ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ

ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

"ΧΡΗΣΗ ΑΝΟΙΧΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΓΙΑ ΔΙΑΧΕΙΡΙΣΗ, ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΕΛΕΓΧΟ ΙΔΙΩΤΙΚΟΥ ΔΙΚΤΥΟΥ"

Τηλέμαχος(Ι.) Γιαννάκης

ΑΜ:2795

Επιβλέπων Καθηγητής: Ιωάννης Τζήμας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

- Ονοματεπώνυμο, Υπογραφή
- Ονοματεπώνυμο, Υπογραφή
- Ονοματεπώνυμο, Υπογραφή

Υπεύθυνη Δήλωση Φοιτητή

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη εργασία. Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος. Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή Τηλέμαχου Γιαννάκη που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο Πανεπιστήμιο Πελοποννήσου, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Τζήμα Ιωάννη επειδή δέχτηκε να αναλάβει το θέμα που του πρότεινα και την βοήθεια που μου πρόσφερε όποτε την χρειάστηκα.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία ασχολείται, με τον έλεγχο, τη διαχείριση και την ασφάλεια ιδιωτικού δικτύου με χρήση λογισμικό ανοιχτού κώδικα. Περιγράφονται ζητήματα σχετικά τόσο με την διαχείριση, τον έλεγχο και την ασφάλεια του δικτύου, όσο και με τον σχεδιασμό, την δομή και την συνδεσιμότητα του. Παρέχονται ακόμα, σχετικά σχήματα για την καλύτερη κατανόηση των όσων αναφέρθηκαν.

Στο πρώτο κεφάλαιο, περιλαμβάνεται μια εισαγωγή, η οποία αναφέρεται στο ζήτημα της χρήσης λογισμικού ανοιχτού κώδικα για την διαχείριση, τον έλεγχο και την ασφάλεια του δικτύου. Ενώ, αναφερόμαστε στο σκοπό και τι περιμένουμε να επιτύχει η ιδέα της συγκεκριμένης πτυχιακή.

Το δεύτερο κεφάλαιο, ασχολείται με την συνδεσιμότητα και την κατεύθυνση που θα λάβει ο σχεδιασμός του δικτύου. Αναφερόμαστε σε «Ανοιχτή Αρχιτεκτονική» γιατί όπως το λογισμικό έτσι και ο εξοπλισμός πρέπει να προσαρμόζεται σε πολλές διαφορετικές τεχνολογίες και συσκευές ώστε να μπορεί να επεκτείνεται εύκολα. Επίσης, επεξηγούνται τα πρωτόκολλα συνδεσιμότητας που χρησιμοποιεί το δίκτυο μας και τέλος αναλύουμε σε βάθος την τεχνολογία των LAN, VLAN.

Στο τρίτο κεφάλαιο, εξετάζουμε γενικότερα τις συσκευές και το λογισμικό που χρησιμοποιούμε για την μέγιστη ασφάλεια του δικτύου. Ταυτόχρονα, με το πρωτόκολλο Kerberos παρέχουμε ασφάλεια εσωτερικά του δικτύου ελέγχοντας την είσοδο των χρηστών σε αυτό.

Στο τέταρτο κεφάλαιο, παρουσιάζεται πως γίνεται η διαχείριση και ο έλεγχος του δικτύου εφικτός, με λογισμικό ανοιχτού κώδικα. Ενώ, στη συνέχεια παρατηρούμε πως τρείς διακομιστές μετατρέπονται σε σύμπλεγμα διακομιστών και καταφέρνουμε να έχουμε την μέγιστη δυνατή διαθεσιμότητα.

Στο πέμπτο και τελευταίο κεφάλαιο, παρουσιάζουμε ένα υπαρκτό έργο που έχει υλοποιημένο δίκτυο «ανοιχτής αρχιτεκτονικής», κάνει χρήση λογισμικού ανοιχτού κώδικα και συνδυάζει όλο τον εξοπλισμό που αναφέραμε παραπάνω για την συνδεσιμότητα, την ασφάλεια , τον έλεγχο και τη διαχείριση του. Τέλος, παρατηρούμε ποια είναι τα συμπεράσματα της δημιουργίας αυτού του δικτύου.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Δρομολογητής

Διακομιστής

Πρωτόκολλο

Ασφάλεια

Εικονικό

Περιβάλλον

Διαθεσιμότητα

Δίκτυο

Συνδεσιμότητα

Τηλεπικοινωνία

ABSTRACT

This paper deals with the control, management and security of a private network using open-source software. Issues related to both network management, control and security, as well as its design, structure and connectivity are described. Related figures are also provided for a better understanding of what was mentioned.

The first chapter provides an introduction to the issue of using open-source software for network management, control and security. While, we are referring to the purpose and what we expect the idea of the specific degree to achieve.

The second chapter deals with the connectivity and direction the network design will take. We refer to "Open Architecture" because like our software, our hardware must adapt to many different technologies and devices so that it can be easily expanded. Also, the connectivity protocols used by our network are explained and finally we analyze in depth the technology of LANs, VLANs.

In the third chapter we examine in general the devices and software we use for maximum network security. At the same time, with the Kerberos protocol we provide security internally to the network by controlling user access to it.

In the fourth chapter it is presented how the management and control of the network is possible, with open-source software. While, then we notice how three servers turn into a server cluster and we manage to have the maximum availability.

In the fifth chapter we present an existing project that has implemented an "open architecture" network, whom uses open software, and combines all the equipment mentioned above for its connectivity, security, control, and management. Finally, we observe what are the conclusions of the creation of this network.

KEYWORDS

Lan

Vlan

Open-Source

Squid

ProxMox

Kerberos

Switch

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

OSS	Λογισμικό Ανοιχτού Κώδικα
VLAN	Εικονικό τοπικό δίκτυο
VTP	Πρωτόκολλο Κορμού Εικονικού τοπικού δικτύου
QOS	Ποιότητα Υπηρεσιών
VPN	Εικονικό Ιδιωτικό Δίκτυο
OSI	Διασύνδεση Ανοικτών Συστημάτων
TCP	Πρωτόκολλο Ελέγχου Μεταφοράς
UDP	Πρωτόκολλο Δεδομενογράμματος Χρήστη
LAN	Τοπικό Δίκτυο Υπολογιστών
DRBD	Συσκευή Κατανεμημένων Αναδιπλασιασμένων Μπλοκ
CARP	Πρωτόκολλο Πλεονασμού Κοινής Διεύθυνσης
IP	Πρωτόκολλο Δικτύου
ΔΔ	Δίκτυο Δεδομένων
ΠΣ	Πληροφοριακό Σύστημα
ΔΚΔ	Δίκτυο Κεντρικών Διακομιστών
ΟΠΣ	Ολοκληρωμένο Πληροφοριακό Σύστημα
ΟΔΔ	Οριζόντιο Δίκτυο Διανομής
ΕΔΔ	Εξωτερικό Δίκτυο Δεδομένων
LLC	Έλεγχος Λογικού Συνδέσμου
DNS	Σύστημα ονομάτων Τομέα
HTTPS	Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκειμένου
CBQ	Ουρά Βάση Κλάσεων
HBB	Ιεραρχική Κατανομή Εύρους Ζώνης
TFH	Στοχαστική Δίκαιη Ουρά
SMB	Μπλοκ Μηνυμάτων Διακομιστή
CIFS	Κοινό Σύστημα Αρχείων Διαδικτύου

AD	Ενεργό Αρχείο
GPO	Αντικειμένων Πολιτικής Ομάδας
NAT	Μετάφραση Διεύθυνσης Δικτύου
ΚΔΚ	Κέντρο Διανομής Kerberos
ΔΕΤ	Διακομιστή Ελέγχου Ταυτότητας
ΔΧΕ	Διακομιστή Χορήγησης Εισιτηρίων
CLI	Εργαλείο γραμμής εντολών
ΔΚΜ	Διακομιστής
ΜΤΓ	Μεταγωγέας
CPU	Επεξεργαστής
RAM	Μνήμη Τυχαίας Προσπέλασης
SAS	Συνημμένο Σειριακό (Μικρής διεπαφής συστήματος υπολογιστή)
SAN	Αποθηκευτική Περιοχή Δικτύου
NAS	Δικτυακός Αποθηκευτικός Χώρος
VM	Εικονική Μηχανή
NFS	Σύστημα Αρχείων Δικτύου
SSD	Συσκευή Αποθήκευσης Στερεάς-Κατάστασης
IEEE	Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών
ISL	Σύνδεσμος Μεταξύ-Μεταγωγέων
TCE	Επιτάχυνση Κατηγορίας Κυκλοφορίας
DMF	Δυναμικό Φιλτράρισμα Πολλαπλής-Εκπομπής
MAC	Έλεγχος Πρόσβασης Πολυμέσων
NVRAM	Μη Πτητική Μνήμη Τυχαίας Προσπέλασης
MIB	Βάσης Πληροφοριών Διαχείρισης
DES, 3DES, AES, SHA-1	Αλγόριθμοι Κρυπτογράφησης

1. ΕΙΣΑΓΩΓΗ

Το λογισμικό ανοιχτού κώδικα (OSS) προσφέρει πολλά τεχνικά οφέλη στους χρήστες, όπως αξιοπιστία, ασφάλεια, ποιότητα, απόδοση, ευελιξία χρήσης, μεγάλη βάση προγραμματιστών και ελεγκτών, συμβατότητα και βελτιωμένη εναρμόνιση.

Γενικά, η διαχείριση και ο έλεγχος ενός ιδιωτικού δικτύου με OSS περιλαμβάνει τη χρήση εργαλείων OSS για την παρακολούθηση και τη διαχείριση της απόδοσης, της ασφάλειας και της διαμόρφωσης του δικτύου. Αυτό εμπεριέχει τη χρήση εργαλείων όπως λογισμικό παρακολούθησης δικτύου, τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών και εργαλεία διαχείρισης διαμόρφωσης. Αξιοποιώντας τα πλεονεκτήματα του OSS, όπως η αξιοπιστία, η ασφάλεια και η ευελιξία, οι διαχειριστές δικτύου μπορούν να διαχειρίζονται και να ελέγχουν αποτελεσματικά το ιδιωτικό δίκτυο προκειμένου να εξασφαλίσουν υψηλή διαθεσιμότητα, αξιοπιστία και ασφάλεια. Επιπλέον, η μεγάλη βάση προγραμματιστών και ελεγκτών του OSS μπορεί να παρέχει πολύτιμη υποστήριξη και πόρους για την αντιμετώπιση προβλημάτων και τη βελτιστοποίηση της απόδοσης του δικτύου. Συνολικά, η χρήση OSS για διαχείριση και έλεγχο δικτύου μπορεί να προσφέρει μια οικονομικά αποδοτική και αξιόπιστη λύση για ιδιωτική υποδομή δικτύου.

Όσον αφορά την ασφάλεια, το OSS παρέχει υψηλή ασφάλεια λόγω της διαθεσιμότητας του πηγαίου κώδικα, ο οποίος επιτρέπει μεγαλύτερη διαφάνεια και λογοδοσία. Επίσης, η μειωμένη απειλή από ιούς και η επιπλέον ευαισθητοποίηση σχετικά με την ασφάλεια στη φάση του σχεδιασμού των προϊόντων καθιστούν το OSS μια πιο ασφαλή επιλογή.

Χρησιμοποιώντας το δικτύου ανοιχτής αρχιτεκτονικής και το OSS μαζί, οι οργανισμοί μπορούν να επιτύχουν μεγαλύτερη ευελιξία και προσαρμοστικότητα στην υποδομή δικτύου τους, επιτρέποντάς τους να ανταποκρίνονται γρήγορα στις μεταβαλλόμενες ανάγκες και τις τεχνολογικές εξελίξεις. Επιπλέον, η διαφάνεια και η συνεργατική φύση του OSS μπορεί να προσφέρει μεγαλύτερη ασφάλεια και αξιοπιστία επιτρέποντας τη συνεχή παρακολούθηση, τη δοκιμή και τη βελτίωση του λογισμικού και των εργαλείων δικτύου.

Συνολικά, ο στόχος της ιδέας αυτής της πτυχιακής, είναι η παροχή μιας αξιόπιστης, ασφαλούς και οικονομικά αποδοτικής λύσης για τη διαχείριση των πόρων του δικτύου, τη μείωση του χρόνου διακοπής λειτουργίας και τη διασφάλιση ότι το δίκτυο είναι διαθέσιμο και λειτουργεί βέλτιστα.

2. ΣΧΕΔΙΑΜΟΣ ΚΑΙ ΣΥΝΔΕΣΙΜΟΤΗΤΑ ΔΙΚΤΥΟΥ

Για να φτάσουμε να μιλήσουμε για λογισμικό ανοιχτού κώδικα, είναι σημαντικό πρώτα, να αναλύσουμε πως πρέπει να είναι δομημένα κάποια πολύ κύρια μέρη μέσα στο δίκτυο.

Αυτά είναι:

- η αρχιτεκτονική σχεδιαστική κατεύθυνση του
- η συνδεσιμότητα του
- η τηλεπικοινωνία του
- ο εξοπλισμός

Το Δίκτυο μας είναι «Ανοικτής Αρχιτεκτονικής» και εύκολα μπορεί να προσαρμοστεί σε καινούργια δεδομένα που αφορούν την επέκταση του (αριθμός χρηστών, διασυνδέσεις με άλλα σημεία, επί πλέον εφαρμογές κλπ).

Ο υπάρχων εξοπλισμός του πρέπει, να συμβαδίζει πλήρως με τις προδιαγραφές που έχουν τεθεί, όπως επίσης και αυτός που προβλέπεται να απαιτηθεί θα είναι πλήρως συμβατός με τον ήδη εγκατεστημένο εξοπλισμό ώστε να αποτελούν ένα ενιαίο σύστημα και να εξασφαλίζουν την ασφαλέστερη, αξιόπιστη και όσο γίνεται τη βέλτιστη συμπεριφορά και απόδοσή του.

Οι ανάγκες αυτές προκύπτουν τόσο στα πλαίσια των εφαρμογών που θα χρησιμοποιηθούν όσο και στα πλαίσια του γενικότερου εκσυγχρονισμού των εγκαταστάσεων και των παρεχόμενων επικοινωνιακών υπηρεσιών του κτηρίου μας.

Ένα σύγχρονο Δίκτυο θα πρέπει να βασίζεται σε βασικές αρχές που μεγιστοποιούν τη χρησιμότητα του και αξιολογούν στο μέγιστο τα ενδεχόμενα στην εγκατάσταση του, κοστολόγια.

Τέτοιες βασικές αρχές είναι:

- Ενοποίηση τηλεπικοινωνιακών υπηρεσιών.
- Αξιοποίηση σύγχρονης τεχνολογίας.
- Προοπτική εξέλιξης.
- Συμφωνία με διεθνή πρότυπα και προδιαγραφές και βιομηχανικά πρότυπα.
- Ευελιξία στη διαχείριση.
- Επεκτασιμότητα.

Βασικό κομμάτι του εξοπλισμού μας είναι οι μεταγωγείς και πόσο μάλλον οι εικονικοί διαχωρισμοί μεταξύ του κάθε ένα για τη δημιουργία VLAN.

Ας εξετάσουμε το ακόλουθο παράδειγμα για την καλύτερη κατανόηση περί συνδεσιμότητας με VLAN: Είμαστε μέλος ενός γυμναστηρίου και έχουμε φτάσει στην κατάσταση "πλατινένιου". Ως αποτέλεσμα, έχουμε πρόσβαση σε όλες τις τοποθεσίες του γυμναστηρίου σε όλο τον κόσμο. Αλλά ας υποθέσουμε ότι πηγαίνουμε σε άλλη πόλη για δουλειά και η εταιρεία στην οποία εργαζόμαστε μας κάνει κράτηση σε ένα ξενοδοχείο που έχει γυμναστήριο στο κτήριο του. Όταν προσπαθούμε να αποκτήσουμε πρόσβαση στο γυμναστήριο, μας διώχνουν επειδή δεν έχουμε τις σωστές πληροφορίες μέλους. Αυτό μπορεί να συγκριθεί με τη συνδρομή μας στο γυμναστήριο που ανήκει σε ένα VLAN και το γυμναστήριο του ξενοδοχείου που ανήκει σε διαφορετικό VLAN. Χωρίς την κατάλληλη ετικέτα VLAN, το προσωπικό στη ρεσεψιόν (μεταγωγέας) δεν μπορεί να επαληθεύσει τη συνδρομή μας και να μας επιτρέψει την πρόσβαση. Έτσι λειτουργούν τα VLAN σε έναν μεταγωγέα. Οι μεταγωγείς διαιρούν τους τομείς σύγκρουσης και οι δρομολογητές διαιρούν τους τομείς εκπομπής. Χρησιμοποιώντας ένα VLAN, ένας μεταγωγέας μπορεί να αναλύσει τους τομείς μετάδοσης σε μικρότερους τομείς υπο-εκπομπής. Από προεπιλογή, το πακέτο εκπομπής ενός μεταγωγέα μεταδίδεται από κάθε διεπαφή και σε όλες τις συσκευές του δικτύου. Χρησιμοποιώντας VLAN, οι διαχειριστές δικτύου μπορούν να περιορίσουν ορισμένες θύρες και συσκευές από τη λήψη περιττών καρέ.

Οφέλη VLAN:

- Οι διαχειριστές δικτύου θα διαχωρίσουν την κυκλοφορία δικτύου με βάση την τοποθεσία ή το ρόλο του χρήστη.
- Οι χρήστες εντός του ίδιου VLAN μπορούν να επικοινωνούν μεταξύ τους, αλλά όχι με χρήστες άλλων VLAN.
- Τα VLAN βελτιώνουν την ασφάλεια του δικτύου περιορίζοντας την περιττή κίνηση δικτύου. (Carthern Chris, 2015)

2.1 ΣΧΕΔΙΑΣΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ

Στα σύγχρονα δίκτυα, είναι κοινή πρακτική να ενοποιείται η υποδομή για την παροχή υπηρεσιών, ανεξάρτητα από την ακριβή φύση και μορφή των υπηρεσιών αυτών. Γενικότερα, υπηρεσία μπορεί να θεωρηθεί οποιαδήποτε υπηρεσία μετάγει πληροφορία μεταξύ απομακρυσμένων σημείων.

Στις υπηρεσίες αυτές συγκαταλέγονται:

- η συμβατική φωνητική τηλεφωνία,
- η ψηφιακή τηλεφωνία με προηγμένες υπηρεσίες,
- η τηλεφωνία ολοκληρωμένων υπηρεσιών (ISDN),
- η μετάδοση εικόνας,
- η βιντεοφωνία,
- η μεταγωγή δεδομένων,
- IP τηλεφωνία.

Η υποδομή για την παροχή τέτοιων υπηρεσιών εκτείνεται σε μια μεγάλη περιοχή, που καλύπτει από φυσικά μέσα μετάδοσης, έως τις τερματικές συσκευές του χρήστη.

Η σύγχρονη τάση για το σχεδιασμό δικτύων τείνει να ενοποιεί, όσο το δυνατόν περισσότερο, την υποδομή αυτή στο επίπεδο του φυσικού μέσου διάδοσης, χρησιμοποιείται κοινή τεχνολογία καλωδίωσης και επικοινωνιών για τη μετάδοση πληροφορίας όλων των τύπων των υπηρεσιών.

Οι συσκευές που υλοποιούν τις επικοινωνιακές και δικτυακές υπηρεσίες, τείνουν όλο και περισσότερο να βρίσκονται στο χώρο και την εποπτεία του χρήστη. Με τον τρόπο αυτό, χωρίς τη μεσολάβηση κάποιου φορέα, ο χρήστης μπορεί όλο και περισσότερο να επιδρά στη φύση, το είδος, τη ποιότητα και τις λειτουργικές επιλογές των παρεχόμενων σε αυτόν υπηρεσιών.

Η σημερινή εξέλιξη στο χώρο των τηλεπικοινωνιών και τηλεπικοινωνιακών υπηρεσιών είναι από τις ταχύτερες στο χώρο της επιστήμης και της τεχνολογίας. Για το λόγο αυτό, η υποδομή και οι υπηρεσίες του είδους αυτού καθίστανται ξεπερασμένες, στη πάροδο του χρόνου με πολύ πιο γρήγορο ρυθμό από άλλες. Έτσι ο σχεδιασμός και η υλοποίηση τους με τρόπο που να επιτρέπει την εύκολη εξέλιξη τους, την ενσωμάτωση καινούριων τεχνολογιών και τη βελτίωση των υφιστάμενων, είναι από τους παράγοντες που πρέπει να προσεχθούν ιδιαίτερα στο χώρο των τηλεπικοινωνιών.

Ο τομέας των τηλεπικοινωνιακών και δικτυακών υπηρεσιών κυβερνάται σε τεράστιο βαθμό από την προσήλωση των προϊόντων διαφορετικών κατασκευαστών σε κοινές μεθοδολογίες, πρότυπα, προδιαγραφές και βιομηχανικά πρότυπα.

Ο παράγοντας αυτός επιτρέπει στο χρήστη να ενσωματώνει στην υποδομή του, συσκευές και υπηρεσίες από διαφορετικούς φορείς και κατασκευαστές, εκμεταλλευόμενος με το βέλτιστο τρόπο την παρεχόμενη τεχνολογία .

Καθώς η φύση της απαραίτητης υποδομής για την παροχή υπηρεσιών γίνεται όλο και πιο πολύπλοκη, νέοι τρόποι είναι απαραίτητοι για τη καθημερινή επίβλεψη της καλής λειτουργίας και τη διαχείριση των υπηρεσιών αυτών.

Στα σύγχρονα δίκτυα, ο παράγοντας διαχείρισης είναι από τους σημαντικότερους για τη σωστή και αδιάλειπτη παροχή των επιθυμητών υπηρεσιών, τη ταχύτητα στην εγκατάσταση αλλαγών στο σύστημα και την ικανοποίηση των αναγκών του χρήστη.

Η πράξη δείχνει ότι ο τομέας των δικτύων είναι από τους πιο ραγδαία επεκτεινόμενους διεθνώς. Επειδή τα κοστολόγια για την αρχική εγκατάσταση της απαραίτητης για την παροχή υπηρεσιών υποδομής δεν είναι καθόλου αμελητέα, η αρχική υποδομή θα πρέπει να εγκαθίσταται με τη σχετική πρόβλεψη η οποία θα πρέπει να περιέχει τα απαραίτητα πλεονάσματα σε θέσεις-κλειδιά του σχεδιασμού, ώστε να μην απαιτούνται επανεγκαταστάσεις σε μαζική κλίμακα για την κάλυψη των αυξημένων μελλοντικά αναγκών.

