βρεθεί ένας ευάλωτος υπολογιστής υποδοχής,ο Code Red προκαλεί υπερχείλιση μνήμης του εξυπηρετητή, και στη συνέχεια εισάγει έναν ιό ο οποίος με τη σειρά του επιτίθεται άλλους εξυπηρετητές [4].

6.2.2 Προστασία

Εξελιγμένα εργαλεία που αντιμετωπίζουν τις επιθέσεις είναι διαθέσιμα στο κοινό και γίνονται ολοένα και πιο φιλικά προς το χρήστη. Αυτό σημαίνει ότι οποιοσδήποτε με πρόσβαση στο διαδίκτυο μπορεί να βρει μια μεγάλη ποικιλία από τέτοια εργαλεία. Συνήθως οι περισσότερες επιθέσεις κατά των συστημάτων συμβαίνουν από πηγές που υπάρχουν στο εσωτερικό δίκτυο. Η αυξανόμενη ανάγκη για την προστασία των εσωτερικών συσκευών και των εφαρμογών από επιθέσεις και προσπάθειες μη εξουσιοδοτημένης πρόσβασης είναι αντικατοπτρίζεται άμεσα στα αποτελέσματα της έρευνας. Τα κέντρα δεδομένων θα πρέπει να αποσκοπούν στην προστασία τους από επιθέσεις που πραγματοποιούνται από εξωτερικούς υπολογιστές-πελάτες (clients) (στο Διαδίκτυο), από εσωτερικές συσκευές και από εξυπηρετητές που έχουν παραβιαστεί [4].

6.2.3 LAN εργαλεία

Σήμερα παρέχεται μια σειρά από υπηρεσίες και προϊόντα ανίχνευσης εισβολών παρέχοντας ασφαλείς λειτουργίες όπως [4]:

- Ελεγχόμενη πρόσβαση στους εξυπηρετητές
  Οι περισσότερες εφαρμογές σήμερα έχουν αναπτυχθεί σε μια πολύ-επίπεδη αρχιτεκτονική. Το πολύ-επίπεδο μοντέλο αποτελείται από τη χρήση ξεχωριστών μηχανημάτων εξυπηρετητών που παρέχουν διαφορετικές λειτουργικότητες. Τα πολύ-επίπεδα συμπλέγματα εξυπηρετητών παρέχουν πρόσθετη ασφάλεια, επειδή ο πελάτης (client)μπορεί να υποβιβάσει την ασφάλεια ενός διακομιστή ιστοσελίδων, χωρίς να έχει πρόσβαση στην ίδια την εφαρμογή αλλά ούτε και στη βάση δεδομένων. Ο διαχωρισμός μεταξύ των βαθμίδων(tiers) μπορεί να επιτευχθεί χρησιμοποιώντας VLANs. Η πρόσβαση client-to-server και server-to-server περιορίζεται στη νόμιμη κυκλοφορία χρησιμοποιώντας τεχνολογίες όπως λίστες ελέγχου πρόσβασης (ACLS), VLANs και ιδιωτικά VLANs.
- Προστασία από επιθέσεις κατανεμημένης άρνησης υπηρεσίας
  Υπάρχει ένα ευρύ φάσμα για την αντιμετώπιση από επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Distributed Denial-of-Service, DDoS) που απειλούν τις επιχειρήσεις σήμερα. Με αυτές τις ενσωματωμένες δυνατότητες ασφάλειας, η υποδομή του δικτύου μπορεί να αντέξει ακόμη και τις πιο μαζικές επιθέσεις και να προστατεύσει το κέντρο δεδομένων και τις κρίσιμες εφαρμογές του.
- Ενισχυμένα TCP / IP Πρωτόκολλα

Πολλά IP πρωτόκολλα δεν έχουν σχεδιαστεί με γνώμονα την ασφάλεια και η πλαστογράφηση είναι πολύ εύκολη. Ως ένα πρωτόκολλο, το πρωτόκολλο TCP παρέχει κάποιες εγγυήσεις για να αποφεύγεται η νοθεία, αλλά εξακολουθεί να είναι ευάλωτο σε πιο εξελιγμένες επιθέσεις. Όλα αυτά τα πρωτόκολλα μπορούν να ενισχυθούν με χαρακτηριστικά όπως η επιθεώρηση του ARP, TCP SYN-Cookies, η τυχαιότητα του αριθμού (ISN) και η δρομολόγηση του πρωτόκολλου ταυτοποίησης.

- Ταυτοποίηση πελάτη και διακομιστή, ακεραιότητα δεδομένων και εμπιστευτικότητας
  Τα πρωτόκολλα Secure Sockets Layer (SSL) και IPSec (IP Security) μπορούν να παρέχουν πιστοποίηση για πρόσβαση σε εφαρμογές εξυπηρετητή καθώς και την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Παρέχονται κρυπτογραφικές λειτουργίες εκφόρτωσης από τους διακομιστές και λειτουργίες διανομής Δημόσιου Κλειδιού.
- Ανίχνευση εισβολών και πρόληψης
  Λύσεις ανίχνευσης των εισβολών, όπως συστήματα ανίχνευσης εισβολών (IDSM2) και λύσεις πρόληψης εισβολής, προστατεύουν τους εξυπηρετητές από επιθέσεις που εκμεταλλεύονται το λειτουργικό σύστημα και τα τρωτά σημεία της εφαρμογής. Η τεχνολογία αυτή συμπληρώνεται με τη χρήση των τεχνολογιών κατοπτρισμού(mirroring), όπως το εικονικό ACL (VACL) , το Remote Switched Port Analyzer (RSPAN) και το NetFlow.
- Συσκευές ασφαλείας δικτύου
  Η διαχείριση των συσκευών δικτύου σε ένα κέντρο δεδομένων θα πρέπει να εξασφαλίζει την αποφυγή της μη εξουσιοδοτημένης πρόσβασης και να αποτρέπει τις επιθέσεις DoS εναντίον του δικτύου. Η ασφαλής διαχείριση της πρόσβασης έχει αναπτυχθεί με τη χρήση τεχνολογιών ACL, ταυτοποίησης, εξουσιοδότησης και χρήσης πρωτοκόλλων [4].

6.2.4 Έλεγχος πρόσβασης και τμηματοποίηση

Μέσα από τις μονάδες υπηρεσιών τοίχου προστασίας (firewall) μπορούν να παρασχεθούν οι παρακάτω λειτουργίες:

- Τα ACLs και τα VACLs επιτρέπουν το φιλτράρισμα της κυκλοφορίας στο επίπεδο4 (Layer4), εμποδίζοντας έτσι την πρόσβαση σε υπηρεσίες που έχουν ανοίξει κατά λάθος στους εξυπηρετητές. Μέσα από μια σειρά πακέτων προστασίας παρέχονται οι δυνατότητες φιλτραρίσματος όπως και οι εναλλαγές, επιτρέποντας σχέδια όπου η κίνηση από τον πελάτη (client) στον εξυπηρετητή πρέπει να περάσει μέσα από πολλά στρώματα του ACL .Τα τοίχοι προστασίας (firewalls) μπορούν να ανοίξουν στο επίπεδο4(Layer4) θύρες δυναμικά με βάση τη διαπραγμάτευση ελέγχου που συνήθως αναφέρονται ως διορθώσεις (fixups).
- Ένας μεταγωγέας στο επίπεδο σύνδεσης είναι μια συσκευή ικανή να ομαδοποιεί τα υποσύνολα από τις θύρες του μέσα σε εικονικές περιοχές εκπομπής οι οποίες απομονώνονται μεταξύ τους. Αυτές οι περιοχές είναι γνωστές ως εικονικά δίκτυα LAN (VLAN). Οι δημοφιλείς τεχνολογίες VLAN-ετικοποίηση (tagging) όπως το Inter-Switch Link (ISL) ή 802.1Q στις φυσικές συνδέσεις χρησιμοποιούνται για να διατηρηθούν οι πληροφορίες των εικονικών τοπικών δικτύων (VLAN). Τα εικονικά τοπικά δίκτυα (VLANs) μπορούν να χρησιμοποιηθούν για να διαχωρίσουν εξυπηρετητές αλλά μπορούν αν συνδυαστούν και με τείχη προστασία(firewalls) να φιλτράρουν την κυκλοφορία από εικονικό σε εικονικό δίκτυο. (VLAN-to-VLAN).
- Τα ιδιωτικά VLANs (PVLANs) παρέχουν απομόνωση μεταξύ των θυρών που ανήκουν στο ίδιο VLAN. Με τη χρήση ιδιωτικών VLANs, μπορεί να χρησιμοποιείται ένα μόνο υποδίκτυο και να αναγκάζει όλη την κίνηση που δημιουργείται από τον εξυπηρετητή να πηγαίνει όλη σε άλλη θύρα, που στην ουσία είναι θύρα που αντιστοιχεί σε δρομολογητή ή στη διεπαφή του VLAN στο τείχος προστασίας (firewall).Με τον τρόπο αυτό, οι εξυπηρετητές μπορούν να προστατευθούν από επιθέσεις στο επίπεδο σύνδεσης, όπως η πλαστογράφηση ARP, ακόμα και αν μπορούν να παραβιαστούν άλλες συσκευές μέσα στο ίδιο VLAN.
- Πολλά κέντρα δεδομένων διαθέτουν τοπολογία που βασίζεται στους μεταγωγείς χωρίς να υπάρχει κόμβος(hub), και όλες οι συνδέσεις είναι πλήρως αμφίδρομες. Οι πλημμύρες (flooding) στο επίπεδο σύνδεσης χρησιμοποιούνται μόνο κατά τη διάρκεια αλλαγών στην τοπολογία. Οι τεχνολογίες που βασίζονται σε πλημμύρες προκαλούν υποβάθμιση των επιδόσεων του δικτύου. Οι πλημμύρες μπορούν επίσης να είναι το αποτέλεσμα μιας

επίθεσης στην ασφάλεια και για αυτό το λόγο η ασφάλεια της θύρας πρέπει να ρυθμίζεται στις θύρες πρόσβασης. Για την αποφυγή πλημμυρών MAC, χρησιμοποιούνται θύρες ασφαλείας, σύμφωνα με τις οποίες καθορίζονται οι διευθύνσεις MAC σε περιορισμένο αριθμό από MAC διευθύνσεις. Όταν μια ασφαλή θύρα λάβει ένα πακέτο, η διεύθυνση MAC του πακέτου συγκρίνεται με μία λίστα από ασφαλείς πηγαίες διευθύνσεις οι οποίες έχουν ρυθμιστεί χειροκίνητα ή έχουν μαθευτεί στη θύρα. Αν η MAC διεύθυνση μία συσκευής η οποία συνδέεται σε θύρα διαφέρει από τη λίστα με τις ασφαλείς διευθύνσεις, η θύρα απενεργοποιείται προσωρινά, ή απορρίπτει τα πακέτα που λαμβάνει από τον άγνωστο/επικίνδυνο υπολογιστή υποδοχής.