2.1.2 ΔΟΜΗ ΔΙΚΤΥΟΥ

Το προδιαγραφόμενο Δίκτυο Δεδομένων πρέπει, στη βάση όλων των σχεδιαστικών αναγκών να παρέχει τελική επικοινωνία των χρηστών όλων των Υπηρεσιών που στεγάζονται σε ένα κτήριο :

- Διεπικοινωνία
- Με τις εφαρμογές του Ολοκληρωμένου Πληροφοριακού Συστήματος
- Με Υπουργεία (για υπηρεσίες)
- Με το διαδίκτυο

Στα πλαίσια αυτά, καλείται να καλύψει τις εξής βασικές περιοχές αναγκών:

- Γρήγορη και αξιόπιστη επικοινωνία μεταξύ των κύριων διακομιστών του Πληροφοριακού Συστήματος (ΠΣ). Το μέρος αυτό του Δικτύου Δεδομένων (ΔΔ) ονομάζεται, για τους σκοπούς της προδιαγραφής **Δίκτυο Κεντρικών Διακομιστών.**

- Κάλυψη με φυσικό μέσο (οπτικές ίνες και καλώδια χαλκού) των χώρων του κτηρίου, μαζί με τη λογική και λειτουργική διάρθρωση των ενεργών συσκευών που απαιτούνται για τη λειτουργία του Δικτύου. Το μέρος αυτό ονομάζεται **Δίκτυο Διανομής.**
- Δυνατότητα διασύνδεσης του Δ.Δ. με άλλα εξωτερικά δίκτυα. Το μέρος αυτό του δικτύου ονομάζεται **Εξωτερικό Δίκτυο**.
- Διαχείριση του Δ.Δ. και λειτουργικές απαιτήσεις για τη σύνδεση στο Δίκτυο και τη διαχείριση των τερματικών σταθμών εργασίας και των άλλων συσκευών. Το μέρος αυτό αποκαλείται **Διαχείριση Δικτύου.**

2.1.3 ΔΙΚΤΥΟΥ ΔΙΑΝΟΜΗΣ

Η σημαντικότερη συνιστώσα στην επιτυχή λειτουργία του Δ.Δ είναι το μέρος που είναι υπεύθυνο για τη σωστή μετάδοση της πληροφορίας μεταξύ των ενεργών στοιχείων και από αυτά προς τον τελικό χρήστη.

Η ραχοκοκαλιά αυτή του Δικτύου πρέπει να είναι σχεδιασμένη και υλοποιημένη ώστε να καλύπτει απόλυτα τις σχεδιαστικές κατευθύνσεις που διατυπώθηκαν προηγουμένως.

Όπως ήδη αναφερθήκαμε, το μέρος αυτό του Δικτύου απαιτεί κάποιες διαδικασίες, ενδεχόμενα δαπανηρές και χρονοβόρες, για την εγκατάσταση του. Για το λόγο αυτό, θα πρέπει να πληροί τις απαιτήσεις λειτουργικότητας, επεκτασιμότητας και διαχειρισιμότητας που περιγράφηκαν προηγουμένως, καθώς και τις ενδεχόμενες μελλοντικές απαιτήσεις των χρηστών.

Σε ό,τι αφορά αυτές, οι προδιαγραφές του Δικτύου Διανομής καλύπτουν τους εξής στόχους :

- Μέγιστη ταχύτητα πρόσβασης του τελικού χρήστη μέχρι 1000 Mbps
- Ικανοποιητικός αριθμός απολήξεων Δικτύου με μετάδοση με χαλκό.
- Δυνατότητα ενσωμάτωσης δικτύων τηλεφωνίας και δεδομένων.

Σε ότι αφορά τη δομή του Δικτύου Διανομής, οι αντίστοιχοι στόχοι είναι:

- Υψηλές ταχύτητες (100 Mbps ή 1000 Mbps) σε κάθε χρήστη.
- Μεγιστοποίηση της επεκτασιμότητας με ελάχιστο αρχικό κόστος.
- Μεγιστοποίηση της αξιοπιστίας με τη χρησιμοποίηση ελάχιστου πλεονασμού.
- Μεγιστοποίηση των δυνατοτήτων διαχείρισης συνδέσεων και παροχών με ελαχιστοποίηση της απαιτούμενης προσπάθειας.
- Δυνατότητα χρήσης νέων τεχνολογιών και ενσωμάτωσης τους στο Δίκτυο Δεδομένων.

2.1.3.1 ΔΟΜΗ ΔΙΚΤΥΟΥ ΔΙΑΝΟΜΗΣ

Το Δίκτυο διανομής χωρίζεται δομικά στα εξής μέρη :

1. Οριζόντιο Δίκτυο Διανομής Χαλκού,
2. Κατακόρυφο Δίκτυο Διανομής Οπτικών Ινών,
3. Κατακόρυφο Δίκτυο Διανομής Χαλκού,
4. Ενεργά στοιχεία και μικτονομίσεις.

2.1.3.2 ΟΡΙΖΟΝΤΙΟ ΔΙΚΤΥΟ ΔΙΑΝΟΜΗΣ

Το Οριζόντιο Δίκτυο Διανομής (Ο.Δ.Δ) καλύπτει την ανάγκη παροχής δικτυακών υπηρεσιών από το τελευταίο ενεργό στοιχείο του Δικτύου Διανομής στον τελικό χρήστη.

Το Ο.Δ.Δ βασίζεται σε αναμετάδοση με καλώδια χαλκού τεσσάρων ζευγών που έχουν δυνατότητα παροχής δικτυακών συνδέσεων σε ταχύτητες μέχρι 1000 Mbps.

Καθώς το μέρος αυτό είναι από τα δαπανηρότερα του Δικτύου, η τεχνολογία που προδιαγράφεται είναι τέτοια ώστε να καλύπτει τόσο τις παρούσες, όσο και τις μελλοντικές ανάγκες των χρηστών, χωρίς να χρειάζεται αλλαγή της καλωδιακής υποδομής .

2.1.3.3 ΚΑΤΑΚΟΡΥΦΟ ΔΙΚΤΥΟ ΔΙΑΝΟΜΗΣ ΟΠΤΙΚΩΝ ΙΝΩΝ

Το Κατακόρυφο Δίκτυο Διανομής Οπτικών Ινών έχει ως σκοπό την παροχή αξιόπιστων συνδέσεων υψηλών ταχυτήτων στα ενεργά στοιχεία κάθε κτιρίου.

Το Δίκτυο αυτό παρέχει οπτικές συνδέσεις στους τηλεπικοινωνιακούς κατανεμητές του κτιρίου. Για τη στοιχειώδη λειτουργία του Δικτύου Δεδομένων όπως αυτό προδιαγράφεται, αρκεί σε κάθε τηλεπικοινωνιακό κατανεμητή να καταλήγει τουλάχιστον ένα ζεύγος πολυτροπικών οπτικών ινών.

Ωστόσο, τόσο για λόγους επεκτασιμότητας, όσο και για λόγους ασφαλείας και αξιοπιστίας, προτείνεται να υπάρχει αρκετός πλεονασμός. Καθώς οι διαδρομές δεν είναι εξαιρετικά μεγάλες, ο πλεονασμός αυτός δεν αναμένεται να επιβαρύνει ουσιαστικά το κόστος της εγκατάστασης .

Η αφετηρία όλων των καλωδίων οπτικών ινών θα πρέπει να είναι στο χώρο που θα στεγάζει τον Δρομολογητή / Μεταγωγό του κεντρικού Δικτύου, ενώ καθένα από τα καλώδια αυτά θα πρέπει να καταλήγει στον αντίστοιχο τηλεπικοινωνιακό κατανεμητή ορόφου και θα διασυνδέει τον αντίστοιχο Μεταγωγό ορόφου.

Για τα προδιαγραφόμενα πρωτόκολλα φυσικών μέσων, το μήκος κάθε καλωδίου ινών δεν θα ξεπερνά τα 275 μέτρα για την υποστήριξη του GigaBit Ethernet.

2.1.3.4 ΕΝΕΡΓΑ ΣΤΟΙΧΕΙΑ ΚΑΙ ΜΙΚΤΟΝΟΜΙΣΕΙΣ

Σε καίρια σημεία του κτιρίου προδιαγράφεται η εγκατάσταση τηλεπικοινωνιακών κατανεμητών όπου θα στεγάζονται οι Μεταγωγοί Ethernet 10/100/1000 Mbps για την υλοποίηση του δικτύου διανομής.

Ο αριθμός και οι θέσεις των τηλεπικοινωνιακών κατανεμητών είναι τέτοιοι ώστε να τηρείται το όριο απόστασης των 90 μέτρων μεταξύ κάθε τερματικής απόληξης και του αντίστοιχου τηλεπικοινωνιακού κατανεμητή.

2.1.3.5 ΔΙΚΤΥΟ ΚΕΝΤΡΙΚΩΝ ΔΙΑΚΟΜΙΣΤΩΝ

Το Δίκτυο Κεντρικών Διακομιστών (ΔΚΔ) είναι αυτό που θα διασυνδέει τους προδιαγραφόμενους διακομιστές του Ολοκληρωμένου Πληροφοριακού Συστήματος (ΟΠΣ).

Στο δίκτυο αυτό συνδέονται οι κύριοι διακομιστές του Πληροφοριακού Συστήματος, καθώς και ο δρομολογητής (ή οι δρομολογητές) που θα παρέχουν δικτυακές υπηρεσίες στο υπόλοιπο Δίκτυο.

Οι λειτουργίες που καλείται να υλοποιήσει το ΔΚΔ είναι, συνεπώς, δύο ειδών:

- Λειτουργία που αφορά τη διασύνδεση και την καλή λειτουργία των διακομιστών
- Λειτουργία που αφορά την πρόσβαση των υπολοίπων χρηστών του Δικτύου Δεδομένων στους διακομιστές.

Η καλή λειτουργία των διακομιστών βασίζεται στους υψηλούς ρυθμούς μετάδοσης και την αυξανόμενη αξιοπιστία, του συνολικού συστήματος.

Για τη μεταγωγή των απαραίτητων δεδομένων σε ικανοποιητικούς χρόνους, το ΔΚΔ θα βασίζεται σε σύγχρονες τεχνολογίες με ρυθμό μετάδοσης δεδομένων 100Mbps ή 200Mbps (Full Duplex) ή 1000 Mbps.

Για την επίτευξη υψηλής αξιοπιστίας, το ΔΚΔ θα πρέπει να πληροί τα εξής χαρακτηριστικά:

- Δεν θα πρέπει να περιλαμβάνει ενεργά στοιχεία πλην των άμεσα συνδεδεμένων σε αυτό συσκευών (πχ. Μετατροπείς, πομποδέκτες), για την αποφυγή συνολικής δυσλειτουργίας λόγω βλάβης μεμονωμένης συσκευής.

- Το πρωτόκολλο διαχείρισης του φυσικού μέσου που θα χρησιμοποιηθεί θα πρέπει να παρέχει ικανοποιητικό χρόνο απομόνωσης από το Δίκτυο κάθε μεμονωμένης συσκευής που θα τίθεται εκτός λειτουργίας και αναδιοργάνωσης του λογικού Δικτύου ώστε να περιλαμβάνει όλες τις υπόλοιπες συσκευές. Για τη λειτουργία αυτή δε θα πρέπει να απαιτεί ανθρώπινη παρέμβαση ή εξωτερική διαχειριστική λειτουργία.
- Θα πρέπει να παρέχεται η δυνατότητα ανεμπόδιστης λειτουργίας του Δικτύου, ακόμα και σε περίπτωση διακοπής λειτουργίας περισσοτέρων της μιας συσκευής. Η συνέχιση της λειτουργίας του ΔΚΔ στην περίπτωση αυτή μπορεί να γίνεται και σε μικρότερους ρυθμούς από τους αρχικούς, πιθανά με τη χρήση δευτερευουσών συνδέσεων. Θα πρέπει ακόμα και σε τέτοιες περιπτώσεις, το ΔΚΔ να μπορεί να επαναλειτουργήσει άμεσα (χωρίς να αποκλείεται ανθρώπινη παρέμβαση ή άλλη διαχειριστική λειτουργία).
- Θα πρέπει να προσκομιστούν πιστοποιητικά διαλειτουργικότητας (interoperability certificates) μεταξύ όλων των συσκευών που θα συνδεθούν στο Δίκτυο αυτό (μεταγωγοί και δρομολογητές / μεταγωγοί, σύστημα Διαχείρισης Δικτύου) εφόσον δεν προέρχονται από τον ίδιο κατασκευαστή.

2.1.3.6 ΕΞΩΤΕΡΙΚΟ ΔΙΚΤΥΟ ΔΕΔΟΜΕΝΩΝ

Το Εξωτερικό Δίκτυο Δεδομένων (Ε.Δ.Δ.) έχει κύριο σκοπό να ολοκληρώσει το Δίκτυο μας με εξωτερικούς φορείς και παροχής υπηρεσιών διασυνδεσιμότητας δεδομένων.

Το Ε.Δ.Δ θα υλοποιείται μέσω των ενεργών συσκευών (Δρομολογητών) που θα πρέπει να είναι μέρος του συστήματος του Κεντρικού Δρομολογητή Μεταγωγού με την προσθήκη στοιχείων Wide Area Network. Με τον τρόπο αυτό επιτυγχάνεται η άμεση μεταγωγή των δεδομένων του ΔΔ στο εξωτερικό δίκτυο.

Θα πρέπει λοιπόν ο Δρομολογητής / Μεταγωγός να υποστηρίζει πρωτόκολλα μεταγωγής πάνω από σειριακές γραμμές μετάδοσης δεδομένων, σε ταχύτητες μέχρι και 2 Mbps. Ο δρομολογητής που θα υλοποιεί τις λειτουργίες αυτές θα παρέχει και την αντίστοιχη εικόνα του ενιαίου λογικού Δικτύου στις υπόλοιπες συσκευές. (Anon., χ.χ.)

2.2 ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΞΟΠΛΙΣΜΟΥ

Το Δίκτυο Κεντρικών Διακομιστών, το Δίκτυο Διανομής και οι εξωτερικές δικτυακές συνδέσεις ολοκληρώνονται σε ένα ενιαίο Δίκτυο με τη σύνδεση στον Κεντρικό Δρομολογητή / Μεταγωγό.

Ο αριθμός των δρομολογητών δεν συμπεριλαμβάνεται στις προδιαγραφές, αλλά θα πρέπει με το βέλτιστο συνδυασμό απόδοσης και διαθεσιμότητας προς κόστος να πληρούνται οι προδιαγραφές αυτού του κεφαλαίου.

2.2.1 Δρομολογητές / Μεταγωγοί

Οι δρομολογητές / Μεταγωγοί θα πρέπει να διακρίνονται γενικά από τα εξής χαρακτηριστικά:

- Υψηλή απόδοση, επαρκή μνήμη και δυνατότητα απρόσκοπτης λειτουργίας.
- Μεγάλη ποικιλία στα επιδεχόμενα προσαρμοστικών Δικτύου και δυνατότητα προσάρτησης ικανού αριθμού τέτοιων προσαρμοστικών.
- Υποστήριξη πολλών προσαρμοστικών και πρωτοκόλλων σειριακών γραμμών.
- Αποδεδειγμένα καλή συνεργασία με τον υπόλοιπο δικτυακό εξοπλισμό που προδιαγράφεται, διακίνηση πολλαπλών πρωτοκόλλων (επιπέδου 2, 3 και 4 στην ιεραρχία OSI) και προσήλωση στα διεθνή δικτυακά πρότυπα και προδιαγραφές.
- Υποστήριξη σύγχρονων πρωτοκόλλων διαχείρισης δικτύων.
- Αναβαθμίσιμο λειτουργικό σύστημα.
- Δυνατότητα υποστήριξης λειτουργιών ασφαλείας.

Το σύστημα πρέπει να είναι συμβατό με τις ακόλουθες προδιαγραφές ασφαλείας και ηλεκτρομαγνητικής συμβατότητας.

- Ασφάλεια : UL 1950 , CSA A22.2 No950, EN60950, IEC950 και 72/73/EEC.
- Ηλεκτρομαγνητική Συμβατότητα (EMC): FCC part 15. CSA C108.8, EN555022, VVCI V-3/93.01, EN50082-1 και 89/336/EEC.

2.2.2 Μεταγωγείς Ethernet Οριζοντίου Δικτύου Διανομής

Η λειτουργία των Μεταγωγέων Ethernet έγκειται στην υλοποίηση του οριζόντιου δικτύου διανομής και την διασύνδεση με το δίκτυο κορμού που υλοποιείται στους Δρομολογητές / Μεταγωγούς .

Το δίκτυο διανομής πρέπει να είναι υψηλής τεχνολογίας βασισμένο στην τοπολογία Ethernet 10/100/1000 Base TX και να εγγυάται μετάδοση δεδομένων στον κάθε χρήστη του δικτύου 1000 Mbps με τη βοήθεια του κατάλληλου εξοπλισμού.

Για την επικοινωνία τους με το κατακόρυφο υποδίκτυο θα πρέπει:

- Να υπάρχει η δυνατότητα σύνδεσης με τον Κεντρικό Μεταγωγό με πολλαπλές θύρες 1000 Mbps που να λειτουργούν σαν μία λογική σύνδεση υψηλού εύρους τουλάχιστον 1000 Mbps
- Να έχουν τη δυνατότητα σχηματισμού νοητών υποδικτύων μεταξύ των θυρών, καθώς και τη δυνατότητα απομόνωσης συγκεκριμένης θύρας ή ομάδας θυρών από το υπόλοιπο υποδίκτυο σε περίπτωση δυσλειτουργίας
- Οι Μεταγωγείς να υποστηρίζουν τουλάχιστον μία στοιχειώδη υλοποίηση του πρωτοκόλλου IP που να επιτρέπει την απομακρυσμένη ρύθμιση των λειτουργικών τους λεπτομερειών (πχ. Ενεργοποίηση θυρών κτλ.) μέσω του πρωτοκόλλου TELNET.
- Να υποστηρίζονται τα πρωτόκολλα SNMP.
- Να παρέχεται η βάση διαχείρισης τους και να είναι ενσωματώσιμη λογισμικό διαχείρισης .
- Οι Μεταγωγείς να μπορούν να ρυθμιστούν έτσι ώστε να ειδοποιούν, με τη χρήση της λειτουργίας, τον σταθμό διαχείρισης σε περιπτώσεις συγκεκριμένων δυσλειτουργιών.

Θα χρειαστούμε ένα σύστημα Workgroup Switch που να ανταποκρίνεται τουλάχιστον στις ακόλουθες προδιαγραφές :

- Πρέπει να μπορεί να δεχθεί μέχρι 24 θύρες 10/100/1000 Base TX .
- Πρέπει να προβλέπεται τουλάχιστον 4 θύρες SFP-based Gigabit Ethernet.
- Πρέπει να έχει στοιχείο μεταγωγής fabric με χωρητικότητα 4.2 Gbps , ώστε να μην είναι στοιχείο συμφόρησης του δικτύου.
- Πρέπει να παρέχει πλήρη υποστήριξη διαχείρισης των θυρών και των παραμέτρων τους μέσω θύρας για κονσόλα και μέσω WEB Browser – από οποιοδήποτε σταθμό standard SNMP ΔΙΑΧΕΊΡΙΣΗΣ .

- Πρέπει να είναι συμβατό με το πρότυπο VLAN 802.1q.
- Πρέπει να έχει δυνατότητα Full-Duplex επικοινωνίας και αυτοδιαπραγμάτευσης για τις πόρτες 10/100 Base TX) πάνω σ' όλες τις πόρτες .
- Πρέπει να έχει έναν πίνακα τουλάχιστον 12.228 διευθύνσεων MAC έτσι ώστε να επιτρέπει την εισαγωγή ακόμη και σε δίκτυα μεγάλων διαστάσεων.

2.2.3 ΜΕΤΑΤΡΟΠΕΑΣ ΗΛΕΚΤΡΙΚΟΥ ΣΗΜΑΤΟΣ ΣΕ ΟΠΤΙΚΟ ΣΗΜΑ

Εναλλακτική λύση για την αύξηση της ταχύτητας του Δικτύου μας αποτελεί η Οπτική Ίνα (Κατακόρυφη Καλωδίωση) μέσω της οποίας θα γίνει η διασύνδεση των Μεταγωγέων του Οριζοντίου Δικτύου Διανομής και των Μεταγωγέων του Κατακόρυφου Δικτύου Διανομής.

Για να επιτευχθεί όμως η φυσική μηχανική σύνδεση των ενεργών συσκευών απαιτούνται διατάξεις, οι οποίες θα μετατρέψουν το ηλεκτρικό σήμα Ethernet σε Οπτικό και αντίστροφα, προσαρμοσμένοι στις απαιτήσεις του πρωτοκόλλου IEEE 802.3ab, IEEE 802.3z 1000BaseSX/LX standards, με auto MDI/MDI-X Rj45 και Οπτική πόρτα SC σε 1000 base-SX.

Σε κάθε Τηλεπικοινωνιακό Κατανεμητή θα εγκατασταθούν τόσοι Μετατροπείς όσοι και οι Μεταγωγείς που φιλοξενούνται σ' αυτό και διασυνδέονται με τους Μεταγωγείς του Κατακόρυφου Δικτύου Διανομής.

Αντίστοιχα, στον Κεντρικό Τηλεπικοινωνιακό Κατανεμητή θα τοποθετηθούν τόσοι Μετατροπείς όσο είναι το συνολικό άθροισμα των επί μέρους Μετατροπέων και θα βυσματωθούν σε ειδικό πλαίσιο, στερεωμένο σε μεταλλική βάση επί του ικριώματος όπου θα εγκατασταθεί ο Ενεργός Εξοπλισμός. (Anon., χ.χ.)

2.3 ΣΥΝΔΕΣΙΜΟΤΗΤΑ ΔΙΚΤΥΟΥ

Αρχικά μιλώντας για συνδεσιμότητα σε ένα δίκτυο θα πρέπει να ξέρουμε τι εννοούμε όταν μιλάμε για επίπεδα (layers). Τα επτά επίπεδα που χρησιμοποιούν τα συστήματα υπολογιστών για την επικοινωνία μέσω ενός δικτύου περιγράφονται από το μοντέλο Διασύνδεσης Ανοικτών Συστημάτων (OSI). Στις αρχές της δεκαετίας του 1980, όλες οι σημαντικές εταιρείες υπολογιστών και τηλεπικοινωνιών το υιοθέτησαν ως το πρώτο βιομηχανικό πρότυπο για δικτυακές επικοινωνίες:

7	**Επίπεδο εφαρμογής**	Επίπεδο αλληλεπίδρασης ανθρώπου-υπολογιστή, όπου οι εφαρμογές μπορούν να έχουν πρόσβαση στις υπηρεσίες δικτύου
6	**Επίπεδο παρουσίασης**	Διασφαλίζει ότι τα δεδομένα είναι σε χρησιμοποιήσιμη μορφή και είναι το σημείο όπου πραγματοποιείται κρυπτογράφηση των δεδομένων
5	**Επίπεδο συνόδου**	Διατηρεί τις συνδέσεις και είναι υπεύθυνο για τον έλεγχο των θυρών και των συνεδριών
4	**Επίπεδο μεταφοράς**	Μεταδίδει δεδομένα χρησιμοποιώντας πρωτόκολλα μετάδοσης συμπεριλαμβανομένων των TCP και UDP
3	**Επίπεδο δικτύου**	Αποφασίζει ποια φυσική διαδρομή θα ακολουθήσουν τα δεδομένα
2	**Επίπεδο ζεύξης δεδομένων**	Καθορίζει τη μορφή των δεδομένων στο δίκτυο
1	**Φυσικό επίπεδο**	Μεταδίδει ακατέργαστο ρεύμα bit πάνω από το φυσικό μέσο

Πίνακας 1. Το μοντέλο Διασύνδεσης Ανοικτών Συστημάτων (OSI) 7 επιπέδων

(Kumar, 2014)

2.3.1 VLAN ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΣΥΝΔΕΣΙΜΟΤΗΤΑΣ

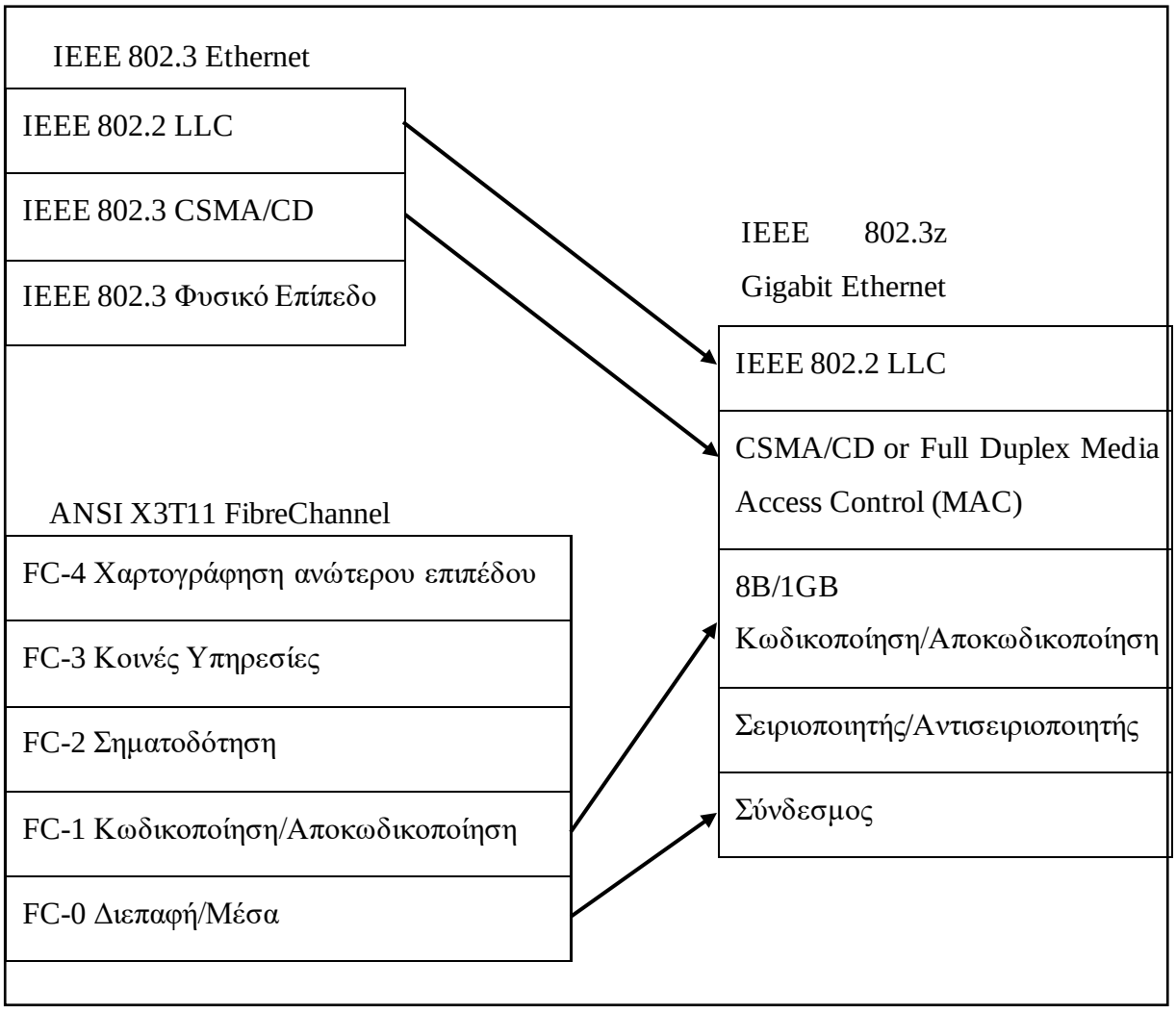
Το δίκτυο μας δεν θα μπορούσε να λειτουργεί χωρίς πρωτόκολλα Αφού αναλύσουμε το κάθε ένα από τα πρωτόκολλά μας ξεχωριστά και εξηγήσουμε γιατί είναι απαραίτητα, στη συνέχεια θα παρατηρήσουμε πως παρέχουν ποιότητα υπηρεσιών (QoS).

2.3.1.1 Πρωτόκολλα IEEE

Τα πρότυπα που περιγράφονται στο IEEE (Institute of Electrical and Electronics Engineers) είναι τρία και είναι τα ακόλουθα :

- Το πρωτόκολλο 802.1Q περιγράφει την αρχιτεκτονική, τις υπηρεσίες, τα πρωτόκολλα και τους αλγόριθμους για τα VLANs. Αν και αυτό το πρότυπο δεν περιλαμβάνει συγκεκριμένους μηχανισμούς Ποιότητας Υπηρεσίας (QoS), περιλαμβάνει μια κρίσιμη απαίτηση για την παροχή QoS, όπως τη δυνατότητα αναγέννησης της προτεραιότητας χρήστη των ληφθέντων πλαισίων χρησιμοποιώντας πληροφορίες προτεραιότητας στο πλαίσιο και τον πίνακα αναγέννησης προτεραιότητας χρήστη για τη θύρα λήψης.
- Το ενημερωμένο πρωτόκολλο 802.1D περιλαμβάνει όλες τις πτυχές της επιτάχυνσης της κατηγορίας κυκλοφορίας και του δυναμικού φιλτραρίσματος πολλαπλής εκπομπής που περιγράφονται στο πρότυπο IEEE 802.1p. Το πρότυπο IEEE 802.1p έχει συγχωνευθεί με προηγούμενες εκδόσεις του προτύπου IEEE 802.1D και καλύπτει όλα τα ζητήματα QoS.
- Το πρωτόκολλο 802.1p, το οποίο ασχολείται με το TCE και το DMF, είναι σημαντικό για την παροχή QoS στο επίπεδο MAC.
- Το GigaBit Ethernet, γνωστό και ως 1000BASE-X, χρησιμοποιεί την ίδια αρχιτεκτονική πρωτοκόλλου με το Ethernet 10/100 Mbps από το τμήμα Logical Link Control (LLC) του επιπέδου Ζεύξης Δεδομένων και άνω. Ωστόσο, χρησιμοποιεί διαφορετικά μέσα πρόσβασης και φυσικά στρώματα για να επιτύχει μετάδοση μέσω καλωδίου οπτικών ινών. Για να επιτευχθεί αυτό, το πρότυπο 802.3z υιοθέτησε τις τεχνολογίες πρόσβασης και κωδικοποίησης μέσων που χρησιμοποιούνται στη στοίβα πρωτοκόλλου Fiber Channel. Συγκεκριμένα, χρησιμοποιεί το επίπεδο FC1 του Fiber Channel, το οποίο ενσωματώνει την κωδικοποίηση 8B/10B, για να βοηθήσει στην εξισορρόπηση της διαφοράς 1 και 0 που μπορεί να υπάρχει σε μια μετάδοση. Χρησιμοποιεί επίσης το φυσικό επίπεδο FC0 για τον έλεγχο της σηματοδότησης στο φυσικό μέσο. Χρησιμοποιώντας αυτές τις τεχνολογίες, το GigaBit Ethernet είναι σε

θέση να επιτύχει πολύ μεγαλύτερες ταχύτητες μετάδοσης από το Ethernet 10/100 Mbps, καθιστώντας το ιδανικό για εφαρμογές δικτύωσης υψηλής ταχύτητας.



Σχήμα 1. Επίπεδα πρωτοκόλλου καναλιού οπτικών ινών ενσωματωμένα σε 802.3z (Hamad Ammar, 2015)

Το πρότυπο IEEE 802.1p έχει ένα σχήμα προτεραιοτήτων που λειτουργεί καλά. Τα πακέτα με χαμηλότερα επίπεδα προτεραιότητας δεν θα σταλούν εάν υπάρχουν πακέτα με υψηλότερη προτεραιότητα στην ουρά. Ωστόσο, το πρότυπο δεν περιλαμβάνει πρωτόκολλα ελέγχου εισαγωγής, γεγονός που οδηγεί σε πιθανότητα συμφόρησης δικτύου. Η Microsoft το αναγνωρίζει αυτό, αλλά θεωρεί ότι είναι ευθύνη των προγραμμάτων οδήγησης κάρτας διασύνδεσης δικτύου να το αποτρέψουν. Μπορούμε να ελπίζουμε ότι οι κατασκευαστές καρτών διασύνδεσης δικτύου παράγουν αποτελεσματικά προγράμματα οδήγησης. Το ίδιο το πρότυπο δεν περιορίζει τους πόρους που μπορεί να χρησιμοποιήσει μια εφαρμογή, αλλά πολλές υλοποιήσεις κάνουν, καθιστώντας μια βελτίωση υψηλής προτεραιότητας μηχανισμό για τη διαπραγμάτευση εγγυημένης ποιότητας για κάθε εφαρμογή. (Niclas, 1999)

2.3.1.2 Πρωτόκολλο ISL

Το ISL (Inter-Switch Link) είναι ένα πρωτόκολλο επικοινωνίας που επιτρέπει τη μεταφορά πληροφοριών VLAN και κίνησης δεδομένων VLAN μεταξύ διαφορετικών συσκευών δικτύωσης, όπως μεταγωγείς, δρομολογητές και διακομιστές. Αυτό επιτυγχάνεται με τη διαμόρφωση του ISL στη θύρα ενός μεταγωγέα που συνδέεται απευθείας με άλλες συσκευές δικτύου. Αυτό επιτρέπει την ανάθεση και τη διαμόρφωση των VLAN σε ολόκληρο το δίκτυο. Με απλούστερους όρους, το ISL βοηθά στη διαχείριση της ροής δεδομένων σε ένα δίκτυο που χρησιμοποιεί VLAN συνδέοντας διαφορετικές συσκευές δικτύωσης και επιτρέποντας τη ρύθμιση των VLAN σε όλο το δίκτυο. (Zheng, 2016)

2.3.1.3 VLAN Trunking Protocol (VTP)

Η βασική ιδέα του VTP είναι ότι οι τροποποιήσεις γίνονται σε διακομιστές VTP. Στη συνέχεια, οι υπόλοιποι διακομιστές και πελάτες VTP στον τομέα ενημερώνονται με αυτές τις τροποποιήσεις. Οι μεταγωγείς μπορούν να ρυθμιστούν χειροκίνητα ως πελάτες , διακομιστές ή διαφάνειας. Ένας διαφανής μεταγωγέας VTP λαμβάνει και μεταδίδει ενημερώσεις VTP, αλλά δεν τροποποιεί τη διαμόρφωσή του για να λαμβάνει υπόψη τις αλλαγές που περιέχουν. Ανάλογα με τον μεταγωγέα, η προεπιλεγμένη ρύθμιση μπορεί να είναι VTP διακομιστής ή διαφάνειας. Σε έναν μεταγωγέα σε λειτουργία πελάτη, η διαμόρφωση VLAN δεν μπορεί να γίνει τοπικά. (Gary, 2007)

Το VTP έχει τρεις λειτουργίες και είναι οι ακόλουθες:

- Στη λειτουργία **διακομιστή,** οι μεταγωγείς έχουν τη δυνατότητα δημιουργίας, διαγραφής ή τροποποίησης VLAN στον τομέα VTP. Όποιες αλλαγές γίνουν στον διακομιστή VTP θα μεταδοθούν σε ολόκληρο τον τομέα.
- Στη λειτουργία **πελάτη**, όλοι οι μεταγωγείς λαμβάνουν πληροφορίες VLAN από τον διακομιστή VTP και μπορούν να στείλουν ενημερώσεις, αλλά δεν αποθηκεύουν δεδομένα VLAN στο NVRAM.
- Διαφανής λειτουργία: Οι μεταγωγείς σε αυτήν τη λειτουργία δεν συμμετέχουν στον τομέα VTP και θα μεταδίδουν αλλαγές VTP μέσω συνδέσεων κορμού. Ωστόσο, αυτοί οι μεταγωγείς διατηρούν τη δική τους τοπική βάση δεδομένων VLAN και δεν την μοιράζονται με άλλους μεταγωγείς στο δίκτυο. (Carthern Chris, 2015)

2.3.1.4 Πρωτόκολλο IP

Το Πρωτόκολλο Διαδικτύου (IP) είναι ένα θεμελιώδες πρωτόκολλο στη σουίτα πρωτοκόλλων Διαδικτύου που χρησιμοποιείται για τη δρομολόγηση πακέτων δεδομένων πέρα από τα όρια του δικτύου. Είναι ένα πρωτόκολλο χωρίς σύνδεση που λειτουργεί στο επίπεδο δικτύου (Επίπεδο 3) του μοντέλου OSI και παρέχει υπηρεσίες διευθυνσιοδότησης και κατακερματισμού σε δεδομένα που αποστέλλονται μέσω του δικτύου. Το IP είναι το πρωτόκολλο που επιτρέπει την επικοινωνία μεταξύ διαφορετικών συσκευών μέσω του Διαδικτύου. (Hall, 2000)

2.3.1.5 Πρωτόκολλο TELNET

Το πρωτόκολλο Telnet χρησιμοποιείται για τη δημιουργία μιας εικονικής σύνδεσης τερματικού μεταξύ δύο συσκευών μέσω ενός δικτύου. Επιτρέπει σε έναν χρήστη σε έναν υπολογιστή να έχει πρόσβαση και να ελέγχει έναν άλλον υπολογιστή εξ αποστάσεως σαν να ήταν φυσικά συνδεδεμένος σε αυτόν. Το Telnet λειτουργεί στο επίπεδο εφαρμογής (Layer 7) του μοντέλου OSI και χρησιμοποιεί μια αρχιτεκτονική πελάτη-διακομιστή για να παρέχει απομακρυσμένη πρόσβαση στους πόρους. (Postel, 1983)

2.3.1.6 Πρωτόκολλο SNMP

Το Simple Network Management Protocol (SNMP) είναι ένα τυπικό πρωτόκολλο Διαδικτύου που χρησιμοποιείται για τη διαχείριση και την παρακολούθηση συσκευών σε ένα δίκτυο. Το SNMP επιτρέπει στους διαχειριστές δικτύου να παρακολουθούν την απόδοση και την κατάσταση συσκευών δικτύου όπως δρομολογητές, μεταγωγείς και διακομιστές. Λειτουργεί στο επίπεδο εφαρμογής (Layer 7) του μοντέλου OSI και χρησιμοποιεί μια αρχιτεκτονική πελάτη-διακομιστή για την ανταλλαγή πληροφοριών διαχείρισης μεταξύ συσκευών δικτύου. (Case, 1990)

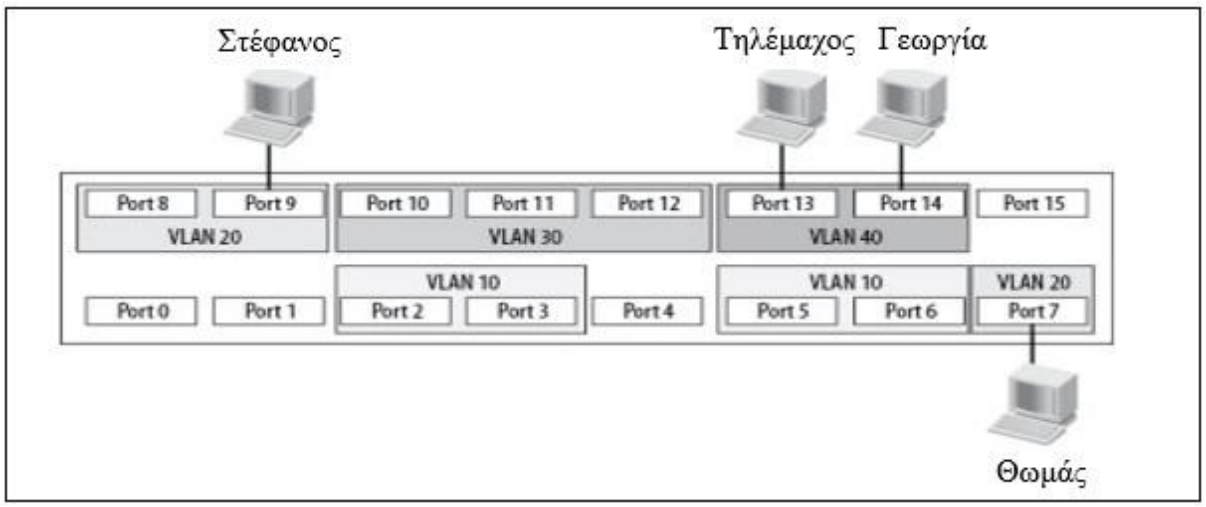
2.3.2 VLAN

Το δίκτυο μας θα βασιστεί στη συνδεσιμότητα με τα εικονικά LAN, ή τα VLAN, τα οποία είναι εικονικοί διαχωρισμοί εντός ενός μεταγωγέα που παρέχουν ξεχωριστά LAN που το καθένα συμπεριφέρεται σαν να είχε διαμορφωθεί σε ξεχωριστό φυσικό μεταγωγέα. Πριν από την εισαγωγή των VLAN, ένας μεταγωγέας μπορούσε να εξυπηρετήσει μόνο ένα LAN. Τα VLAN επέτρεψαν ένα μόνο μεταγωγέα να μπορεί να εξυπηρετήσει πολλαπλά δίκτυα LAN. Υποθέτοντας ότι δεν υπάρχουν τρωτά σημεία στο λειτουργικό σύστημα του μεταγωγέα, δεν θα πρέπει να υπάρχει τρόπος για ένα πακέτο που προέρχεται από ένα VLAN να φτάσει σε άλλο.

2.3.2.1 Συνδεσιμότητα VLAN

Το Σχήμα 2 δείχνει ένα μεταγωγέα με πολλαπλά VLAN. Τα VLAN έχουν αρίθμηση 10, 20, 30 και 40. Γενικά, τα VLAN μπορούμε να τα ονομάσουμε ή να τα αριθμήσουμε. Η υλοποίηση της Cisco χρησιμοποιεί αριθμούς για την αναγνώριση των VLAN από προεπιλογή. Το προεπιλεγμένο VLAN έχει αριθμό 10. Εάν συνδέσουμε διάφορες συσκευές σε ένα μεταγωγέα χωρίς να αντιστοιχίσουμε τις θύρες σε συγκεκριμένο VLAN, όλες οι συσκευές θα αντιστοιχούν στο VLAN 1.

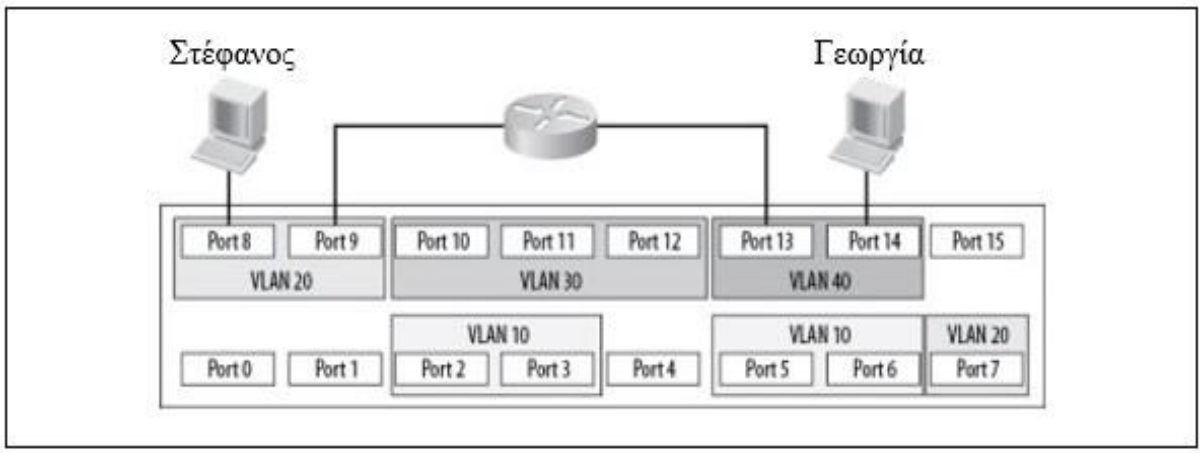
Τα πακέτα δεν μπορούν να φύγουν από τα VLAN από τα οποία προέρχονται. Αυτό σημαίνει ότι στο σχεδιασμό του παραδείγματος, ο Τηλέμαχος μπορεί να επικοινωνήσει με την Γεωργία και ο Στέφανος μπορεί να επικοινωνήσει με τον Θωμά, αλλά ο Στέφανος και ο Θωμάς δεν μπορούν να επικοινωνήσουν με τον Τηλέμαχο ή την Γεωργία με οποιονδήποτε τρόπο.



Σχήμα 2. VLAN σε ένα μεταγωγέα

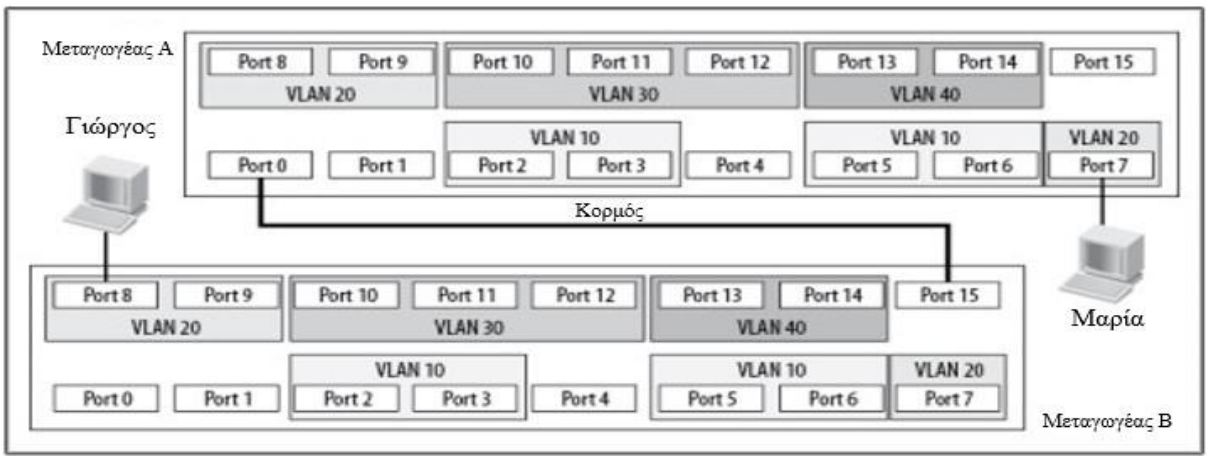
Ένας εξωτερικός δρομολογητής πρέπει να συνδεθεί σε καθένα από τα VLAN που πρέπει να δρομολογηθούν προκειμένου ένα πακέτο να μετακινηθεί από το ένα VLAN στο άλλο. Το Σχήμα 3 δείχνει πώς το VLAN 20 και το VLAN 40 συνδέονται με έναν εξωτερικό δρομολογητή. Υποθέτοντας ότι ο δρομολογητής έχει ρυθμιστεί σωστά, ο Στέφανος και η Γεωργία μπορούν τώρα να επικοινωνήσουν, αλλά κανένας σταθμός εργασίας δεν θα εμφανίσει καμία ένδειξη ότι είναι συνδεδεμένοι στον ίδιο φυσικό μεταγωγέα.