- Το πρότυπο IEEE 802.1X ορίζει ένα πελάτη-εξυπηρετητή πρωτόκολλο βασισμένο στην πρόσβαση ελέγχου και στην αυθεντικοποίηση, το οποίο αποτρέπει τους πελάτες από τη σύνδεση σε τοπικό δίκτυο LAN μέσω θυρών που είναι δημοσίως προσβάσιμες. Ο εξυπηρετητής ελέγχου ταυτότητας ελέγχει την προέλευση κάθε πελάτη που συνδέεται με τη θύρα ενός μεταγωγέα και εκχωρεί τη θύρα στο VLAN πριν γίνουν διαθέσιμες οποιεσδήποτε υπηρεσίες που προσφέρονται από το διακόπτη ή το LAN. Μέχρι να ταυτοποιηθεί ο πελάτης, το 802.1X επιτρέπει την κίνηση μόνο από το πρωτόκολλο EAP(Extensible Authentication Protocol) μέσω τοπικού δικτύου LAN (EAPOL) και μέσω της θύρας στην οποία ο πελάτης είναι συνδεδεμένος. Μόλις ολοκληρωθεί επιτυχώς η ταυτοποίηση, η κίνηση μπορεί να περάσει και πάλι κανονικά από τη θύρα.[4]

6.2.5 TCP/IP πρωτοκόλλα ασφαλείας

Ειδικοί μεταγωγείς και τείχη προστασίας μπορούν να προσφέρουν τις παρακάτω λειτουργίες ασφαλείας:

- Ο έλεγχος με το πρωτόκολλο ARP, παρέχει έναν πίνακα με μια προεπιλεγμένη διεύθυνση IP και της αντίστοιχης διεύθυνσης MAC. Αν ο μεταγωγέας βλέπει έναν πίνακα ARP του οποίου τα δεδομένα δεν ισχύουν, τότε ο μεταγωγέας απορρίπτει το πακέτο, εμποδίζοντας έτσι ARP επιθέσεις πλαστογράφησης.
- Η προώθηση δεδομένων με Unicast Reverse Path Forwarding (URPF) ελέγχει κάθε πακέτο για να επιβεβαιώσει ότι προέρχεται από τις προβλεπόμενες πηγές και τις αναμενόμενες διεπαφές, περιορίζοντας έτσι τις πλαστογραφήσεις πηγής-διεύθυνσης. Ο έλεγχος συνίσταται στην επαλήθευση ότι υπάρχει ένας πίνακας δρομολόγησης με την αντιστοιχία της διεύθυνσης της πηγής με το περιβάλλον στο οποίο έφτασε το πακέτο.
- Με τη χρήση ειδικού λογισμικού δίνεται η δυνατότητα στα ACLs και στα VACLs να επιτρέπουν ή να αποτρέπουν την προώθηση κατακερματισμένων δεδομένων, μετά από ειδικό φιλτάρισμα αυτών. Αυτή η δυνατότητα μπορεί να ενισχυθεί επιπλέον με την επανασυναρμολόγηση ή επικύρωση των ήδη κατακερματισμένων δεδομένων.
- Η υλοποίηση της TCP/IP στοίβας ορισμένων λειτουργικών συστημάτων γεννάει ISNs με έναν προβλέψιμο τρόπο, με αποτέλεσμα να είναι εύκολη η παραβίαση των TCP συνεδριών (sessions). Χρησιμοποιώντας εξελιγμένα τείχη προστασίας τα ISNs μπορούν να παράγονται με τυχαίο τρόπο και να χρησιμοποιούνται από τους εξυπηρετητές για τις TCP συνδέσεις.
- Είναι δυνατό να διατηρείται η πληροφορία της κατάστασης της σύνδεσης κατά την κυκλοφορία μέσα στο δίκτυο. Για παράδειγμα, ένα πλαστό τμήμα TCP το οποίο αποστέλλεται σε κάποιο δρομολογητή προωθείται κανονικά σαν οποιοδήποτε άλλο IP πακέτο. Με τη χρήση εξελιγμένων τειχών προστασίας το πλαστό κομμάτι δεν προωθείται αφού δεν υπάρχει TCP σύνδεση για αυτό.
- Το VTP είναι ένα πρωτόκολλο ανταλλαγής μηνυμάτων του επιπέδου Ethernet που διατηρεί τις VLAN ρυθμίσεις διαχειριζόμενο την προσθήκη, τη διαγραφή, και την ονοματολογία των VLANs σε όλη την κλίμακα του δικτύου. Η VTP ταυτοποίηση συμβάλλει στη διασφάλιση της γνησιότητας και της ακεραιότητας του μεταγωγέα προς εναλλαγή των VTP μηνυμάτων από μεταγωγέα σε μεταγωγέα. Το VTP εισάγει έναν πρόσθετο μηχανισμό για την επικύρωση του κύριου εξυπηρετητή VTP ως τη μοναδική συσκευή που επιτρέπεται να δυνατότητα να αλλάξετε τις ρυθμίσεις του VLAN σε όλη την κλίμακα του δικτύου.[4]

6.2.6 Ταυτοποίηση ακεραιότητα και εμπιστευτικότητα δεδομένων μεταξύ πελάτη και εξυπηρετητών

Οι μεταγωγείς και οι υπηρεσίες των VPN μέσα από τη χρήση των παρακάτω πρωτοκόλλων μπορούν να προσφέρουν ασφάλεια στο δίκτυο.

- Το πρωτόκολλο SSL(Secure Sockets Layer) σχεδιάστηκε για να παρέχει ασφάλεια κατά τη μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Σχεδόν κάθε εφαρμογή που χρησιμοποιεί το πρωτόκολλο TCP/IP ως πρωτόκολλο μεταφοράς μπορεί να χρησιμοποιεί υπηρεσίες που παρέχονται από το SSL και να δημιουργεί SSL συνδέσεις με τη χρήση SSL υποδοχών (sockets). Κατά αυτόν τον τρόπο οι εξυπηρετητές «ξεφορτώνονται» την αποκρυπτογράφηση ισχυρά κωδικοποιημένων πληροφοριών (όπως ο [3DES] Triple Data Encryption Stand) και απλοποιείται η διαχείριση των ψηφιακών πιστοποιητικών
- Το πρωτόκολλο IPSecure βοηθά στη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της ταυτοποίησης των δεδομένων. Το πρωτόκολλο IPSec λειτουργεί μεταξύ το επιπέδου δικτύου και του επιπέδου μεταφοράς της στοίβας πρωτοκόλλου TCP/IP. Οι εφαρμογές δεν αντιλαμβάνονται τη χρήση του IPSec. Το IPSec είναι ώριμο πρωτόκολλο, δοκιμασμένο στο χρόνο και παρέχει ισχυρούς μηχανισμούς στο IP επίπεδο.

6.2.7 Ασφάλεια των συσκευών δικτύου

Η διαχείριση των διεπαφών των συσκευών του δικτύου πρέπει να είναι ασφαλής έτσι ώστε να προλαμβάνεται η μη εξουσιοδοτημένη πρόσβαση: ένας κακόβουλος χρήστης που έχει πρόσβαση στην κονσόλα μιας συσκευής δικτύου μπορεί να αλλάξει εύκολα τις ρυθμίσεις του δικτύου, παρέχοντας ένα άνοιγμα που μπορεί να παρακάμψει τα μέτρα ασφαλείας. Συνήθως, οι μεταγωγείς και άλλες υπηρεσίες παρέχουν τις παρακάτω λειτουργίες ασφάλειας:

- Η πιστοποίηση και η εξουσιοδότηση του χρήστη αποτελούν μια αρχιτεκτονική που μπορεί να χρησιμοποιηθεί για να ελέγχει την πρόσβαση σε ευαίσθητες πληροφορίες όπως είναι οι εξυπηρετητές και οι συσκευές δικτύου, ανάλογα κάθε φορά με τους χρήστες και ομάδες χρηστών που τα χρησιμοποιούν. Η αρχιτεκτονική αυτή χρησιμοποιήσει τον κωδικό χρήστη και το συνθηματικό της τοπικής βάσης δεδομένων στο μεταγωγέα ή χρησιμοποιεί πρωτόκολλα για την πρόσβαση σε έναν ταυτοποιημένο εξυπηρετητή.
- Το SSH(Secure Shell) παρέχει ασφαλή απομακρυσμένη πρόσβαση μέσω της χρήσης της ταυτοποίησης και της κρυπτογράφησης. Το SSH πρωτόκολλο μπορεί να χρησιμοποιηθεί ως εναλλακτική λύση για επισφαλή πρωτόκολλα όπως το telnet και rlogin. Το SSH μπορεί να χρησιμοποιηθεί σε συνδυασμό και με άλλα πρωτόκολλα.
- Το SNMP είναι ένα πρωτόκολλο του επιπέδου εφαρμογής που διευκολύνει την ανταλλαγή πληροφοριών μεταξύ των συσκευών δικτύου. Παρέχει έλεγχο ταυτότητας, ακεραιότητα, και κρυπτογράφηση δεδομένων. Η SNMP κυκλοφορία κρυπτογραφείται με το Data Encryption Standard (DES) αλγόριθμο, και φέρει τον HMAC MD5 ή SHA HMAC αλγόριθμο για τη διαδικασία της αυθεντικοποίησης και της ακεραιότητας.
- Τα Syslog μηνύματα είναι ανεπιθύμητες ειδοποιήσεις όπου μια συσκευή δικτύου μπορεί να σώσει σε ένα αρχείο καταγραφής ή να τα κατευθύνει σε ένα syslog διακομιστή. Τα Syslog μηνύματα περιλαμβάνουν χρονικές σημάνσεις (timestamps) από το διακομιστή syslog, το όνομα της συσκευής, έναν αύξοντα αριθμό, η χρονική σήμανση (timestamp) από τη συσκευή δικτύου και το ίδιο το μήνυμα.
- Το Network Time Protocol χρησιμοποιείται για να συγχρονίσει τα ρολόγια του συστήματος στις συσκευές δικτύου και είναι θεμελιώδους σημασίας για να χρησιμοποιούνται τα μηνύματα syslog που προέρχονται από πολλαπλές πηγές, των οποίων η χρονική σήμανση (timestamp) επιτρέπει να συσχετίσει τα γεγονότα που υπάρχουν στο ιστορικό δηλαδή ποιες συσκευές έχουν συνδεθεί και πότε.
- Οι μεταγωγείς κατακλύζονται εύκολα από κίνηση, επειδή επεξεργάζονται το πρώτο πακέτο της ροής στο λογισμικού. Το πρόβλημα αυτό λύνεται διατηρώντας όλες τις αποστολές στο υλικό (hardware).

- Ο έλεγχος πολιτικής (Control Plane Policy) επιτρέπει στους χρήστες να διαμορφώνουν την ποιότητα υπηρεσιών (QoS) μέσα από φίλτρο που διαχειρίζεται τη ροή των πακέτων για την προστασία του επιπέδου ελέγχου του μεταγωγέα κατά των DoS επιθέσεων. Αυτό βοηθά στη διατήρηση της κυκλοφορίας των πακέτων ανεξάρτητα από το γεγονός επιθέσεων ή του μεγάλου φορτίο κίνησης στο μεταγωγέα.
- Το Πρωτόκολλο Address Resolution Protocol (ARP) throttling περιορίζει το ρυθμό με τον οποίο προωθούνται τα πακέτα μέσα σε ένα συνδεδεμένο δίκτυο στην περίπτωση που η διεύθυνση MAC τους δεν έχει βρεθεί ακόμη (γειτνίαση). [4]

6.2.8 Ανάλυση κίνησης, Ανίχνευσης εισβολών και Πρόληψη

Οι υπηρεσίες/λειτουργίες που μπορούν να προσφερθούν σχετικά με την ανάλυση της κυκλοφορίας περιγράφονται παρακάτω.

- Η τεχνολογία Switch Port Analyzer (SPAN) και Remote SPAN (RSPAN) αντιγράφει την κίνηση από μία ή περισσότερες θύρες ενός μεταγωγέα (η πηγή SPAN) σε μία άλλη θύρα στον ίδιο διακόπτη (ο προορισμός SPAN). Αυτό συχνά αποκαλείται «Τοπικό SPAN». Το RSPAN επιτρέπει ο σκοπός της ανάλυσης να επεκταθεί και να συμπεριλάβει πολλούς μεταγωγείς διασυνδεδεμένους στο ίδιο επίπεδο. Το RSPAN και τα VACLs μπορούν να συνδυαστούν πολύ για την ανάλυση της κίνησης διαφοροποιώντας τη αντιγραμμένη κυκλοφορία.
- Η VACL δέσμευση είναι τεχνολογία που επιτρέπει στο ACLs να οριστεί για την παροχή ελέγχου πάνω στην κυκλοφορία που συλλαμβάνεται.
- Το NetFlow είναι μια τεχνολογία για την αποτελεσματική συλλογή και εξαγωγή στατιστικών στοιχείων από την κίνηση που ρέει μέσω μεταγωγών και δρομολογητών. Στο πλαίσιο της ασφάλειας, το NetFlow χρησιμοποιείται για τα DoS του,τα κατανεμημένα Dos (DDoS), και για την ανίχνευση ιών.
- Οι IDS αισθητήρες μπορούν να ανιχνεύσουν κακόβουλη δραστηριότητα βασισμένοι σε ανωμαλίες της κυκλοφορίας, ή σε ένα σταθερό ταίριασμα των γεγονότων που περιγράφονται από τις υπογραφές. Ένας IDS αισθητήρας μπορεί να ανιχνεύσει μια επίθεση από την αρχή της, προσδιορίζοντας την σχολαστικά. Οι IDS αισθητήρες μπορούν να λειτουργήσουν σε συνδυασμό με το μεταγωγέα ή το τοίχος προστασίας για να απομονώσουν έναν εξυπηρετητή που διακυβεύεται, πριν μολύνει και άλλες συσκευές μέσα στο δίκτυο. Η κατανομή κυκλοφορίας σε πολλαπλούς αισθητήρες IDS μπορεί να επιτευχθεί με τη χρήση μια σειράς τεχνολογιών κατοπτρισμού (mirroring)(RSPAN και VACL) για την ανάλυση μεγάλων ποσών κίνησης. Εκτός από το δίκτυο που βασίζεται η ανάλυση της κυκλοφορίας, ο εντοπισμός και η πρόληψη εισβολέων αποτελούν πρόσθετες εγγυήσεις ασφάλειας που μπορούν να εγκατασταθούν στους εξυπηρετητές. [4]

6.2.9 SAN εργαλεία

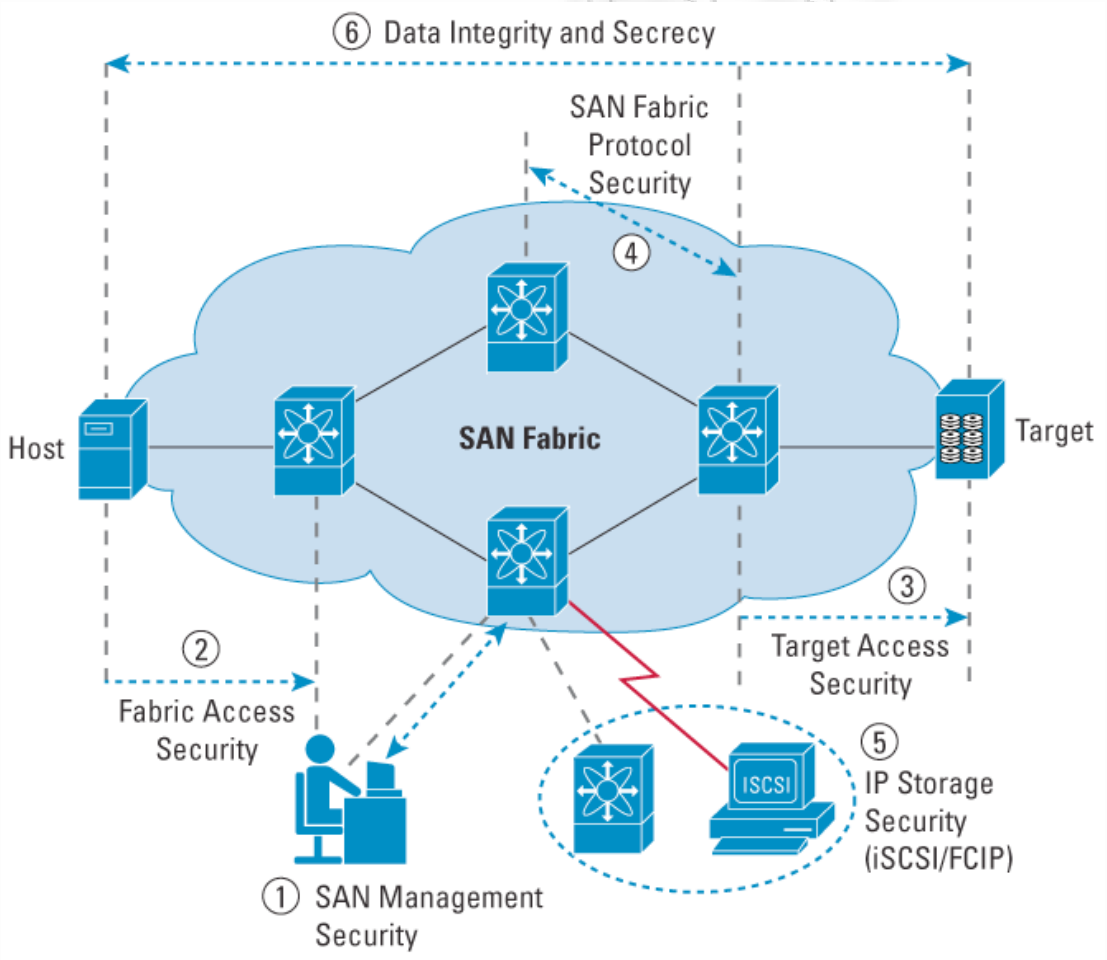
Παραδοσιακά, τα SANs έχουν θεωρηθεί "ασφαλή" επειδή οι SAN αναπτύξεις έχουν περιοριστεί σε ένα υποσύνολο ενός ενιαίου κέντρου δεδομένων-ουσιαστικά δηλαδή σε ένα απομονωμένο δίκτυο. Ένας επικίνδυνος υπολογιστής υποδοχής έχει τη δυνατότητα να διαταράξει άλλους υπολογιστές που συνδέονται με το SAN, με μη εξουσιοδοτημένη πρόσβαση στα δεδομένα του SAN, ή παρακάμπτοντας υφιστάμενα τοίχοι προστασίας (firewalls) και συστήματα ανίχνευσης εισβολής, εάν χρησιμοποιείται IP μέσω του Fibre Channel (RFC 2625).

Σήμερα δεν είναι ασυνήθιστο να βρεθεί ένα SAN το οποίο εκτείνεται έξω από ένα κέντρο δεδομένων για συνέχιση των επιχειρήσεων και για σκοπούς αποκατάστασης καταστροφών. Η υιοθέτηση τεχνολογιών όπως τα iSCSI και FCIP, τα οποία χρησιμοποιούν το πρωτόκολλο TCP/IP για τη μεταφορά, τονίζουν την ανάγκη για ασφάλεια του SAN λόγω των ευαίσθητων πληροφοριών που περνούν μέσω κοινών δικτύων δεδομένων.
Η ασφάλεια του SAN πρέπει να μελετηθεί από τρεις οπτικές γωνίες:
1. Διασφάλιση του SAN από εξωτερικές απειλές (για παράδειγμα, οι χάκερ και οι άνθρωποι με κακόβουλη πρόθεση)
2. Διασφάλιση του SAN από εσωτερικές απειλές (για παράδειγμα, μη εξουσιοδοτημένο προσωπικό και επικίνδυνες συσκευές)
3. Διασφάλιση του SAN από ακούσιες απειλές από εξουσιοδοτημένους χρήστες (λανθασμένες ρυθμίσεις και ανθρώπινα λάθη)
Τα δύο πρώτα είναι σχετικά απλά και κατανοητά καλά από την άποψη της ασφάλειας. Η τρίτη οπτική γωνία είναι λιγότερο σαφής και μόνο ελάχιστη ή καμία προσοχή στο παρελθόν έχει καταβληθεί για ακούσιες απειλές κατά της ασφάλειας από τους εξουσιοδοτημένους χρήστες. Είτε πρόκειται για UNIX ή για Windows περιβάλλον, πρέπει να ελαχιστοποιούνται οι προσβάσεις χρηστών με δικαιώματα διαχειριστή (administrator).