Ένα δίκτυο σαν το δικό μας προφανώς και θα χρησιμοποιεί VLANs και ένα τέτοιο δίκτυο αντιμετωπίζει τους ίδιους περιορισμούς. Ο νέος μεταγωγέας μπορεί να προωθήσει πακέτα από ή προς το VLAN 20 μόνο εάν είναι συνδεδεμένος σε μια θύρα που έχει ρυθμιστεί για VLAN0. Θα πρέπει να υπάρχουν τέσσερις σύνδεσμοι μεταξύ των μεταγωγέων, ένας για κάθε VLAN. Αν θέλουμε να συνδέσουμε δύο μεταγωγείς που ο καθένας έχει τέσσερα VLAN. Η ρύθμιση των κορμών μεταξύ μεταγωγέων είναι ένας τρόπος αντιμετώπισης αυτού του ζητήματος. Οι σύνδεσμοι γνωστοί ως κορμοί φέρουν πακέτα για πολλαπλά VLAN.



Σχήμα 3. Εξωτερική δρομολόγηση μεταξύ VLAN

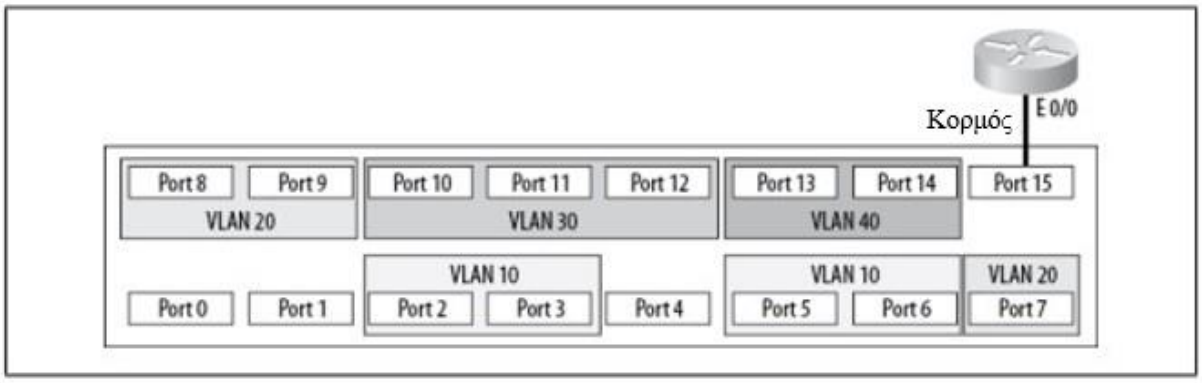
Το Σχήμα 4 δείχνει δύο μεταγωγείς συνδεδεμένους με κορμό. Η Μαρία είναι συνδεδεμένη με το VLAN 20 στον μεταγωγέα Α, ενώ ο Γιώργος συνδέεται με το VLAN 20 στον μεταγωγέα Β. Ο Γιώργος θα μπορεί να επικοινωνεί με την Μαρία επειδή ένα κορμό συνδέει αυτούς τους δύο μεταγωγείς, υποθέτοντας ότι ο κορμός επιτρέπεται να μεταφέρει πακέτα για όλα τα διαμορφωμένα VLANs. Λαμβάνουμε υπόψη ότι δεν έχουν εκχωρηθεί VLAN στις θύρες στις οποίες είναι συνδεδεμένος ο κορμός. Ως θύρες κορμού, αυτές οι θύρες δεν αποτελούν μέρος ενός μόνο VLAN.



Σχήμα 4. Δύο μεταγωγείς συνδεδεμένοι με κορμό

Ένας κορμός είναι μια διεπαφή ή σύνδεσμος που μπορεί ταυτόχρονα να μεταφέρει πακέτα για πολλαπλά VLAN, με βάση την ορολογία της Cisco. Όπως είδαμε ένα κορμό μπορεί να συνδέσει δύο μεταγωγείς, επιτρέποντας την επικοινωνία μεταξύ συσκευών στα ίδια VLAN σε διαφορετικούς μεταγωγείς. Οι μεταγωγείς συνδέονται στο επίπεδο ζεύξης δεδομένων χρησιμοποιώντας κορμό, εκτός εάν υπάρχει μόνο ένα VLAN που πρέπει να συνδεθεί. Δύο μεταγωγείς συνδέονται με ένα κορμό στο Σχήμα 4.

Οι κορμοί δίνουν επίσης στους μεταγωγείς πρόσβαση σε μια άλλη δυνατότητα. Το σχήμα 3 δείχνει πώς δύο VLAN μπορούν να συνδεθούν μεταξύ τους χρησιμοποιώντας έναν δρομολογητή σαν να ήταν διαφορετικά φυσικά δίκτυα. Ας υποθέσουμε ότι θέλουμε να δημιουργήσουμε μια διαδρομή μεταξύ κάθε VLAN στο μεταγωγέα. Ένα τέτοιο σχέδιο αν το κάναμε πράξη παραδοσιακά, η λύση θα ήταν να δοθεί σε κάθε δίκτυο που πρέπει να δρομολογηθεί μία μόνο σύνδεση από το δρομολογητή. Κάθε δίκτυο σε αυτόν τον μεταγωγέα είναι VLAN, επομένως απαιτείται φυσική σύνδεση μεταξύ κάθε δρομολογητή και κάθε VLAN.

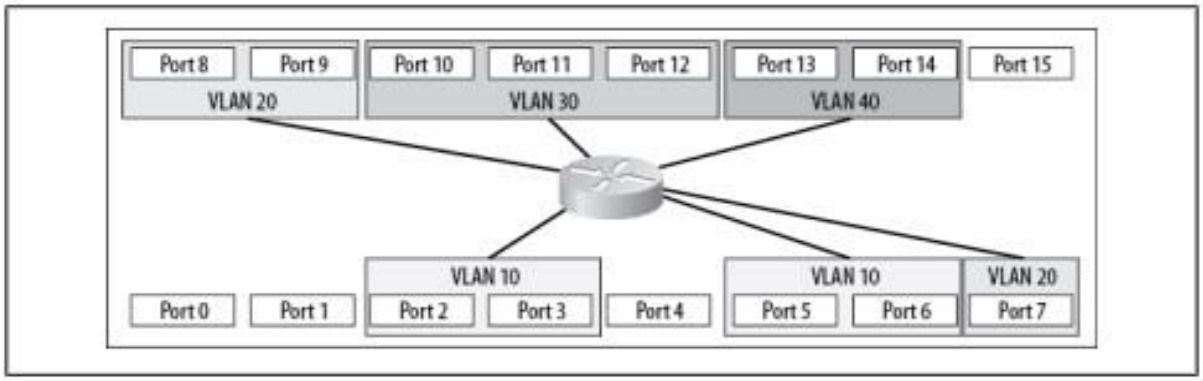


Σχήμα 5. Router-on-a-stick

Η διαμόρφωση router-on-a-stick είναι μια μέθοδος δρομολόγησης μεταξύ VLAN. Μπορείτε να συνδέσετε τον μεταγωγέα στον δρομολογητή χρησιμοποιώντας ένα μόνο κορμό αντί να συνδέετε κάθε VLAN με ξεχωριστή διεπαφή δρομολογητή. Στη συνέχεια, όπως απεικονίζεται στο Σχήμα 5, όλα τα VLAN θα ταξιδεύουν με μία μόνο σύνδεση.

Η χρήση ενός router-on-a-stick εξοικονομεί σημαντικό αριθμό διεπαφών τόσο στον μεταγωγέα όσο και στον δρομολογητή. Ο κορμός έχει μόνο μία σύνδεση και το συνολικό εύρος ζώνης σε αυτήν τη σύνδεση είναι μόνο 10 Mbps, το οποίο είναι ένα μειονέκτημα. Αντίθετα, κάθε VLAN έχει 10 Mbps για τον εαυτό του όταν το κάθε ένα έχει τη δική του σύνδεση. Επίσης δεν ξεχνάμε ότι ο δρομολογητής μεταφέρει δεδομένα μεταξύ VLAN, επομένως είναι πιθανό κάθε πακέτο να ταξιδεύει στον ίδιο σύνδεσμο δύο φορές, μία για να φτάσει στο δρομολογητή και μία για να επιστρέψει στο VLAN προορισμού.

Το Σχήμα 6 απεικονίζει βασικά πώς θα μπορούσε να εφαρμοστεί ο ίδιος σχεδιασμός χρησιμοποιώντας έναν μεταγωγέα Επιπέδου 3 (Layer 3). Δεν χρειάζονται εξωτερικές συνδέσεις επειδή ο δρομολογητής είναι ενσωματωμένος στον μεταγωγέα. Κάθε θύρα σε μεταγωγέα Layer-3 μπορεί να διατεθεί για συσκευές ή να χρησιμοποιηθεί ως κορμός για άλλους μεταγωγείς.



Σχήμα 6. Μεταγωγέας επιπέδου 3

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ

Ο τομέας της ασφάλειας δικτύου αποτελείται από μέτρα για την αποτροπή, την πρόληψη, τον εντοπισμό και τη διόρθωση παραβιάσεων ασφάλειας που περιλαμβάνουν τη μετάδοση πληροφοριών. Η προστασία που παρέχεται σε ένα αυτοματοποιημένο σύστημα πληροφοριών πρέπει να επιτυγχάνει τους στόχους, διατήρησης της ακεραιότητας, της διαθεσιμότητας, και εμπιστευτικότητας των πόρων του πληροφοριακού συστήματος. Γι' αυτό λοιπόν θα πρέπει να αναφερθούμε αρχικά στην ασφάλεια των υπολογιστών.

Αυτοί είναι οι τρείς βασικοί στόχοι που βρίσκονται στο επίκεντρο της ασφάλειας υπολογιστών:

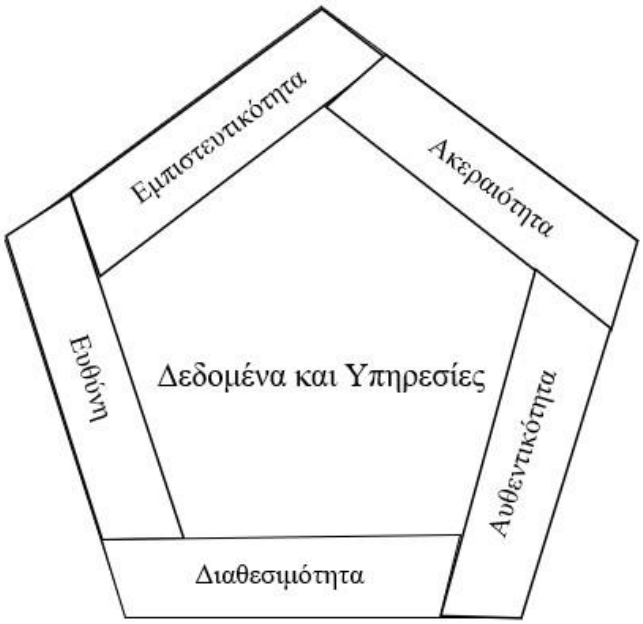
- **Εμπιστευτικότητα:** Αυτός ο όρος καλύπτει δύο σχετικές έννοιες:
    - **Εμπιστευτικότητα δεδομένων:** Διαβεβαιώνει ότι οι ιδιωτικές πληροφορίες δεν διατίθενται ούτε αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
    - **Ιδιωτικότητα:** Διαβεβαιώνει ότι τα άτομα ελέγχουν ποιες πληροφορίες μπορούν να συλλεχθούν και να αποθηκευτούν που σχετίζονται με αυτούς και από ποιον και σε ποιον μπορεί να αποκαλυφθούν αυτές οι πληροφορίες.
- **Ακεραιότητα:** Αυτός ο όρος καλύπτει δύο σχετικές έννοιες:
    - **Ακεραιότητα δεδομένων:** Διαβεβαιώνει ότι οι πληροφορίες και τα προγράμματα αλλάζουν μόνο σε καθορισμένο και εξουσιοδοτημένο τρόπος.
    - **Ακεραιότητα συστήματος:** Διαβεβαιώνει ότι ένα σύστημα εκτελεί την προβλεπόμενη λειτουργία χωρίς προβλήματα, χωρίς σκόπιμα ή ακούσια μέσα για την μη εξουσιοδοτημένη χρήση του συστήματος
- **Διαθεσιμότητα:** Διαβεβαιώνει ότι τα συστήματα λειτουργούν έγκαιρα και ότι δεν απαγορεύεται η εξυπηρέτηση χρηστών.

Αυτές οι τρείς έννοιες ενσωματώνουν τους θεμελιώδεις στόχους ασφάλειας τόσο για τα δεδομένα όσο και για τις υπηρεσίες πληροφοριών και υπολογιστών. Αυτός είναι ο χαρακτηρισμός αυτών των τριών στόχων ως προς τις απαιτήσεις και τον ορισμό της απώλειας ασφάλειας σε κάθε κατηγορία:

- **Εμπιστευτικότητα:** Διατήρηση εξουσιοδοτημένων περιορισμών στην πρόσβαση και αποκάλυψη πληροφοριών, συμπεριλαμβανομένων των μέσων για την προστασία του προσωπικού απορρήτου και των ιδιόκτητων πληροφοριών. Η απώλεια της εμπιστευτικότητας είναι η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών.
- **Ακεραιότητα:** Προστασία από ακατάλληλη τροποποίηση ή καταστροφή πληροφοριών, συμπεριλαμβανομένης της διασφάλισης της αυθεντικότητας των

πληροφοριών. Απώλεια ακεραιότητας είναι η μη εξουσιοδοτημένη τροποποίηση ή καταστροφή πληροφοριών.

- **Διαθεσιμότητα:** Εξασφάλιση έγκαιρης και αξιόπιστης πρόσβασης και χρήσης των πληροφοριών. Απώλεια διαθεσιμότητας είναι η διακοπή της πρόσβασης ή της χρήσης πληροφοριών ή συστημάτων πληροφορίων.



Σχήμα 7. Βασικές απαιτήσεις ασφάλειας δικτύου

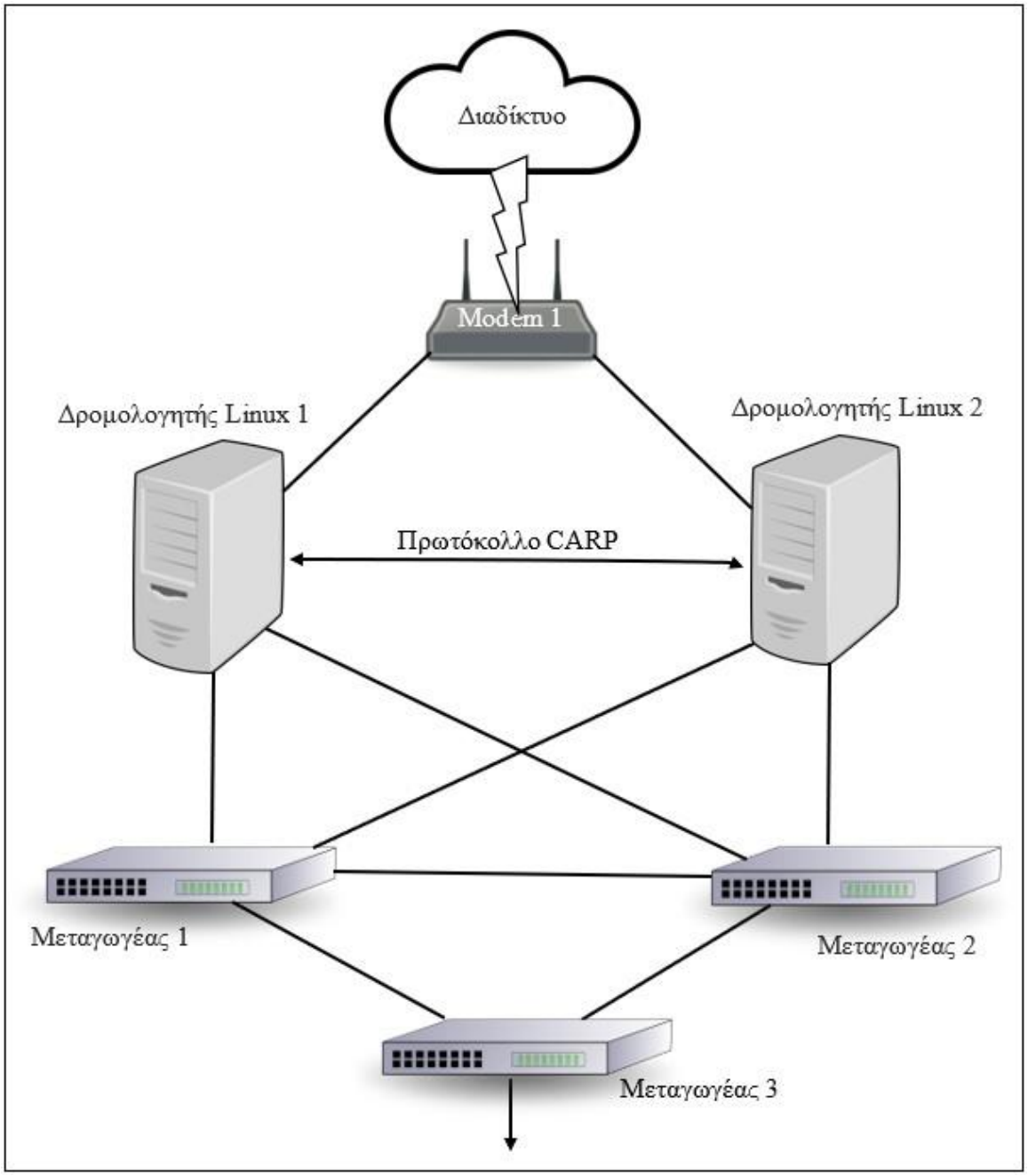
Δύο πρόσθετες έννοιες που χρειαζόμαστε για τον καθορισμό στόχων ασφάλειας. Αυτά είναι τα ακόλουθα δυο:

- **Αυθεντικότητα:** Η ιδιότητα του να είναι γνήσιο, έμπιστο και να μπορεί να επαληθευτεί. Αυτό σημαίνει πως επαληθεύεται ότι οι χρήστες είναι αυτοί που λένε ότι είναι και ότι κάθε είσοδος που έφθασε στο σύστημα προήλθε από μια αξιόπιστη πηγή.
- **Υπευθυνότητα:** Ο στόχος ασφάλειας που δημιουργεί την απαίτηση για ενέργειες μιας οντότητας που πρέπει να ανιχνευθεί μοναδικά. Αυτό υποστηρίζει αποτροπή, απομόνωση σφαλμάτων, ανίχνευση και πρόληψη εισβολής και ανάκτηση μετά από ενέργεια. Επειδή τα πραγματικά ασφαλή συστήματα δεν είναι ακόμη ένας επιτεύξιμος στόχος, πρέπει να είμαστε σε θέση να εντοπίσουμε μια παραβίαση ασφάλειας σε μία ομάδα. Τα συστήματα πρέπει να διατηρούν αρχεία για τις δραστηριότητές τους για να επιτρέψουν τη μετέπειτα ανάλυση για τον εντοπισμό παραβιάσεων ασφάλειας. (William, 2017)

3.1 ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΣΥΣΚΕΥΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΙΚΤΥΟΥ

Εφόσον αναφερόμαστε σε επιχειρήσεις, εταιρίες και δημόσιες υπηρεσίες το λογισμικό και η συσκευή προστασίας δικτύου μας είναι δύο τερματικά που χρησιμοποιούν το λειτουργικό σύστημα Linux και δουλεύουν ως δρομολογητές, οι οποίοι έχουν μία πληθώρα πλεονεκτημάτων, συμπεριλαμβανομένου του μηδενικού κόστους και της ευελιξίας. Οι δρομολογητές Linux δεν θα χρησιμοποιηθούν για μία απλή δρομολόγηση αλλά για πολλά περισσότερα.

Ας αναλύσουμε το ακόλουθο κομμάτι δικτύου μας:



Σχήμα 8. Δρομολογητές Linux

Το κομμάτι δικτύου που παρατηρούμε ξεκινάει από το διαδίκτυο και τελειώνει στο modem το οποίο συνδέεται με το υπόλοιπο μας δίκτυο που δεν μας αφορά την συγκεκριμένη στιγμή. Για το κομμάτι δικτύου που μας αφορά και παρατηρούμαι στο σχήμα 8, χρειαζόμαστε σύνδεση στο διαδίκτυο. Για μία πετυχημένη σύνδεση στο διαδίκτυο χρειαζόμαστε ένα modem, το οποίο αυτό συνδέεται με δυο δρομολογητές Linux, αυτοί συνδέονται μεταξύ τους και με δυο μεταγωγείς ο καθένας ξεχωριστά. Τέλος οι μεταγωγείς συνδέονται και αυτοί μεταξύ τους και με ένα ακόμα μεταγωγέα όπου αυτός στη συνέχεια συνδέεται με το διακομιστή μεσολάβησης Squid και Samba διακομιστή. Έχουμε δυο δρομολογητές και δυο μεταγωγείς για να έχουμε μέγιστη ασφάλεια και διαθεσιμότητα. Με αυτή τη συνδεσιμότητα παρέχουμε στο δίκτυο μας πλεονασμό ανακατεύθυνσης. Αυτή την έννοια θα την εξηγήσουμε σε επόμενο κεφάλαιο.

3.1.1 Πρωτόκολλο CARP

Ένα σύνολο διευθύνσεων IP μπορεί να μοιράζεται από πολλούς κεντρικούς υπολογιστές που είναι συνδεδεμένοι στο ίδιο τοπικό δίκτυο χάρη στο πρωτόκολλο δικτύωσης υπολογιστών που είναι γνωστό ως CARP. Η κύρια λειτουργία του είναι ο πλεονασμός ανακατεύθυνσης, ειδικά όταν χρησιμοποιείται με τείχη προστασίας και δρομολογητές. Όπως στη συγκεκριμένη περίπτωση που χρησιμοποιείται από τους Linux δρομολογητές. (Anon., n.d.)

Κάθε εταιρία, επιχείρηση και δημόσια υπηρεσία έχει τουλάχιστον τρία τμήματα, για παράδειγμα το τμήμα της πληροφορικής, το πωλήσεων και λογιστηρίου και το εκτελεστικό τμήμα. Η εταιρεία μας έχει τρία μικρότερα δίκτυα για κάθε ένα από τα τμήματα:

- Το τμήμα της πληροφορικής διαθέτει, εκτός από τον διαχειριστή πληροφορικής, ένα ή περισσότερους διαχειριστές δικτύου. Έχουν ξεχωριστό δίκτυο και είναι η αποστρατικοποιημένη ζώνη μας γιατί τα παιδιά της πληροφορικής είναι έμπειροι χρήστες υπολογιστών και γνωρίζουν πώς να ασφαλίζουν τους υπολογιστές τους.
- Το εκτελεστικό τμήμα περιλαμβάνει τους υπολογιστές για όλα τα στελέχη της εταιρείας. Τα στελέχη συνήθως έχουν τον ελάχιστο δυνατό περιορισμό για ειδικές εφαρμογές συνομιλίας και ούτω καθεξής (και επίσης κοινή χρήση αρχείων).
- Τα τμήματα πωλήσεων και λογιστηρίου διαθέτουν ένα μεγάλο δίκτυο, καθώς η εταιρεία διαθέτει μεγάλο αριθμό πωλητών. Αυτό είναι το μέρος του δικτύου που απαιτεί τη μεγαλύτερη προσοχή μας αφού συνήθως οι πωλήσεις είναι το τμήμα με τα περισσότερα προβλήματα πληροφορικής. Επίσης υπάρχουν και οι δημόσιες υπηρεσίες που δεν έχουν τμήμα πωλήσεων αντ' αυτού θα έχουν ξεχωριστά μικρότερα δίκτυα για κάθε μια με δύο τμήματα που παρέχουν.