Βέβαια και σε αυτή την αντιμετώπιση υπάρχουν πολλές πτυχές -τα οφέλη που προκύπτουν από το κλείδωμα των δικαιωμάτων χρήσης σε ένα μεταγωγέα χρησιμοποιώντας το ρόλο της ταυτοποίησης είναι εύκολα κατανοητό αλλά όπως η ελαχιστοποίηση της πιθανότητας μιας

λανθασμένης ρύθμισης σε επίπεδο οπτικής ίνας που προκύπτει από λανθασμένη ρύθμιση σε μεταγωγέα είναι λιγότερο κοινά. Πολλές από αυτές τις προσεγγίσεις καθιστούν ασαφή όρια για την ασφάλεια του SAN, τις βέλτιστες πρακτικές σχεδίασης του SAN και της σχεδίασης ενός SAN υψηλής διαθεσιμότητας, αλλά όλες είναι σημαντικές από την άποψη ότι μία σωστά ρυθμισμένη, ασφαλή μετάβαση μπορεί να βοηθήσει στην πρόληψη τόσο των σκόπιμων όσο και της ακούσιων διακοπών. Η ασφάλεια του SAN εμφανίζεται καλύτερα από ένα αρχιτεκτονικό επίπεδο, όπου υπάρχουν έξι βασικοί τομείς εστίασης (Σχήμα 16). Οι έξι περιοχές περιλαμβάνουν:

- Πρόσβαση στην οπτική ίνα: Ασφαλή πρόσβαση στο δίκτυο οπτικών ινών καθώς και στις υπηρεσίες που προσφέρει.
- Πρόσβαση στο στόχο: Ασφαλής πρόσβαση στους στόχους και τους λογικούς αριθμούς μονάδων (LUN)
- SAN πρωτόκολλο: Ασφαλή επικοινωνία και εξουσιοδότηση από μεταγωγέα σε μεταγωγέα (switch to switch)
- Αποθήκευση της IP πρόσβασης: Ασφαλείς FCIP και iSCSI υπηρεσίες
- Ακεραιότητα των δεδομένων και του απορρήτου-Κρυπτογράφηση δεδομένων κατά τη μεταφορά
- SAN διαχείρισης πρόσβασης : Ασφαλή πρόσβαση στις υπηρεσίες διαχείρισης [4].



Σχήμα 16: Αναπαράσταση οργάνωσης SAN δικτύου [4]

6.3 Φυσική ασφάλεια

Εκτός από την ασφάλεια σε επίπεδο δικτύου και πληροφοριών υπάρχουν και κάποιοι κανόνες που πρέπει να τηρούνται και αφορούν τη φυσική ασφάλεια του κέντρου δεδομένων. Παρακάτω παρουσιάζονται όλες οι προδιαγραφές που πρέπει να έχει ο φυσικός χώρος που εκτείνεται το κέντρο δεδομένων ώστε να τηρεί τα πρότυπα ασφαλείας:

1. Η τοποθεσία του κέντρου δεδομένων
   - Η θέση της τοποθεσίας του κέντρου δεδομένων πρέπει να είναι σε μέρος όπου ο κίνδυνος των φυσικών καταστροφών είναι γνωστός και σχετικά μικρός. Οι φυσικές καταστροφές περιλαμβάνουν, αλλά δεν περιορίζονται μόνο σε δασικές πυρκαγιές, καταιγίδες, ανεμοστρόβιλους , τυφώνες, σεισμούς και πλημμύρες.
   - Η θέση της τοποθεσίας πρέπει να βρίσκεται σε μια περιοχή όπου η δυνατότητα των τεχνητών καταστροφών είναι χαμηλή. Οι ανθρωπογενείς καταστροφές περιλαμβάνουν αλλά δεν περιορίζονται μόνο σε αεροπορικά δυστυχήματα, ταραχές, εκρήξεις και πυρκαγιές. Η περιοχή δεν πρέπει να είναι δίπλα σε αεροδρόμια, φυλακές, αυτοκινητόδρομους, γήπεδα, τράπεζες, διυλιστήρια, αγωγούς, δεξαμενές αποθήκευσης.
   - Η παροχή της ηλεκτρικής ενέργειας στο χώρο πρέπει να είναι της τάξης του 99,9%. Η ηλεκτρική ενέργεια πρέπει να λαμβάνεται από δύο ξεχωριστούς υποσταθμούς (ή από περισσότερους) κατά προτίμηση από δύο ξεχωριστές μονάδες παραγωγής ενέργειας. Το νερό πρέπει να είναι διαθέσιμο από περισσότερες από μία πηγή.
   - Ένα κέντρο δεδομένων δεν πρέπει να μοιράζεται το ίδιο κτίριο με άλλα γραφεία, και ειδικά όταν πρόκειται για γραφεία που δεν ανήκουν στον ίδιο οργανισμό. Εάν ο χώρος πρέπει αναγκαστικά να μοιράζεται λόγω θεμάτων κόστους, τότε το κέντρο δεδομένων δεν πρέπει να έχει τοίχους που γειτνιάζουν με τα άλλα γραφεία.

2. Η περίμετρος του χώρου που βρίσκεται το κέντρο δεδομένων
   - Θα πρέπει να υπάρχει ένας φράκτης γύρω από την εγκατάσταση τουλάχιστον 20 μέτρα από το κτίριο για όλες του τις πλευρές και κάθε σημείο πρόσβασης να φυλάσσεται από έναν φρουρό. Επιπλέον, πρέπει να υπάρχει μια αυτόματη μέθοδο ελέγχου ταυτότητας των δεδομένων των εργαζομένων που δουλεύουν στο κέντρο δεδομένων. Η περιοχή γύρω από την εγκατάσταση πρέπει να φωτίζεται καλά και πρέπει να μην υπάρχουν εμπόδια εμποδίζουν την επιτήρηση μέσω καμερών και περιπολιών. Όπου είναι δυνατόν, οι χώροι στάθμευσης πρέπει να είναι τουλάχιστον 25 μέτρα από το κτίριο για να ελαχιστοποιηθεί η ζημιά από παγιδευμένα αυτοκίνητα. Δεν πρέπει να υπάρχει κάποιο σημάδι στο κτίριο που να φανερώνει ότι είναι στην πραγματικότητα ένα κέντρο δεδομένων ή σε ποια εταιρεία ανήκει.
   - Θα πρέπει να υπάρχουν κάμερες εκτός του κτιρίου για την παρακολούθηση και των γειτονικών ακινήτων και των παρκαρισμένων αυτοκινήτων.Μόνο οχήματα που ανήκουν στους εργαζομένους του κέντρου δεδομένων, στους εργολάβους, στους φύλακες, και στο προσωπικό καθαρισμού θα πρέπει να έχουν άδειες στάθμευσης. Τα οχήματα των επισκεπτών θα πρέπει να σταθμεύονται σε χώρους στάθμευσης για επισκέπτες. Οχήματα που δεν εντάσσονται σε καμία από αυτές τις κατηγορίες θα πρέπει να ρυμουλκούνται.

3. Αίθουσα Ηλεκτρονικών Υπολογιστών
   - Η τοποθεσία δεν πρέπει να έχει εξωτερικά παράθυρα στις αίθουσες των ηλεκτρονικών υπολογιστών. Αν ένα δωμάτιο υπολογιστών πρέπει να έχει έναν τοίχο κατά μήκος ενός εξωτερικού τοίχου θα πρέπει να υπάρχει φυσικό εμπόδιο που να μην επιτρέπει την εύκολη πρόσβαση σε εκείνο τον τοίχο.
   - Θα πρέπει να υπάρχουν σημάδια στην πόρτα(ες) που σηματοδοτούν την αίθουσα, όπως περιορισμένη πρόσβαση και την απαγόρευση των τροφίμων, ποτών και του καπνίσματος στις αίθουσες των υπολογιστών. Οι πόρτες πρέπει να είναι θωρακισμένες. Πρέπει να υπάρχουν μόνο δύο πόρτες σε κάθε αίθουσα υπολογιστών . Η πρόσβαση θα πρέπει να περιορίζεται σε εκείνους που χρειάζονται για την διατήρηση των εξυπηρετητών ή των υποδομών του δωματίου.

- Τα δωμάτια των υπολογιστών θα πρέπει να παρακολουθούνται από κάμερες. Κάθε δωμάτιο θα πρέπει να έχουν πρόσβαση σε συστήματα παροχής ενέργειας και ψύξης και φυσικά στο δίκτυο. Θα πρέπει να υπάρχουν περιοχές που παρέχουν αέρα και πρέπει να έχουν υποδομές για το φιλτράρισμα του αέρα. Επιπλέον, θα πρέπει να έχουν ψηλά ταβάνια για να είναι δυνατή η διασπορά της θερμότητας.
- Κάθε δωμάτιο του υπολογιστή θα πρέπει να έχει θερμοκρασία μεταξύ 55 και 75 βαθμούς Φαρενάιτ και υγρασία μεταξύ 20 και 80 τοις εκατό. Περιβαλλοντικοί αισθητήρες θα πρέπει να καταγράφουν την θερμοκρασία και την υγρασία του δωματίου.
- Είναι απαραίτητη η ύπαρξη πυροσβεστήρων σε κάθε αίθουσα υπολογιστών. Πρέπει να υπάρχει η παροχή ηλεκτρικής ενέργειας έκτακτης ανάγκης σε κάθε δωμάτιο.

4. Εγκαταστάσεις του κέντρου δεδομένων
   - Πρέπει να υπάρχει αυτάρκεια από συστήματα ψύξης σε ένα κέντρο δεδομένων.
   - Σε περίπτωση ανάγκης πρέπει να υπάρχει η δυνατότητα χρήσης μπαταρίας με επαρκή διάρκεια ώστε στη συνέχεια να εγκατασταθεί από την παραγωγή ηλεκτρικής ενέργειας με τη χρήση βενζίνης. Αν δεν υπάρχουν αποθέματα βενζίνης τότε θα πρέπει να παρέχεται 24 ώρες ενέργεια από τη μπαταρία. Θα πρέπει να υπάρχουν γεννήτριες βενζίνης στο χώρο με δυνατότητα λειτουργίας 24 ωρών.
   - Όλα τα έγγραφα που περιέχουν ευαίσθητες πληροφορίες θα πρέπει να τεμαχίζονται επιτόπου ή να στέλνονται σε καταστροφέα εγγράφων προτού πεταχτούν στα σκουπίδια. Οι κάδοι θα πρέπει να παρακολουθούνται από κλειστό κύκλωμα τηλεόρασης.

5. Σχέδιο ανάκαμψης από καταστροφή
   Το κέντρο δεδομένων πρέπει να έχει ένα σχέδιο αποκατάστασης των καταστροφών. Το σχέδιο πρέπει να καλύπτει τα εξής ερωτήματα: Τι συνιστά μια καταστροφή; Ποιος πρέπει να ειδοποιηθεί σχετικά με την αντιμετώπιση της καταστροφής και πώς; Ποιος διενεργεί αξιολόγηση των ζημιών και αποφασίζει ποιοι εφεδρικοί πόροι χρησιμοποιούνται ; Που βρίσκεται ο χώρος φύλαξης των αντιγράφων ασφαλείας; Πόσο συχνά και κάτω από ποιες συνθήκες ενημερώνεται το πλάνο/σχέδιο δράσης; Μια λίστα των ανθρώπων που εργάζονται στον οργανισμό πρέπει να διατηρείται και να περιλαμβάνει πληροφορίες για τα γραφεία, τα σπίτια και τους αριθμούς των κινητών τηλεφώνων τους.
   - Πρέπει να υπάρχει η τακτικής της δημιουργίας και φύλαξης αντιγράφων ασφαλείας των ουσιωδών πληροφοριών εκτός του χώρου του κέντρου δεδομένων. Πρέπει να υπάρχει πολιτική για τις εφεδρείες που να περιγράφει τη διαδικασία για την επαναφορά των πληροφοριών από τα αντίγραφα ασφαλείας και να επιτρέπει τους συχνούς ελέγχους για την εξασφάλιση της σωστής λειτουργίας του συστήματος λειτουργίας αντιγράφων.
   - Εφεδρικοί εξυπηρετητές μπορούν να τοποθετηθούν σε άλλο κέντρο δεδομένων. Επίσης, δοκιμαστικές λειτουργίες πρέπει γίνονται συχνά ώστε να εξασφαλίζεται η ασφαλής μετάβαση των λειτουργιών κατά τη διάρκεια μιας καταστροφής

6. Προδιαγραφές που σχετίζονται με τους ανθρώπους που έχουν πρόσβαση στο κέντρο δεδομένων
   - Οι φύλακες ασφαλείας πρέπει να υποβάλλουν συνεχείς έλεγχους στο κτίριο. Βασικά, πρέπει να εκπαιδεύονται για να ακολουθούν και να επιβάλουν αυστηρά την πολιτική ασφάλειας του χώρου.
   - Το προσωπικό καθαρισμού θα πρέπει να εργάζεται σε ομάδες τουλάχιστον των δύο ατόμων. Καθαρισμός του χώρου πρέπει να περιορίζεται στα γραφεία . Αν το προσωπικό καθαρισμού για οποιονδήποτε λόγο πρέπει να αποκτήσει πρόσβαση σε μια αίθουσα υπολογιστών θα πρέπει να συνοδεύονται από προσωπικό ασφαλείας.
   - Η είσοδος και η εγκατάλειψη του κτιρίου από τους μηχανικούς πρέπει να καταγράφεται.
   - Οι επισκέπτες πρέπει πάντα να συνοδεύονται από πρόσωπα ασφαλείας του χώρου και δεν πρέπει να έχουν πρόσβαση στις αίθουσες υπολογιστών χωρίς τη γραπτή έγκριση του διαχειριστή του κέντρου δεδομένων. Όλοι οι επισκέπτες που εισέρχονται αίθουσες ηλεκτρονικών υπολογιστών πρέπει να υπογράφουν σύμφωνα εμπιστευτικότητας.

7. Κανόνες που αφορούν τους χρήστες των κέντρων δεδομένων

- Οι χρήστες πρέπει να εκπαιδεύονται ώστε να προσέχουν και να αντιλαμβάνονται τους πιθανούς εισβολείς. Πρέπει επιπλέον να εξασφαλίζουν θέσεις εργασίας και φορητούς υπολογιστές εντός και εκτός της εγκατάστασης, να έχουν αντίληψη του περιβάλλοντος, καθώς και να γνωρίζουν τις διαδικασίες έκτακτης ανάγκης.
- Όλοι οι χρήστες που κινούνται μέσα στις εγκαταστάσεις πρέπει να υπογράφουν σύμφωνα εμπιστευτικότητας.
- Ένα οργανόγραμμα θα πρέπει να διατηρεί λεπτομερώς τις δουλειές και τια αρμοδιότητες του καθενός εργαζόμενου μέσα στο κέντρο δεδομένων. Ιδανικά, το οργανόγραμμα θα έχει πληροφορίες για τα καθήκοντα που έχει κάθε ο εργαζόμενος και πάνω σε τι πρέπει να εκπαιδευτεί.
- Δεν είναι αρκετό να καταγράφεται μόνο ό, τι γνωρίζουν οι ενεργεία υπάλληλοι για τα υπάρχοντα συστήματα. Όλες οι νέες εργασίες και οι αλλαγές, πρέπει να τεκμηριώνονται καθώς και να καταγράφονται.
- Οι εργαζόμενοι πρέπει να εκπαιδεύονται συνεχώς και σε νέα καθήκοντα πέρα από τη θέση εργασίας τους έτσι ώστε να είναι έτοιμοι να διαχειριστούν όλα τα θέματα που μπορεί να προκύψουν σε καταστάσεις κρίσης
- Μια βάση δεδομένων επαφής πρέπει να διατηρείται με τα στοιχεία επικοινωνίας όλων των υπαλλήλων του κέντρου δεδομένων.
- Οι εργαζόμενοι πρέπει να εκπαιδεύονται και να μπορούν να δουλεύουν από απόσταση σε περίπτωση που συμβεί κάτι στο φυσικό χώρο του κέντρου και είναι αδύνατη η πρόσβαση. [6]

7. «Πράσινο» κέντρο δεδομένων

Τα υψηλά λειτουργικά κόστη και η αναντιστοιχία ανάμεσα στη χρήση του κέντρου δεδομένων και στην κατανάλωση ενέργειας έχουν κεντρίσει το ενδιαφέρον για τη βελτίωση της ενεργειακής αποτελεσματικότητας. Μελέτες έχουν δείξει ότι οι εξυπηρετητές καταναλώνουν το 45% του συνολικού κόστους των κέντρων δεδομένων. Η ενέργεια που χρειάζεται για να λειτουργήσει ο IT εξοπλισμός σε ένα κέντρο δεδομένων σε συνδυασμό με την υποδομή ψύξης που απαιτείται, καταναλώνουν περίπου το 40% της συνολικής κατανάλωσης στα κέντρα δεδομένων. Από την άλλη η δικτύωση συνεισφέρει ένα ποσοστό της τάξης του 15% από τη συνολική κατανάλωσης ενέργειας. Η εξοικονόμηση ενέργειας μπορεί να επιτευχθεί με τη χρήση ποιο αποτελεσματικού εξοπλισμού (εξυπηρετητές και εξοπλισμό δικτύου) σε κατανάλωση ενέργειας. Πρέπει να σημειωθεί ότι πολλές προσπάθειες έχουν γίνει για την εξοικονόμηση ενέργειας μέσω διαχείρισης της ενέργειας σε εξυπηρετητές και σε clusters αποθήκευσης. Επιπλέον, προηγμένες αρχιτεκτονικές δικτύων μπορούν να μειώσουν την κατανάλωση ενέργειας σε ένα κέντρο δεδομένων. Έξυπνες τεχνολογίες έχουν αναπτυχθεί για την μετάδοση ενέργειας αλλά και για την ψύξη οι οποίες έχουν σαν αποτέλεσμα τη σημαντική μείωση ενέργειας. Η σημαντικότητα της οικολογικής διάστασης που πρέπει να χαρακτηρίζει ένα κέντρο δεδομένων έχει οδηγήσει στην ίδρυση ειδικών συστημάτων και μέτρων που βαθμολογούν την ενεργειακή απόδοση των κέντρων δεδομένων και παρέχουν τις απαραίτητες πιστοποιήσεις για τη λειτουργία τους. Παρακάτω, ακολουθεί μια μικρή αναφορά των μέτρων/συστημάτων ενεργειακής αξιολόγησης:

- PUE (Power Usage Effectiveness)

Δημιουργήθηκε από τα μέλη του Green Grid και είναι ένα μέτρο που καθορίζει την ενεργειακή αποτελεσματικότητα ενός κέντρου δεδομένων.Το PUE προκύπτει διαιρώντας το ποσό της ενέργειας που εισάγεται στο κέντρο δεδομένων με την πραγματική ενέργεια που χρησιμοποιείται για να λειτουργήσει όλη η υποδομή του. Εκφράζεται σαν ποσοστό, όπου η αποτελεσματικότητα αγγίζει το 1. Μία συνηθισμένη τιμή για ένα κέντρο δεδομένων είναι το 1,3 και ένας μέσος όρος της τάξης του 2, 5 – 3 μπορεί να χαρακτηριστεί ως κακός-αναποτελεσματικός.

- DCiE (Data Center Infrastructure Efficiency)

Δημιουργήθηκε από τα μέλη του Green Grid και αποτελεί ένα ακόμα μέτρο για την αξιολόγηση της ενεργειακής αποτελεσματικότητας και είναι αντίστροφο του PUE. Εκφράζεται σαν ποσοστό και υπολογίζεται διαιρώντας την ενέργεια που χρησιμοποιείται από το εξοπλισμό του κέντρου δεδομένων προς τη συνολική ενέργεια της υποδομής. Η αποτελεσματικότητα βελτιώνεται όσο το DCiE πλησιάζει το 100%. Ποσοστά που αγγίζουν το 77% θεωρούνται ικανοποιητικά , ενώ τιμές όπως 33% και 40% δεν θεωρούνται καλές.