Για εύκολη κατανόηση του δικτύου, έχουμε τοποθετήσει τρεις μεταγωγείς που ανήκουν στα τρία ξεχωριστά δίκτυα, ένα για το τμήμα πωλήσεων και λογιστηρίου, ένα για τα διευθυντικά γραφεία και ένα για το τμήμα πληροφορικής. Θα χρησιμοποιήσουμε ένα διαχειριζόμενο μεταγωγέα σε αυτήν την περίπτωση για να δημιουργήσουμε τρία ξεχωριστά VLANs. Αυτή είναι η εταιρεία μας τώρα, με τρία μικρότερα δίκτυα. Είναι καιρός να ορίσουμε τη πολιτική ασφαλείας

3.1.2 Καθορισμός της Πολιτικής Ασφαλείας

Δεδομένου ότι τα μέλη του προσωπικού της πληροφορικής είναι έμπειροι χρήστες υπολογιστών, το δίκτυο του τμήματος της πληροφορικής λειτουργεί ως η αποστρατικοποιημένη ζώνη μας. Πρέπει να ανοίξουμε τις θύρες 80 και 110 για πρόσβαση στο διαδίκτυο, 25 και 110 για αλληλογραφία και για χρήση πρωτοκόλλου SSH, επειδή οι διακομιστές ιστού και αλληλογραφίας πρέπει να είναι προσβάσιμοι από οπουδήποτε. Απαιτούμε πρόσβαση SSH και στους δύο διακομιστές Linux στο δίκτυο από υπολογιστές στο τμήμα πληροφορικής και από μερικές δημόσιες διευθύνσεις IP που έχουμε στο σπίτι.

Το πρωτόκολλο SSH κρυπτογραφεί τα δεδομένα που μεταδίδονται μεταξύ ενός πελάτη και ενός διακομιστή για την προστασία της σύνδεσης. Για την αποτροπή επιθέσεων δικτύου, κρυπτογραφούνται όλες οι μεταφορές ταυτότητας χρήστη, εντολές, έξοδοι και αρχεία. (Ylonen, 2017)

Τόσο ο διακομιστής αρχείων όσο και ο διακομιστής ενδοδικτύου (intranet) πρέπει να έχουν πρόσβαση μόνο από υπολογιστές εργασίας. Αν και οι δύο διακομιστές στεγάζονται στον ίδιο υπολογιστή, χρησιμοποιούμε τον όρο "διακομιστής" για να αναφερθούμε στις υπηρεσίες σε αυτό το πλαίσιο.

Το εκτελεστικό τμήμα χρειάζεται πρόσβαση σε οτιδήποτε υπάρχει στο Διαδίκτυο, επομένως μοιάζει με την αποστρατικοποιημένη ζώνη. Ωστόσο, ίσως θέλουμε να τους επιβάλουμε ορισμένους περιορισμούς:

- Άρνηση πρόσβασης σε τρίτους να μπορούν να δουν τα κοινόχρηστα αρχεία τους στο εκτελεστικό δίκτυο.
- Για να μην έχουν πρόσβαση στα αρχεία .pif και .scr, χρησιμοποιούμε έναν διαφανή διακομιστή μεσολάβησης.

Οι υπολογιστές των τμημάτων πωλήσεων, λογιστηρίου και υπολοίπων τμημάτων επιτρέπεται να κάνουν τα εξής:

- Περιήγηση στον ιστό, αλλά δεν επιτρέπεται η λήψη αρχείων .pif, .scr, .exe, .zip και .rar, και επίσης η επίσκεψη ιστοσελίδων με σεξουαλικό περιεχόμενο
- Πρόσβαση σε διαδικτυακές τραπεζικές υπηρεσίες
- Αποστολή και λήψη email χρησιμοποιώντας τον διακομιστή αλληλογραφίας της εταιρείας
- Πρόσβαση στο ενδοδίκτυο και στους διακομιστές αρχείων

3.1.3 Διαμόρφωση Διακομιστή Μεσολάβησης Squid

Πριν από οτιδήποτε άλλο, πρέπει να διαμορφώσουμε τον διακομιστή μεσολάβησης Squid έτσι ώστε να μπορεί να εκτελεί διαφανείς λειτουργίες διακομιστή μεσολάβησης για τους υπολογιστές των υπαλλήλων και να εμποδίζει την πρόσβαση σε ορισμένους ιούς και πορνογραφικούς ιστότοπους.

Ο διακομιστής μεσολάβησης Squid πρέπει να κάνει τα ακόλουθα:

- Χρησιμοποιείται ως διαφανής διαμεσολαβητής
- Απορρίπτει τα επικίνδυνα αρχεία (.vba και .exe) για τους διαχειριστές, αλλά επιτρέπει όλα τα άλλα για αυτούς
- Απορρίπτει επικίνδυνα αρχεία και ιστότοπους σεξουαλικού περιεχομένου για τα τμήματα πωλήσεων, λογιστηρίου και υπόλοιπα παρεμφερή αλλά επιτρέπει οτιδήποτε άλλο

3.1.4 Αντίστροφος Διακομιστής Μεσολάβησης Squid

Ο αντίστροφος διακομιστής μεσολάβησης που θα χρησιμοποιήσουμε είναι ο πιο δημοφιλής διακομιστής μεσολάβησης λογισμικό ανοιχτού κώδικα για Linux. Αυτός είναι ο Squid και είναι διαθέσιμος στις περισσότερες διανομές και μπορούμε να τον βρούμε στη διεύθυνση www.squid-cache.org.

Ο αντίστροφος διακομιστής μεσολάβησης είναι ένα σύστημα υπολογιστή που ενεργεί ως ενδιάμεσος μεταξύ ενός πελάτη και ενός διακομιστή-στόχου. Όταν ένας πελάτης υποβάλλει αίτηση για έναν πόρο του διαδικτύου, ο διακομιστής μεσολάβησης υποκλέπτει την αίτηση και την αποστέλλει στον διακομιστή-στόχο εκ μέρους του πελάτη. Στη συνέχεια, ο διακομιστής μεσολάβησης λαμβάνει την απάντηση από τον διακομιστή-στόχο και την επιστρέφει στον πελάτη, δίνοντας την εντύπωση ότι ο πελάτης έχει επικοινωνήσει απευθείας με τον διακομιστή-στόχο.

Οι αντίστροφοι διακομιστές μεσολάβησης μπορούν να εκτελέσουν μια ποικιλία εργασιών, όπως η μείωση της χρήσης εύρους ζώνης, η βελτίωση της εμπειρίας περιήγησης με την προσωρινή αποθήκευση εγγράφων ιστού, η επιβολή πολιτικών πρόσβασης στο δίκτυο, η παρακολούθηση της κυκλοφορίας των χρηστών, η ενίσχυση του απορρήτου των χρηστών, η κατανομή του φορτίου μεταξύ των διακομιστών, το φιλτράρισμα των αιτήσεων ή των απαντήσεων και η εξισορρόπηση της κυκλοφορίας του δικτύου. Μπορούν επίσης να χρησιμοποιηθούν για την αναμετάδοση της κυκλοφορίας εντός ενός τοπικού δικτύου.

Σε προχωρημένες μορφές, οι αντίστροφοι διακομιστές μεσολάβησης μπορούν να εφαρμόζουν κανόνες στα αιτήματα και τις απαντήσεις, επιτρέποντας ή αρνούμενοι την πρόσβαση με βάση διάφορα κριτήρια, όπως η διεύθυνση IP του πελάτη ή του διακομιστή-στόχου, το πρωτόκολλο που χρησιμοποιείται, ο τύπος περιεχομένου των εγγράφων ιστού και ούτω καθεξής. Οι αντίστροφοι διακομιστές μεσολάβησης μπορούν επίσης να τροποποιούν αιτήσεις ή απαντήσεις ή να αποθηκεύουν απαντήσεις από τον διακομιστή-στόχο τοπικά για μεταγενέστερη χρήση, μια διαδικασία γνωστή ως προσωρινή αποθήκευση. Η προσωρινή αποθήκευση χρησιμοποιείται συχνά για την εξοικονόμηση εύρους ζώνης, την ενίσχυση των διακομιστών ιστού και τη βελτίωση της εμπειρίας περιήγησης του χρήστη.

3.1.5 Κατασκευή τείχους προστασίας

Το παρακάτω σύνολο κανόνων εφαρμόζονται στο δίκτυο μας. Αυτοί οι κανόνες εφαρμόζονται για τον έλεγχο της κίνησης που εισέρχεται και εξέρχεται από το δίκτυο του υπολογιστή, καθώς και για την ανακατεύθυνση ορισμένων τύπων κίνησης σε συγκεκριμένους προορισμούς.

- Τροποποίηση των αιτημάτων DNS που υποβάλλονται από υπολογιστές σε ορισμένα τμήματα.
- Ανακατεύθυνση όλων των αιτημάτων Ιστού σε έναν διακομιστή μεσολάβησης, εκτός από τα αιτήματα σε έναν διακομιστή ενδοδικτύου.
- Τροποποίηση αιτημάτων HTTPS που υποβάλλονται από υπολογιστές σε ορισμένα τμήματα.
- Απόρριψη όλων των πακέτων που προέρχονται από τα τμήματα πωλήσεων και λογιστηρίων και πηγαίνουν στο Διαδίκτυο.
- Ανακατεύθυνση των αιτημάτων ιστού που υποβάλλονται από διαχειριστές για χρήση του διακομιστή μεσολάβησης.
- Επιτρέπεται η πρόσβαση στο SSH σε ορισμένους διακομιστές από μια συγκεκριμένη λίστα διευθύνσεων IP.

- Άρνηση πρόσβασης στον διακομιστή αρχείων Samba από οπουδήποτε εκτός από ορισμένα δίκτυα.
- Επιτρέπεται η πρόσβαση στον διακομιστή DNS από ορισμένα δίκτυα.
- Τέλος, επιτρέπεται η πρόσβαση στον διακομιστή αλληλογραφίας από ορισμένα δίκτυα

Αφού υλοποιηθούν αυτοί οι κανόνες έχουμε κατασκευάσει το τείχος προστασίας μας (Anon., n.d.)

3.1.6 Κατανομή εύρους ζώνης με Ποιότητα Υπηρεσιών (QoS)

Παρακάτω περιγράφουμε τον τρόπο ρύθμισης ορίων εύρους ζώνης για διαφορετικά τμήματα εντός μιας εταιρείας χρησιμοποιώντας ένα εργαλείο που ονομάζεται CBQ.

Η τεχνική κλάσης-βασισμένο σε ουρές (CBQ), είναι μια τεχνική για υλοποίηση δικτύου που επιτρέπει την κυκλοφορία να μοιράζεται εξίσου το εύρος ζώνης αφού κατηγοριοποιηθεί σε κλάσεις. Οι κλάσεις μπορούν να καθοριστούν από διάφορους παράγοντες, όπως η προτεραιότητα, η διεπαφή ή το αρχικό πρόγραμμα.

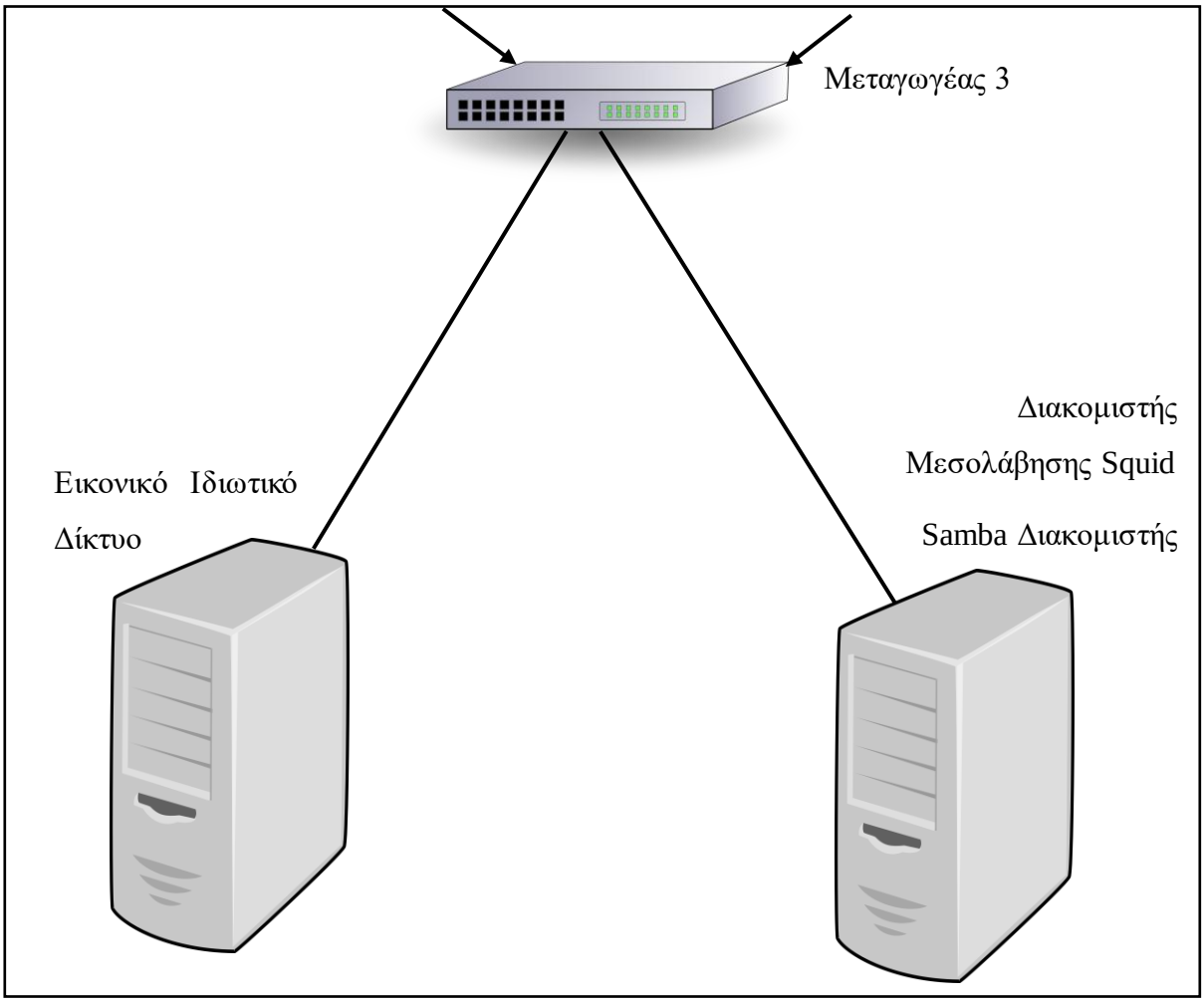
Για παράδειγμα το συνολικό διαθέσιμο εύρος ζώνης είναι 6 Mbps και θέλουμε να διαιρέσουμε αυτό το εύρος ζώνης μεταξύ διαφορετικών τμημάτων χρησιμοποιώντας το CBQ. Επίσης θα χρησιμοποιήσουμε ένα άλλο εργαλείο που ονομάζεται HBB για την προσαρμογή διαφόρων παραμέτρων στο CBQ και τη βελτίωση της απόδοσης. Στη συνέχεια θα ρυθμίσουμε το CBQ για να δημιουργήσουμε τάξεις για κάθε τμήμα, καθώς χρησιμοποιώντας ένα άλλο εργαλείο που ονομάζεται TFH αντιστοιχίζουμε την κίνηση σε συγκεκριμένες διευθύνσεις IP ή υποδίκτυα. Συνολικά, ο στόχος είναι να περιοριστεί η ποσότητα του εύρους ζώνης που μπορεί να χρησιμοποιήσει κάθε τμήμα, έτσι ώστε κανένα τμήμα να μην καταναλώνει πάρα πολύ από το συνολικό διαθέσιμο εύρος ζώνης. (Lucian, 2006)

3.2 ΔΙΑΚΟΜΙΣΤΗΣ SAMBA/ΜΕΣΟΛΑΒΗΣΗΣ ΚΑΙ VPN

Έχοντας δημιουργήσει την πρώτη γραμμή άμυνας απέναντι σε εξωτερικούς και εσωτερικούς κινδύνους, το επόμενο απαραίτητο βήμα για την ύψιστη ασφάλεια του δικτύου μας είναι η χρήση ενός εικονικού ιδιωτικού δικτύου (VPN) και ενός ελεγκτή τομέα.

Στη συνέχεια θα αναλύσουμε τα θεμελιώδη βήματα που απαιτούνται για τη σωστή διαμόρφωση ενός Samba 4 Ενεργού Αρχείου ώστε να λειτουργεί ως Ελεγκτής Τομέα του δικτύου.

Η συνέχεια του δικτύου μας που θα αναλύσουμε:



Σχήμα 9. Εικονικό ιδιωτικό δίκτυο-Διακομιστής μεσολάβησης Squid και Samba

Το Samba είναι ένα δωρεάν πακέτο λογισμικού ανοιχτού κώδικα που χρησιμοποιεί τα πρωτόκολλα Server Message Block (SMB) και Κοινό Σύστημα Αρχείων Διαδικτύου (CIFS) για να προσφέρει υπηρεσίες αρχείων και εκτύπωσης σε συμβατούς πελάτες. Η πιο πρόσφατη έκδοση Samba, το Samba 4, υποστηρίζει την υπηρεσία ως ελεγκτής τομέα Ενεργού Αρχείου (AD).

3.2.1 Κατανόηση του Ελεγκτής Τομέα

Ως ελεγκτής τομέα, το Samba 4 επιτρέπει τη δημιουργία τομέων, οι οποίοι μπορούν να διαχειρίζονται κεντρικά έχοντας πολλά πλεονεκτήματα, από ένα δίκτυο υπολογιστών. Τα πλεονεκτήματα αυτά συνίστανται σε:

- Ο κεντρικός έλεγχος ταυτότητας επιτρέπει στους χρήστες να συνδέονται σε οποιονδήποτε υπολογιστή στον τομέα χρησιμοποιώντας ένα ενιαίο σύνολο διαπιστευτηρίων χάρη στην ικανότητα του Samba 4 να αποθηκεύει λογαριασμούς χρηστών και κωδικούς πρόσβασης σε μια κεντρική τοποθεσία.
- **Κεντρική εξουσιοδότηση**: Το Samba 4 μπορεί να χρησιμοποιηθεί για τον περιορισμό της πρόσβασης σε πόρους δικτύου, όπως κοινόχρηστα αρχεία ή εκτυπωτές, ανάλογα με τη συμμετοχή χρηστών ή ομάδων.
- **Υποστήριξη πολιτικής ομάδας**: Το Samba 4 επιτρέπει στους διαχειριστές να διαμορφώνουν ομοιόμορφα τις ρυθμίσεις και τις πολιτικές σε όλο το δίκτυο, ενεργοποιώντας την εφαρμογή Αντικειμένων Πολιτικής Ομάδας (GPO) σε υπολογιστές στον τομέα.
- **Διαχείριση σε όλο τον τομέα**: Με το Samba 4, οι διαχειριστές μπορούν να διαχειρίζονται ολόκληρο τον τομέα από μια τοποθεσία αντί να χρειάζεται να διαχειρίζονται κάθε υπολογιστή ξεχωριστά.

Ο Ελεγκτής Τομέα Ενεργού Αρχείου του Samba 4, υποστηρίζει την Πολιτική Ομάδας, προσφέρει κεντρικό έλεγχο ταυτότητας και εξουσιοδότηση, διαχείριση σε όλο τον τομέα και άλλα πλεονεκτήματα για την οργάνωση και τη λειτουργία ενός δικτύου υπολογιστών. (Marcelo, 2017)

3.2.2 Εικονικού Ιδιωτικού Δικτύου (VPN)

Το εικονικό ιδιωτικό δίκτυο που χρησιμοποιούμε είναι το SoftEther VPN, το οποίο είναι μια δωρεάν εφαρμογή λογισμικού ανοιχτού κώδικα που παρέχει μια λύση εικονικού ιδιωτικού δικτύου (VPN). Αναπτύχθηκε από τον Daiyuu Nobori, καθηγητή στο Πανεπιστήμιο της Tsukuba στην Ιαπωνία, και την ομάδα του.

Το SoftEther VPN Server είναι ένα πρόγραμμα λογισμικού που επιτρέπει σε έναν υπολογιστή να λειτουργεί ως διακομιστής. Είναι συμβατό με πολλά πρωτόκολλα εικονικού ιδιωτικού δικτύου και μπορεί να τρέξει σε πολλά λειτουργικά συστήματα. Ένα μοναδικό χαρακτηριστικό του SoftEther VPN Server είναι ότι μία μόνο παρουσία του λογισμικού μπορεί να υποστηρίξει

πολλαπλά πρωτόκολλα εικονικού ιδιωτικού δικτύου ταυτόχρονα. Αυτό γίνεται εφικτό από μια μονάδα που ονομάζεται προσαρμογέας Επιπέδου 2, η οποία επιτρέπει την επικοινωνία μεταξύ διαφορετικών πρωτοκόλλων εικονικού ιδιωτικού δικτύου να διέρχεται μέσω ενός εικονικού διακόπτη Επιπέδου 2.

Ένα άλλο μοναδικό χαρακτηριστικό του SoftEther VPN Server είναι η ικανότητά του να υποστηρίζει πολλαπλούς μισθωτές, που επιτρέπει υπηρεσίες εικονικής φιλοξενίας και εικονικοποίηση της διαχείρισης χρηστών και των λειτουργιών δικτύου. Ο διακομιστής SoftEther VPN έχει βρεθεί ότι είναι ταχύτερος σε πειράματα ταχύτητας επικοινωνίας σε σύγκριση με άλλα προγράμματα εγγενών διακομιστών εικονικού ιδιωτικού δικτύου.