- LEED((Leadership in Energy and Environmental Design) Certified

Αναπτύχθηκε από το U.S. Green Building Council (USGBC), το LEED site είναι διεθνώς αναγνωρισμένο σύστημα πιστοποίησης πράσινων κτιρίων. Παρέχει επιβεβαίωση από τρίτους (third party) ότι το κτίριο έχει κτιστεί και σχεδιαστεί χρησιμοποιώντας στρατηγικές που βοηθούν στην αύξηση της αποδοτικότητας σε όλα τα σημαντικά μέτρα όπως την εξοικονόμηση ενέργειας, την αποδοτικότητα νερού, τη μείωση των εκπομπών διοξειδίου του άνθρακα (CO_2), την ποιότητα του εσωτερικού περιβάλλοντος, τη διαχείριση των πόρων και τις επιπτώσεις τους στο γενικότερο περιβάλλον.

- The Green Grid

Μία μη κερδοσκοπική παγκόσμια ένωση εταιρειών και εκπαιδευτικών φορέων για τη βελτίωση την ενεργειακής αποτελεσματικότητας στα κέντρα δεδομένων. Green Grid δεν προσυπογράφει εμπορικά προϊόντα και λύσεις αλλά αντίθετα παρέχει συμβουλές για καλύτερες πρακτικές, μέτρα και τεχνολογίες που θα αναπτύξουν εξολοκλήρου την ενεργειακή αποτελεσματικότητα του κέντρου δεδομένων.

Για παράδειγμα το κέντρο δεδομένων του Facebook που βρίσκεται στο Prineville, Oregon έχει λάβει χρυσή πιστοποίηση LEED από το U.S Green Building Council. Η αποτελεσματικότητα της χρήσης της ενέργειας (PUE) ποικίλει από 1.06 μέχρι 1.1, καθιστώντας το ένα πράσινο κτίριο που καταναλώνει τη μισή ενέργεια από αυτή που θα κατανάλωνε ένα απλό κτίριο.
Επίσης και το δεύτερο υπολογιστικό κέντρο του Facebook (βλέπε Σχήμα17) είναι γεγονός και βρίσκεται στην Βόρεια Καρολίνα των ΗΠΑ, βασίζει στα οικολογικά βήματα του πρώτου και

στοχεύει σε όσο το δυνατόν οικολογικότερη λειτουργία, χρησιμοποιώντας ένα σύστημα κλιματισμού σχεδιασμένο από την OpenCompute, που ανακυκλώνει τον εξωτερικό δροσερό αέρα για την ψύξη των μηχανημάτων στο εσωτερικό. Για την αποτελεσματικότερη χρήση της ενέργειας το κτίριο έχει ένα τροφοδοτικό που στέλνει συνεχές ρεύμα στους διακομιστές, το οποίο εξοικονομεί ενέργεια μειώνοντας τις μετατροπές μεταξύ εναλλασσόμενου ρεύματος από το δίκτυο και του συνεχούς ρεύματος που χρησιμοποιείται από τον τεχνικό εξοπλισμό (hardware). Οι εξυπηρετητές ρυθμίζονται ανάλογα και είναι ικανοί να λειτουργούν σε υψηλότερες θερμοκρασίες, γεγονός που μειώνει τις ανάγκες ψύξης του αέρα.
Βέβαια το πόσο φιλικό είναι στο περιβάλλον μπορεί να επιδέχεται αμφισβητήσεις. Η Greenpeace επανειλημμένα έχει κατακρίνει υπολογιστικά κέντρα για την γενικευμένη χρήση ηλεκτρικού ρεύματος που παράγεται από παραδοσιακές ρυπογόνες τεχνολογίες, ενώ η χρήση ηλιακών πάνελ (110 KW) για την παροχή ενέργειας στα γραφεία στο καινούργιο κέντρο του Facebook αλλά και της Apple στο Maiden λέγεται ότι είναι μόνο για θέμα δημοσίων σχέσεων και όχι ουσιαστικής συμβολής στην μείωση των ρύπων.

Σχήμα 17: Το νέο κέντρο δεδομένων του facebook [5]

Παρακάτω ακολουθούν μερικές λύσεις για την επίτευξη ενεργειακά αποτελεσματικών κέντρων δεδομένων.

7.1.1 Εξυπηρετητές ενεργειακής απόδοσης

Σύμφωνα με έρευνες το 45% της συνολικής κατανάλωσης ενέργειας ενός κέντρου δεδομένων πάει στους εξυπηρετητές. Οι λόγοι για τους οποίους υπάρχει αυτό το μεγάλο μέγεθος στην κατανάλωση ενέργειας είναι δύο: η μικρή χρήση των εξυπηρετητών και η έλλειψη σωστής αναλογίας στην κατανάλωση ενέργειας, δηλαδή σε χαμηλά επίπεδα εργασίας , οι εξυπηρετητές καταναλώνουν μεγάλα ποσοστά ενέργειας. Όταν ένας ενεργειακά αποτελεσματικός εξυπηρετητής βρίσκεται σε κατάσταση αδράνειας καταναλώνει πάνω από το 50% της ενέργειας όταν βρίσκεται σε κατάσταση αιχμής και πολύ συχνά μπορεί να φτάσει και το 80% όταν πρόκειται για έναν κοινό εξυπηρετητή. Τα μεγάλα ποσά ενέργειας που σπαταλούνται όταν ένας εξυπηρετητής βρίσκεται σε χαμηλή κατάσταση λειτουργίας έχουν δείξει την ανάγκη ανασχεδιασμού κάθε εξαρτήματος του υπολογιστικού συστήματος έτσι ώστε να βρει εφαρμογή η έννοια της αναλογικής ενέργειας. Συγκεκριμένα, οι επεξεργαστές αποτελούν το πιο πολυδάπανο εξάρτημα καθώς μπορούν να καταναλώσουν πάνω από το 55% της συνολικής ενέργειας που καταναλώνει ένας εξυπηρετητής. Έρευνες έχουν γίνει ώστε να εξερευνηθεί ο σχεδιασμός του επεξεργαστή για να ελαττωθεί η ενέργεια που καταναλώνει η CPU με Dynamic Voltage/Frequency scale (DVFS). Το DVFS μπορεί να αναπτυχθεί για την εξοικονόμηση ενέργειας μειώνοντας την τάση και τη συχνότητα. Έχει αποδειχθεί ότι η αποτελεσματικότητα του DFVS στην εξοικονόμηση ενέργειας κάτω από μέτριο φόρτο εργασίας είναι σημαντική καθώς μπορεί να σώσει από το 23% μέχρι το 36% της συνολικής ενέργειας της κεντρικής μονάδας επεξεργασίας και παράλληλα να διατηρεί την ανταπόκριση του εξυπηρετητή σε λογικά όρια στον επεξεργαστή. Παρόλα αυτά στους σύγχρονους εξυπηρετητές δεν είναι οι επεξεργαστές που κυριαρχούν στην κατανάλωση ενέργειας, αφού συμμετέχουν στο 25% της συνολικής ενέργειας. Το chipset είναι αυτό που καταναλώνει σταθερά και μεγάλα ποσά ενέργειας στους σύγχρονους εξυπηρετητές. Το chipset είναι αυτό που καταναλώνει σταθερά την περισσότερη ενέργεια στους σύγχρονους εξυπηρετητές.

Πολλές τεχνικές μπορούν να εφαρμοστούν για τη μείωση την κατανάλωσης ενέργειας από τη μνήμη αλλά και από τα άλλα υποσυστήματα δίσκου. Μία καινοτόμα τεχνική διαχείρισης ενέργειας σε επίπεδο συστήματος προτάθηκε με σκοπό να επαναϋπολογίζει τη διαθέσιμη ενέργεια ανάμεσα στον επεξεργαστή και τη μνήμη και να διατηρεί τον προϋπολογισμό ενέργειας του εξυπηρετητή. Παρόλα αυτά, σε τέτοιου είδους τεχνικές έχει παρατηρηθεί να παραβιάζεται ο προϋπολογισμός ενέργειας που έχει υπολογιστεί αλλά και να υποβαθμίζεται η απόδοση χωρίς να υπάρχει αναγκαιότητα. Για το λόγο οι Bruno et al. πρότειναν τέσσερεις τεχνικές την Knapsack, LRUGreedy, LRU-Smooth και LRU-ordered για να περιορίσουν δυναμικά την κατανάλωση ενέργειας ρυθμίζοντας την κατανάλωση ρεύματος από τις συσκευές μνήμης , ως συνάρτηση του φόρτου σε ένα υποσύστημα μνήμης. Επιπλέον, γνωστοποίησαν , ότι με αυτές τις τεχνικές γίνεται ανταλλαγή ανάμεσα στην κατανάλωση ενέργειας και στην επίδοση. Οι Bruno et al. πρότειναν και το mini-rank , μία διαφορετική αρχιτεκτονική της μνήμης DRAM, όπου η βαθμίδα μιας τυπική DRAM «σπάει» σε πολλές μικρότερες βαθμίδες που ενώνονται με μία μικρή γέφυρα και κατά αυτό τον τρόπο μειώνεται η κατανάλωση ενέργειας από τη DRAM.

Για να κατασκευαστεί ένα ενεργειακά αναλογικό υπολογιστικό σύστημα, κάθε εξάρτημα του πρέπει να καταναλώνει ενέργεια ανάλογη με τη χρήση του. Πράγμα που σημαίνει ότι εάν ένα εξάρτημα δεν χρησιμοποιείται ή βρίσκεται σε κατάσταση μικρού φόρτου εργασίας δεν πρέπει να καταναλώνει μεγάλα ποσά ενέργειας. Όσο απλό και αν ακούγεται αυτό, στην πραγματικότητα δεν είναι και αποτελεί μία έρευνα πρόκληση. Διάφορα σχήματα διαχείρισης ενέργειας έχουν προταθεί για μείωση της ενέργειας που καταναλώνεται , θέτοντας τους αδρανείς εξυπηρετητές σε κατάσταση ύπνου. [9]

7.1.2 Χρήση εναλλακτικών πηγών ενέργειας

Η ηλιακή, η αιολική, η υδροηλεκτρική, οι κυψέλες καυσίμου, το βιο-αέριο και άλλες πηγές ενέργειας έχουν προκαλέσει το ενδιαφέρουν των συντελεστών των κέντρων δεδομένων λόγω της αβεβαιότητας και της ανησυχίας που προκαλεί η ηλεκτρική ενέργεια σε θέματα κόστους, ανανέωσης/ανεφοδιασμού και εκπομπών CO_2, αλλά και ακολουθώντας μία γενικότερη κοινωνική κατεύθυνση προς την αναζήτηση ενεργειακών λύσεων φιλικών προς το περιβάλλον.

Με βάση την τοποθεσία του κέντρου δεδομένων (κλιματικοί και γεωγραφικοί παράγοντες λαμβάνονται υπόψη) μία από τις παραπάνω τεχνολογίες μπορεί να βρει εφαρμογή αν όχι σαν μία ολοκληρωτική λύση αλλά το λιγότερο σαν μερική. Βέβαια, πριν την επιλογή κάποιας από τις

παραπάνω μορφές ενέργειες θέματα όπως η αξιοπιστία, οι διαθέσιμοι πόροι, η διασύνδεση και το κόστος πρέπει να εξεταστούν.

Πρέπει να σημειωθεί ότι οι εναλλακτικές/ανανεώσιμες πηγές ενέργειας είναι δύσκολο να εφαρμοστούν σε μεγάλα κέντρα δεδομένων. Για αυτό το λόγο το USGBC (United States Green Building Council στο δικό τους LEED) σύστημα αξιολόγησης των κέντρων δεδομένων δίνει σαν μέγιστο στόχο το 20% της συνολικής ενέργειας που καταναλώνεται σε ένα κέντρο δεδομένων να προέρχεται από ανανεώσιμες πηγές. Αυτό το ποσοστό με το πέρασμα του χρόνου μπορεί να αλλάξει καθώς τα περισσότερα κέντρα δεδομένων δείχνουν όλο και περισσότερη προθυμία να «αγκαλιάσουν» τις ανανεώσιμες πηγές ενέργειας αλλά και να επιτύχουν καλύτερες επιδόσεις.

Η ηλιακή ενέργεια, τα φωτοβολταικά είναι γενικά η προτεινόμενη μορφή ηλιακής ενέργειας και είναι η πρώτη τεχνολογία που μας έρχεται στο μυαλό όταν αναφερόμαστε σε εναλλακτικά ενεργειακά συστήματα. Φορολογικές ελαφρύνσεις, κίνητρα και εκπτώσεις προσφέρονται από κράτη σε όλο τον κόσμο ώστε να ενισχύσουν τη χρήση της ηλιακής ενέργειας. Ωστόσο Solar Thermal αρχίζει να αποκτά ευρύτερη αποδοχή από την αγορά, είναι σε θέση να εξισώσει το κόστος της "αιχμής" στους σταθμούς παραγωγής ηλεκτρικής ενέργειας, και είναι κατάλληλη για μεγάλα κέντρα δεδομένων.

Η αιολική ενέργεια θεωρείται από τις φθηνότερες τεχνολογίες για την παραγωγή ενέργειας από ανανεώσιμες πηγές, αφού αν οι ανεμογεννήτριες τοποθετηθούν σε μέρη με ευνοϊκό άνεμο είναι ικανές να παράγουν μεγάλα ποσά ενέργειας (50MW τη φορά). Οι ιδιοκτήτες των κέντρων δεδομένων συχνά συνάπτουν συμβόλαια με εταιρείες παραγωγής αιολικής ενέργειας και συνήθως κλειδώνουν συμφωνίες με ευνοϊκές τιμές ηλεκτρικής ενέργειας , χωρίς την εκπομπή CO_2. Πολλές φορές οι ιδιοκτήτες παρέχουν χώρο στις εταιρείες μέσα στα σύνορα της έκτασης που βρίσκεται το κέντρο δεδομένων για την τοποθέτηση των ανεμογεννητριών. Άλλες φορές μεγάλα κέντρα δεδομένων που φιλοξενούν κέντρα δεδομένων από πολλές εταιρείες διαπράττουν συμφωνίες με τις κατάλληλες ενεργειακές εταιρείες ώστε να αναπτύξουν τη δική τους μονάδα παραγωγής ενέργειας. Οι SCE and PG&E για παράδειγμα παράγουν ένα σημαντικό μέρος της συνολικής τους ενέργειας από τον άνεμο. Το ποσοστό αυτό αγγίζει το 30% της συνολικής τους ενέργειας. Η χαμηλή ενέργεια και ο αρχιτεκτονικά προηγμένος άνεμος αποτελούν σύγχρονα μέσα στο χώρο των κέντρων δεδομένων. Ανάλογα με τις ενεργειακές ανάγκες του κάθε κέντρου δεδομένων τα συστήματα αυτά μπορούν να παράγουν από ένα μικρό ποσοστό ενέργειας μέχρι τη συνολική ενέργεια που απαιτείται για να καλυφθούν οι απαιτήσεις ενός κέντρου δεδομένων. Αυτά τα ενεργειακά συστήματα μπορούν να χρησιμοποιηθούν από ήδη υπάρχοντα κτίρια με ελάχιστες έως και ανύπαρκτες επιπτώσεις στις καθημερινές λειτουργίες. Με λίγα λόγια, δεν χρειάζεται ένα κτίριο να έχει κατασκευαστεί από την αρχή με υποδομές που επιδέχονται τη χρήση εναλλακτικών μορφών ενέργειας, η χρήση της αιολικής ενέργειας μπορεί να γίνει ακόμα και από παλιότερα κατασκευασμένα κτίρια ύστερα από κάποιες αλλαγές.

Η υδροηλεκτρική ενέργεια αποτελεί πλέον μία από διαδεδομένες πηγές ενέργειας και η πρώτη επιλογή από μεγάλα κέντρα δεδομένων για να καλύψει μεγάλο μέρος των αναγκών τους σε ενέργεια εξαιτίας του μικρού της κόστους. Βέβαια, δεν αποτελεί μία βιώσιμη λύση για όσους θέλουν να αναπτύξουν τη δικιά τους πηγή ενέργειας. Μόνο μεγάλα κρατικά data canters έχουν τη δυνατότητα έκδοση άδειας για την εκμετάλλευση της υδροηλεκτρικής ενέργειας μέσα από δικές τους εγκαταστάσεις. Όπως συμβαίνει και με την αιολική ενέργεια υπάρχουν μικρές λύσεις–εταιρείες στην αγορά για την παραγωγή υδροηλεκτρικής ενέργειας. Παρόλα αυτά η έρευνα και η προετοιμασία που απαιτείται για τη δημιουργία τέτοιων εγκαταστάσεων καθώς και η διαδικασία αδειοδότησης αφήνουν το χώρο κυρίως στις εταιρείες κοινής ωφέλειας μου είναι τον εξοπλισμό και την τεχνογνωσία να διαχειριστούν τέτοιες διαδικασίες.

Οι κυψέλες καυσίμου, αποτελούν μία ακόμη μορφή εναλλακτικής ενέργειας. Σε μια κυψέλη καυσίμου (fuel cell) καίγεται υδρογόνο, στα μόρια του οποίου υπάρχει αποθηκευμένη χημική ενέργεια και παράγεται ηλεκτρική ενέργεια, νερό και θερμότητα. Οι κυψέλες καυσίμου δεν αποθηκεύουν στο εσωτερικό τους ενέργεια όπως π.χ. οι μπαταρίες. Το καύσιμο, δηλαδή το υδρογόνο, αποθηκεύεται εξωτερικά σε ειδική δεξαμενή και περιμένει να χρησιμοποιηθεί (όπως π.χ. η βενζίνη στη μηχανή του αυτοκινήτου ή τα ξύλα για το τζάκι). Η νέα εναλλακτική μορφή ενέργειας ξεκινά να βρίσκει εφαρμογή σε πολλά κέντρα δεδομένων, ιδίως όταν μπορούν να επωφεληθούν από ολόκληρο τον κύκλο ενέργειας τω ν κυψέλων καυσίμου, συμπεριλαμβανομένης της ενέργειας που χάνεται που μπορεί όμως να χρησιμοποιηθεί ως πηγή ενέργειας από τους ψύχτες απορρόφησης. Μέτρια σε κατανάλωση ενέργειας κέντρα δεδομένων της τάξης των 200 μέχρι 500kW με τα κατάλληλα κίνητρα μπορούν να επιτύχουν

ευνοϊκούς συντελεστές απόδοσης. Σε μικρότερου μεγέθους εφαρμογές της χρήσης των κυψελών καυσίμου , έχει ξεκινήσει η αντικατάσταση της παραδοσιακής μπαταρίας . Η ποιότητα της ενέργειας που προσφέρουν οι κυψέλες καυσίμου σε συνδυασμό με το κόστος συντήρησης , τις μηδαμινές εκπομπές βλαβερών αερίων για το περιβάλλον και τα φορολογικά κίνητρα που δίνουν αποτελούν πολλούς σοβαρούς λόγους για να επιλέξει κάποιος αυτή τη μορφή ενέργειας.

Το βιοαέριο και οι ανεμογεννήτριες αποτελούν ένα συνδυασμό ανεμογεννητριών με το φυσικό αέριο ή το βιοαέριο ως μία μορφή εναλλακτικής ενέργειας. Παρόλο που αυτά τα συστήματα δεν έχουν μηδενικές εκπομπές CO_2, βοηθούν στην αναμόρφωση του χώρο που θα χρησιμοποιηθούν όπως επιπλέον περιορίζουν όλα τα επικίνδυνα θέματα που προκύπτουν από τη διαχείριση του φυσικού αερίου στην εκάστοτε περιοχή. Όπως συμβαίνει με όλα τα συστήματα παραγωγής ενέργειας έτσι και με αυτό πρέπει να ελεγχτούν τυχούσες φοροαπαλλαγές ή επιχορηγήσεις από την USGBC για την χρήση αυτής της μορφής ενέργειας. Επιπλέον, η αναζήτηση συνεργασιών με τις τοπικές αρχές όπως και η παροχή βοηθητικών προγραμμάτων από συγκεκριμένους φορείς μπορούν να δώσουν όλα τα βασικά εχέγγυα για την ανάπτυξη και διάδοση αυτής της νέας μορφής ενέργειας.