Το SoftEther VPN έχει επίσης μια σειρά από άλλες δυνατότητες που το καθιστούν μια ισχυρή και ευέλικτη λύση εικονικού ιδιωτικού δικτύου. Αυτά περιλαμβάνουν:

- Υποστήριξη για πολλαπλούς τρόπους σύνδεσης, συμπεριλαμβανομένων από σημείο σε σημείο, τοποθεσίας σε τοποθεσία και απομακρυσμένης πρόσβασης
- Υποστήριξη για γεφυρωμένες ή δρομολογημένες διαμορφώσεις
- Υποστήριξη για δυναμική διέλευση DNS (DDNS) και NAT
- Υποστήριξη για IPv6
- Υποστήριξη για κρυπτογράφηση έως και 4096-bit
- Μια φιλική προς το χρήστη κονσόλα διαχείρισης για τη διαμόρφωση και τη διαχείριση συνδέσεων εικονικού ιδιωτικού δικτύου

Ως εφαρμογή λογισμικού ανοιχτού κώδικα, το SoftEther VPN είναι επίσης εξαιρετικά προσαρμόσιμη. Ο πηγαίος κώδικας για το λογισμικό είναι διαθέσιμος στο κοινό και μπορεί να τροποποιηθεί και να διανεμηθεί ελεύθερα. Αυτό επιτρέπει στους χρήστες να προσαρμόσουν το λογισμικό για να ανταποκρίνονται στις συγκεκριμένες ανάγκες τους και επίσης επιτρέπει στην κοινότητα ανάπτυξης να συνεισφέρει στο έργο και να βοηθήσει στη βελτίωση του λογισμικού.

Συνολικά, το SoftEther VPN είναι μια αξιόπιστη και πλούσια σε χαρακτηριστικά λύση VPN που είναι κατάλληλη για χρήση σε διάφορα σενάρια, συμπεριλαμβανομένης της απομακρυσμένης πρόσβασης, των συνδέσεων τοποθεσίας σε τοποθεσία και ως διακομιστής VPN γενικής χρήσης. Είναι ιδιαίτερα χρήσιμο για οργανισμούς ή άτομα με ποικίλο σύνολο συσκευών και λειτουργικών συστημάτων, καθώς είναι συμβατό με ένα ευρύ φάσμα πρωτοκόλλων και μπορεί να εκτελεστεί σε πολλές πλατφόρμες. Συγκεκριμένα στην δικιά μας περίπτωση ο λόγος που θα χρησιμοποιήσου με το συγκεκριμένο εικονικό ιδιωτικό δίκτυο είναι η απομακρυσμένη πρόσβαση. (Daiyuu, 2015)

3.3 ΠΡΩΤΟΚΟΛΛΟ KERBEROS

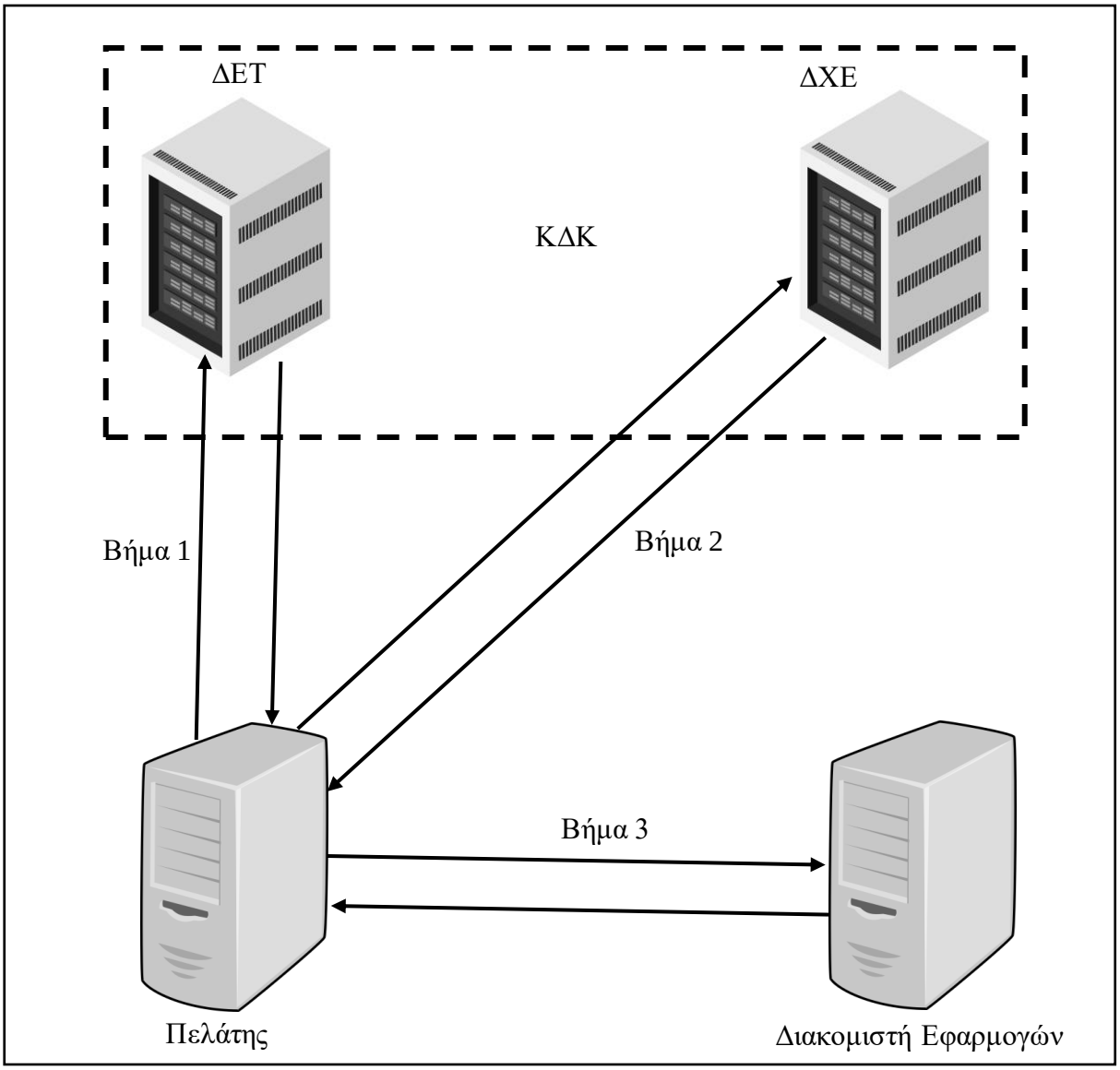
Σε αυτό το κεφάλαιο θα αναφερθούμε στη χρήση ενός πρωτοκόλλου που ονομάζεται Kerberos για τον έλεγχο ταυτότητας των χρηστών σε ένα δίκτυο υπολογιστών. Το πρωτόκολλο Kerberos βασίζεται σε ένα αξιόπιστο τρίτο μέρος, που ονομάζεται Κέντρο Διανομής Kerberos (ΚΔΚ), το οποίο χρησιμοποιείται για τον έλεγχο ταυτότητας χρηστών και διακομιστών. Το κείμενο αναφέρει επίσης ότι το Kerberos βασίζεται στη συμμετρική κρυπτογράφηση, η οποία είναι πιο αποτελεσματική από την κρυπτογράφηση δημόσιου κλειδιού, καθιστώντας το λιγότερο επιρρεπές σε επιθέσεις άρνησης υπηρεσίας. Επίσης το Kerberos χρησιμοποιείται ευρέως στα σύγχρονα δίκτυα υπολογιστών και διατίθεται με τα περισσότερα μεγάλα λειτουργικά συστήματα. Επιπλέον, η ασφάλεια του Kerberos έχει μελετηθεί και βελτιωθεί σε πολλά έργα, συμπεριλαμβανομένης της τελευταίας έκδοσης του Kerberos 5.

3.3.1 Επισκόπηση του πρωτόκολλου Kerberos

Το πρωτόκολλο Kerberos είναι ένας τρόπος για έναν πελάτη, όπως ένας χρήστης υπολογιστή, να αποδείξει την ταυτότητά του σε πολλούς διακομιστές σε ένα δίκτυο. Ο πελάτης έχει ένα μακροπρόθεσμο μυστικό κλειδί που είναι κοινόχρηστο με το σύστημα Kerberos, το οποίο δημιουργείται χρησιμοποιώντας τον κωδικό πρόσβασης του πελάτη. Εάν ο πελάτης θέλει να αποκτήσει πρόσβαση σε έναν διακομιστή εφαρμογών, η διαδικασία πραγματοποιείται σε τρία βήματα:

1. Ο πελάτης στέλνει ένα αίτημα στον διακομιστή ελέγχου ταυτότητας Kerberos (ΔΕΤ) για ένα ειδικό εισιτήριο που ονομάζεται "εισιτήριο χορήγησης εισιτηρίου". Το ΔΕΤ στέλνει πίσω ένα μήνυμα με το εισιτήριο και ένα νέο μυστικό κλειδί για να το χρησιμοποιήσει ο πελάτης με το Διακομιστή Χορήγησης Εισιτηρίων (ΔΧΕ).
2. Ο πελάτης στέλνει το εισιτήριο και ένα ειδικό μήνυμα που ονομάζεται ο "authenticator" στο ΔΧΕ, ζητώντας ένα εισιτήριο υπηρεσίας που θα χρησιμοποιηθεί για πρόσβαση στον διακομιστή εφαρμογών. Το ΔΧΕ στέλνει πίσω ένα μήνυμα με το δελτίο υπηρεσίας και ένα νέο μυστικό κλειδί για να το χρησιμοποιήσει ο πελάτης με τον διακομιστή εφαρμογών.
3. Ο πελάτης στέλνει το δελτίο υπηρεσίας και έναν άλλον έλεγχο ταυτότητας στον διακομιστή εφαρμογής, ζητώντας πρόσβαση σε μια συγκεκριμένη υπηρεσία. Εάν τα εισιτήρια και τα μυστικά κλειδιά του πελάτη είναι έγκυρα, ο διακομιστής εφαρμογής θα ελέγξει την ταυτότητα του πελάτη και θα παρέχει την υπηρεσία.

Αξίζει να σημειωθεί ότι η δεύτερη φάση, που είναι η ανταλλαγή μεταξύ του πελάτη και του ΔΧΕ, χρησιμοποιείται κάθε φορά που ένας χρήστης πραγματοποιεί έλεγχο ταυτότητας σε έναν νέο διακομιστή εφαρμογών, ενώ η τρίτη φάση χρησιμοποιείται κάθε φορά που ο χρήστης επαληθεύεται στον διακομιστή εφαρμογών.



Σχήμα 10. Επισκόπηση του πρωτόκολλου Kerberos

3.3.2 Που χρησιμοποιείται το πρωτόκολλο Kerberos

Το Kerberos δεν χρησιμοποιείται μόνο σε παραδοσιακά δίκτυα υπολογιστών, αλλά και σε ασύρματα δίκτυα, δίκτυα κινητής τηλεφωνίας και δίκτυα IPv6. Οι ερευνητές έχουν προτείνει τη χρήση του Kerberos σε ασύρματα δίκτυα, δίκτυα κινητής τηλεφωνίας και δίκτυα IPv6, χρησιμοποιώντας διαφορετικούς αλγόριθμους και τεχνικές κρυπτογράφησης όπως DES, 3DES, AES και SHA-1. Επιπλέον, η Nitin et al. πρότεινε τη χρήση εικόνων ως κωδικού πρόσβασης και υλοποίησε ένα σύστημα ελέγχου ταυτότητας που βασίζεται σε εικόνες χρησιμοποιώντας το πρωτόκολλο Kerberos. Επίσης το Kerberos έχει γίνει το πιο ευρέως διαδεδομένο σύστημα ελέγχου ταυτότητας και εξουσιοδότησης στα σύγχρονα δίκτυα υπολογιστών και αποστέλλεται με όλα τα μεγάλα λειτουργικά συστήματα υπολογιστών και μπορεί να είναι μια καθολική λύση για το κατανεμημένο πρόβλημα ελέγχου ταυτότητας και εξουσιοδότησης.

3.3.3 Αδυναμίες του πρωτόκολλου Kerberos

Παρακάτω περιγράφονται ορισμένα μειονεκτήματα του πρωτοκόλλου Kerberos:

- Το Kerberos είναι ευάλωτο σε επιθέσεις «εικασίας κωδικού πρόσβασης», όπου ένας εισβολέας μπορεί να προσπαθήσει να αποκρυπτογραφήσει μηνύματα επιχειρώντας επανειλημμένα να χρησιμοποιήσει ένα κλειδί που προέρχεται από τον κωδικό πρόσβασης ενός χρήστη.
- Το Κέντρο Διανομής Kerberos πρέπει να είναι πάντα διαθέσιμο για τη λειτουργία του συστήματος, διαφορετικά θα αντιμετωπίσει ένα πρόβλημα με ένα μόνο σημείο αστοχίας. Ωστόσο, αυτό μπορεί να μετριαστεί με τη χρήση πολλαπλών ΚΔΚ.
- Τα ρολόγια στους υπολογιστές που συμμετέχουν στο πρωτόκολλο πρέπει να είναι συγχρονισμένα, διαφορετικά ο έλεγχος ταυτότητας θα αποτύχει. Αυτό γίνεται συνήθως χρησιμοποιώντας δαίμονες πρωτοκόλλου ώρας δικτύου για να διατηρούνται τα ρολόγια συγχρονισμένα.
- Δεν υπάρχουν τυπικές οδηγίες για τον τρόπο διαχείρισης του πρωτοκόλλου Kerberos και διαφορετικές υλοποιήσεις διακομιστή ενδέχεται να έχουν διαφορετικές μεθόδους. (El-Emam Eman, 2009)

4. ΕΛΕΓΧΟΣ ΚΑΙ ΔΙΑΧΕΙΡΗΣΗ ΔΙΚΤΥΟΥ

Για τον έλεγχο και τη διαχείριση του δικτύου μας με λογισμικό ανοιχτού κώδικα που θα χρησιμοποιήσουμε είναι το Εικονικό Περιβάλλον Proxmox. Το Proxmox είναι βασισμένο στη διανομή του Debian Linux (που ονομάζεται επίσης υπερεπόπτης ή ελεγκτής εικονικής μηχανής) για εικονικούς διακομιστές. Επιτρέπει ένα χρήστη να εγκαταστήσει διαφορετικά λειτουργικά συστήματα (για παράδειγμα, Windows, Linux, Unix, και άλλα) σε έναν μόνο υπολογιστή ή σε ένα σύμπλεγμα που χτίστηκε από την ομαδοποίηση υπολογιστών μαζί. Αποτελείται από ισχυρές εικονικές μηχανές που βασίζονται στον πυρήνα και ελαφρύ OpenVZ κοντέινερ ως εναλλακτική λύση.

Παρακάτω συνοψίζονται τα κύρια χαρακτηριστικά του Εικονικού Περιβάλλοντος Proxmox ως εξής:

- **Open source**: είναι πλήρως ανοιχτού κώδικα, που σημαίνει ότι μπορείτε ελεύθερα να δείτε, να αλλάξετε, και να αφαιρέσετε πηγαίο κώδικα, και να διανέμουν τη δική σας έκδοση για όσο διάστημα είστε συμβατό με την άδεια.
- **Ζωντανή μεταγωγή**: αυτό επιτρέπει τη μετακίνηση μιας τρέχουσας εικονικής μηχανής από ένα φυσικό διακομιστή σε ένα άλλο χωρίς διακοπή λειτουργίας.
- **Υψηλή διαθεσιμότητα**: στη λειτουργία συμπλέγματος Proxmox, όταν ένας κόμβος αποτύχει, τότε οι υπόλοιπες εικονικές μηχανές θα μετακινηθούν σε έναν υγιή κόμβο για να βεβαιωθούν υπάρχει ελάχιστη διακοπή υπηρεσίας.
- **Γεφυρωμένη δικτύωση**: το Proxmox ΕΠ επιτρέπει σε έναν χρήστη να δημιουργήσει ένα ιδιωτικό δίκτυο μεταξύ των εικονικών μηχανών. Οι επιλογές VLAN είναι επίσης διαθέσιμες.
- **Δυναμική αποθήκευση**: ένα ευρύ φάσμα των επιλογών αποθήκευσης είναι διαθέσιμο, συμπεριλαμβανομένου τοπικές και βασισμένες στο δίκτυο τεχνολογίες αποθήκευσης όπως το σύστημα αρχείων Cluster και το σύστημα αρχείων CEPH.
- **Προγραμματισμένη δημιουργία αντιγράφων ασφαλείας**: μια φιλική προς τον χρήστη διεπαφή παρέχεται στους χρήστες, έτσι ώστε να μπορούν να ορίσουν μέχρι και τη δική τους στρατηγική δημιουργίας αντιγράφων ασφαλείας. Τα αρχεία αντιγράφων ασφαλείας μπορούν να αποθηκευτούν τοπικά ή σε οποιαδήποτε υποστηριζόμενη επιλογή αποθήκευσης που έχετε ρυθμίσει.

- **Εργαλείο γραμμής εντολών (CLI):** το Proxmox VE παρέχει διαφορετική διαχείριση που επιτρέπει στους χρήστες να έχουν πρόσβαση στο δοχείο εικονικής μηχανής, να διαχειρίζονται τους πόρους που διατίθενται και ούτω καθεξής. (Cheng, 2014)

4.1 ΥΨΗΛΗ ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Έχουμε προσέξει ότι υπάρχει ένα μόνο σημείο αποτυχίας, θα μπορούσαμε απλά να προσθέσουμε έναν ίδιο διακομιστή για να το λύσει. Ακόμα και αν εμείς χειροκίνητα κάναμε εγκατάσταση το ίδιο λογισμικό σε δυο πανομοιότυπα μηχανήματα, πως θα μπορούσαμε να συγχρονίσουμε τα δεδομένα μεταξύ τους? Δεν είναι ιδανικό να αντιγράψουμε νέα δεδομένα στον διακομιστή αντιγράφων ασφάλειας με μη αυτόματο τρόπο. Γι' αυτό δημιουργήθηκε η Υψηλή Διαθεσιμότητα

Για να καταλάβουμε τι σημαίνει διαθεσιμότητα θα πρέπει να ασχοληθούμε με τον τύπο που υπολογίζεται η διαθεσιμότητα. Πρέπει να διαιρέσουμε την αφαίρεση της **Διάρκεια διακοπής λειτουργίας** από τον **Αναμενόμενο χρόνο λειτουργίας** με τον **Αναμενόμενο χρόνο λειτουργίας** και μετά να το πολλαπλασιάσουμε με το 100. Η Διαθεσιμότητα εκφράζεται επι τις εκατό από το χρόνο λειτουργίας σε ένα χρόνο. Ο τύπος είναι ο εξής:

Διαθεσιμότητα (%) = 10* **(Αναμενόμενος χρόνος λειτουργίας - Διάρκεια χρόνου διακοπής λειτουργίας) / Αναμενόμενος χρόνος λειτουργίας**

Οι όροι που χρησιμοποιούνται στον τύπο είναι οι ακόλουθοι:

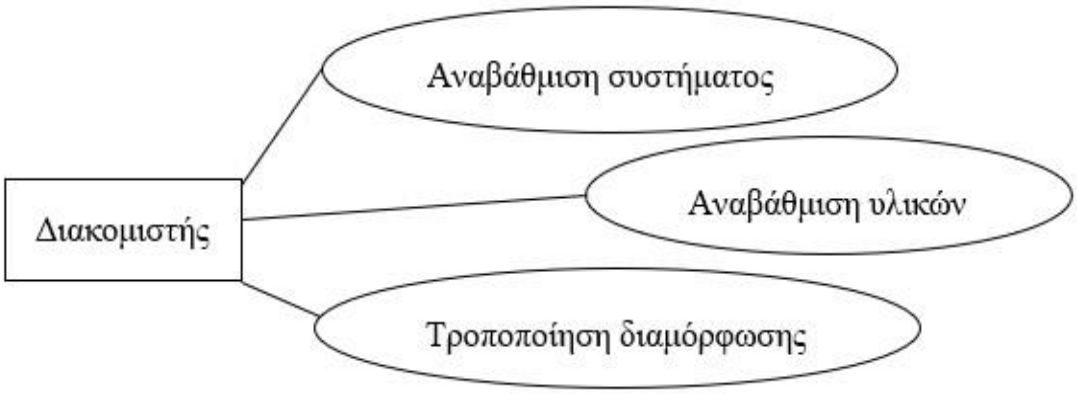
- **Διάρκεια διακοπής λειτουργίας**: Αυτός αναφέρετε για των αριθμό ωρών που το σύστημα δεν θα είναι διαθέσιμο
- **Αναμενόμενος χρόνος λειτουργίας:** Αυτός αναφέρεται στο αναμενόμενο διαθέσιμο σύστημα, κανονικά περιμένουμε το σύστημα να είναι διαθέσιμο 365*24*7 ώρες.

Για παράδειγμα, εάν ένας διακομιστής αντιμετωπίζει 100, 200 και 300 διακοπές λειτουργίας κάθε μήνα, καθένας από τους οποίους διαρκεί τέσσερις ώρες, θα έχουμε τους ακόλουθους αριθμούς διαθεσιμότητας:

Διάρκεια διακοπής λειτουργίας	**Αναμενόμενο χρόνο λειτουργίας**	**Διαθεσιμότητα**
100 * 4 = 400 ώρες	8760 ώρες	95%
200 * 4 = 800 ώρες	8760 ώρες	91%
300 * 4 = 1200 ώρες	8760 ώρες	86%

Υπάρχουν δυο τύποι διακοπής λειτουργίας:

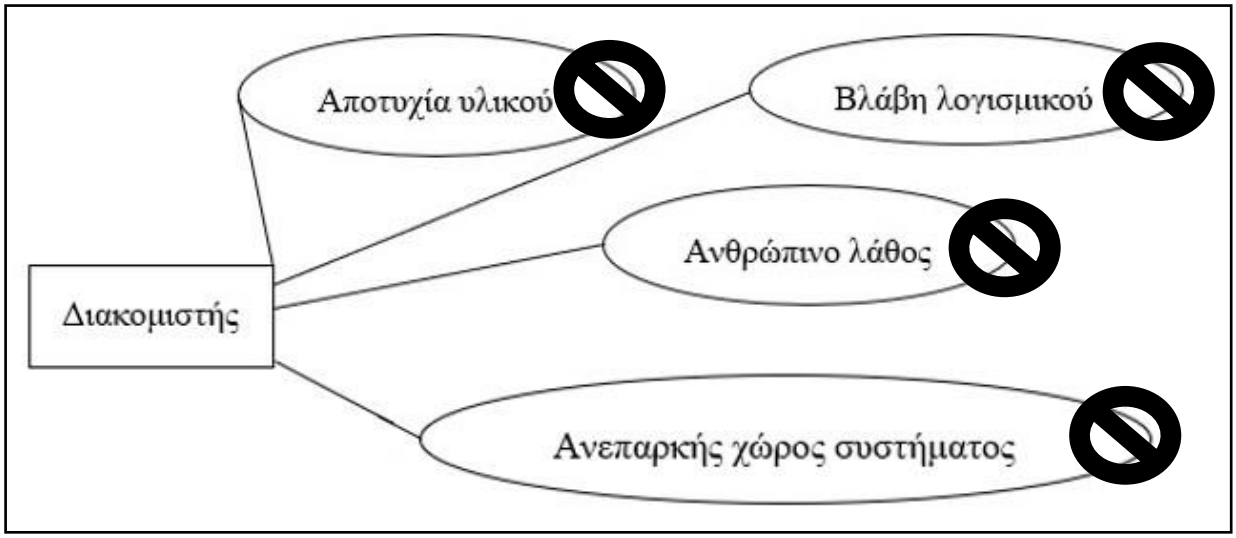
- **Προγραμματισμένος χρόνος διακοπής λειτουργίας:** Σε αυτό τον τύπο χρόνου διακοπής λειτουργίας κανονικά, πρέπει να βρούμε χρόνο για τις ενημερώσεις πακέτων του διακομιστή, αναβαθμίσεις του υλικού και του συστήματος, και τροποποίηση της διαμόρφωσης. Αυτός ο τύπος χρόνου διακοπής λειτουργίας είναι αναπόφευκτος, ο οποίος θα πρέπει να μην είναι βλαβερός, μα αυξάνει τη σταθερότητα και τη λειτουργικότητα του διακομιστή. Ο συγκεκριμένος χρόνος διακοπής είναι υπό έλεγχο και η διάρκεια του είναι σχετικά σύντομη. Το παρακάτω διάγραμμα επεξηγεί το χρόνο διακοπής λειτουργίας:



Σχήμα 11. Προγραμματισμένος χρόνος διακοπής λειτουργίας

- **Μη προγραμματισμένος χρόνος διακοπής λειτουργίας:** Αυτός τώρα ο χρόνος διακοπής λειτουργίας περιλαμβάνει αστοχίες υλικού, σφάλματα λογισμικού, ανθρώπινα λάθη και άλλα. Η διάρκεια του μη προγραμματισμένου χρόνου διακοπής λειτουργίας είναι αόριστη, άλλα σίγουρα είναι πολύ περισσότερη από έναν προγραμματισμένο. Κάθε μη προγραμματισμένος χρόνος διακοπής λειτουργίας πρέπει να λαμβάνεται υπόψη πολύ σοβαρά και να αποφεύγεται κατά πάσα πιθανότητα.