Η γεωθερμική ενέργεια παρόλα που κερδίζει ολοένα την αποδοχή της αγοράς είναι εξαιρετικά περιορισμένη λόγω γεωγραφικών συνθηκών καθώς δεν είναι διαθέσιμη παντού και εξαρτάται από το έδαφος της κάθε περιοχής. Για αυτούς του λόγους θεωρείται μία σπάνια και ακριβή μορφή ενέργειας και η εκμετάλλευση της απαιτεί σημαντικές και κλιμακούμενες εργασίες ώστε να επιτευχθεί το λιγότερο δυνατό κόστος.

Άλλες πηγές ενέργειας που μπορούν να χρησιμοποιηθούν είναι η δύναμη της παλίρροιας και των κυμάτων. Γενικά, η ακαδημαϊκή κοινότητα έχει προβεί σε έρευνες για την εκμετάλλευση τους αλλά λόγω του μεγάλου κόστους μόνο οι εταιρείες κοινής ωφέλειας μπορούν να επωφεληθούν από την εκμετάλλευση τους [7].

8. Συμπεράσματα- Εργασία για το μέλλον

Τα κέντρα δεδομένων έχουν πλέον αγγίζει κάθε κομμάτι της σημερινής οικονομίας. Η χρήση των υπηρεσιών που προσφέρουν είναι ευρεία και χρησιμοποιούνται από επιχειρήσεις, κυβερνήσεις, εκπαιδευτικούς οργανισμούς, αποτελούν αναπόσπαστο εργαλεία της καθημερινής ζωής. Οι υπηρεσίες και οι εφαρμογές τους είναι αναρίθμητες και για αυτό τα επιτάσσει να αναπτύσσονται συνεχώς με βάση της τελευταίες εξελίξεις της τεχνολογίας και τις ανάγκες του διαδικτυακού κόσμου. Μέσα σε αυτήν τη διατριβή έγιναν αναφορές σε εισαγωγικά στοιχεία των κέντρων δεδομένων, στις αρχιτεκτονικές που χρησιμοποιούνται, στα προβλήματα συμφόρησης, στα προβλήματα του επιπέδου μεταφοράς, στα θέματα ενέργειας και στα θέματα ασφάλειας των κέντρων δεδομένων. Διάφορα είδη αρχιτεκτονικών αναλύθηκαν και αναφέρθηκαν ξεχωριστά τα χαρακτηριστικά και οι απατήσεις της κάθε αρχιτεκτονικής. Μελετήθηκαν και συγκρίθηκαν αλγόριθμοι ελέγχου συμφόρησης αναφορικά με τα προβλήματα συμφόρησης που παρατηρούνται στους μεταγωγείς που χρησιμοποιούντα στα κέντρα δεδομένων. Μια σύντομη αναφορά έγινε και στο φαινόμενο του tcp incast και προτάθηκαν λύσεις για την αντιμετώπιση του. Όπως είναι αναμενόμενο, όταν μιλάμε για μεγάλου μεγέθους κέντρα δεδομένων τα οποία φυλάσσουν και διακινούν σημαντικές πληροφορίες, το θέμα της ασφάλειας είναι πολύ βασικό. Για το λόγο αυτό έγινε μια περιγραφή του προβλήματος και προτάθηκαν εργαλεία-λύση για την πρόληψη, διάγνωση και αντιμετώπιση ανεπιθύμητων εισβολέων. Τέλος έγινε μια μικρή αναφορά στα ενεργειακά θέματα των κέντρων δεδομένων, καθώς αποτελούν πολυδάπανες μονάδες κατανάλωσης ενέργειας. Τα ποσοστά κατανάλωσης ενέργειας πρέπει να περιοριστούν μέσα στο πλαίσιο του κινήματος για έναν πιο πράσινο πλανήτη. Μέσα σε αυτήν τη διατριβή προτείνονται κάποιες λύσεις για την επίτευξη πιο πράσινων κέντρων δεδομένων.

Η διατριβή αυτή μπορεί να εμπλουτιστεί στο μέλλον με προσομοιώσεις πάνω στους αλγόριθμους συμφόρησης έτσι ώστε τα αποτελέσματα και τα συμπεράσματα να στηρίζονται πάνω σε πραγματικούς αριθμούς και δεδομένα. Επιπλέον, στα θέματα εξοικονόμησης ενέργειας μπορεί να γίνει περισσότερη έρευνα σε ότι αφορά το δικτυακό εξοπλισμό, τα συστήματα ψύξης, στα συστήματα αποθήκευσης αλλά και στις αρχιτεκτονικές των κέντρων δεδομένων με στόχο τη μείωση της κατανάλωσης ενέργειας. Καλύπτει τις εισαγωγικές έννοιες του κόσμου των κέντρων δεδομένων και απευθύνεται τόσο σε αναγνώστες που δεν έχουν αλλά και σε αναγνώστες που έχουν τεχνολογικό υπόβαθρο.

9. Αναφορές

[1] "Data center tier classifications and five-nines availability" διαθέσιμο στο http://www.cablinginstall.com/index/display/article-display.articles.cabling-installation-maintenance.**volume-18.issue**-2.features.data-center_tier_classifications.html
[2] "Data center" Διαθέσιμο στο http://en.wikipedia.org/wiki/Data_center
[3] Andrew S. Tanenbaum,"Computer Networks", Fourth Edition
[4] "Data center Networking security" διαθέσιμο στο http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps4358/prod_white_paper0900aecd80281e21.pdf// Data network security by Cisco
[5] " Secret to Facebook's green data center? Water misters" διαθέσιμο στο http://news.cnet.com/8301-11128_3-57327477-54/secret-to-facebooks-green-data-center-water-misters/
[6] "Data center physical security" διαθέσιμο στο http://www.sans.org/reading_room/whitepapers/awareness/data-center-physical-security-checklist_416
[7] Jinjing Jiang and Raj Jain, "Analysis of Backward Congestion Notification (BCN) for Ethernet In Datacenter Applications", Washington University in Saint Louis
[8] Albert Greenberg James R. Hamilton Navendu Jain, Srikanth Kandula Changhoon Kim Parantap Lahiri, David A. Maltz Parveen Patel Sudipta Sengupta, "VL2: A Scalable and Flexible Data Center Network"
[9] Zhang Yan and Ansari Nirwan, "A Survey on Architecture Design, Congestion Control, TCP Incast and Power Consumption in Data Center Networks" , January 2011
[10] Berk Atikoglu, Abdul Kabbani and Balaji Prabhakar, "Congestion Notification in Ethernet: Part of the IEEE 802.1 Data Center Bridging standardization effort"
[11] "Data Center Resource Infrastructure Guide" διαθέσιμο στο http://www.anixter.com/AXECOM/AXEDocLib.nsf/(UnID)/F9F7765DAF87FF1B86257383004E9C5F/$file/Data_Center_Guide.pdf
[12] Jinjing Jiang and Raj Jain, "Analysis of Backward Congestion Notification (BCN) for Ethernet In Datacenter Applications".
[13] "QCN pseudo-code" διαθέσιμο στο http://www.ieee802.org/1/files/public/docs2008/au-rong-qcn-serial-hai-pseudo-code%20rev2.0.pdf.
[14] Y. Zhang and N. Ansari, "On Mitigating TCP Incast in Data Center Networks," in Proc. of IEEE conference on Information Communications 2011 (INFOCOM 2011), Shanghai, China, April 10-15, 2011.
[15] "IEEE 802 Tutorial: Congestion Notification" , San Diego, CA, 17 July 2006 διαθέσιμο στο http://www.ieee802.org/802_tutorials/06-July/au-thaler-cn-tutorial-print.pdf
[16] A. Greenberg, P. Lahiri, D. A. Maltz, P. Patel, and S. Sengupta, "Towards a Next Generation Data Center Architecture: Scalability and Commoditization," in Proc. of the ACM workshop on Programmable Routers for Extensible Services of Tomorrow 2008 (PRESTO '08), Seattle, WA, USA, August 22, 2008, pp. 57–62.
[17] R. Niranjan Mysore, A. Pamboris, N. Farrington, N. Huang, P. Miri, S. Radhakrishnan, V. Subramanya, and A. Vahdat, "PortLand: a Scalable Fault-Tolerant Layer 2 Data Center Network Fabric," in Proc. of the ACM SIGCOMM Conference on Data Communication 2009 (SIGCOMM '09), Barcelona, Spain, August 17-21, 2009, pp. 39–50.
[18] J. Mudigonda, P. Yalagandula, M. Al-Fares, and J. C. Mogul, "SPAIN: COTS Data-Center Ethernet for Multipathing over Arbitrary Topologies," in Proc. of the 7th USENIX Symposium on Networked Systems Design and Implementation (NSDI '10), San Jose, CA, April 2010.
[19] J. Kim, W. J. Dally, and D. Abts, "Flattened Butterfly: a Cost-Efficient Topology for High-Radix Networks," in Proc. of the 34th annual International Symposium on Computer Architecture, vol. 35, no. 2, May 2007, pp. 126–137.
[20] D. Li, C. Guo, H. Wu, K. Tan, Y. Zhang, and S. Lu, "FiConn: Using Backup Port for Server Interconnection in Data Centers," in Proc. Of the 28th conference on Information Communications 2009 (INFOCOM '09), April 19-25, 2009, pp. 2276 –2285.
[21] Y. Liao, D. Yin, L. Gao, "DPillar: Scalable Dual-Port Server Interconnection for Data Center Networks," in Proc. of the 19th International Conference on Computer Communications and Networks, 2010 (ICCCN'10), Zurich, Switzerland, Aug. 2-5, 2010.

[22] C. Guo, H. Wu, K. Tan, L. Shi, Y. Zhang, and S. Lu, “DCell: a Scalable and Fault-Tolerant Network Structure for Data Centers,” in Proc. of the ACM SIGCOMM Conference on Data Communication 2008 (SIGCOMM ’08), Seattle, WA, August 17-22, 2008, pp. 75–86.
[23] C. Guo, G. Lu, D. Li, H. Wu, X. Zhang, Y. Shi, C. Tian, Y. Zhang, and S. Lu, “BCube: a High Performance, Server-Centric Network Architecture for Modular Data Centers,” in Proc. of the ACM SIGCOMM Conference on Data Communication 2009 (SIGCOMM ’09), Barcelona, Spain, August 17-21, 2009, pp. 63–74.
[23] “Data Center Architecture Overview” διαθέσιμο στο http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_1.html