Αυτός ο χρόνος διακοπής εξηγείται πιο ξεκάθαρα στο παρακάτω διάγραμμα:



Σχήμα 12. Μη προγραμματισμένος χρόνος διακοπής λειτουργίας

Μιλήσαμε για προγραμματισμένο και μη προγραμματισμένο χρόνο διακοπής λειτουργίας και μπορούμε να καταλάβουμε ότι ο χρόνος διακοπής λειτουργίας είναι κακό πράγμα.

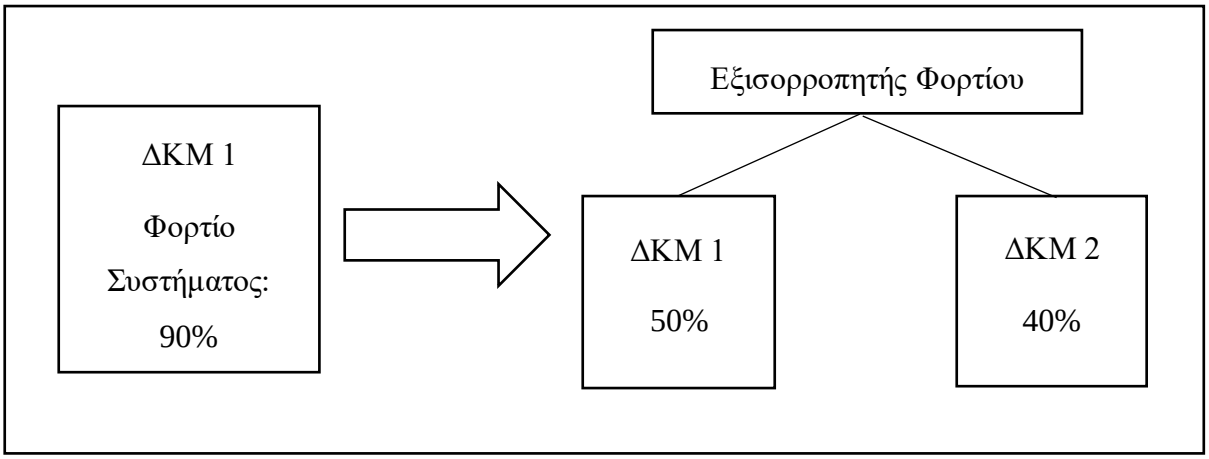
Οι ακόλουθες είναι οι αρνητικές επιπτώσεις που θα προκληθούν λόγω του χρόνου διακοπής λειτουργίας:

- Απώλεια εμπιστοσύνης πελατών
- Ο χρόνος αποκατάστασης του συστήματος είναι μεγαλύτερος από τον αναμενόμενο
- Μείωση της παραγωγικότητας του προσωπικού

4.1.1 Στρατηγικές επίτευξης Υψηλής Διαθεσιμότητας

Αρχικά αυτό που πρέπει να κάνουμε είναι να χτίσουμε ανάλογες υποδομές για να ξεφύγουμε από αυτές τις διακοπές. Οι ακόλουθες στρατηγικές θα μας βοηθήσουν να επιτύχουμε το στόχο μας:

- **Εξισορρόπηση φορτίου:** Εάν ο χρόνος διακοπής λειτουργίας οφείλεται σε ανεπαρκείς πόρους του συστήματος, τότε είναι απαραίτητη η προσθήκη ενός νέου διακομιστή με έναν εξισορροπητή φορτίου ώστε να αυξήσουμε το επίπεδο διαθεσιμότητας. Το πλεονέκτημα της εξισορρόπησης φορτίου είναι ότι δεν απαιτεί πανομοιότυπες μηχανές διακομιστή. Με τη βοήθεια αυτής της τεχνικής, μπορούμε να μειώσουμε το φορτίο του συστήματος που για παράδειγμα είναι 90% σε 50%. Έτσι, αυτό βοηθά στη μείωση της πιθανότητας αποτυχίας του συστήματος λόγω ανεπαρκών πόρων.

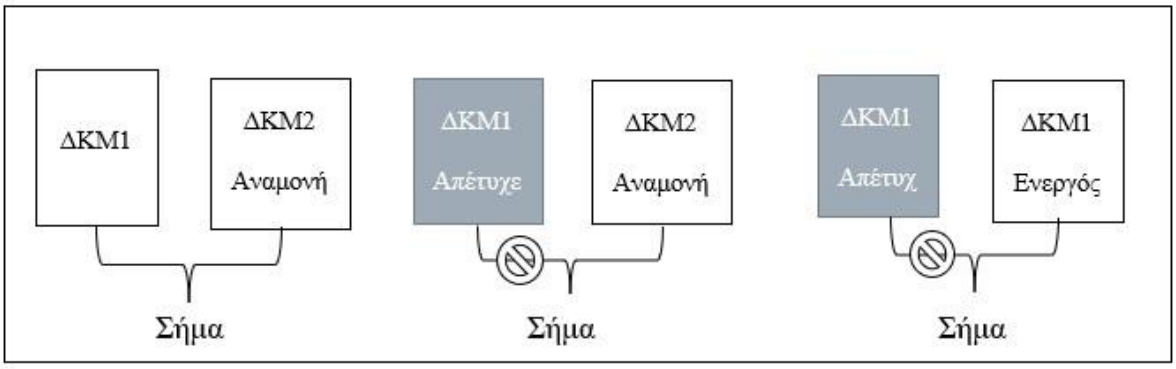


Σχήμα 13. Εξισορρόπηση Φορτίου

Εφόσον εξηγήσαμε την εξισορρόπηση φορτίου και τη λειτουργία της, μπορούμε να επιστρέψουμε πίσω στον αντίστροφο διακομιστή μεσολάβησης. Οι δυο αυτές λειτουργίες είναι πανομοιότυπες, απλώς εμείς προτιμάμε τον αντίστροφο διακομιστή μεσολάβησης και συγκεκριμένα τον Squid γιατί είναι ανοιχτού λογισμικού και εύκολο στην διαμόρφωση.

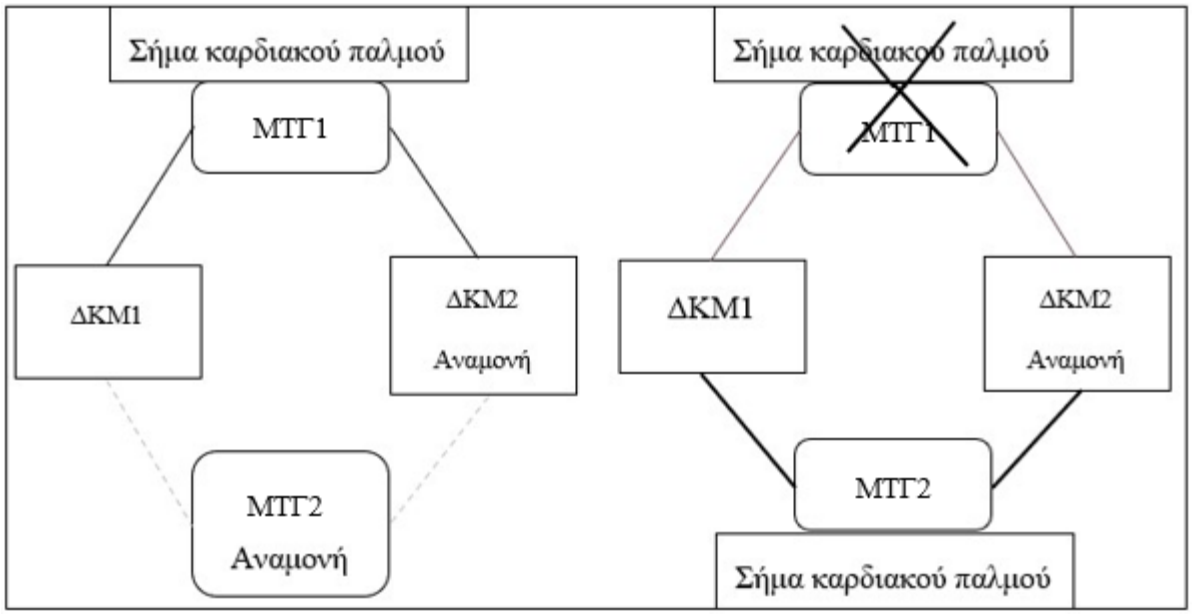
- **Μηχανισμός ανακατεύθυνση:** Αυτή η λειτουργία είναι παρόμοια με την εξισορρόπηση φορτίου, αλλά απαιτεί ίδιο διακομιστή μηχάνημα ως αναμονή. Κάντε εικόνα πως έχουμε δυο πανομοιότυπους διακομιστές και υπάρχει ένας καρδιακός παλμός μεταξύ των δύο διακομιστών για να προσδιοριστεί εάν κάποιο από τα συστήματα έχει αποτύχει ή όχι. Τα ακόλουθα σημεία εξηγούν πώς λειτουργεί:
    - Αρχικά υπάρχει ένα σήμα που ονομάζεται «καρδιακός παλμός» μεταξύ Διακομιστή 1 και Διακομιστή 2, ο οποίος Διακομιστής 2 είναι σε αναμονή
    - Όταν ο Διακομιστής 1 αποτύχει, το σήμα « καρδιακού παλμού» από τον Διακομιστή 1 έχει χαθεί και ειδοποιεί τον Διακομιστή2
    - Ο Διακομιστής 2 παίρνει τον έλεγχο των υποχρεώσεων του Διακομιστή1 και γίνεται ενεργός.

Παρακάτω εξηγείται και με ένα σχήμα:



Σχήμα 14. Μηχανισμός Ανακατεύθυνσης

- **Σήμα καρδιακού παλμού:** Ο συγκεκριμένος είναι βασικός όρος για ένα περιβάλλον με Υψηλή Διαθεσιμότητα. Χρησιμοποιείται για να ελέγχει τη διαθεσιμότητα κάθε μέλους του συμπλέγματος και να εκτελεί ορισμένες ενέργειες ανάλογα με τις αλλαγές της κατάστασης του συστήματος. Υπάρχουν μερικά είδη λειτουργειών που απαιτείται για την ανίχνευση ενός τέτοιου προβλήματος. Για παράδειγμα μπορούμε να ρυθμίσουμε τις εξής δύο καταστάσεις με το σήμα καρδιακού παλμού:
    - **Πρώτη συνθήκη:** Τα πακέτα αποστέλλονται μεταξύ ΔΚΜ1 και ΔΚΜ2, προκειμένου να ελεγχθεί η τρέχουσα κατάσταση του ΔΚΜ1. Αν ο ΔΚΜ1 δεν είναι διαθέσιμος, το σήμα του καρδιακού παλμού θα επιστρέψει ένα αποτυχημένο αποτέλεσμα και θα ενεργοποιήσει τις τρέχουσες υπηρεσίες του ΔΚΜ1 στον ΔΚΜ2. Αυτή η δοκιμή γίνεται όταν θέλουμε να διαπιστώσουμε εάν η σύνδεση μεταξύ ΔΚΜ1 και ΔΚΜ2 λειτουργεί σωστά.
    - **Δεύτερη συνθήκη:** Εκτελείται λειτουργία ping ανάμεσα στους ΔΚΜ1 και ΔΚΜ2 σε μία εξωτερική διεύθυνση IP. Αυτό εγγυάται ότι η σύνδεση και των δύο διακομιστών σε ένα εξωτερικό δίκτυο είναι λειτουργική. Εάν μία από τις συνθήκες εμφανίζει ψευδής κατάσταση, τότε ο αντίστοιχος κόμβος διακομιστή είτε θα τερματιστεί είτε θα αποσυνδεθεί και θα μεταφέρει τις εικονικές μηχανές στον άλλον κόμβο.
- **Πλεονασμός:** Έχει παρατηρηθεί ότι υπάρχει πρόβλημα με τη λειτουργία ανακατεύθυνσης και τη σύνδεση μεταξύ ΔΚΜ1 και ΔΚΜ2, ο πλεονασμός βελτιώνει την απλή μέθοδο ανακατεύθυνσης. Η μέθοδος ανακατεύθυνσης δεν εφαρμόζεται μόνο σε επίπεδο διακομιστή αλλά και σε επίπεδο υποδομής. Παρακάτω έχουμε ένα διάγραμμα για την καλύτερη κατανόηση:



Σχήμα 15. Πλεονασμός

Υπάρχει ένας μεταγωγέας αναμονής (ΜΤΓ2) ανάμεσα σε δύο διακομιστές. Όταν ο μεταγωγέας (ΜΤΓ1) αποτυγχάνει, οι ΔΚΜ1 και ΔΚΜ2 θα διαλέξουν το ΜΤΓ2 ως τη νέα διαδρομή για την αποστολή του σήματος καρδιακού παλμού. Ώστε, να μη χρειαστεί να απενεργοποιήσουμε έναν κόμβο διακομιστή κατά λάθος. (Cheng, 2014)

4.2 ΣΥΜΠΛΕΓΜΑ ΚΑΙ ΣΥΣΤΗΜΑ ΑΡΧΕΙΩΝ

Τώρα, έχουμε κάποια ιδέα για το πώς να μετρήσουμε το επίπεδο διαθεσιμότητας για έναν διακομιστή. Η αύξηση της διαθεσιμότητας είναι πολύ σημαντική για εμάς. Είναι δυνατόν για το Proxmox να ασχοληθεί με αυτό αλλά μόνο σε λειτουργία συμπλέγματος (cluster). Η βασική διαφορά μεταξύ μεμονωμένης παρουσίας έναντι συμπλεγμάτων στο Proxmox είναι η εξής:

Προϊόν	**Proxmox ΕΠ**	**Proxmox ΕΠ Σύμπλεγμα**
Αριθμός κόμβων	1	2(ελάχιστο) 3(προτεινόμενο)
Δίσκος απαρτίας	Όχι	Ναι
Αποθηκευτικός χώρος	Τοπικός	Κοινόχρηστος
Υψηλή Διαθεσιμότητα	Όχι	Ναι

Εμείς στη συνέχεια πρέπει να παρέχουμε κοινόχρηστο χώρο αποθήκευσης ώστε το σύμπλεγμα να διατηρεί τα δεδομένα των εικονικών μηχανών. Στη διαμόρφωσή μας, θα χρησιμοποιούμε ένα πακέτο που ονομάζεται DRBD, το οποίο μας επιτρέπει να χρησιμοποιούμε τοπική αποθήκευση και από τους δύο διακομιστές για να σχηματίσουν έναν κοινόχρηστο χώρο αποθήκευσης. Ο συγχρονισμός δεδομένων θα το διαχειρίζεται αυτόματα το πακέτο DRBD. Επομένως, δεν χρειάζεται να αγοράσουμε επιπλέον αποθηκευτικό χώρο για το δίκτυο μας.

4.2.1 Εισαγωγή στο DRBD

Το DRBD είναι μια σύντομη φόρμα για Συσκευή Κατανεμημένων Αναδιπλασιασμένων Μπλοκ, προορίζεται για χρήση κάτω από περιβάλλον με Υψηλή Διαθεσιμότητα. Το DRBD παρέχει υψηλή διαθεσιμότητα αντικατοπτρίζοντας το υπάρχον σύστημα σε άλλο μηχάνημα, συμπεριλαμβανομένης της αποθήκευσης δίσκου, της κατάστασης της κάρτας δικτύου, και υπηρεσίες που λειτουργούν στο υπάρχον σύστημα. Έτσι, εάν το υπάρχον σύστημα είναι εκτός υπηρεσία, μπορούμε να μεταβούμε αμέσως στο εφεδρικό σύστημα για να αποφύγουμε τη διακοπή της υπηρεσίας.

Εκτός από την Υψηλή Διαθεσιμότητα, υπάρχουν μερικές ακόμη λειτουργίες που παρέχονται από τη λειτουργία συμπλέγματος Proxmox, αλλά το πιο σημαντικό είναι η ζωντανή μεταγωγή. Σε αντίθεση με την κανονική μεταγωγή, σε ένα Proxmox cluster, η μετεγκατάσταση μπορεί να επιτευχθεί χωρίς να τερματιστεί η λειτουργία της εικονικής μηχανής. Μια τέτοια προσέγγιση ονομάζεται ζωντανή μεταγωγή, η οποία μειώνει σημαντικά τον χρόνο διακοπής λειτουργίας κάθε εικονική μηχανή.

4.2.2 Απαιτήσεις συστήματος για το σύμπλεγμα Proxmox

Για να χρησιμοποιήσουμε αυτήν τη λειτουργία, έχουμε να προετοιμάσουμε πρώτα τουλάχιστον δύο μηχανήματα που είναι εγκατεστημένα με το Proxmox VE. Εφόσον εμείς θέλουμε μια βασική πλατφόρμα δοκιμών, οι ελάχιστες απαιτήσεις για τις μηχανές μας;

Οι ελάχιστες απαιτήσεις συστήματος όπως αναφέρονται στον ιστότοπο της Proxmox είναι οι εξής:

- CPU: 64-bit (Intel EMT64 ή AMD64)
- CPU/Mainboard με δυνατότητα Intel VT/AMD-V
- Τουλάχιστον 1 GB RAM
- Σκληρός δίσκος
- Μία κάρτα δικτύου

Ωστόσο, θα συνιστούσα να έχετε τουλάχιστον 2 GB μνήμης εφόσον θέλουμε να δοκιμάσουμε τη ζωντανή μεταγωγή στην πλατφόρμα των Windows.

Για περιβάλλον παραγωγής, το ακόλουθο υλικό προτείνεται από την Proxmox:

- Η CPU πρέπει να υποστηρίζει 64-bit (Intel EMT64 ή AMD64), CPU πολλαπλών πυρήνων συνιστάται και απαιτείται CPU/mainboard με δυνατότητα Intel VT/AMD-V
- Τα 8 GB RAM είναι καλά. όσο περισσότεροι τόσο το καλύτερο
- Οι γρήγοροι σκληροί δίσκοι, όπως οι δίσκοι SAS με 15k rpm θα δώσουν το καλύτερο αποτελέσματα
- Τουλάχιστον δύο κάρτες δικτύου ανά διακομιστή Proxmox
- Σε λειτουργία συμπλέγματος, χρειαζόμαστε τουλάχιστον δύο φυσικούς διακομιστές που να πληρούν τις απαιτήσεις που αναφέρθηκαν προηγουμένως, ένα δίκτυο για τη σύνδεση και των δύο, και κοινόχρηστο χώρο αποθήκευσης για τη διατήρηση δεδομένων εικονικού δίσκου

Ανεξάρτητα από το αν προτιμάτε τις ελάχιστες ή προτεινόμενες απαιτήσεις συστήματος, πρέπει επίσης να προετοιμάσετε τα πράγματα που αναφέρονται στα ακόλουθα σημεία:

- Απαιτείται τουλάχιστον ένας διακόπτης με δυνατότητα πολλαπλής εκπομπής.
- Απαιτείται κοινόχρηστος χώρος αποθήκευσης που είναι προσβάσιμος και από τους δύο διακομιστές Proxmox ένας δίσκος απαρτίας εάν έχουμε μόνο δύο κόμβους

διακομιστή. Ένας δίσκος απαρτίας χρησιμοποιείται για να προσθέσουμε μια επιπλέον ψήφο μέσα στο σύμπλεγμα.
- Απαιτούνται συσκευές περίφραξης σε όλους τους κόμβους του διακομιστή, μπορεί να βασίζεται σε δίκτυο ή κόμβος διακομιστή που βασίζεται σε ενέργεια.

Προσωπικά, θα δημιουργήσω το δικό μου σύμπλεγμα Proxmox με τρεις μηχανές. Θα μειώσει την πιθανότητα να λάβουμε σφάλματα με το ίδιο το σύμπλεγμα, ειδικά το πρόβλημα που προκαλείται από την έλλειψη αρκετών ψήφων σχετικά με το λειτουργίες του συμπλέγματος. Αυτό θα μπλοκάρει οποιαδήποτε δραστηριότητα που σχετίζεται με το σύμπλεγμα.

4.2.3 Κοινόχρηστος αποθηκευτικός χώρος

Για να εξασφαλίσουμε Υψηλή Διαθεσιμότητα, δεν πρέπει να έχουμε ούτε ένα σημείο αστοχίας, που σημαίνει ότι κάθε εικονική μηχανή θα πρέπει να είναι προσβάσιμη από πολλούς διακομιστές Proxmox. Αν ένας διακομιστής Proxmox έχει αποτύχει, θα πρέπει να υπάρχει ένας άλλος διακομιστής για να χειριστεί τα ανάλογα VM. Συνεπώς, δεν πρέπει να αποθηκεύουμε τα VM μας σε τοπικό χώρο αποθήκευσης, ενώ αντιθέτως ο κοινόχρηστος χώρος αποθήκευσης είναι κατάλληλος για οποιοδήποτε δίκτυο. Σε ένα μοντέρνο τεχνολογικό περιβάλλον, η αποθήκευση δικτύου γίνεται συνήθως κοινόχρηστα, γεγονός που οδήγησε στη δημιουργία δυο όρων, την αποθήκευση δικτύου περιοχής (SAN) και τον αποθηκευτικό χώρο συνδεδεμένο με το δίκτυο (NAS).

Βασικά, τα δεδομένα μέσα σε ένα VM μπορούν να αποθηκευτούν τόσο σε SAN όσο και σε NAS. Ωστόσο, για καλύτερη απόδοση και σταθερότητα, προτείνεται η αποθήκευση δεδομένων να γίνετε σε κάτι παρόμοιο με το SAN.

Εκτός από τους τύπους αποθήκευσης που αναφέρθηκαν προηγουμένως, το Proxmox υποστηρίζει επίσης συστήματα αρχείου. Επομένως έχουμε τις ακόλουθες επιλογές αποθήκευσης διαθέσιμες στο Proxmox:

- Ευρετήριο
- Λογικό διαχειριστή τόμου
- Στόχος iSCSI
- Μερίδιο NFS
- Σύστημα αρχείων Cluster
- Σύστημα αρχείων Ceph

4.2.4 Το σύστημα αρχείων Ceph

Εμείς θα επικεντρωθούμε στο σύστημα αρχείων Ceph γιατί είναι ένα κατανεμημένο σύστημα αρχείων που παρέχει αποθήκευση σε υψηλό επίπεδο (petabyte) αλλά είναι περισσότερο επικεντρωμένο στην εξάλειψη ενός μόνο σημείου αποτυχίας. Για να διασφαλιστεί η Υψηλή Διαθεσιμότητα, δημιουργούνται αντίγραφα σε άλλους κόμβους αποθήκευσης.

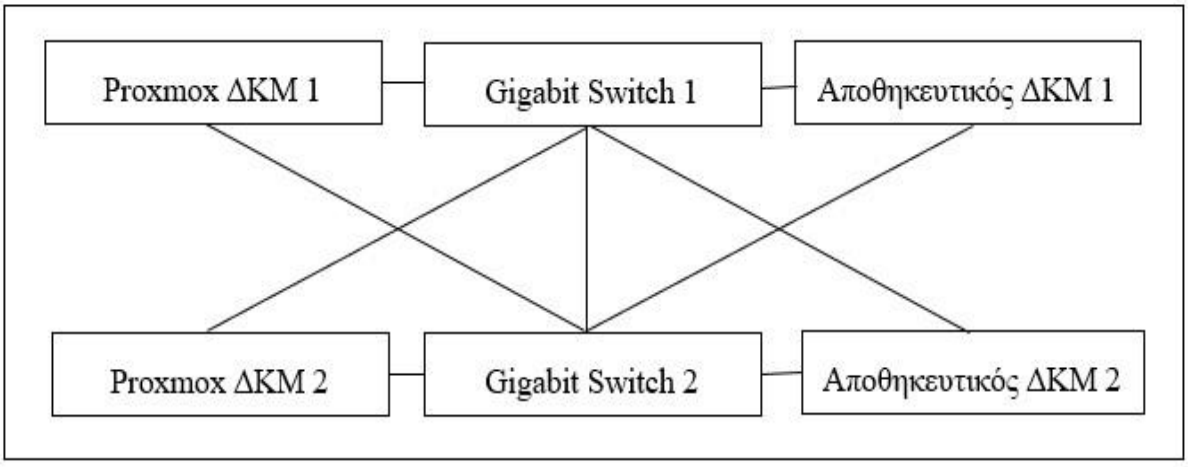
Τα παρακάτω είναι τα πλεονεκτήματα του Ceph:

- Υπάρχει ένας ενσωματωμένος διακομιστής CEPH για το Proxmox. Επομένως, είναι ευκολότερο να εφαρμοστεί
- Τα μεταδεδομένα μπορούν να αποθηκευτούν σε έναν SSD για καλύτερες επιδόσεις
- Έχει την ικανότητα της αυτοίασης, η οποία παρέχεται από τον αλγόριθμο CRUSH

4.2.5 Αξιόπιστο δίκτυο

Με βάση τις ρυθμίσεις μας, σχεδόν όλα τα στοιχεία εκτελούνται μέσω δικτύου. Επομένως ένα σταθερό και γρήγορο δίκτυο είναι απαραίτητο. Η καλύτερη επιλογή είναι να χωρίσουμε το δίκτυο για αναπαραγωγή, αποθήκευση και διαχείριση δεδομένων. Για ένα γρήγορο δίκτυο θα επιλέξουμε μόνο gigabit Ethernet ή ταχύτερη έκδοση. Αυτό σημαίνει ότι όλοι οι διακομιστές θα πρέπει να έχουν κάρτες gigabit Ethernet στο τοπικό δίκτυο. Επιπλέον, όλοι οι κόμβοι που τρέχουν θα πρέπει να βρίσκονται στο ίδιο υποδίκτυο για να αποφευχθεί η εμπλοκή περαιτέρω διαδικασιών δρομολόγησης

Για τη σταθερότητα του δικτύου, πρέπει να κατασκευάσουμε ένα δίκτυο με Υψηλή Διαθεσιμότητα, όπως φαίνεται στο παρακάτω διάγραμμα:



Σχήμα 16. Τύπος αξιόπιστου δικτύου για Υψηλή Διαθεσιμότητα

4.2.6 Δίσκος απαρτίας

Ο δίσκος απαρτίας είναι ένας μικρός κοινόχρηστος αποθηκευτικός χώρος σε ένα σχέδιο συμπλέγματος και είναι απαραίτητος για ένα σύμπλεγμα Proxmox δυο ή περισσότερων κόμβων για να λειτουργεί σωστά. Εφόσον έχουμε μόνο δύο κόμβους μέλη σε ένα σύμπλεγμα, θα προκαλέσει προβλήματα υπερφόρτωσης όταν ένας από τους κόμβους είναι εκτός λειτουργίας. Στο δικό μας παράδειγμα θα χρησιμοποιήσουμε έναν δίσκο απαρτίας για να λύσουμε το πρόβλημα μας. Οι λειτουργίες ενός τέτοιου δίσκου παρατίθενται ως εξής:

- **Αποφασιστικότητα παλμών:** Ο κόμβος ενημερώνει έναν δίσκο απαρτίας και αλλάζει τη χρονική σήμανση, η οποία χρησιμοποιείται για να αποφασίσει εάν ο κόμβος είναι σε αναστολή ή όχι. Εάν υπάρχουν ορισμένες ελλείψεις κατά τη διάρκεια της ευρετικής δοκιμής, ο κόμβος δηλώνεται ως εκτός σύνδεσης.
- **Εκλογή αρχηγού:** Αυτή είναι μια σημαντική διαδικασία για ένα σύμπλεγμα, γιατί μόνο ένας κόμβος μπορεί να εκλεγεί ως αρχηγός. Η διαδικασία της ψηφοφορίας είναι απλή, ο κόμβος με το χαμηλότερο αναγνωριστικό κόμβου κερδίζει.

Η διαδικασία του δίσκου απαρτίας μπορεί να συνοψιστεί ως εξής:

- Ο διαχειριστής του συμπλέγματος πιστεύει ότι ο κόμβος είναι συνδεδεμένος.
- Αυτός ο κόμβος έχει κάνει αρκετές συνεχόμενες, έγκαιρες εγγραφές στο δίσκο απαρτίας.
- Ο κόμβος έχει αρκετά υψηλή βαθμολογία για να θεωρηθεί ότι είναι ενεργός

(Cheng, 2014)

5. ΕΦΑΡΜΟΓΗ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

Το δίκτυο που δημιουργείται συνδυάζοντας όλες αυτές τις τεχνολογίες, στρατηγικές, πρωτοκολλά και εξοπλισμό, στην πραγματικότητα υπάρχει στο «Μαμάτσειο» Γενικό Νοσοκομείο Κοζάνης.

Το καλωδιακό δίκτυο καλύπτει όλες τις σύγχρονες ανάγκες και ακολουθεί τα παρακάτω πρότυπα όπως επίσης και τους κανονισμούς του Ελληνικού κράτους περί «Εσωτερικών Ηλεκτρικών Εγκαταστάσεων»

Το δίκτυο ικανοποιεί ανάγκες μετάδοσης:

- Φωνής
- Δεδομένων
- Εικόνας
- Σημάτων ελέγχου

Και καλύπτει τα παρακάτω πρωτόκολλα επικοινωνίας Υψηλής και Χαμηλής ταχύτητας:

- ISDN BRI S/T/O.
- RS 232 C/E για NCR, Hewlett Packard, Honeywell, Prime.
- IBM Twinax, Coax etc.
- RS 232 C Asychronous/Synchronous
- RS 422,RS 423.
- Arcnet & Fast Arcnet (2,5 &25Mbits/sec).
- Ethernet 10-Base (10 Mbits/sec).
- Fast Ethernet 100-Base T ή 100V6 (100 Mbits/sec).
- Gigabit Ethernet 1000-Base T (1000 Mbits/sec).
- Οπτικό Ethernet 1000-Base Fx (0.5-1 Ghz).
- ATM (56/155/622 Mbps).
- Token Ring (4/16 Mbits/sec).

Το καλωδιακό δίκτυο αποτελεί "Ανοικτό Καλωδιακό Σύστημα" και εξασφαλίζει την διασύνδεση οποιασδήποτε εφαρμογής οποιουδήποτε κατασκευαστή τόσο για τις τωρινές ανάγκες όσο και για τις μελλοντικές.

Για το λόγο αυτό διαθέτει όλες τις σχετικές προδιαγραφές της εφαρμοσμένης σύγχρονης τεχνολογίας με αυστηρά κριτήρια ποιότητας ώστε από τα επιμέρους στοιχεία να εξασφαλίζονται :

- Υψηλές προδιαγραφές εγκατάστασης
- Ευελιξία σε διασυνδέσεις και επεκτάσεις (VLAN, LAN, WAN)
- Μακροβιότητα
- Κεντρική διαχείριση
- Υποστήριξη όλων των συστημάτων και νέων τεχνολογιών (έως 1000 Mbits/sec)
- Ανεξαρτησία από χρησιμοποιούμενο Τερματικό Εξοπλισμό (Η/Υ, Printers, Fax, κλπ.)

Τα υλικά είναι καινούρια και διαθέτουν εγγύηση καλής λειτουργίας. Οι παθητικοί τερματισμοί διαθέτουν εγγύηση έως είκοσι πέντε (25) χρόνια έτσι ώστε το δίκτυο να αποκτήσει πρόσθετη αξία και ασφάλεια ενώ για τα υπόλοιπα αναλώσιμα υλικά (καλώδια μικτονόμησης κλπ) έχει δοθεί εγγύηση τριών (3) ετών. Για να εξασφαλιστεί η αξιοπιστία του δικτύου οι φορείς του καλωδιακού δικτύου, οι παθητικοί τερματισμοί και τα καλώδια διασύνδεσης είναι της ίδιας κατηγορίας υλικών ή ανώτερης έτσι ώστε το δίκτυο να πληρεί ένα ενιαίο καλωδιακό σύστημα (όσον αφορά την κατηγορία λειτουργίας).

Τα πλαστικά υλικά του παθητικού εξοπλισμού, που χρειάστηκαν, (πλαστικά κανάλια, μανδύες καλωδίων, πλαστικά μέρη πριζών, κλπ) είναι αυτοσβενόμενου τύπου και σε περίπτωση πυρκαγιάς δεν εκλύουν δηλητηριώδη αέρια.

Η άνω προδιαγραφή καλύπτει τις απαιτήσεις της Ευρωπαϊκής Ένωσης και συμφωνεί με τα πρότυπα IEC 332-3C, EN50167 που περιγράφουν κανόνες υγιεινής και ασφάλειας των εργαζομένων και συναλλασσόμενων που ευρίσκονται σε κλειστούς χώρους.

5.1 ΥΛΟΠΟΙΗΣΗ ΕΡΓΟΥ

Ο σκοπός του συγκεκριμένου έργου είναι η υλοποίηση της καλωδιακής υποδομής, αναβάθμιση των συστημάτων ασφάλειας, διαχείρισης και ελέγχου του δικτύου στο κεντρικό κτήριο του «Μαμάτσειου» Γενικού Νοσοκομείου Κοζάνης . Η αρχιτεκτονική ανάπτυξης του καλωδιακού δικτύου είναι η Διανεμημένη Διαχείριση Δικτύου (Distributed Network Administration), δηλ. κατανομή και έλεγχος του δικτύου μέσω διαφορετικών σημείων.

Η άνω σχεδίαση κρίθηκε απαραίτητη έτσι ώστε το δίκτυο να εξασφαλίζει:

1. Μέγιστο μήκος οριζοντίου καλωδίου 90 μέτρα.
2. Ευκολία εγκατάστασης και μελλοντικής επέκτασης.
3. Ευκολία πρόσβασης και συντήρησης του δικτύου.

Έτσι αναπτύχθηκαν ανεξάρτητα τοπικά δίκτυα τα οποία διασυνδεθούν έτσι ώστε να αποτελέσουν ένα ενιαίο δίκτυο με σκοπό την παροχή των παρακάτω υπηρεσιών στους χρήστες:

- Ηλεκτρονικό ταχυδρομείο (e-mail) εντός και εκτός των κτιρίων
- Ηλεκτρονική μεταφορά εγγράφων.
- Πρόσβαση σε βάσεις δεδομένων που βρίσκονται εντός και εκτός του κτιρίου (INTERNET).
- Διάχυση ενημέρωσης (WEBSERVER).
- Χρήση πόρων από απόσταση.
- Ανάπτυξη εφαρμογών.
- Τηλεδιάσκεψη (VIDEOCONFERENCE).
- Εφαρμογές Πολυμέσων (MULTIMEDIA).
- IP τηλεφωνία.

Η ανάπτυξη του καλωδιακού δικτύου έχει γίνει σε μορφή ιεραρχικού αστέρα (star topology). Έτσι χρησιμοποιούνται τα κεντρικά σημεία ελέγχου (τηλεπικοινωνιακοί κατανεμητές και κάθε σταθμός ή συσκευή του τηλεπικοινωνιακού συστήματος διασυνδέεται μέσω point to point καλωδίωσης με αυτά).

Οι τηλεπικοινωνιακοί κατανεμητές διασυνδέονται με τη σειρά τους διαμέσου point to point καλωδιώσεων με κεντρικό σημείο του δικτύου έτσι ώστε να ενοποιηθεί η καλωδιακή υποδομή. Χρησιμοποιώντας ως πλατφόρμα την τοπολογία αστέρα είναι εφικτή να πραγματοποιηθεί οποιαδήποτε άλλη μορφή ανάπτυξης δικτύων (τοπολογίες ring-bus).

5.2 ΕΛΕΓΧΟΣ ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΟΥ

Στη συνέχεια δίδονται γενικές πληροφορίες για το έργο σε σχέση με τη διαχείριση και τον έλεγχο, έτσι όπως συμφωνήθηκε στις προηγούμενες συσκέψεις με αρμόδια στελέχη του «Μαμάτσειου» Γενικού Νοσοκομείου Κοζάνης.

Σύμφωνα με τα συμφωνηθέντα το Δίκτυο περιλαμβάνει:

- Περίπου επτακόσιες Θέσεις Εργασίας **(~700 Θ.Ε.),**
- Δέκα Σημεία εξυπηρέτησης Μέσων Μαζικής Επικοινωνίας και των Ειδικών Λειτουργιών, όπως εκλογές, συντονισμός Οργάνων σε ημέρες κρίσεων.

Στον πρώτο όροφο του κτιρίου έχει δημιουργηθεί η Αίθουσα Ελέγχου εντός του οποίου:

- Έχει εγκατασταθεί λοιπός εξοπλισμός που έχει απαιτηθεί για τον εμπλουτισμό του Δικτύου
- Έχει γίνει σημείο διαχείρισης-συντήρησης του Δικτύου για την ομαλή λειτουργία αυτού.
- Έχει εγκατασταθεί το απαραίτητο λογισμικό ελέγχου, διαχείρισης και επίβλεψης των διακομιστών (ProxMox).

5.3 ΑΣΦΑΛΕΙΑ ΔΙΚΤΎΟΥ

Στο συγκεκριμένο έργο όσον αφορά την ασφάλεια του δικτύου έχουν εγκατασταθεί οι συσκευές και ο εξοπλισμός, ενώ έχει εφαρμοστεί η τεχνική πλεονασμού όπως μπορούμε να δούμε πιο αναλυτικά στο σχήμα 8. Παράλληλα, βλέπουμε πως συνεχίζεται η ασφάλεια του δικτύου μας με το διακομιστή Samba μαζί με τον διακομιστή μεσολάβησης Squid και το Εικονικό Ιδιωτικό Δίκτυο (VPN). Στον εξοπλισμό έχει εγκατασταθεί το ανοιχτό λογισμικό όπως ακριβώς αναλύουμε στα κεφάλαια 3.1, 3.2.

5.4 ΜΕΘΟΔΟΛΟΓΙΑ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ ΥΛΟΠΟΙΗΜΕΝΟΥ ΔΙΚΤΥΟΥ

Η εγκατάσταση των καλωδιώσεων και των υλικών της υποδομής έχουν γίνει σύμφωνα με το πρότυπο EIA/TIA569.

Τα καλώδια στην κάθετη καλωδίωση έχουν εγκατασταθεί εντός:

- Μεταλλικών σχαρών που εγκαταστάθηκαν στους μηχανολογικούς οχετούς.

Τα καλώδια στην οριζόντια καλωδίωση έχουν εγκατασταθεί εντός:

- Πλαστικών σωλήνων που έχουν εγκατασταθεί εντός των τοίχων.
- Επάνω από ψευδοροφές και εντός μεταλλικών σχαρών

Η κατασκευή του έργου έγινε με την ευθύνη έμπειρου και εξειδικευμένου προσωπικού έτσι ώστε να διατηρηθούν τα ηλεκτρικά, οπτικά και λοιπά χαρακτηριστικά μετάδοσης των καλωδίων.

Για το σκοπό αυτό:

1. Το μέγιστο μήκος καλωδίου UTP δεν υπερβαίνει τα 90m.
2. Τα καλώδια δε εφελκύονται με δυνάμεις μεγαλύτερες των επιτρεπόμενων.
3. Τα καλώδια δεν κάμπτονται στιγμιαία ή μόνιμα σε ακτίνες μεγαλύτερες των επιτρεπόμενων.
4. Τα καλώδια δεν συνθλίβονται.
5. Τα καλώδια δεν περιστρέφονται περί του άξονα τους.
6. Δεν δένονται σφικτά έτσι ώστε να μεταβάλλεται η εξωτερική τους διάμετρος.
7. Τα καλώδια δεν σταθεροποιούνται σε σημεία ξένα με τα υλικά υποδομής.

Σε κάθε περίπτωση συμπεραίνουμε ότι τα υλικά και ο εξοπλισμός υποδομής προσφέρουν:

1. Επάρκεια χώρου έτσι ώστε να είναι εφικτή η επέκταση των υποδικτύων.
2. Ασφάλεια κατά τη τοποθέτηση των καλωδίων έτσι ώστε η δύναμη εφελκυσμού που ασκείται σ ’αυτά να μην είναι μεγαλύτερη από την μέγιστη επιτρεπόμενη.
3. Εξασφάλιση ότι οι κάμψεις των καλωδίων δεν είναι μεγαλύτερες από τις μέγιστες επιτρεπόμενες .
4. Εύκολη και γρήγορη εξυπηρέτηση κατά τη συντήρηση και λειτουργία του δικτύου.
5. Εξασφάλιση ότι τηρούνται οι ελάχιστες δυνατές αποστάσεις από πηγές ανάπτυξης Ηλεκτρομαγνητικών Παρεμβολών.
6. Εξασφάλιση ότι αποφεύγεται η παράλληλη όδευση με ισχυρά ρεύματα.
7. Επάρκεια χώρου σ’ όλες τις διατρήσεις/διανοίξεις που θα γίνουν.
8. Προστασία έναντι πυρκαγιάς εφόσον όλες οι διατρήσεις/διανοίξεις προστατεύονται με πυρίμαχα υλικά. Συγκεκριμένη και σαφώς καθορισμένη αρχιτεκτονική ανάπτυξης έτσι ώστε να μη διαταράσσει την καλαισθησία του χώρου και παράλληλα εξασφαλίζει το δίκτυο έναντι βλαβών από εργασίες που θα εκτελεσθούν από τρίτους, στο μέλλον, εντός του κτιρίου.

Συμπεραίνουμε ότι έχουμε τα παρακάτω βασικά οφέλη μετά το τέλος της ολοκλήρωσης του έργου:

- Ασφάλεια δικτύου (εξωτερική και εσωτερική)
- Κεντρικός έλεγχος
- Κεντρική διαχείριση
- Κεντρική εποπτεία
- Χαμηλό κόστος
- Φιλτράρισμα περιεχομένου
- Ευελιξία
- Επεκτασιμότητα
- Προσαρμοστικότητα
- Απομακρυσμένη πρόσβαση

ΒΙΒΛΙΟΓΡΑΦΙΑ

Anon., χ.χ. *American National Standards Institute - ANSI.* [Ηλεκτρονικό] Available at: https://www.ansi.org/american-national-standards/ans-introduction/essential-requirements

Anon., χ.χ. *Ubuntu Manpage: ucarp — Automatic IP failover.* [Ηλεκτρονικό] Available at: https://manpages.ubuntu.com/manpages/bionic/man8/ucarp.8.html [Πρόσβαση 8 12 2022].

Carthern Chris, W. W. B. R. R. N., 2015. VLANs, Trunking, VTP, and MSTP. Στο: *Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA.* s.l.:Apress.

Case, J. M. F. J. D., 1990. SNMP Research. Στο: *Performance Systems International.* s.l.:s.n., p. 36.

Cheng, S. M. C., 2014. *Proxmox High Availability: Introduce, design, and implement high availability clusters using Proxmox.* Birmingham Mumbai: Packt Publishing.

Daiyuu, N. Y. S. S. S., 2015. SoftEther VPN Server: Multi-protocol compatible Cross-platform open source VPN server. *コンピュータ ソフトウェア*, pp. 4_3-4_30.

El-Emam Eman, K. M. K. H. F. A. O., 2009. *An optimized Kerberos authentication protocol.* Egypt: IEEE.

Gary, D., 2007. *Network Warrior.* s.l.:O'Reilly Media, Inc..

Hall, E., 2000. *Internet Core Protocols: The Definitive Guide.* s.l.:O'Reilly Media, Inc..

Hamad Ammar, K. M., 2015. *SONET over Ethernet.* Montreal, Canada: Annual Global Online Conference on Information and Computer Technology.

Kumar, S. S. V., 2014. THE OSI MODEL: OVERVIEW ON THE SEVEN LAYERS OF COMPUTER NETWORKS. p. 6.

Lucian, G., 2006. *Designing and implementing linux firewalls and Qos using netfilter, iproute2, NAT, and L7-filter: learn how to secure your system and implement QoS using real-world scenarios for networks of all sizes.* Birmingham Mumbai: Packt Publ.

Marcelo, L., 2017. *Implementing Samba 4: exploit the real power of Samba 4 Server by leveraging the benefits of an Active Directory Domain Controller.* Birmingham, UK: Packt Pub.

Niclas, E., 1999. *IEEE 802.1 P,Q - QoS on the MAC level.* [Ηλεκτρονικό] Available at: http://www.cse.tkk.fi/fi/opinnot/T-110.5190/1999/papers/08IEEE802.1QosInMAC/qos.html [Πρόσβαση 29 1 2023].

Postel, J. J. R., 1983. *Telnet Protocol Specification.* [Ηλεκτρονικό] Available at: https://www.rfc-editor.org/info/rfc854 [Πρόσβαση 2023].

William, S., 2017. *Cryptography and network security: principles and practice.* Seventh edition επιμ. Boston: Pearson.

Ylonen, T., 2017. *SSH Secure Shell home page, maintained by SSH protocol inventor Tatu Ylonen. SSH clients, servers, tutorials, how-tos..* [Ηλεκτρονικό] Available at: https://www.ssh.com/academy/ssh [Πρόσβαση 13 12 2022].

Zheng, Z., 2016. *Analysis of Virtual Local Area Networking Technology.* Tianjin, China: Atlantis Press.